MATH 788F: THE THEORY OF IRREDUCIBLE POLYNOMIALS

COURSE DESCRIPTION:

The choice of topics will depend on students' interests. Some of the possible topics include Eisenstein's criterion, Newton polygons, irreducibility criteria, finite fields, factoring algorithms, density results, cyclotomic polynomials, other special polynomials, Capelli's theorem, covering problems, Hilbert's irreducibility theorem, sieve methods, and "almost" prime values of polynomials. Some typical results and questions to be considered are:

(1) If $d_n d_{n-1} \dots d_0$ is the decimal representation of a prime, then $f(x) = \sum_{j=0}^{n} d_j x^j$ is irreducible (over $\mathbb{Z}$). For example, since my phone number 7776589 is prime,

$$7x^6 + 7x^5 + 7x^4 + 6x^3 + 5x^2 + 8x + 9$$

is irreducible.

(2) If $f(x) \in \mathbb{Z}[x]$ with $\deg f(x) = n$ and there exist $n + 5$ integers m such that $f(m)$ is prime, then $f(x)$ is irreducible.

(3) The probability that a random polynomial in $\mathbb{Z}[x]$ is irreducible over the rationals is 1.

(4) Given any integers $a_1, a_2, \dots, a_{n-1}$, the polynomial

$$\frac{x^n}{n!} + a_{n-1}\frac{x^{n-1}}{(n-1)!} + \cdots + a_2\frac{x^2}{2!} + a_1 x \pm 1$$

is irreducible over the rationals.

(5) Suppose that $f(x)$ and $g(x)$ are in $\mathbb{Z}[x]$ with $f(x)$ irreducible. When can we conclude that $f(g(x))$ is irreducible?

(6) The polynomial

$$(5x^9 + 6x^8 + 3x^6 + 8x^5 + 9x^3 + 6x^2 + 8x + 3)x^n + 12$$

is reducible for all $n \geq 0$. What does this have to do with another problem Erdős and Selfridge are willing to pay money for (assuming you come up with the right answer)?

(7) What do we know about prime values of irreducible polynomials? Very little. In particular, if $f(x) = x^2 + 1$, no one has established yet that there are infinitely many integers m for which $f(m)$ is prime? However, in this case, it is known that there are infinitely many integers m for which $f(m)$ has ≤ 2 prime factors. What's known in the general case?

CHAPTER 1

INTRODUCTION

Oh, we know you do not like Mathematics,
but we promise not to use it as an instrument of torture....

– Lillian R. Lieber

The Education of T. C. MITS

The storm starts when the drops start dropping
When the drops stop dropping then the storm starts stopping

– Dr. Seuss

Oh Say Can You Say?

1.1. The purpose of this book is to explore various problems and results on irreducible polynomials. This section discusses some basic definitions and a theorem of Gauss. We begin by clarifying the direction of this book. Throughout this book, we will make use of the following basic notation and definitions:

$\mathbb{Z}$ represents the set of integers.

$\mathbb{Q}$ represents the set of rational numbers.

$\mathbb{R}$ represents the set of real numbers.

$\mathbb{C}$ represents the set of complex numbers.

$R[x]$ represents the set of polynomials with coefficients coming from a ring R (for ex-

ample, R may be $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, or the integers modulo m where m denotes an integer $m > 1$).

$\deg f(x)$ represents the degree of a non-zero polynomial $f(x)$.

As suggested in the above definition of the degree of $f(x)$, we will make an effort to avoid referring to the degree of the polynomial 0. Nevertheless, it will be convenient sometimes to do so. We will view the degree of 0 in such cases as being $-\infty$ with the understanding that $-\infty$ is less than any given integer. With the further understanding that $-\infty + a = -\infty$ for any integer a, we obtain as a consequence of this definition that the degree of the product of two polynomials is the sum of the degrees of the two polynomials.

Observe that equality, addition, and multiplication in $R[x]$, where R denotes a ring, are defined in the obvious way. More specifically, suppose that $f(x) = \sum_{j=0}^{n} a_j x^j$, $g(x) = \sum_{j=0}^{r} b_j x^j$, and $h(x) = \sum_{j=0}^{s} c_j x^j$ are all in $R[x]$. Define $a_j = 0$ for $j > n$, $b_j = 0$ for $j > r$, and $c_j = 0$ for $j > s$. Then $g(x) = h(x)$ means that $b_j = c_j$ for every $j \in \{0, 1, 2, \dots\}$, $f(x) = g(x) + h(x)$ means that $a_j = b_j + c_j$ for every $j \in \{0, 1, 2, \dots\}$, and $f(x) = g(x)h(x)$ means that $a_k = \sum_{j=0}^{k} b_j c_{k-j}$ for every $k \in \{0, 1, 2, \dots\}$.

Definition 1. *A polynomial $f(x) \in \mathbb{Z}[x]$ is irreducible (or irreducible over $\mathbb{Z}$) provided that $f(x) \not\equiv \pm 1$ and whenever $f(x) = g(x)h(x)$ with $g(x)$ and $h(x) \in \mathbb{Z}[x]$, either $g(x) \equiv \pm 1$ or $h(x) \equiv \pm 1$. If $f(x) \in \mathbb{Z}[x]$ is not irreducible and is not 0, 1, or -1, then $f(x)$ is reducible (or reducible over $\mathbb{Z}$). The polynomials 0, 1, and -1 are considered neither reducible nor irreducible.*

Definition 2. *A polynomial $f(x) \in \mathbb{Q}[x]$ is irreducible over $\mathbb{Q}$ provided that $f(x)$ is not constant and whenever $f(x) = g(x)h(x)$ with $g(x)$ and $h(x) \in \mathbb{Q}[x]$, either $\deg g(x) = 0$ or $\deg h(x) = 0$. If $f(x) \in \mathbb{Q}[x]$ has degree at least one and is not irreducible over $\mathbb{Q}$, then $f(x)$ is reducible over $\mathbb{Q}$. Constant polynomials are considered neither reducible nor irreducible over the rationals.*

Thus, for example, $x^2 + 1$ is irreducible over $\mathbb{Z}$ and over $\mathbb{Q}$, but $3x - 3$ is reducible over $\mathbb{Z}$ and irreducible over $\mathbb{Q}$. Although, at this point we will not need the more general

definition, we point out that the above definitions agree with the algebraic concepts of irreducibility and reducibility. More specifically, if R is a ring, then $f \in R$ is irreducible provided that f is not a unit in R and whenever $f = gh$ with g and $h \in R$, either g or h is a unit in R; furthermore, if $f \in R$ is not irreducible, is non-zero, and is not a unit in R, then f is reducible. Note that the statements "f is irreducible" and "f is not reducible" have slightly different meanings. The reader should keep this in mind when reading the statements of theorems in this book.

We will mainly focus our attention on irreducibility over $\mathbb{Z}$ and irreducibility over $\mathbb{Q}$. Thus, we will not emphasize irreducibility over general rings. However, later, we will explore irreducibility over other fields bearing in mind that from such irreducibility results one can often deduce irreducibility results over $\mathbb{Z}$ and over $\mathbb{Q}$.

There is an important connection between irreducibility over $\mathbb{Z}$ and irreducibility over $\mathbb{Q}$. This connection was suggested in our simple irreducibility examples above. It is due to Gauss (cf. Hasse [1]).

Theorem 1. *Let $f(x) \in \mathbb{Z}[x]$. If $f(x)$ is not reducible over $\mathbb{Z}$, then $f(x)$ is not reducible over $\mathbb{Q}$. Furthermore, if $f(x)$ is irreducible over $\mathbb{Q}$ and the greatest common divisor of its coefficients is 1, then $f(x)$ is irreducible over $\mathbb{Z}$.*

To prove Theorem 1, we first define the content of $f(x) \in \mathbb{Z}[x]$, where $f(x) \not\equiv 0$, to be the greatest common divisor of the coefficients of $f(x)$. We consider the following lemma before proceeding.

Lemma. *Let $g(x)$ and $h(x) \in \mathbb{Z}[x]$ be such that the contents of $g(x)$ and $h(x)$ are both 1. Then the content of $g(x)h(x)$ is 1.*

Proof. Let d be the content of $g(x)h(x)$. It suffices to show that if p is a prime, then $p \nmid d$. Let p be a prime. Write $g(x)$ and $h(x)$ in the form $g(x) = \sum_{j=0}^{r} b_j x^j$ and $h(x) = \sum_{j=0}^{s} c_j x^j$. Define $b_j = 0$ for $j > r$, and define $c_j = 0$ for $j > s$. Let k be the minimal $j \in \{0, ..., r\}$ such that $p \nmid b_j$. Let ℓ be the minimal $j \in \{0, ..., s\}$ such that $p \nmid c_j$. These exist since the contents of $g(x)$ and $h(x)$ are 1. Since each of $b_0, b_1, \ldots, b_{k-1}$ and each of $c_0, c_1, \ldots, c_{\ell-1}$

are divisible by p, the coefficient of $x^{k+\ell}$ in $g(x)h(x)$ is

$$b_0c_{k+\ell} + b_1c_{k+\ell-1} + \cdots + b_{k-1}c_{\ell+1} + b_kc_\ell + b_{k+1}c_{\ell-1} + \cdots + b_{k+\ell}c_0 \equiv b_kc_\ell \not\equiv 0 \pmod{p}.$$

Thus, there is a coefficient in $g(x)h(x)$ which is not divisible by p, proving that $p \nmid d$. ■

Proof of Theorem 1. The theorem is easily verified in the case that $f(x)$ is a constant. We restrict then to the case that $\deg f(x) \geq 1$. We begin by showing that if $f(x) \in \mathbb{Z}[x]$ is reducible over $\mathbb{Q}$, then $f(x)$ is reducible over $\mathbb{Z}$. Suppose $f(x) = u(x)v(x)$ where $u(x)$ and $v(x) \in \mathbb{Q}[x]$, $\deg u(x) > 0$, and $\deg v(x) > 0$. Let a be the content of $f(x)$ so that $f(x) = af_0(x)$ where $f_0(x) \in \mathbb{Z}[x]$ and $f_0(x)$ has content 1. Let b and c be integers such that $bu(x) \in \mathbb{Z}[x]$ and $cv(x) \in \mathbb{Z}[x]$. Let d be the content of $bu(x)$, and let e be the content of $cv(x)$. Hence, there exist polynomials $u_0(x)$ and $v_0(x) \in \mathbb{Z}[x]$ with content 1 such that $bu(x) = du_0(x)$ and $cv(x) = ev_0(x)$. Thus,

$$abcf_0(x) = bcf(x) = (bu(x))(cv(x)) = (du_0(x))(ev_0(x)) = deu_0(x)v_0(x).$$

By the lemma, the content of $u_0(x)v_0(x)$ is 1 so that the content of $deu_0(x)v_0(x)$ is de. Therefore, since the content of $abcf_0(x)$ is abc, we get that $abc = de$. So, $f_0(x) = u_0(x)v_0(x)$. Thus, $f(x) = af_0(x) = au_0(x)v_0(x)$. Note that $au_0(x)$ and $v_0(x) \in \mathbb{Z}[x]$. Also, $\deg(au_0(x)) = \deg u(x) > 0$ and $\deg v_0(x) > 0$. Hence, $f(x)$ is reducible over $\mathbb{Z}$.

The second statement of Theorem 1 follows directly from considering its contrapositive and the definitions of reducibility over $\mathbb{Z}$ and over $\mathbb{Q}$. This completes the proof. ■

To prove that a polynomial $f(x) \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Q}$, we will often use the next result which follows easily from the proof of Theorem 1 given above.

Theorem 2. *If $f(x) \in \mathbb{Z}[x]$ is a reducible polynomial over $\mathbb{Q}$, then there exist $g(x) \in \mathbb{Z}[x]$ and $h(x) \in \mathbb{Z}[x]$ with $f(x) = g(x)h(x)$, $\deg g(x) > 0$, and $\deg h(x) > 0$.*

One can conclude a little more than Theorem 2. If $f(x) \in \mathbb{Z}[x]$ and $f(x)$ factors over the rationals as $f(x) = g(x)h(x)$ with $g(x) \in \mathbb{Q}[x]$, $h(x) \in \mathbb{Q}[x]$, $\deg g(x) \geq 1$, and

$\deg h(x) \geq 1$, then there are rational numbers a and b such that $f(x) = (ag(x))(bh(x))$ (i.e., $ab = 1$) and both $ag(x)$ and $bh(x)$ have integer coefficients.

1.2. We will need the notion of fields at various points in this book, and so we briefly discuss them now. A field F is a set of at least 2 elements together with 2 operations, addition ($+$) and multiplication ($\times$), having the properties: (i) the sum or product of 2 elements of F is in F, (ii) sums and products each commute (i.e., $a + b = b + a$ and $a \times b = b \times a$ for every a and b in F), (iii) the associative laws for addition and multiplication hold ($(a + b) + c = a + (b + c)$ and $(a \times b) \times c = a \times (b \times c)$), (iv) there is an additive identity element (denoted 0) and a multiplicative identity element (denoted 1) in F with $0 \neq 1$ ($a + 0 = a$ and $a \times 1 = a$ for every $a \in F$), (v) there is an additive inverse for every $a \in F$ (denoted $-a$ so that $-a + a = 0$) and a multiplicative inverse for every non-zero $a \in F$ (denoted a^{-1} so that $a^{-1} \times a = 1$), and (vi) the distributive law for multiplication over addition holds ($a \times (b + c) = a \times b + a \times c$ for every $a, b, c \in F$). In other words, F is a ring in which the non-zero elements form an abelian group under multiplication. As usual, we will often use $a \cdot b$ or simply ab to denote $a \times b$. The rational numbers, the real numbers, the complex numbers, and integers modulo a prime p with their usual operations of addition and multiplication are easily seen to be fields.

Let F be a field. Corresponding to the definition of irreducibility over $\mathbb{Q}$, we define a non-constant polynomial $f(x) \in F[x]$ to be irreducible over F if $f(x) = g(x)h(x)$ with $g(x)$ and $h(x)$ in $F[x]$ implies that either $g(x)$ or $h(x)$ is a constant. If a polynomial $f(x) \in F[x]$ is not constant and is not irreducible over F, then we say that $f(x)$ is reducible over F. Certainly of some relevance to the subject of irreducibility is the fact that there is unique factorization in $F[x]$.

Theorem 3. *Every non-constant monic polynomial in $F[x]$ can be uniquely written as a product of monic irreducible polynomials in $F[x]$ except for the order in which the factors occur.*

There is really no loss in generality in considering only monic polynomials in the statement

of Theorem 3. For example, if $f(x) = 2x^3 - x^2 + 2x - 1$ and one wishes to apply the theorem with $F = \mathbb{Q}$ (or any field with characteristic different from 2), then one simply considers the theorem with $(1/2)f(x) = x^3 - (1/2)x^2 + x - (1/2)$. To establish the theorem, we first establish a lemma (the Division Algorithm for Polynomials). We note, though, that the proof of the theorem will only depend on the existence (and not the uniqueness) of the polynomials $q(x)$ and $r(x)$ in the lemma.

Lemma. *Let $f(x)$ and $g(x)$ be in $F[x]$ with $g(x) \not\equiv 0$. Then there exist unique polynomials $q(x)$ and $r(x)$ in $F[x]$, with either $r(x) \equiv 0$ or $\deg r(x) < \deg g(x)$, such that*

$$f(x) = g(x)q(x) + r(x). \tag{1.1}$$

Proof. We first show the existence of such $q(x)$ and $r(x)$. If (1.1) is possible with $r(x) \equiv 0$, then we are through. Suppose then that (1.1) is not possible with $r(x) \equiv 0$. In particular, $f(x) \not\equiv 0$. Observe that (1.1) (without any degree restrictions on $r(x)$) is satisfied with $q(x) \equiv 0$ and $r(x) = f(x)$. Consider a $q(x)$ and $r(x) \in F[x]$ satisfying (1.1) with $\deg r(x)$ as small as possible. We write $g(x) = \sum_{j=0}^{r} b_j x^j$ and $r(x) = \sum_{j=0}^{s} c_j x^j$, where b_r and c_s are non-zero. To show the existence of $q(x)$ and $r(x)$ as in the theorem, it suffices to show that $s < r$. If $s \geq r$, then observe that $f(x) = g(x)q_0(x) + r_0(x)$ where $q_0(x) = q(x) + b_r^{-1}c_s x^{s-r}$ and $r_0(x) = r(x) - b_r^{-1}c_s x^{s-r}g(x)$. Since either $r_0(x) \equiv 0$ or $\deg r_0(x) < \deg r(x)$, this situation is impossible (since (1.1) is impossible with $r(x) \equiv 0$ and since we chose $r(x)$ so that $\deg r(x)$ is minimal). Therefore, $s < r$.

To prove uniqueness, for $j = 1$ and 2, consider $q_j(x)$ and $r_j(x)$ in $F[x]$ such that either $r_j(x) \equiv 0$ or $\deg r_j(x) < \deg g(x)$ and such that $f(x) = g(x)q_j(x) + r_j(x)$. Then

$$g(x)\,(q_2(x) - q_1(x)) = r_1(x) - r_2(x).$$

Hence, $r_1(x) \equiv r_2(x)$ since otherwise $g(x)$ divides a non-zero polynomial of degree $< \deg g(x)$ (namely, $r_1(x) - r_2(x)$). It follows that $q_1(x) \equiv q_2(x)$, completing the proof. ■

Proof of Theorem 3. If $f(x) \in F[x]$ with $\deg f(x) > 0$, then either $f(x)$ can be written as the product of smaller degree polynomials or $f(x)$ is irreducible. The existence of a

factorization for non-constant monic polynomials $f(x) \in F[x]$ into a product of monic irreducible polynomials easily follows by induction on the degree of $f(x)$. To establish the uniqueness of such a factorization, we show that whenever

$$g_1(x)g_2(x)\cdots g_\ell(x) = h_1(x)h_2(x)\cdots h_k(x), \tag{1.2}$$

where each $g_j(x)$ and each $h_j(x)$ is a monic irreducible polynomial in $F[x]$, the polynomials $g_1(x), \ldots, g_\ell(x)$ are some rearrangement of the polynomials $h_1(x), \ldots, h_k(x)$. We assume that there exist monic irreducible $g_j(x)$ and $h_j(x)$ in $F[x]$ as in (1.2) with $g_1(x), \ldots, g_\ell(x)$ not some rearrangement of the polynomials $h_1(x), \ldots, h_k(x)$. Among all such examples, we consider one with $\deg g_1(x)$ minimal. Set $g(x) = g_1(x)$. For each $j \in \{1, \ldots, k\}$, we consider $q_j(x)$ and $r_j(x)$ in $F[x]$ with $\deg r_j(x) < \deg g(x)$ and with $h_j(x) = g(x)q_j(x) + r_j(x)$ (such $q_j(x)$ and $r_j(x)$ exist by the lemma). From (1.2), we get that

$$r_1(x)\cdots r_k(x) = g(x)w(x) \tag{1.3}$$

for some $w(x) \in F[x]$. In (1.3), we factor out the leading coefficients from $w(x)$ and each $r_j(x)$ and cancel to obtain a factorization of the form (1.3) where $w(x)$ and each $r_j(x)$ is monic. We express these polynomials as possibly empty products of monic irreducible polynomials from $F[x]$. Since $\deg r_j(x) < \deg g(x)$ for each $j \in \{1, \ldots, k\}$, each of the resulting monic irreducible factors on the left-hand side of (1.3) will be different from $g(x)$. We divide both sides of the resulting equation by whatever monic irreducible factors both sides of the equation have in common. Since $g(x)$ will remain as a factor on the right-hand side, there will still be at least one monic irreducible factor on the left-hand side as well. We are left with an equation of the form (1.2) where each polynomial on the left-hand side is a monic irreducible polynomial in $F[x]$ of degree $< \deg g(x) = \deg g_1(x)$ and where $g(x)$ is a factor occurring on the right-hand side. This contradicts the minimality of $\deg g_1(x)$, completing the proof. ■

Before closing this section, we make a remark on the last lemma that will be of use to us later. Suppose that $f(x)$ and $g(x)$ are in $\mathbb{Z}[x]$. Since $\mathbb{Z}[x] \subseteq \mathbb{Q}[x]$, the lemma implies that

there exist unique polynomials $q(x)$ and $r(x)$ in $\mathbb{Q}[x]$ such that $f(x) = g(x)q(x) + r(x)$ and either $r(x) \equiv 0$ or $\deg r(x) < \deg g(x)$. It is often the case that the polynomials $q(x)$ and $r(x)$ are not in $\mathbb{Z}[x]$ (for example, consider $f(x) = x^2 + 1$ and $g(x) = 2x + 1$). However, whenever $g(x)$ is monic, $q(x)$ and $r(x)$ are in $\mathbb{Z}[x]$. To see this, observe that it suffices to show that $q(x) \in \mathbb{Z}[x]$. Assume $q(x) \notin \mathbb{Z}[x]$, and let k be the maximal non-negative integer for which the coefficient of x^k in $q(x)$, say c, is in $\mathbb{Q}$ but not in $\mathbb{Z}$. If $m = \deg g(x)$, then it follows that the coefficient of x^{m+k} on the right side of $f(x) = g(x)q(x) + r(x)$ is of the form c plus an integer and, hence, is not an integer. This contradicts that the coefficients on the left side are integral. Thus, $q(x) \in \mathbb{Z}[x]$.

1.3. As in the previous section, we let F denote a field. Fix $g(x) = \sum_{j=0}^{r} b_j x^j$ and $h(x) = \sum_{j=0}^{s} c_j x^j$ in $F[x]$ with $b_r \neq 0$. Consider the set of all polynomials of the form

$$u(x)g(x) + v(x)h(x), \tag{1.4}$$

where $u(x)$ and $v(x)$ denote elements in $F[x]$. Observe that if $u(x) = b_r^{-1}$ and $v(x) = 0$, then the polynomial in (1.4) is monic. Let $w(x)$ be a monic polynomial of the form given in (1.4) with smallest possible degree. In particular, $\deg w(x) \leq \deg g(x)$. Observe that if there is a polynomial $d(x) \in F[x]$ that divides both $g(x)$ and $h(x)$, then since $w(x)$ is of the form given in (1.4), $d(x)$ divides $w(x)$. Thus, every common divisor of $g(x)$ and $h(x)$ divides $w(x)$. We show that $w(x)$ is itself a common divisor of $g(x)$ and $h(x)$. By the lemma to Theorem 3, we know that there is a $q(x)$ and an $r(x)$ in $F[x]$ such that $g(x) = w(x)q(x) + r(x)$ and either $r(x) \equiv 0$ or $\deg r(x) < \deg w(x)$. If $r(x) \not\equiv 0$, then there is a $b \in F$ such that $br(x)$ is monic and $\deg(br(x)) < \deg w(x)$. If $u(x)$ and $v(x)$ are fixed so that the expression in (1.4) is equal to $w(x)$, we then obtain that

$$(b - bu(x)q(x))\, g(x) + (-bv(x)q(x))\, h(x) = br(x),$$

contradicting the minimality of $\deg w(x)$. Thus, we get that $r(x) \equiv 0$ so that $w(x)$ divides $g(x)$. Similarly, $w(x)$ divides $h(x)$. Observe that, although we fixed $g(x)$ above to be a non-zero polynomial, the same conclusions would follow if instead we only knew that $h(x)$ was non-zero.

Definition. *The greatest common divisor of two polynomials $g(x)$ and $h(x)$ in $F[x]$, with at least one of $g(x)$ or $h(x)$ non-zero, is the monic polynomial in $F[x]$ of largest degree which divides both $g(x)$ and $h(x)$ and is denoted by* $\gcd(g(x), h(x))$.

Let $g(x)$ and $h(x)$ be as in the definition. Clearly, there is a monic polynomial of largest degree as in the definition. We justify that this definition uniquely defines this polynomial (as suggested by the wording in the definition). As before, we set $w(x) \in F[x]$ to be a non-zero monic polynomial of smallest possible degree that can be written in the form (1.4). Suppose $\widetilde{w}(x)$ satisfies the definition of the greatest common divisor of $g(x)$ and $h(x)$ above. Then, as we have just seen, $\widetilde{w}(x)$ divides $w(x)$ so that $\deg \widetilde{w}(x) \leq \deg w(x)$. On the other hand, $w(x)$ divides $g(x)$ and $h(x)$, so by the definition of the greatest common divisor of $g(x)$ and $h(x)$, we obtain $\deg \widetilde{w}(x) \geq \deg w(x)$. Therefore, $\deg \widetilde{w}(x) = \deg w(x)$ and $w(x)$ divides $\widetilde{w}(x)$. We deduce that $\widetilde{w}(x) = cw(x)$ for some $c \in F$. Since $\widetilde{w}(x)$ and $w(x)$ are both monic, we obtain $c = 1$ and $\widetilde{w}(x) = w(x)$. This is true for any $\widetilde{w}(x)$ satisfying the definition above; hence, the greatest common divisor of $g(x)$ and $h(x)$ is uniquely determined by this definition. Furthermore, we obtain that there must be exactly one non-zero monic polynomial in $F[x]$ of smallest degree which can be written in the form (1.4) and that it is the same as the greatest common divisor of $g(x)$ and $h(x)$.

We consider the trivial example of $g(x) = 2x$ and $h(x) = x + 1$ and $F = \mathbb{Q}$. Here, it is easy to see from the definition that the greatest common divisor of $g(x)$ and $h(x)$ is 1. Also, the expression in (1.4) is 1 with $u(x) = -1/2$ and $v(x) = 1$. Observe that for every choice of $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$, we have that

$$u(x)(2x) + v(x)(x + 1) \neq 1$$

(since otherwise we could let $x = 1$ to get that $1 = 2u(1) + 2v(1)$, an even number). It is important to keep in mind that if (1.4) is the greatest common divisor of $g(x)$ and $h(x)$ in $F[x]$, then the coefficients of $u(x)$ and $v(x)$ belong to the *field* F.

For computational purposes, it is convenient to know Euclid's algorithm for computing the greatest common divisor of two polynomials. Euclid's algorithm can be described

as follows. Let $g(x)$ and $h(x)$ be in $F[x]$ with $g(x) \not\equiv 0$. Define $r_{-1}(x) = g(x)$ and $r_0(x) = h(x)$. For k a positive integer, define $r_k(x)$ recursively by taking $q_k(x)$ and $r_k(x)$ to be the unique polynomials in $F[x]$ (see the lemma to Theorem 3) such that

$$r_{k-2}(x) = r_{k-1}(x)q_k(x) + r_k(x) \tag{1.5}$$

with

$$r_k(x) \equiv 0 \quad \text{or} \quad \deg r_k(x) < \deg r_{k-1}(x).$$

Since $r_k(x) \equiv 0$ or $r_k(x)$ has smaller degree than $r_{k-1}(x)$, we deduce that there exists a smallest integer $t \geq 0$ such that $r_t(x) \equiv 0$. If $t = 0$, then it is easy to see that there is an $a \in F$ such that $ar_{t-1}(x) = \gcd(g(x), h(x))$ (a in this case being the element in F which is an inverse of the leading coefficient of $g(x)$). We show in general that a multiple of $r_{t-1}(x)$ is the greatest common divisor of $g(x)$ and $h(x)$. Beginning with $k = 1$ in (1.5) and by incrementing k, we obtain inductively that any common divisor of $g(x) = r_{-1}(x)$ and $h(x) = r_0(x)$ divides $r_k(x)$. In particular, $\gcd(g(x), h(x))$ divides $r_{t-1}(x)$. Beginning with $k = t$ in (1.5) and by decrementing k, we obtain that $r_{t-1}(x)$ is a divisor of $r_{k-2}(x)$ for $k \in \{1, 2, \ldots, t\}$. Hence, $r_{t-1}(x)$ divides both $g(x)$ and $h(x)$. The desired result that a multiple of $r_{t-1}(x)$ is $\gcd(g(x), h(x))$ easily follows.

The above outlines a method for determining the greatest common divisor of two given polynomials in $F[x]$. The method is called the Euclidean algorithm (for polynomials). Observe that if $h(x) \not\equiv 0$, then $t \leq 1 + \deg h(x)$ so that at most $1 + \deg h(x)$ "steps" are needed above to determine $\gcd(g(x), h(x))$. If $g(x)h(x) \not\equiv 0$, then we can replace the roles of $g(x)$ and $h(x)$ if necessary to compute the greatest common divisor in $\leq \min\{\deg g(x), \deg h(x)\} + 1$ steps.

As an example, consider

$$g(x) = x^5 - x^4 + 3x^3 + 2 \quad \text{and} \quad h(x) = x^4 - 2x^3 + 4x^2 - 3x + 2$$

as polynomials in $\mathbb{Q}[x]$. Then we get

$$r_{-1}(x) = x^5 - x^4 + 3x^3 + 2, \quad r_0(x) = x^4 - 2x^3 + 4x^2 - 3x + 2,$$

$$r_1(x) = x^3 - x^2 + x, \quad r_2(x) = 2x^2 - 2x + 2, \quad r_3(x) = 0,$$

$$q_1(x) = x + 1, \quad q_2(x) = x - 1, \quad \text{and} \quad q_3(x) = x/2.$$

To obtain the greatest common divisor of $g(x)$ and $h(x)$, we multiply $r_2(x)$ by an appropriate constant (namely, $1/2$) to obtain a monic polynomial. Thus,

$$\gcd(g(x), h(x)) = x^2 - x + 1.$$

In this example, we have used the Euclidean algorithm directly. When computing greatest common divisors by hand, there are many short cuts one can make along the way. Using the notation before the example, we know that $\gcd(g(x), h(x))$ divides $r_k(x)$ for every k. Thus, the monic factor of $r_k(x)$ of largest degree which divides both $g(x)$ and $h(x)$ will be the greatest common divisor of $g(x)$ and $h(x)$. In the example, we could have noticed that $r_1(x) = x^3 - x^2 + x = x(x^2 - x + 1)$ and checked whether each of x and $x^2 - x + 1$ divides $g(x)$ and $h(x)$. The latter does and the former doesn't, so we could have concluded that $\gcd(g(x), h(x)) = x^2 - x + 1$ without computing $r_2(x)$ or $r_3(x)$. More can be said in this direction; for every $k \leq t$, $\gcd(r_{k-1}(x), r_k(x)) = \gcd(g(x), h(x))$. Hence, after factoring $r_1(x)$, we could have simply noticed that x is not a factor of $h(x)$, checked that $x^2 - x + 1$ is a factor of $h(x)$, and concluded that $\gcd(g(x), h(x)) = x^2 - x + 1$. We were also fortunate that there were not a great deal of non-integral coefficients that came into play in this example. When working in $\mathbb{Q}[x]$, one can in general multiply $q_k(x)$ and $r_k(x)$ by non-zero constants as one computes them if one wishes to avoid dealing with non-integral coefficients.

Let $d(x) = \gcd(g(x), h(x))$. Recall that we have already seen that there must exist $u(x)$ and $v(x)$ in $F[x]$ such that

$$u(x)g(x) + v(x)h(x) = d(x).$$

One can calculate such a $u(x)$ and $v(x)$ as one does the Euclidean algorithm. Define

$$u_{-1}(x) = 1, \; u_0(x) = 0, \; v_{-1}(x) = 0, \; \text{and } v_0(x) = 1.$$

For $k \geq 1$, define

$$u_k(x) = q_k(x)u_{k-1}(x) + u_{k-2}(x) \quad \text{and} \quad v_k(x) = q_k(x)v_{k-1}(x) + v_{k-2}(x).$$

By observing that

$$\begin{aligned} &u_{k-1}(x)v_k(x) - u_k(x)v_{k-1}(x) \\ &\qquad = u_{k-1}(x)\left(q_k(x)v_{k-1}(x) + v_{k-2}(x)\right) - \left(q_k(x)u_{k-1}(x) + u_{k-2}(x)\right)v_{k-1}(x) \\ &\qquad = -\left(u_{k-2}(x)v_{k-1}(x) - u_{k-1}(x)v_{k-2}(x)\right), \end{aligned}$$

one gets by using induction that

$$u_{k-1}(x)v_k(x) - u_k(x)v_{k-1}(x) = (-1)^k \quad \text{for every } k \geq 0.$$

Similar induction arguments give

$$u_{k-1}(x)r_k(x) + u_k(x)r_{k-1}(x) = h(x) \quad \text{for every } k \geq 0$$

and

$$v_{k-1}(x)r_k(x) + v_k(x)r_{k-1}(x) = g(x) \quad \text{for every } k \geq 0.$$

In particular, by letting $k = t$, we get that

$$u_t(x)r_{t-1}(x) = h(x), \quad v_t(x)r_{t-1}(x) = g(x),$$

and

$$\begin{aligned} (-1)^t r_{t-1}(x) &= \left(u_{t-1}(x)v_t(x) - u_t(x)v_{t-1}(x)\right)r_{t-1}(x) \\ &= u_{t-1}(x)\left(v_t(x)r_{t-1}(x)\right) - v_{t-1}(x)\left(u_t(x)r_{t-1}(x)\right) \\ &= u_{t-1}(x)g(x) - v_{t-1}(x)h(x). \end{aligned}$$

Recalling that $r_{t-1}(x)$ is a multiple of $\gcd(g(x), h(x))$, we can multiply through by an appropriate constant above to get the representation of $\gcd(g(x), h(x))$ in the form (1.4).

Next, we turn to roots of polynomials and prove

Theorem 4. *If $f(x)$ is a non-zero polynomial in $F[x]$ of degree n, then there are at most n distinct $a \in F$ such that $f(a) = 0$.*

Proof. Assume that the theorem is not true, and let $f(x)$ be a non-zero polynomial in $F[x]$ of minimal degree n with more than n distinct roots in F. There exist distinct elements $a_1, \ldots, a_{n+1}$ in F with $f(a_j) = 0$ for each $j \in \{1, \ldots, n+1\}$. By the lemma to Theorem 3, there exist $q(x)$ and $r(x)$ in $F[x]$ such that

$$(x - a_1)(x - a_2) \cdots (x - a_n) = f(x)q(x) + r(x) \tag{1.6}$$

and such that either $r(x) \equiv 0$ or $\deg r(x) < \deg f(x)$. By substituting each of $a_1, \ldots, a_n$ for x into (1.6), we get that

$$r(a_1) = r(a_2) = \cdots = r(a_n) = 0.$$

By the minimality condition on $\deg f(x)$ above, we get that $r(x) \equiv 0$. Since $\deg f(x) = n$, we get that $\deg q(x) = 0$. Thus, there is an $a \in F$ such that

$$f(x) = a(x - a_1)(x - a_2) \cdots (x - a_n).$$

Since $f(x) \not\equiv 0$, $a \neq 0$. Hence,

$$f(a_{n+1}) = a(a_{n+1} - a_1)(a_{n+1} - a_2) \cdots (a_{n+1} - a_n) \neq 0,$$

giving a contradiction and completing the proof. ■

Finally, we mention that throughout this book, we will make use of the Fundamental Theorem of Algebra that a polynomial $f(x)$ with complex coefficients of degree ≥ 1 has at least one root in the set of complex numbers. From the Fundamental Theorem of Algebra, it is not difficult to conclude that if $f(x) \in \mathbb{C}[x]$ and $\deg f(x) = n$, then there exist n complex numbers $\alpha_1, \ldots, \alpha_n$ (not necessarily distinct) and a complex number a such that

$$f(x) = a(x - \alpha_1) \cdots (x - \alpha_n).$$

We do not prove the Fundamental Theorem of Algebra here but simply comment that its proof can be found in (almost) any book on complex analysis and in many books on algebra.

Problems

(1.1) Let a be an integer, and let $f(x) \in \mathbb{Z}[x]$. Suppose that $f(x+a)$ is irreducible over $\mathbb{Z}$ (or over $\mathbb{Q}$). Prove that $f(x)$ is irreducible over $\mathbb{Z}$ (or over $\mathbb{Q}$, respectively). (We will usually use this result in this form, but observe that the role of $x+a$ in this problem can be replaced by any $g(x) \in \mathbb{Z}[x]$ with $\deg g(x) \geq 1$.)

(1.2) Let $f(x) \in \mathbb{Z}[x]$ with $f(0) \neq 0$, and let $n = \deg f(x)$. Suppose that $x^n f(1/x)$ is irreducible over $\mathbb{Z}$ (or over $\mathbb{Q}$). Prove that $f(x)$ is irreducible over $\mathbb{Z}$ (or over $\mathbb{Q}$, respectively).

(1.3) Find a necessary and sufficient condition for a quadratic $f(x) = ax^2+bx+c \in \mathbb{Z}[x]$ to be irreducible. Your condition should be written in terms of a, b, and c and should make use of Theorem 1.

(1.4) If $f(x) \in \mathbb{Z}[x]$ is monic, of degree ≥ 1, and reducible over the rationals, then show that there are monic polynomials $g(x)$ and $h(x)$ in $\mathbb{Z}[x]$ each of degree ≥ 1 and such that $f(x) = g(x)h(x)$.

(1.5) Let $f(x)$ denote a non-zero polynomial of degree n with arbitrary coefficients. Prove that

$$f(m) = \sum_{j=0}^{n} (-1)^{n-j} \binom{m}{j} \binom{m-j-1}{n-j} f(j)$$

holds for all integers $m > n$. Deduce that if $f(x) \in \mathbb{Z}[x]$, then $\gcd(f(0), f(1), \ldots, f(n))$ is a divisor of $f(m)$ for every $m \in \mathbb{Z}$.

(1.6) If $f(x) \in \mathbb{Z}[x]$ and p is a prime, then we can view $f(x)$ as a polynomial in $\mathbb{Z}_p[x]$ where $\mathbb{Z}_p$ denotes the finite field with p elements (i.e., arithmetic modulo p). Thus, $f(x)$ is reducible modulo p if and only if there exist $g(x)$ and $h(x)$ in $\mathbb{Z}_p[x]$ of degree > 0 such that $f(x) \equiv g(x)h(x) \pmod{p}$.

(a) Give an example of a polynomial $f(x) \in \mathbb{Z}[x]$ and a prime p such that $f(x)$ is

irreducible modulo p but $f(x)$ is reducible over $\mathbb{Q}$.

(b) Let $f(x) \in \mathbb{Z}[x]$, and let p be a prime. Suppose that the leading coefficient of $f(x)$ is not divisible by p. Prove that if $f(x)$ is irreducible modulo p, then $f(x)$ is irreducible over $\mathbb{Q}$.

(1.7) Let $f(x)$ and $g(x)$ be irreducible polynomials in $\mathbb{Z}[x]$. Prove that if there is a number α which is a root of both $f(x)$ and $g(x)$, then $f(x) \equiv \pm g(x)$. Also, explain what the analogous result is if $f(x)$ and $g(x)$ are irreducible polynomials in $\mathbb{Q}[x]$.

(1.8) Let $f(x)$ be an irreducible polynomial in $\mathbb{Z}[x]$ or $\mathbb{Q}[x]$. Prove that $f(x)$ has no multiple roots (i.e., prove that there does not exist an $\alpha \in \mathbb{C}$ such that $(x-\alpha)^2$ is a factor of $f(x)$ in $\mathbb{C}[x]$).

(1.9) Let $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$. Let a and b be relatively prime integers with $b \neq 0$. Prove that if $f(a/b) = 0$, then $a|a_0$ and $b|a_n$. (This is the Rational Root Test and provides a way to find the linear factors for a given $f(x) \in \mathbb{Z}[x]$.)

(1.10) Let $f(x)$ and $g(x)$ be in $\mathbb{Z}[x]$ with $g(x) \not\equiv 0$ and the content of $g(x)$ being 1. Suppose that $f(x) = g(x)h(x)$ with $h(x) \in \mathbb{Q}[x]$. Prove that $h(x) \in \mathbb{Z}[x]$.

(1.11) (a) Let $f(x)$ and $g(x)$ be in $\mathbb{Z}[x]$, and suppose that there are infinitely many integers m such that $g(m)|f(m)$. Prove that there is a polynomial $h(x) \in \mathbb{Q}[x]$ such that $f(x) = g(x)h(x)$. (Hint: Use the lemma to Theorem 3.)

(b) Find an example of an $f(x)$ and $g(x)$ as in part (a) for which no $h(x) \in \mathbb{Z}[x]$ exists such that $f(x) = g(x)h(x)$.

(1.12) Prove the assertions

$$u_{k-1}(x)r_k(x) + u_k(x)r_{k-1}(x) = h(x) \quad \text{for every } k \geq 0$$

and

$$v_{k-1}(x)r_k(x) + v_k(x)r_{k-1}(x) = g(x) \quad \text{for every } k \geq 0$$

given in Section 1.3.

(1.13) Let $f(x) = 2x^7 + 3x^6 + 2x^5 + 8x^4 + 4x^3 + 3x^2 + 4x + 1$ and $g(x) = 2x^6 + x^5 + x^4 + 5x^3 + x + 2$. Calculate the greatest common divisor of $f(x)$ and $g(x)$ in $\mathbb{Q}[x]$.

(1.14) Recall the example with $g(x) = x^5 - x^4 + 3x^3 + 2$ and $h(x) = x^4 - 2x^3 + 4x^2 - 3x + 2$ in Section 1.3. Find $u(x)$ and $v(x)$ such that $g(x)u(x) + h(x)v(x) = x^2 - x + 1$.

CHAPTER 2

THE SCHÖNEMANN - EISENSTEIN CRITERION AND NEWTON POLYGONS

Gauss is reported to have said,

"There have been but three epoch-making mathematicians,

Archimedes, Newton, and Eisenstein."

– E. T. Bell

Men of Mathematics

2.1. In this chapter, we explore a certain criterion for the irreducibility of polynomials and its generalizations. The main result in this section, often referred to as Eisenstein's Criterion, is a classical one. It was first proved by Schönemann [1] in a slightly more general setting, and shortly afterwards Eisenstein [1] published the same result.

Theorem 5. *Let* $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ *where* n *is a positive integer. Suppose that there exists a prime* p *such that* $p \nmid a_n$, $p | a_j$ *for all* $j < n$, *and* $p^2 \nmid a_0$. *Then* $f(x)$ *is irreducible over* $\mathbb{Q}$.

Proof 1. By Theorem 2, it suffices to show that $f(x)$ cannot be written in the form $f(x) = g(x)h(x)$ where $g(x)$ and $h(x) \in \mathbb{Z}[x]$, $\deg g(x) > 0$, and $\deg h(x) > 0$. Assume that $f(x)$ can be written in this form. Write $g(x)$ and $h(x)$ in the form $g(x) = \sum_{j=0}^{r} b_j x^j$ and

$h(x) = \sum_{j=0}^{s} c_j x^j$ where $r + s = n$. Define $b_j = 0$ for $j > r$, and define $c_j = 0$ for $j > s$. Let k be the minimal $j \in \{0, ..., r\}$ such that $p \nmid b_j$. Let ℓ be the minimal $j \in \{0, ..., s\}$ such that $p \nmid c_j$. These exist since $p \nmid a_n$ and $a_n = b_r c_s$ so that $p \nmid b_r$ and $p \nmid c_s$. The coefficient of $x^{k+\ell}$ in $g(x)h(x)$ is

$$b_0 c_{k+\ell} + b_1 c_{k+\ell-1} + \cdots + b_{k-1} c_{\ell+1} + b_k c_\ell + b_{k+1} c_{\ell-1} + \cdots + b_{k+\ell} c_0 \equiv b_k c_\ell \not\equiv 0 \pmod{p}.$$

On the other hand, all the coefficients of $f(x)$ except a_n are divisible by p. Thus, it must be the case that $k + \ell = n$ so that $k = r$ and $\ell = s$. By the definitions of k and ℓ, we now get that p divides both b_0 and c_0. But this contradicts that $a_0 = b_0 c_0$ is not divisible by p^2 and hence completes the proof. ■

Proof 2. Assume as before that $f(x) = g(x)h(x)$ where $g(x)$ and $h(x) \in \mathbb{Z}[x]$, $r = \deg g(x) > 0$, and $s = \deg h(x) > 0$. Since

$$g(x)h(x) \equiv f(x) \equiv a_n x^n \pmod{p},$$

Theorem 3 (with $F = \mathbb{Z}_p$, the field of integers modulo p) implies that $g(x)$ and $h(x)$ are both constants times a power of x modulo p. Furthermore, the condition that $p \nmid a_n$ implies that the leading coefficient of $g(x)$ and the leading coefficient of $h(x)$ are not divisible by p. Hence, there exist integers b and c such that $g(x) \equiv bx^r \pmod{p}$ and $h(x) \equiv cx^s \pmod{p}$. Since $r > 0$ and $s > 0$, we get that p divides the constant terms of $g(x)$ and $h(x)$. This contradicts that $p^2 \nmid a_0$, completing the proof. ■

Example 1. Theorem 5 with $p = 3$ implies that $f(x) = 2x^6 + 6x^4 + 6$ is irreducible over $\mathbb{Q}$. Here, it is not the case that $f(x)$ is irreducible over $\mathbb{Z}$, so that Theorem 5 does not remain true if the words "over $\mathbb{Q}$" are omitted.

Example 2. The polynomial $f(x) = x^5 + 4x^2 + 2$ is irreducible. Note that Theorem 5 guarantees that $f(x)$ is irreducible over $\mathbb{Q}$. Theorem 1 then implies that $f(x)$ is irreducible over $\mathbb{Z}$.

Example 3. Theorem 5 with $p = 5$ and Problem (1.2) imply that the polynomial $f(x) = 5x^6 + 10x + 3$ is irreducible over $\mathbb{Q}$. Theorem 1 then implies that $f(x)$ is irreducible.

We note that the first proof of Theorem 5 very much resembles the proof given for the Lemma to Theorem 1. There are many possible generalizations of the Schönemann - Eisenstein Criterion; one example of such a generalization is given in Problem (2.9). Momentarily, we shall see how we can view the Schönemann - Eisenstein Criterion as being a simple consequence of a general theorem concerning Newton polygons. Many results similar to Theorem 5 can be obtained from the use of Newton polygons. Before discussing Newton polygons further, however, we explore the concept of Eisenstein polynomials.

2.2. We say that a polynomial $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ is in Eisenstein form (with respect to the prime p) if there is a prime p such that $p \nmid a_n$, $p | a_j$ for $j < n$, and $p^2 \nmid a_0$. An Eisenstein polynomial is an $f(x) \in \mathbb{Z}[x]$ for which there is an integer a and a prime p such that $f(x+a)$ is in Eisenstein form with respect to the prime p. In other words, $f(x) \in \mathbb{Z}[x]$ is Eisenstein if there is an integer a and a prime p such that $f(x+a) = \sum_{j=0}^{n} a'_j x^j$ where $p \nmid a'_n$, $p | a'_j$ for $j < n$, and $p^2 \nmid a'_0$. More specifically, we say that such an $f(x)$ is Eisenstein with respect to the prime p. For example, since $f(x) = x^2 + x + 1$ is such that $f(x+1) = x^2 + 3x + 3$, the polynomial $f(x)$ is Eisenstein with respect to 3. It follows easily from Theorem 5 that if $f(x)$ is Eisenstein with respect to a prime p, then $f(x)$ is irreducible over $\mathbb{Q}$ (see Problem (1.1)).

Suppose one is given an $f(x) \in \mathbb{Z}[x]$ and wishes to decide whether $f(x)$ is Eisenstein with respect to some prime (which is not given). We assume $n = \deg f(x)$ is at least 2. One approach to making such a decision involves the use of discriminants or resultants. Our presentation here will be restricted to resultants. Let $f(x) = \sum_{j=0}^{n} a_j x^j$ and $g(x) = \sum_{j=0}^{r} b_j x^j$ be in $\mathbb{C}[x]$ with $a_n b_r \neq 0$. We define the resultant of $f(x)$ and $g(x)$ in terms of the Sylvester determinant $R(f,g)$ associated with $f(x)$ and $g(x)$. $R(f,g)$ is the determinant of an $(n+r) \times (n+r)$ matrix with the first r rows consisting of the coefficients of $f(x)$, where each of these rows contains one more leading 0 than its predecessor, and with the last n rows consisting of the coefficients of $g(x)$, where each of these rows contains one

more leading 0 than its predecessor. Specifically, we may write*

$$R(f,g) = \begin{vmatrix} a_n & a_{n-1} & a_{n-2} & \dots & a_0 & 0 & 0 & \dots & 0 \\ 0 & a_n & a_{n-1} & \dots & a_1 & a_0 & 0 & \dots & 0 \\ 0 & 0 & a_n & \dots & a_2 & a_1 & a_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ b_r & b_{r-1} & b_{r-2} & \dots & b_0 & 0 & 0 & \dots & 0 \\ 0 & b_r & b_{r-1} & \dots & b_1 & b_0 & 0 & \dots & 0 \\ 0 & 0 & b_r & \dots & b_2 & b_1 & b_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \end{vmatrix}. \tag{2.1}$$

For example, if $f(x) = x^3 + x + 1$ and $g(x) = 2x^2 + x + 3$, then (2.1) becomes

$$R(f,g) = \begin{vmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 2 & 1 & 3 & 0 & 0 \\ 0 & 2 & 1 & 3 & 0 \\ 0 & 0 & 2 & 1 & 3 \end{vmatrix}.$$

Lemma. *Let $f(x)$ and $g(x) \in \mathbb{C}[x]$, and suppose that there is an α such that $f(\alpha) = g(\alpha) = 0$. Then $R(f,g) = 0$.*

Proof. Add to the ith row of the last column (the $(n+r)$th column) of the determinant on the right-hand side of (2.1) the product of the entry in the ith row and jth column with α^{n+r-j}. Then the first r entries in the last column become $\alpha^{r-1}f(\alpha), \alpha^{r-2}f(\alpha), \dots, f(\alpha)$ and the last n entries become $\alpha^{n-1}g(\alpha), \alpha^{n-2}g(\alpha), \dots, g(\alpha)$. By the conditions of the Lemma, these are all 0, and the result follows. ■

If $\alpha_1, \dots, \alpha_n$ are the roots of $f(x)$, one can show that

$$R(f,g) = a_n^r g(\alpha_1) \cdots g(\alpha_n). \tag{2.2}$$

The proof can be found in Uspensky [1]. We will use (2.2) to help deal with the possibility that $R(f,g) = 0$. (If 0 wasn't around, there wouldn't be nothing to worry about.) Observe that (2.2) implies the lemma and also the converse of the lemma. Thus, if $R(f,g) = 0$, then $f(x)$ and $g(x)$ have a root in common. We now show that the following algorithm works to determine whether a given polynomial $f(x)$ is Eisenstein.

*The appearance of the right-hand side of (2.1) is somewhat misleading. The entry a_0 in the first row, for example, is not necessarily in the same column as the entry b_0 in the first row consisting of the b_j's.

Algorithm. *Suppose that $f(x) \in \mathbb{Z}[x]$ of degree $n \geq 2$. Calculate $R(f, f')$ (using the right-hand side of (2.1)). If $R(f, f') = 0$, then $f(x)$ is not Eisenstein with respect to any prime. If $R(f, f') \neq 0$, then factor it. For each prime p dividing $R(f, f')$, check to see if any of the translates $f(x+a)$, where $a \in \{0, 1, ..., p-1\}$, is in Eisenstein form with respect to the prime p. If such a prime p and such an a are such that $f(x + a)$ is in Eisenstein form with respect to p, then $f(x)$ is Eisenstein with respect to p. If no such prime p and no such a are such that $f(x + a)$ is in Eisenstein form with respect to p, then $f(x)$ is not Eisenstein with respect to any prime.*

In justifying the algorithm, we explain how one can use the resultant $R(f, f')$ to determine whether a polynomial $f(x)$ has a multiple factor (a factor which appears with multiplicity > 1) modulo some prime (which is unspecified). To see this, suppose that there is a prime p such that

$$f(x) \equiv g(x)^2 h(x) \pmod{p} \tag{2.3}$$

where $g(x)$ is of degree ≥ 1. Note that if for some integer a we have that $f(x + a)$ is in Eisenstein form with respect to the prime p, then $f(x) \equiv a_n(x - a)^n \pmod{p}$ so that one can take $g(x) = x - a$. Define $f_1(x) = g(x)^2 h(x)$ so that the coefficients of $f(x)$ and of $f'(x)$ are the same as the corresponding coefficients of $f_1(x)$ and $f_1'(x)$ all considered modulo p. In particular, $R(f, f') \equiv R(f_1, f_1') \pmod{p}$. Since

$$f_1'(x) = 2g(x)g'(x)h(x) + g(x)^2 h'(x) = g(x)\left(2g'(x)h(x) + g(x)h'(x)\right),$$

we get that each root of $g(x)$ is a root of $f_1(x)$ and of $f_1'(x)$. By the Lemma, we get that $R(f_1, f_1') = 0$. Hence, $R(f, f') \equiv 0 \pmod{p}$. Thus, p divides $R(f, f')$; and to determine if (2.3) holds for some prime p, we simply need to check whether it holds for each prime divisor p of $R(f, f')$. The fact that the algorithm works when $R(f, f') \neq 0$ is now fairly straight forward, but we need to justify that we can restrict our consideration of integers a to $a \in \{0, 1, \ldots, p-1\}$. For this purpose, we suppose that b is an integer for which $f(x+b)$ is in Eisenstein form with respect to some prime p and show that $f(x + a)$ is also for any

$a \equiv b \pmod{p}$. Since $f(x+b) \equiv f(x+a) \pmod{p}$, we simply need to justify that p^2 does not divide the constant term in $f(x+a)$. In other words, we want to show that $p^2 \nmid f(a)$. Writing $f(x+b) = \sum_{j=0}^{n} a'_j x^j$, we get that $p | a'_j$ for $j < n$ and $p^2 \nmid a'_0$. Writing $a = kp + b$ where k is an integer, we get that

$$f(a) \equiv f(kp+b) \equiv \sum_{j=0}^{n} a'_j k^j p^j \equiv kpa'_1 + a'_0 \equiv a'_0 \pmod{p^2}.$$

Thus, $f(a) \not\equiv 0 \pmod{p^2}$, completing what we set out to show (for the case $R(f, f') \neq 0$).

If $R(f, f') = 0$, the above all works except that every prime is a prime divisor of $R(f, f')$ so it is not reasonable to consider all the prime divisors of $R(f, f')$. But observe that (2.2) implies that $f(x)$ and $f'(x)$ have a root in common. Hence, in this case, $f(x)$ must have a multiple root (the reader should justify this) so that $f(x)$ is reducible over $\mathbb{Q}$ (see Problem (1.8)). In particular, by Theorem 5, we can conclude that $f(x)$ cannot be Eisenstein with respect to any prime.

Example. Consider $f(x) = x^4 + 2x - 1$, and suppose that we wish to find every prime p such that $f(x)$ is Eisenstein with respect to p. We first calculate $R(f, f')$ by using (2.1). To do this somewhat efficiently, we multiply below the first row by -4 and add it to the fourth row. Observe that we will get the same result in the fifth row with an extra leading 0 if we multiply the second row by -4 and add it to the fifth row. Similarly, we can obtain the same result in the sixth row (as the fourth row) with 2 extra leading 0's by considering the third row. We get that

$$R(f,f') = \begin{vmatrix} 1 & 0 & 0 & 2 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 2 & -1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 2 & -1 \\ 4 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 4 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 4 & 0 & 0 & 2 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 & 2 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 2 & -1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 2 & -1 \\ 0 & 0 & 0 & -6 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 & -6 & 4 & 0 \\ 0 & 0 & 0 & 0 & 0 & -6 & 4 \\ 0 & 0 & 0 & 4 & 0 & 0 & 2 \end{vmatrix}.$$

A direct computation now gives

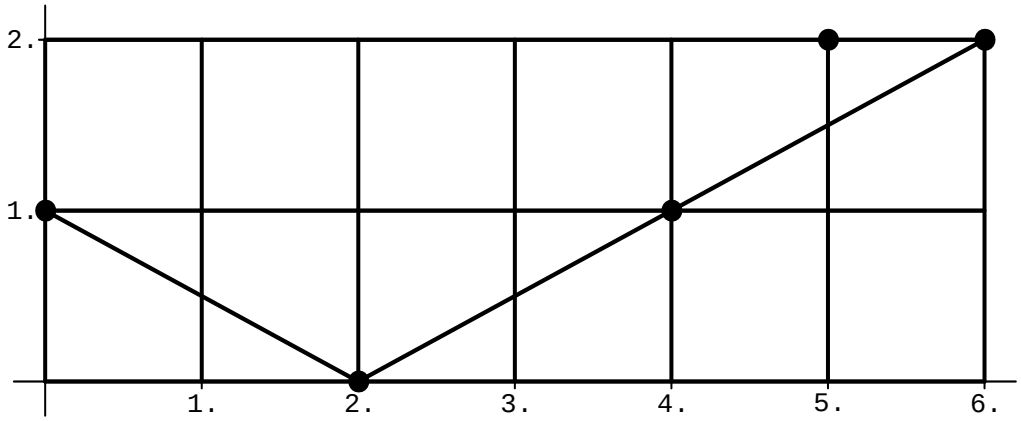
$$R(f,f') = \begin{vmatrix} -6 & 4 & 0 & 0 \\ 0 & -6 & 4 & 0 \\ 0 & 0 & -6 & 4 \\ 4 & 0 & 0 & 2 \end{vmatrix} = -6 \times 72 - 4 \times 64 = -688.$$

Since $688 = 2^4 \times 43$, we only need to deal with the primes 2 and 43. We make use of exercise (2.2). Observe that 2 divides $f(1)$, and so we consider $f(x+1) = x^4 + 4x^3 + 6x^2 + 6x + 2$. Thus, $f(x)$ is Eisenstein with respect to the prime 2 (and, hence, $f(x)$ is irreducible). Observe that 43 divides $f(3)$ but that $f'(3) = 4 \times 27 + 2 = 110$ is not divisible by 43. Thus, $f(x)$ is not Eisenstein with respect to the prime 43. Hence, 2 is the only prime p such that $f(x)$ is Eisenstein with respect to p. Alternatively, we note that Problem (2.7) could have been used to determine that $f(x)$ is not Eisenstein with respect to 43.

In this section, we have considered the problem of determining whether a polynomial $f(x) \in \mathbb{Z}[x]$ can under a translation be shown to be irreducible over $\mathbb{Q}$ by the Schönemann - Eisenstein criterion. In general, if $f(x)$ and $g(x) \in \mathbb{Z}[x]$ and $f(g(x))$ is irreducible over $\mathbb{Q}$, then $f(x)$ is irreducible over $\mathbb{Q}$; hence, it is reasonable to attempt to determine whether a given $f(x)$ is irreducible by applying the Schönemann - Eisenstein criterion after composing $f(x)$ with another polynomial. We leave further consideration of this idea as an exercise (Problem (2.4)).

2.3. In this section, we explore the concept of Newton polygons. Some discussion of Newton polygons can be found in Dorwart [1], Weiss [1], and Chao [1]. Let $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ with $a_0 a_n \neq 0$. Let p be a prime. For $j \in \{0, \ldots, n\}$, we define $x_j = j$ and define $y_j \in \mathbb{Z}^+ \cup \{0\} \cup \{+\infty\}$ to be the exponent of p in the largest power of p dividing a_{n-j}. In other words, $p^{y_j} | a_{n-j}$ and $p^{y_j+1} \nmid a_{n-j}$ if $a_{n-j} \neq 0$ and $y_j = +\infty$ in the case that $a_{n-j} = 0$. Thus, we get a set of points $S = \{(x_0, y_0), \ldots, (x_n, y_n)\}$ in the extended plane. We consider the lower edges along the convex hull of these points. The left-most edge has one endpoint being (x_0, y_0) and the right-most edge has (x_n, y_n) as an endpoint. The endpoints of every edge belong to the set S. If (x_i, y_i) and (x_j, y_j) are the 2 endpoints of such an edge, then every point (x_u, y_u) with $i < u < j$ lies on or above the line passing through (x_i, y_i) and (x_j, y_j). The polygonal path formed by these edges is called the Newton polygon associated with $f(x)$. To clarify the dependence of this polygonal path on p, we will sometimes refer to it as the Newton polygon for $f(x)$ with respect to p. For

example, if $f(x) = 2x^6 + x^4 + 2x^2 + 4x + 4$, then the Newton polygon for $f(x)$ with respect to the prime 2 consists of 2 edges, one from $(0, 1)$ to $(2, 0)$ and the other from $(2, 0)$ to $(6, 2)$.



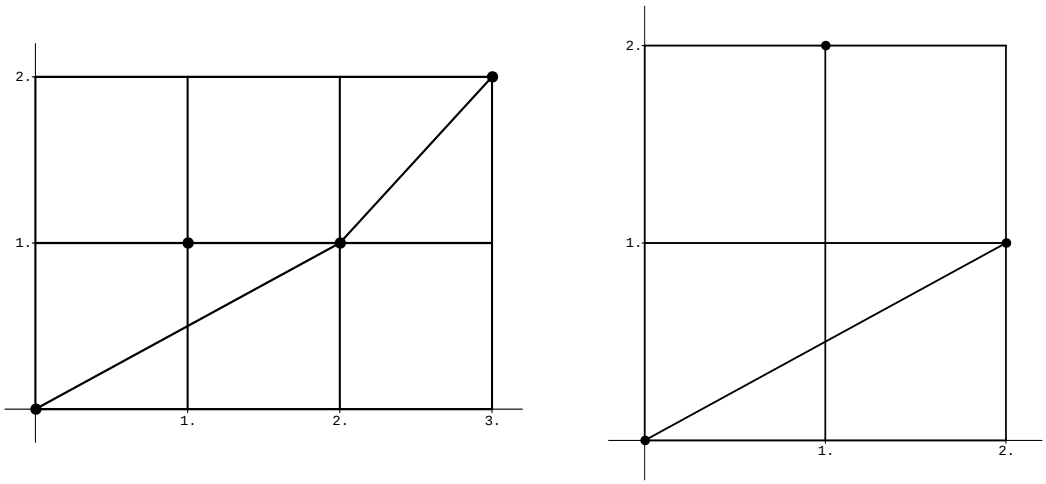
The Newton polygon for $f(x) = 2x^6 + x^4 + 2x^2 + 4x + 4$

Observe that the slope of the edges are always increasing when calculated from the left-most edge to the right-most edge. The following theorem is due to Dumas [1].

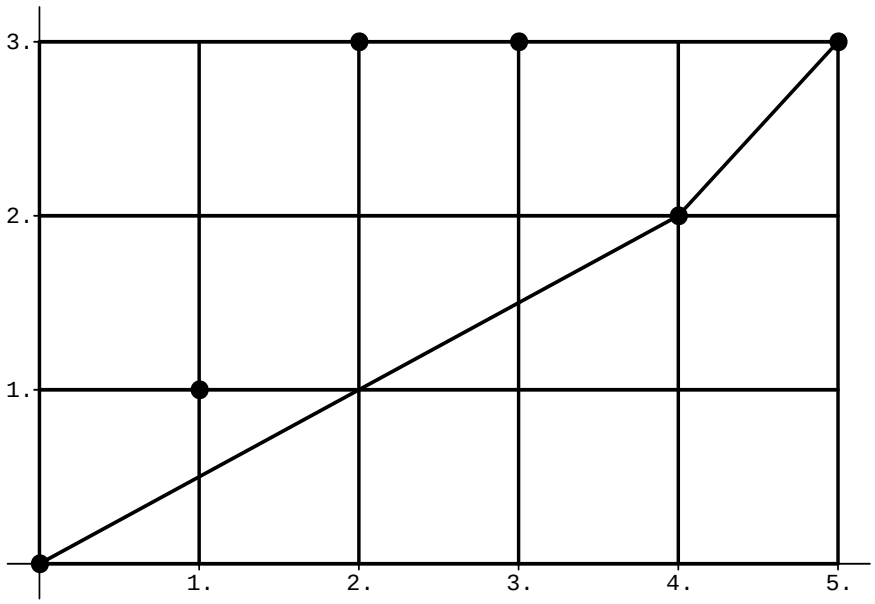
Theorem 6. *Let $g(x)$ and $h(x)$ be in $\mathbb{Z}[x]$ with $g(0)h(0) \neq 0$, and let p be a prime. Let k be a non-negative integer such that p^k divides the leading coefficient of $g(x)h(x)$ but p^{k+1} does not. Then the edges of the Newton polygon for $g(x)h(x)$ with respect to p can be formed by constructing a polygonal path beginning at $(0, k)$ and using translates of the edges in the Newton polygons for $g(x)$ and $h(x)$ with respect to the prime p, using exactly one translate for each edge of the Newton polygons for $g(x)$ and $h(x)$. Necessarily, the translated edges are translated in such a way as to form a polygonal path with the slopes of the edges increasing.*

To help explain the statement of the theorem, we consider a couple of examples. We take $p = 3$ and consider $g(x) = x^3 + 3x^2 + 12x + 9$ and $h(x) = 2x^2 + 9x + 3$. Then the Newton polygon for $g(x)$ consists of 2 edges, one with slope $1/2$ and the other with slope 1; the Newton polygon for $h(x)$ consists of 1 edge having slope $1/2$; and the Newton polygon for $g(x)h(x) = 2x^5 + 15x^4 + 54x^3 + 135x^2 + 117x + 27$ consists of 2 edges, one with slope $1/2$ and the other with slope 1. The translates of the edges of the Newton polygons for

$g(x)$ and $h(x)$ with slope $1/2$ have merged to form a single edge in the Newton polygon for $g(x)h(x)$. We emphasize that, for our purposes, when referring to the "edges" of a Newton polygon, we shall not allow 2 different edges to have the same slope.



The Newton polygons for $g(x) = x^3 + 3x^2 + 12x + 9$ and $h(x) = 2x^2 + 9x + 3$



The Newton polygon for $g(x)h(x) = 2x^5 + 15x^4 + 54x^3 + 135x^2 + 117x + 27$

As a second example, we consider a prime p and an $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ which is in Eisenstein form with respect to p (say with $a_n \neq 0$). Then in our description of the Newton polygon for $f(x)$ above, we get that $(x_0, y_0) = (0, 0)$, $(x_n, y_n) = (n, 1)$, and every other (x_j, y_j) lies on or above the line passing through (x_0, y_0) and (x_n, y_n). Observe that

Theorem 6 would imply that $f(x)$ is irreducible over $\mathbb{Q}$ since if $f(x) = g(x)h(x)$ with $g(x)$ and $h(x) \in \mathbb{Z}[x]$ and with $\deg g(x)$ and $\deg h(x) > 0$, then the Newton polygon for $f(x)$ with respect to p would be able to be represented as translates of 2 or more edges. The latter is impossible since the only lattice points (points with integral coordinates) on the Newton polygon for $f(x)$ are its endpoints (x_0, y_0) and (x_n, y_n). Thus, Theorem 6 can be viewed as a generalization of Theorem 5.

Proof of Theorem 6. We write $g(x) = \sum_{j=0}^{r} b_j x^j$ and $h(x) = \sum_{j=0}^{s} c_j x^j$ with $b_r \neq 0$ and $c_s \neq 0$ and $f(x) = g(x)h(x) = \sum_{j=0}^{n} a_j x^j$ where $a_n \neq 0$. Thus, $n = r + s$. For $j \in \{0, \ldots, n\}$, we represent the exponent in the largest power of p (possibly $+\infty$) dividing a_{n-j} with y_j; for $j \in \{0, \ldots, r\}$, we represent the exponent in the largest power of p dividing b_{r-j} with y'_j; and for $j \in \{0, \ldots, s\}$, we represent the exponent in the largest power of p dividing c_{s-j} with y''_j. We consider an edge of the Newton polygon for $g(x)$ (with respect to the prime p). Let (k_1, u_1) and (k_2, u_2) denote the endpoints of such an edge with $k_2 > k_1$. Thus, $u_1 = y'_{k_1}$ and $u_2 = y'_{k_2}$. Observe that the equation of the line passing through (k_1, u_1) and (k_2, u_2) is

$$(u_2 - u_1)x - (k_2 - k_1)y = (u_2 - u_1)k_1 - (k_2 - k_1)u_1. \tag{2.4}$$

Since every point (i, y'_i) associated with a coefficient of $g(x)$ lies on or above this line, we get that

$$(u_2 - u_1)i - (k_2 - k_1)y'_i \leq (u_2 - u_1)k_1 - (k_2 - k_1)u_1 \quad \text{for } i \in \{0, \ldots, r\}. \tag{2.5}$$

Furthermore, equality can occur in (2.5) only if $k_1 \leq i \leq k_2$. Consider the right-most edge (if such an edge exists) of the Newton polygon for $h(x)$ which has a slope which is $< (u_2 - u_1)/(k_2 - k_1)$, the slope of the line given by (2.4). Let (m_1, v_1) denote the right endpoint of that edge. If no such edge exists, then set $m_1 = 0$ and $v_1 = y''_0$. In any case, $v_1 = y''_{m_1}$. In the case that there is an edge on the Newton polygon for $h(x)$ which has (m_1, v_1) as its left endpoint, we set (m_2, v_2) to be the right endpoint of that edge. Thus, $m_2 > m_1$ (when m_2 is defined). Observe that if (m_2, v_2) is not defined or if the slope of

the line passing through (m_1, v_1) and (m_2, v_2) is $> (u_2 - u_1)/(k_2 - k_1)$, then we need to show that the edge joining (k_1, u_1) and (k_2, u_2) on the Newton polygon for $g(x)$ can be translated to an edge of the Newton polygon for $f(x)$ with endpoints $(k_1 + m_1, u_1 + v_1)$ and $(k_2 + m_1, u_2 + v_1)$. On the other hand, if (m_2, v_2) is defined and the slope of the line passing through (m_1, v_1) and (m_2, v_2) is equal to $(u_2 - u_1)/(k_2 - k_1)$, then we need to show that the edge joining (k_1, u_1) and (k_2, u_2) on the Newton polygon for $g(x)$ and the edge joining (m_1, v_1) and (m_2, v_2) on the Newton polygon for $h(x)$ can be translated to an edge of the Newton polygon for $f(x)$ with endpoints $(k_1 + m_1, u_1 + v_1)$ and $(k_2 + m_2, u_2 + v_2)$.

Let $t \in \{0, \ldots, n\}$ and consider $i \in \{0, \ldots, r\}$ and $j \in \{0, \ldots, s\}$ such that $t = i + j$. The definition of (m_1, v_1) implies that point (j, y_j'') lies on or above the line passsing through (m_1, v_1) with slope $(u_2 - u_1)/(k_2 - k_1)$. In other words,

$$(u_2 - u_1)j - (k_2 - k_1)y_j'' \leq (u_2 - u_1)m_1 - (k_2 - k_1)v_1. \tag{2.6}$$

Furthermore, equality can occur in (2.6) if and only if either (i) $(j, y_j'') = (m_1, v_1)$ or (ii) (m_2, v_2) exists, the line passing through (m_1, v_1) and (m_2, v_2) has slope equal to $(u_2 - u_1)/(k_2 - k_1)$, and (j, y_j'') is on the line segment joining (m_1, v_1) and (m_2, v_2). Combining (2.5) and (2.6), we get that

$$(u_2 - u_1)(i + j) - (k_2 - k_1)(y_i' + y_j'') \leq (u_2 - u_1)(k_1 + m_1) - (k_2 - k_1)(u_1 + v_1). \tag{2.7}$$

Recall that $t = i + j$. We view t as fixed and consider first the case that (m_2, v_2) is not defined or the slope of the line passing through (m_1, v_1) and (m_2, v_2) is $> (u_2 - u_1)/(k_2 - k_1)$. If equality holds in (2.7), then (i) must hold. For the moment, we consider $t = k_1 + m_1$. We get that equality holds in (2.7) if and only if $i = k_1$ and $j = m_1$. Since $t = i + j = k_1 + m_1$ is fixed, (2.7) implies that $y_i' + y_j''$ obtains its minimum when $i = k_1$ and $j = m_1$ and for no other values of i and j. Since $f(x) = g(x)h(x)$, we get that

$$a_{n-t} = \sum_{i+j=t} b_{r-i} c_{s-j}. \tag{2.8}$$

Each term $b_{r-i}c_{s-j}$ is divisible by $p^{y_i' + y_j''}$ (by the definition of y_i' and y_j''). Thus, the fact that the minimality of $y_i' + y_j''$ occurs when $i = k_1$ and $j = m_1$ implies that $p^{u_1 + v_1}$ divides

a_{n-t}. Also, $p^{u_1+v_1+1}$ divides every term $b_{r-i}c_{s-j}$ in (2.8) except for the term $b_{r-k_1}c_{s-m_1}$. Thus, $p^{u_1+v_1}$ must exactly divide a_{n-t}. In other words,

$$y_{k_1+m_1} = u_1 + v_1 = y'_{k_1} + y''_{m_1}. \tag{2.9}$$

Now we consider $t = k_2 + m_1$. From (2.7), $y'_i + y''_j$ obtains its minimum precisely when $i = k_2$ and $j = m_1$. Instead of (2.9), we obtain that

$$y_{k_2+m_1} = u_2 + v_1 = y'_{k_2} + y''_{m_1}.$$

To show that the segment joining $(k_1 + m_1, u_1 + v_1)$ and $(k_2 + m_1, u_2 + v_1)$ actually forms an edge of the Newton polygon for $f(x)$, it remains to show for $t \in \{0, \ldots, n\}$ that (t, y_t) is on or above the line passing through $(k_1 + m_1, u_1 + v_1)$ and $(k_2 + m_1, u_2 + v_1)$ and that if (t, y_t) is on the line, then $k_1 + m_1 \leq t \leq k_2 + m_1$. For $t \in \{0, \ldots, n\}$, observe that (2.8) implies that

$$y_t \geq \min_{i+j=t} \{y'_i + y''_j\}.$$

Fix $t \in \{0, \ldots, n\}$, and fix $i \in \{0, \ldots, r\}$ and $j \in \{0, \ldots, s\}$ so that $t = i+j$ and $y_t \geq y'_i + y''_j$. Then from (2.7), we get that

$$\begin{aligned}(u_2 - u_1)t - (k_2 - k_1)y_t &\leq (u_2 - u_1)(i + j) - (k_2 - k_1)(y'_i + y''_j) \\ &\leq (u_2 - u_1)(k_1 + m_1) - (k_2 - k_1)(u_1 + v_1).\end{aligned} \tag{2.10}$$

This implies that (t, y_t) is on or above the line passing through $(k_1 + m_1, u_1 + v_1)$ and $(k_2 + m_1, u_2 + v_1)$. Recalling that (2.7) was a consequence of (2.5) and (2.6), we see that if equality occurs in (2.10), then $k_1 \leq i \leq k_2$ and $j = m_1$. In other words, if equality occurs in (2.10), then $k_1 + m_1 \leq t \leq k_2 + m_1$. This establishes what we set out to show for the case that (m_2, v_2) is not defined or the slope of the line passing through (m_1, v_1) and (m_2, v_2) is $> (u_2 - u_1)/(k_2 - k_1)$.

Suppose now that (m_2, v_2) exists and the slope of the line passing through (m_1, v_1) and (m_2, v_2) is equal to $(u_2 - u_1)/(k_2 - k_1)$. In this case, if equality holds in (2.6) or (2.7), then

$m_1 \leq j \leq m_2$. If equality holds in (2.7), we also have that $k_1 \leq i \leq k_2$. If $t = k_1 + m_1$, then either $i \leq k_1$ or $j \leq m_1$. Thus, we get that equality holds in (2.7) if and only if $i = k_1$ and $j = m_1$ as before, and (2.9) follows. If $t = k_2 + m_2$, then either $i \geq k_2$ or $j \geq m_2$. In this case, we get that equality holds in (2.7) if and only if $i = k_2$ and $j = m_2$. Thus, we obtain that

$$y_{k_2+m_2} = u_2 + v_2 = y'_{k_2} + y''_{m_2}.$$

As before, we get that (2.10) follows for every $t \in \{0, \ldots, n\}$. Here, if equality holds, then $k_1 \leq i \leq k_2$ and $m_1 \leq j \leq m_2$ so that $k_1 + m_1 \leq t \leq k_2 + m_2$. It follows that the segment joining $(k_1 + m_1, u_1 + v_1)$ and $(k_2 + m_2, u_2 + v_2)$ forms an edge of the Newton polygon for $f(x)$. This completes the proof. ■

The following corollary summarizes important information given by Theorem 6.

Corollary. *Let $f(x) \in \mathbb{Z}[x]$ be of degree n with $f(0) \neq 0$, and suppose that there are polynomials $g_1(x), \ldots, g_r(x) \in \mathbb{Z}[x]$ (not necessarily irreducible) such that $f(x) = g_1(x) \cdots g_r(x)$. Let p be a prime, and let $(x'_0, y'_0), (x'_1, y'_1), \ldots, (x'_k, y'_k)$, with $x'_0 = 0 < x'_1 < \cdots < x'_k = n$, be the complete list of lattice points on the Newton polygon for $f(x)$ with respect to p. For $j \in \{1, \ldots, k\}$, let $b_j = x'_j - x'_{j-1}$. Then there exist $\epsilon_{i,j} \in \{0, 1\}$, where $i \in \{1, \ldots, r\}$ and $j \in \{1, \ldots, k\}$, such that for each j, there is one and only one i for which $\epsilon_{i,j} = 1$, and such that for each i,*

$$\deg g_i(x) = \sum_{j=1}^{k} \epsilon_{i,j} b_j.$$

Example 1. Let p be a prime. Suppose that $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ is such that $p \nmid a_n$, $p | a_j$ for $j \in \{0, \ldots, n-1\}$, and $p^2 \nmid a_1$. We show that either $f(x)$ is irreducible over $\mathbb{Q}$ or $f(x)$ factors as the product of a linear polynomial and an irreducible polynomial over $\mathbb{Q}$ of degree $n - 1$. If $p^2 \nmid a_0$, then we can apply the Schönemann - Eisenstein Criterion to conclude that $f(x)$ is irreducible over $\mathbb{Q}$. Hence, the result follows trivially in this case. Similarly, if $a_0 = 0$, then $f(x) = xg(x)$ and $g(x)$ is irreducible over $\mathbb{Q}$ by the Schönemann-Eisenstein Criterion so that the result holds. Suppose now that $p^2 | a_0$ and $a_0 \neq 0$. Then the

Newton polygon with respect to p contains exactly 2 segments, one from $(0,0)$ to $(n-1,1)$ and the other from $(n-1,1)$ to (n,m) where m is the largest power of p dividing a_0. Thus, Theorem 6 or its Corollary implies that either $f(x)$ is irreducible over $\mathbb{Q}$ or $f(x)$ factors as the product of a linear polynomial and an irreducible polynomial over $\mathbb{Q}$ of degree $n-1$, which is what we set out to show.

Example 2. We show that $f(x) = x^5 + 2x^3 + 2x + 4$ is irreducible. By Problem (1.9), the only possible rational roots of $f(x)$ are ± 1, ± 2, or ± 4. Clearly, $f(x)$ has no positive roots since all of its non-zero coefficients are positive. Also, $f(-1) \equiv 1 \pmod 2$ and $f(-4) \equiv 4 \pmod 8$ imply that -1 and -4 are not roots of $f(x)$. Finally, since $f(-2) = -32 - 16 - 4 + 4 \neq 0$, $f(x)$ has no rational roots. Using $p = 2$ in the previous example, we can conclude that $f(x)$ is irreducible.

We emphasize that the following strengthening of the Corollary is not true. (We do this partially to clear up a misprint which occurs in the literature in Grosswald [2, p. 107, Theorem A′].) Instead of considering every lattice point on the Newton polygon for $f(x)$ with respect to p, suppose that we only consider those lattice points (x_j', y_j') which correspond to the $(x_j, y_j) = (j, y_j)$ described at the beginning of this section in our construction of the Newton polygon for $f(x)$. The idea then is to hope for the same conclusion as in the Corollary with the new list of x_j''s and, hence, b_j's. Such a conclusion, however, does not hold. We have seen an example where this conclusion would not follow, namely when we considered the product of $g(x) = x^3+3x^2+12x+9$ and $h(x) = 2x^2+9x+3$ and the prime $p = 3$. Another easier example is given by $f(x) = x^2 + 4x + 4 = (x+2)^2$ with $p = 2$.

Theorem 6 is an important result which has found applications to some classical polynomials. We will explore some of these later. We observe that the theorem is limited by the fact that it derives all of its information from simply examining the primes dividing the non-zero coefficients of a given polynomial $f(x)$. Other important information is left untouched. We will see in the next chapter, for example, that examining the approximate

location of the complex roots of $f(x)$ often aids in determining whether it is irreducible.

2.4. In this section, we show how Newton polygons can be used to establish the following result due to I. Schur [1].

Theorem 7. *Let n be a positive integer, and let $a_0, a_1, \ldots, a_n$ denote arbitrary integers with $|a_0| = |a_n| = 1$. Then*

$$a_n \frac{x^n}{n!} + a_{n-1} \frac{x^{n-1}}{(n-1)!} + \cdots + a_1 x + a_0$$

is irreducible over the rationals.

For convenience, we make use of the following p-adic notation. For p a prime (which will be clear form the context) and m a non-zero integer, we define $\nu(m)$ as the non-negative integer such that $p^{\nu(m)} | m$ and $p^{\nu(m)+1} \nmid m$. In the case that $m = 0$, we define $\nu(m)$ as $+\infty$. Also, we view $+\infty$ as being a quantitiy greater than any integer.

Our use of Newton polygons for obtaining Theorem 7 is summarized by the following Lemma.

Lemma 1. *Let k and ℓ be integers with $k > \ell \geq 0$. Suppose $g(x) = \sum_{j=0}^{n} b_j x^j \in \mathbb{Z}[x]$ and p is a prime such that $p \nmid b_n$, $p | b_j$ for all $j \in \{0, 1, \ldots, n-\ell-1\}$, and the right-most edge of the Newton polygon for $g(x)$ with respect to p has slope $< 1/k$. Then for any integers $a_0, a_1, \ldots, a_n$ with $|a_0| = |a_n| = 1$, the polynomial $f(x) = \sum_{j=0}^{n} a_j b_j x^j$ cannot have a factor with degree in the interval $[\ell + 1, k]$.*

Proof. We first consider the case that $a_j = 1$ for all $j \in \{0, 1, \ldots, n\}$ so that $f(x) = g(x)$. Assume $f(x)$ in this case has a factor with degree in $[\ell + 1, k]$. Then there exist $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$ with $f(x) = u(x)v(x)$ and $\ell + 1 \leq \deg u(x) \leq k$. We consider the Newton polygon for $f(x) = g(x)$ with respect to p. Since the slopes of the edges of the Newton polygon for $f(x)$ increase from left to right, the conditions of the lemma imply that each edge has slope in $[0, 1/k)$. The left-most edge of the Newton polygon may have slope 0. For now, we consider an edge of the Newton polygon which does not have slope 0. Let

(a,b) and (c,d) be 2 lattice points on such an edge. Then the slope of the line passing through these points is the slope of the edge so that

$$\frac{1}{|c-a|} \leq \frac{|d-b|}{|c-a|} < \frac{1}{k}.$$

Hence, $|c-a| > k$. In other words, any 2 lattice points on an edge with non-zero slope of the Newton polygon for $f(x)$ with respect to p have their $x-$coordinates separated by a distance $> k$. Since $\deg u(x) \leq k$, we get that translates of the edges of the Newton polygon for $u(x)$ with respect to p cannot be found within those edges of the Newton polygon for $f(x)$ with respect to p which have non-zero slope. In other words, the left-most edge of the Newton polygon for $f(x)$ must have slope 0 and length $\geq \deg u(x)$. The conditions of the lemma imply that $\nu(b_{n-j}) \geq 1$ for $j \in \{\ell+1, \ell+2, \ldots, n\}$ so that if the left-most edge of the Newton polygon for $f(x)$ with respect to p has slope 0, then it has length $\leq \ell < \deg u(x)$, giving a contradiction.

Next, we consider the general case of arbitrary integers $a_0, a_1, \ldots, a_n$ with $a_0 = \pm 1$ and $a_n = \pm 1$. The conditions on a_0 and a_n imply that the left and right-most endpoints of the Newton polygon for $f(x)$ with respect to p are the same as the left and right-most endpoints of the Newton polygon for $g(x)$ with respect to p, respectively. Also, $p|a_j b_j$ for all $j \in \{0, 1, \ldots, n-\ell-1\}$. All the edges of the Newton polygon for $g(x)$ with respect to p lie above or on the line containing the right-most edge. The same statement holds for $f(x)$ in place of $g(x)$. Note that $\nu(a_j b_j) \geq \nu(b_j)$ for all $j \in \{0, 1, \ldots, n\}$. Hence, we also get that all the edges of the Newton polygon for $f(x)$ lie above or on the line containing the right-most edge of the Newton polygon for $g(x)$. Since the right-most endpoint for each of these 2 Newton polygons is the same, we deduce that the slope of the right-most edge of the Newton polygon for $f(x)$ is less than or equal to the slope of the right-most edge of the Newton polygon for $g(x)$. Therefore, the right-most edge of the Newton polygon for $f(x)$ must have slope $< 1/k$. Thus, $f(x)$ satisfies the same conditions imposed on $g(x)$ in the statement of the lemma so that by appealing to the first part of the proof, the lemma follows. ■

We will also need the following generalization due to Sylvester [1] of Bertrand's postulate that for every integer $m \geq 1$, there is a prime in the interval $(m, 2m]$ (take $k = m$ below). We do not give its proof here but note that an elementary argument has been obtained by Erdős [1].

Lemma 2. *Let m and k be positive integers with $m \geq k$. Then there is a prime $p \geq k+1$ which divides one of the numbers $m+1, m+2, \ldots, m+k$.*

Proof of Theorem 7. To make use of Lemma 1, we consider

$$g(x) = \sum_{j=0}^{n} \frac{n!}{j!} x^j \quad \text{and} \quad f(x) = \sum_{j=0}^{n} a_j \frac{n!}{j!} x^j.$$

It suffices to show that $f(x)$ is irreducible over the integers. Assume $f(x)$ is reducible. Let k be the smallest degree of an irreducible factor of $f(x)$. Necessarily, $k \leq n/2$. Thus, $n - k \geq k$ so that Lemma 2 implies there is a prime $p \geq k+1$ dividing $n - \ell$ for some $\ell \in \{0, 1, \ldots, k-1\}$. We consider the Newton polygon for $g(x)$ with respect to such a prime p. For $j \in \{0, 1, \ldots, n - \ell - 1\}$, we get that $n!/j!$ is divisible by $n - \ell$ and, hence, p. To obtain a contradiction and thereby prove the theorem, Lemma 1 implies that it suffices to show that the right-most edge of the Newton polygon for $g(x)$ with respect to p has slope $< 1/k$. Observe that the slope of the right-most edge can be determined by

$$\max_{1 \leq j \leq n} \left\{ \frac{\nu(n!) - \nu(n!/j!)}{j} \right\}.$$

Fix $j \in \{1, \ldots, n\}$. Note that $p^{\nu(n!) - \nu(n!/j!)}$ is the largest power of p which divides $j!$. Let r be the non-negative integer for which $p^r \leq n < p^{r+1}$. Then for $j \in \{1, \ldots, n\}$,

$$\nu(n!) - \nu(n!/j!) = \left[\frac{j}{p}\right] + \left[\frac{j}{p^2}\right] + \cdots + \left[\frac{j}{p^r}\right] \leq j\left(\frac{1}{p} + \cdots + \frac{1}{p^r}\right) = j\frac{p^r - 1}{p^r(p-1)}.$$

Therefore,

$$\max_{1 \leq j \leq n} \left\{ \frac{\nu(n!) - \nu(n!/j!)}{j} \right\} \leq \frac{p^r - 1}{p^r(p-1)} < \frac{1}{p-1}.$$

Recall that $p \geq k+1$. Hence, the right-most edge of the Newton polygon for $g(x)$ with respect to p has slope $< 1/k$, and the proof is complete. ■

Problems

(2.1) Using equation (2.1) or equation (2.2), show the following:

(i) If $f(x)$, $g_1(x)$, and $g_2(x)$ are non-zero polynomials in $\mathbb{C}[x]$, then $R(f, g_1g_2) = R(f, g_1)R(f, g_2)$. (Here, g_1g_2 means the product $g_1(x)g_2(x)$.)

(ii) If $f(x) \in \mathbb{C}[x]$ is of degree ≥ 1 and $g(x) = f(x + a)$ where $a \in \mathbb{C}$, then $R(f, f') = R(g, g')$.

(2.2) Let $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ with $a_n \neq 0$ and $n \geq 2$, and let p be a prime. Suppose that there is an integer a such that $p|f(a)$. Prove the following:

(i) $f(x)$ is Eisenstein with respect to p if and only if $f(x+a)$ is in Eisenstein form with respect to p.

(ii) If $p^2|f(a)$, then $f(x)$ is not Eisenstein with respect to the prime p.

(iii) If $f(x)$ is Eisenstein with respect to the prime p, then $p|f^{(m)}(a)/m!$ for every $m \in \{1, \ldots, n-1\}$.

(2.3) For each of the following choices for $f(x)$, determine every prime p such that $f(x)$ is Eisenstein with respect to p.

(a) $f(x) = x^3 + x + 1$

(b) $f(x) = x^3 + x^2 - 2x - 1$

(c) $f(x) = x^3 + x^2 + x + 5$

(d) $f(x) = x^3 - x^2 + 4x + 2$

(2.4) Let $f(x) \in \mathbb{Z}[x]$. Suppose that there exists a $g(x) \in \mathbb{Z}[x]$ such that $f(g(x))$ is in Eisenstein form. Prove that $f(x)$ is Eisenstein. (Hint: Let $a = g(0)$ and prove that $f(x + a)$ is in Eisenstein form.)

(2.5) Let $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ with $a_n \neq 0$ and $n \geq 2$. Let p be a prime which does not divide n. Suppose that a is an integer for which $f(x + a)$ is in Eisenstein form with respect to the prime p. Prove that $a \equiv -a_{n-1}(na_n)^{-1} \pmod{p}$.

(2.6) Suppose that $f(x) \in \mathbb{Z}[x]$ is Eisenstein with respect to a prime p. Prove that $f(x)$ has exactly one root modulo p.

(2.7) (a) Let $f(x) \in \mathbb{Z}[x]$ of degree $n \geq 1$. Suppose that $f(x)$ is Eisenstein with respect to a prime p. Using Problem (2.1) (ii), prove that $p^{n-1} | R(f, f')$.

(b) If in part (a) one also has that $p|n$, prove that $p^n | R(f, f')$.

(2.8) By considering Newton polygons with respect to 2 different primes, prove that $x^5 \pm 6x^4 \pm 6x^3 \pm 24x \pm 72$ is irreducible for any of the 16 combinations of the $\pm$ signs.

(2.9) Let $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$, and let p be a prime.

(a) Let k be an integer relatively prime to n. Suppose that $p \nmid a_n$, $p^k | a_j$ for $j \in \{0, 1, \ldots, n-1\}$, and $p^{k+1} \nmid a_0$. Prove that $f(x)$ is irreducible over $\mathbb{Q}$.

(b) Let k be such that $p^k | a_0$ and $p^{k+1} \nmid a_0$. Suppose that $p \nmid a_n$ and that for each $j \in \{1, 2, \ldots, n-1\}$ we have $p^{e(j)} | a_j$ for some positive integer $e(j)$ satisfying $ne(j) + kj \geq kn$. Prove that $f(x)$ factors in $\mathbb{Q}[x]$ as a product of irreducible polynomials each with degree a multiple of $n/\gcd(n, k)$.

(2.10) Prove that if $f(x)$ is Eisenstein with respect to a prime p, then $f(x)$ is irreducible modulo p^2. In other words, prove that if such an $f(x)$ is of degree n and $f(x) \equiv g(x)h(x) \pmod{p^2}$ for some $g(x)$ and $h(x)$ in $\mathbb{Z}[x]$ of degrees r and s, respectively, with $r + s = n$, then either $r = 0$ or $s = 0$.

(2.11) Show that we can deduce the irreducibility of

$$\frac{x^{19}}{20!} + \frac{x^{18}}{19!} + \frac{x^{17}}{18!} + \cdots + \frac{x^2}{3!} + \frac{x}{2!} + 1$$

over the rationals by multiplying the polynomial by 20! and considering its Newton polygons with respect to 19 and 5.

(2.12) For n an integer ≥ 2, define $f_n(x) = \left((x+1)^n - x^n - 1\right)/x$.

(a) Suppose α is a root of $f_n(x)$. Explain why $1/\alpha$ is a root of $f_n(x)$.

(b) Let $n = 2p$, where p is an odd prime. Consider the Newton polygon for $f_n(x)$ with respect to p and show that either $f_n(x)$ is irreducible over the rationals or $f_n(x) = g(x)h(x)$ where $g(x)$ and $h(x)$ are polynomials in $\mathbb{Z}[x]$ of degree $p-1$ which are irreducible over the rationals.

(c) Assume $f_n(x) = g(x)h(x)$ in part (b) (so $n = 2p$ and $g(x)$ and $h(x)$ are polynomials in $\mathbb{Z}[x]$ of degree $p-1$ which are irreducible over the rationals). We may suppose further that the leading coefficients of $g(x)$ and $h(x)$ are positive (why?). Show that the content of $g(x)$ and the content of $h(x)$ are both 1. Also, show that the constant terms of $g(x)$ and $h(x)$ are both positive.

(d) Assume $f_n(x) = g(x)h(x)$ in part (b). One can obtain a little more information from the Newton polygons considered in part (b). Show that if α is a root of $g(x)$, then $1/\alpha$ is NOT a root of $g(x)$.

(e) Again, assume $f_n(x) = g(x)h(x)$ in part (b). Show that $h(x) = x^{p-1}g(1/x)$.

(f) Show that if $n = 2p$ where p is an odd prime, then $f_n(x)$ is irreducible. In other words, show that the situation in part (e) cannot occur. (Hint: Let $x = 1$.)

(Comment: It may be the case that $f_n(x)$ is irreducible over the rationals for every even positive integer n.)

CHAPTER 3

FURTHER IRREDUCIBILITY CRITERIA

You can try with dogs and roosters.

You can try with goats and geese.

– Dr. Seuss

I Am Not Going To Get Up Today

3.1. The Schönemann - Eisenstein Criterion is one of many criteria for testing the irreducibility of a given polynomial $f(x) \in \mathbb{Z}[x]$. In this chapter, we explore several other criteria. We begin in this section with a criterion due to Perron [1]:

Theorem 8. *If* $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ *with* $n \geq 1$ *is such that* $a_n = 1$, $a_0 \neq 0$, *and* $|a_{n-1}| > 1 + |a_{n-2}| + |a_{n-3}| + \cdots + |a_0|$, *then* $f(x)$ *is irreducible.*

For a generalization and related results see Lipka [1] and Parodi [1]. To prove Theorem 8, we will obtain information about the roots of the polynomials $f(x)$ which satisfy the conditions in the theorem. To obtain this information, we will make use of a simplified version of a classical result from Complex Analysis. The classical result is Rouché's Theorem (cf. Conway [1, p. 125]). Since we are only interested in a special case of it, we will be able to include its proof without requiring much background from the reader. The version

of Rouché's Theorem we want is given as Lemma 2 below. Before discussing it further, we consider a general theorem which connects information about the roots of polynomials to irreducibility.

Lemma 1. *Let $f(x)$ be a monic polynomial in $\mathbb{Z}[x]$ for which $f(0) \neq 0$. Suppose further that $f(x)$ has exactly 1 root α (with multiplicity 1) such that $|\alpha| \geq 1$. Then $f(x)$ is irreducible.*

Proof. Assume $f(x)$ is reducible. Since $f(x)$ is monic, its content is 1. Thus, we can write $f(x) = g(x)h(x)$ where $g(x)$ and $h(x)$ have integer coefficients and are of degree ≥ 1. Furthermore, we may suppose that $g(x)$ and $h(x)$ are monic and that $h(\alpha) = 0$. The given information now implies that $g(0) \neq 0$ and the roots of $g(x)$, say $\beta_1, \ldots, \beta_r$, all have absolute value < 1. Observe that $g(x) = (x - \beta_1)(x - \beta_2) \cdots (x - \beta_r)$. Hence,

$$1 \leq |g(0)| = |\beta_1||\beta_2| \cdots |\beta_r| < 1,$$

giving a contradiction. Therefore, $f(x)$ is irreducible. ■

Lemma 2. *Let $f(x)$ and $g(x)$ be polynomials in $\mathbb{C}[x]$, and let $\mathcal{C} = \{z \in \mathbb{C} : |z| = 1\}$. If the strict inequality $|f(z)+g(z)| < |f(z)|+|g(z)|$ holds for each $z \in \mathcal{C}$, then $f(x)$ and $g(x)$ have the same total number of zeroes (counting multiplicity) inside the circle $\mathcal{C}$ (i.e., in the interior of the region bounded by $\mathcal{C}$).*

Proof. Observe that the condition $|f(z)+g(z)| < |f(z)|+|g(z)|$ for z on the circle $\mathcal{C}$ implies that $f(z)$ and $g(z)$ cannot have zeroes on $\mathcal{C}$. In particular, each of $f(z)$ and $g(z)$ is not identically 0. Let k be the number of roots of $f(z)$ inside the circle $\mathcal{C}$, and let ℓ be the number of roots of $g(z)$ inside the circle $\mathcal{C}$. By the symmetry of the roles of $f(z)$ and $g(z)$ in the statement of Lemma 2, it suffices to show that $k \leq \ell$. Assume $k > \ell$. We will obtain a contradiction by showing that there is a $\theta \in [0, 2\pi)$ such that

$$|f(e^{i\theta}) + g(e^{i\theta})| = |f(e^{i\theta})| + |g(e^{i\theta})|.$$

It suffices to show that there is a $\theta \in [0, 2\pi)$ such that $\arg(f(e^{i\theta})) = \arg(g(e^{i\theta}))$, where for $z \in \mathbb{C}$, we take $\arg(z) \in (-\pi, \pi]$. For $\alpha \in \mathbb{C}$ with $|\alpha| \neq 1$, define $w(\alpha; 0) = \arg(1 - \alpha)$;

and for $\phi \in \mathbb{R} - \{0\}$, define $w(\alpha;\phi) = \arg(e^{i\phi} - \alpha) + 2s\pi$ where $s = s(\phi)$ is an integer chosen so that $w(\alpha;\phi)$ is continuous on $\mathbb{R}$. As ϕ varies over $\mathbb{R}$, the values of $e^{i\phi} - \alpha$ are on a circle of radius 1 centered at $-\alpha$. The circle has 0 in its interior if and only if $|\alpha| < 1$. Geometrically, it is easy to see that

$$w(\alpha;2\pi) - w(\alpha;0) = \begin{cases} 2\pi & \text{if } \alpha \text{ is inside the circle } \mathcal{C} \\ 0 & \text{otherwise.} \end{cases} \tag{3.1}$$

Let a be the leading coefficient of $f(z)$ and b be the leading coefficient of $g(z)$. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the roots of $f(z)$ and $\beta_1, \beta_2, \ldots, \beta_r$ the roots of $g(z)$ (the roots appearing as many times as their multiplicity). Define

$$F(\phi) = \arg(a) + \sum_{j=1}^{n} w(\alpha_j;\phi) + 2u\pi,$$

where u is an integer chosen so that $F(0) \in (-2\pi, 0]$. Define

$$G(\phi) = \arg(b) + \sum_{j=1}^{r} w(\beta_j;\phi) + 2v\pi,$$

where v is an integer chosen so that $G(0) \in [F(0), F(0)+2\pi)$. Hence, $-2\pi < F(0) - G(0) \leq 0$. Also, $F(\phi)$ and $G(\phi)$ are continuous on $\mathbb{R}$. Since

$$\arg\left(f(e^{i\phi})\right) = \arg\left(a\prod_{j=1}^{n}\left(e^{i\phi} - \alpha_j\right)\right) \equiv \arg(a) + \sum_{j=1}^{n}\arg\left(e^{i\phi} - \alpha_j\right) \pmod{2\pi},$$

we get that

$$F(\phi) \equiv \arg\left(f(e^{i\phi})\right) \pmod{2\pi}. \tag{3.2}$$

Similarly,

$$G(\phi) \equiv \arg\left(g(e^{i\phi})\right) \pmod{2\pi}. \tag{3.3}$$

Furthermore, by (3.1),

$$F(2\pi) = F(0) + 2k\pi \quad \text{and} \quad G(2\pi) = G(0) + 2\ell\pi.$$

Let $H(\phi) = F(\phi) - G(\phi)$. Then $H(0) = F(0) - G(0) \leq 0$ and $H(2\pi) = F(2\pi) - G(2\pi) = 2(k-\ell)\pi + F(0) - G(0) > 0$. By the Intermediate Value Theorem, there is a $\theta \in [0, 2\pi)$ for which $H(\theta) = 0$. By (3.2) and (3.3), we now get that

$$\arg\left(f(e^{i\theta})\right) = \arg\left(g(e^{i\theta})\right),$$

completing the proof. ■

Proof of Theorem 8. By Lemma 1, we need only show that $f(x)$ has exactly 1 root with absolute value ≥ 1. Let $w(x) = -a_{n-1}x^{n-1}$. Let $z \in \mathcal{C}$. Then

$$\begin{aligned}
|f(z) + w(z)| &= \left| \left(\sum_{j=0}^{n} a_j z^j \right) - a_{n-1} z^{n-1} \right| \\
&= \left| \left(\sum_{j=0}^{n-2} a_j z^j \right) + a_n z^n \right| \\
&\leq \left(\sum_{j=0}^{n-2} |a_j||z^j| \right) + |a_n||z^n| \\
&= |a_0| + |a_1| + \cdots + |a_{n-2}| + 1 \\
&< |a_{n-1}| \\
&= |a_{n-1} z^{n-1}| \\
&\leq |f(z)| + |w(z)|.
\end{aligned}$$

By Lemma 2, $f(x)$ and $w(x)$ must have the same total number of zeroes in $\mathcal{C}$. Each polynomial will have $n-1$ zeroes strictly inside $\mathcal{C}$ since $w(x) = -a_{n-1}x^{n-1}$ clearly does. Thus, $f(x)$ has exactly 1 root with absolute value ≥ 1, completing the proof. ■

3.2. In this section, we consider two theorems of Schur (cf. Pólya and Szegő [2, pp. 133, 326-327]).

Theorem 9. *Let n be a positive integer. If $a_1, \ldots, a_n$ are distinct integers, then $(x - a_1) \cdots (x - a_n) - 1$ is irreducible.*

Proof. Assume the conclusion of the theorem is false. Let $g(x)$ and $h(x)$ be polynomials in $\mathbb{Z}[x]$ with $g(x) \not\equiv \pm 1$, $h(x) \not\equiv \pm 1$, and $(x-a_1) \cdots (x-a_n)-1 = g(x)h(x)$. For $j \in \{1, \ldots, n\}$, we get that $g(a_j)h(a_j) = -1$ which implies that $g(a_j) = -h(a_j) = \pm 1$. Since $g(x) \not\equiv \pm 1$ and $h(x) \not\equiv \pm 1$, both $g(x)$ and $h(x)$ have degree ≥ 1 and both have degree $\leq n - 1$. Thus, $g(x) + h(x)$ has degree $\leq n - 1$. Since $g(a_j) = -h(a_j)$ for $j \in \{1, \ldots, n\}$, we get that $g(x) + h(x)$ is a polynomial of degree $\leq n - 1$ with $\geq n$ roots and so (by Theorem 4) $g(x) + h(x) \equiv 0$. Hence, $g(x) \equiv -h(x)$. Therefore,

$$(x - a_1) \cdots (x - a_n) - 1 \equiv -\left(g(x)\right)^2,$$

giving a contradiction since the leading coefficient on the left-hand side above is 1 and the leading coefficient on the right-hand side is negative. ■

Theorem 10. *Let n be a positive integer. Let $a_1, \ldots, a_n$ be distinct integers. If $f(x) = (x - a_1) \cdots (x - a_n) + 1$ is reducible, then $f(x)$ is a translation of either $x(x - 2) + 1$ or $x(x - 1)(x - 2)(x - 3) + 1$.*

Proof. Suppose that $f(x)$ is reducible. By translating and relabelling the a_j if necessary, we may take $a_n = 0$, and $1 \leq a_1 < a_2 < \cdots < a_{n-1}$. In particular, $a_j \geq j$ for $j \in \{1, \ldots, n-1\}$. Let $g(x)$ and $h(x)$ be polynomials in $\mathbb{Z}[x]$ with $g(x) \not\equiv \pm 1$, $h(x) \not\equiv \pm 1$, and

$$f(x) = x(x - a_1) \cdots (x - a_{n-1}) + 1 = g(x)h(x).$$

For $j \in \{1, \ldots, n\}$, $g(a_j)h(a_j) = f(a_j) = 1$ so that $g(a_j) = h(a_j) \in \{-1, 1\}$. This implies that the degrees of $g(x)$ and $h(x)$ must be ≥ 1 and also $\leq n - 1$. Now, $g(x) - h(x)$ has n roots and has degree $\leq n - 1$ so that $g(x) - h(x) \equiv 0$. Hence, $g(x) \equiv h(x)$. Thus,

$$f(x) = g(x)^2.$$

This implies that the degree of $f(x)$ is even. Let $m \in \mathbb{Z}$ with $n = 2m$. Now, for $n \geq 6$,

$$
\begin{aligned}
f\left(\frac{1}{2}\right) &= \left(\frac{1}{2}\right)\left(\left(\frac{1}{2}\right) - a_1\right)\cdots\left(\left(\frac{1}{2}\right) - a_{n-1}\right) + 1 \\
&= 1 - (-1)^{n-1}\left(\frac{1}{2}\right)\left(\left(\frac{1}{2}\right) - a_1\right)\cdots\left(\left(\frac{1}{2}\right) - a_{n-1}\right) \\
&= 1 - \left(\frac{1}{2}\right)\left(a_1 - \left(\frac{1}{2}\right)\right)\cdots\left(a_{n-1} - \left(\frac{1}{2}\right)\right) \\
&= 1 - \left(\frac{1}{2}\right)\left((2a_1 - 1)/2\right)\cdots\left((2a_{n-1} - 1)/2\right) \\
&\leq 1 - \left(\frac{1}{2}\right)^n \cdot 1 \cdot 3 \cdot 5 \cdots (2n-3) < 0.
\end{aligned} \tag{3.4}
$$

This is a contradiction (for $n \geq 6$) since $f(1/2) = g(1/2)^2 \geq 0$. Thus, either $m = 1$ or $m = 2$.

Case 1: $m = 1$ (or $n = 2$).

Since $f(1/2) = g(1/2)^2 \geq 0$, we examine $f(1/2)$ as in (3.4) to obtain that

$$1 - (1/4)(2a_1 - 1) \geq 0.$$

Solving for a_1, we get that $a_1 \leq 5/2$. This implies that $a_1 = 1$ or $a_1 = 2$. We cannot have $a_1 = 1$, since then $f(x) = x(x-1) + 1 = x^2 - x + 1$ which is irreducible (and also not a square). Thus, $a_1 = 2$, and in this case, necessarily, $f(x) = x(x-2) + 1 = x^2 - 2x + 1 = (x-1)^2$.

Case 2: $m = 2$ (or $n = 4$).

Using that $a_j \geq j$ for $j \in \{1, \ldots, n-1\}$, we examine $f(1/2)$ as in (3.4) to obtain that

$$
\begin{aligned}
0 \leq f\left(\frac{1}{2}\right) &= 1 - (1/16)(2a_1 - 1)(2a_2 - 1)(2a_3 - 1) \\
&\leq 1 - (1/16)(2-1)(4-1)(2a_3 - 1) = (19 - 6a_3)/16.
\end{aligned}
$$

Thus, $a_3 \leq 19/6$. This can only happen if $a_1 = 1, a_2 = 2$, and $a_3 = 3$. Therefore, in this case,

$$f(x) = x(x-1)(x-2)(x-3) + 1 = x^4 - 6x^3 + 11x^2 - 6x + 1 = (x^2 - 3x + 1)^2,$$

completing the proof. ■

If in Theorem 9 and Theorem 10, one considers instead polynomials of the form $f(x) = a(x-a_1)\cdots(x-a_n)\pm 1$ where $a_1,\ldots,a_n$ are distinct integers and a is an arbitrary positive integer, then in addition to the reducible polynomials which are given in Theorem 10, the only other class of reducible polynomials one gets are the translations of $4x(x-1)+1 = (2x-1)^2$. This result and other related material can be found in Dorwart and Ore [3]. A discussion of this more general situation can also be found in the next section and in the problems at the end of the chapter (see Problems (3.18), (3.19), and (3.20)).

The next result, similar to the results above, was first conjectured by Schur and proved by Seres [1]. Seres' proof made use of Capelli's Theorem which we will discuss in Chapter 9. There the reader can also find a proof of the next theorem in the case that 2 of the a_j differ by more than 4. For our present purposes we simply state the following result of Seres conjectured by Schur.

Theorem 11. *Let n and k be a positive integers. If $a_1,\ldots,a_n$ are distinct integers, then*

$$(x-a_1)^{2^k}(x-a_2)^{2^k}\cdots(x-a_n)^{2^k}+1$$

is irreducible.

We note that Seres [1] actually proved a stronger version of Theorem 11. Other related results can be found in Pirgov [1,2] and Pirgov and Tokarev [3].

3.3. Sometimes it is possible to determine the irreducibility of a polynomial by considering prime values of the polynomial. Indeed, prime values of polynomials play a major role in the theory of irreducible polynomials. We begin this section with a simple result, and then discuss an improvement due to Ore [1].

Theorem 12. *Let $f(x) \in \mathbb{Z}[x]$ be of degree n. If there exist at least $2n+1$ distinct integers m such that $|f(m)|$ is prime, then $f(x)$ is irreducible.*

Proof. Suppose $f(x) \in \mathbb{Z}[x]$ is of degree n and is not irreducible. Clearly, $f(x)$ is not identically 0, 1, or -1. Therefore, $f(x) = g(x)h(x)$ where $g(x)$ and $h(x)$ are in $\mathbb{Z}[x]$, $g(x) \not\equiv \pm 1$, and $h(x) \not\equiv \pm 1$. Let $r = \deg g(x)$ and $s = \deg h(x)$. Note that $\deg f(x) = n = r + s$. Since $\deg g(x) = r$ and $g(x) \not\equiv \pm 1$, each of $g(x)+1$ and $g(x)-1$ has at most r roots. Thus, there are at most r integers m such that $g(m) = 1$ and at most r integers m such that $g(m) = -1$. Therefore, there are at most $2r$ integers m such that $g(m) = \pm 1$. Similarly, there are at most $2s$ integers m such that $h(m) = \pm 1$. If $|f(m)| = |g(m)||h(m)|$ is prime, then either $g(m) = \pm 1$ or $h(m) = \pm 1$. Hence, there are at most $2r + 2s = 2(r + s) = 2n$ integers m such that $|f(m)|$ is prime, establishing the contrapositive of the theorem and therefore the theorem itself. ■

Ore's Theorem is the following:

Theorem 13. *Let $f(x) \in \mathbb{Z}[x]$ be of degree n. If there exist at least $n+5$ distinct integers m such that $|f(m)|$ is prime, then $f(x)$ is irreducible.*

In $n \leq 4$, then Theorem 13 follows from Theorem 12. We will make use of the following

Lemma. *If $g(x)$ is a polynomial in $\mathbb{Z}[x]$ of degree $r \geq 1$, then there exist $\leq r + 2$ integers m such that $g(m) = \pm 1$.*

Observe that once this lemma has been established, Theorem 13 follows as in the proof of Theorem 12 by replacing $2r$ and $2s$ in that argument by $r+2$ and $s+2$, respectively. The proof of the lemma that we present here is based on the method described in Dorwart and Ore [3]. Before proceding, it is worth connecting the lemma to the results of the previous section. In the previous section, we considered

$$f(x) = a(x - a_1)(x - a_2) \cdots (x - a_n) \pm 1, \tag{3.5}$$

where $a_1, \ldots, a_n$ are distinct integers and where there we took $a = 1$. Here, we consider the irreducibility of $f(x)$ with a denoting an arbitrary positive integer. (There is no need to look at the case when $a < 0$ since then the irreducibility of $-f(x)$ could be considered instead.) If the last term in (3.5) is -1, then the argument for proving Theorem 9 applies

directly to give that $f(x)$ is irreducible. So suppose the final term is $+1$. Using the argument for the proof of Theorem 10, we can deduce that $f(x) = g(x)^2$ so that we get immediately that $f(x)$ is irreducible if n is odd. If $r = \deg g(x)$, then $n = 2r$ and each of $g(a_1), g(a_2), \ldots, g(a_n)$ is ± 1. Hence, by the lemma, $2r = n \leq r + 2$ so that $r \leq 2$ and $n \leq 4$. We get the

Corollary. *Let $f(x)$ be as in (3.5) with a denoting a positive integer and $a_1, \ldots, a_n$ denoting distinct integers. If n is odd or $n \geq 5$, then $f(x)$ is irreducible. If $n \in \{2, 4\}$ and $f(x)$ is reducible, then there is a $g(x) \in \mathbb{Z}[x]$ of degree r such that $f(x) = g(x)^2$.*

To prove the lemma, let $a_1, \ldots, a_m$ be distinct integers such that $g(a_j) = 1$ for each $j \in \{1, \ldots, m\}$, and let $a_{m+1}, \ldots, a_{m+k}$ be distinct integers such that $g(a_j) = -1$ for each $j \in \{m+1, \ldots, m+k\}$. By considering $-g(x)$ if necessary, we may suppose that $m \geq k$, so we do so. Suppose further that the a_j are ordered so that $a_1 < a_2 < \cdots < a_m$ and $a_{m+1} < a_{m+2} < \cdots < a_{m+k}$. To prove the lemma, we want to show that $m + k \leq r + 2$. Observe that $m \leq r$ and $k \leq r$. Hence, if $m = 0$ or $k = 0$ (i.e., if there are no integers a such that $g(a) = 1$ or if there are no integers a such that $g(a) = -1$), then $m + k \leq r$, and we are through. Therefore, we suppose that $m \geq 1$ and $k \geq 1$. Since $g(a_j) = 1$ for each $j \in \{1, \ldots, m\}$, we get that $g(x) - 1$ is divisible by $(x - a_1) \cdots (x - a_m)$. In other words,

$$g(x) = (x - a_1) \cdots (x - a_m)h(x) + 1$$

for some $h(x) \in \mathbb{Z}[x]$. (To see this, use the final remarks of Section 1.2 to write $g(x) - 1$ in the form $(x - a_1) \cdots (x - a_m)h(x) + r(x)$ where $h(x)$ and $r(x)$ are in $\mathbb{Z}[x]$ and where $r(x)$ does not have degree $\geq m$ but necessarily satisfies $r(a_j) = 0$ for $j \in \{1, 2, \ldots, m\}$. It follows that $r(x) \equiv 0$ implying the desired result). For each $i \in \{1, \ldots, m\}$ and each $j \in \{m+1, \ldots, m+k\}$, we get that

$$2 = |g(a_j) - g(a_i)| = |a_j - a_1| \cdots |a_j - a_m||h(a_j)|.$$

Since $a_j - a_1, \ldots, a_j - a_m$, and $h(a_j)$ are integers, they are all contained in $\{-1, 1, 2\}$ or all contained in $\{-2, -1, 1\}$. Since also $a_j - a_1, \ldots, a_j - a_m$ are distinct, we get that $m \leq 3$. If

$m = 3$, then either $a_1 = a_j - 1$, $a_2 = a_j + 1$, and $a_3 = a_j + 2$ or $a_1 = a_j - 2$, $a_2 = a_j - 1$, and $a_3 = a_j + 1$. Observe that for fixed a_1, a_2, and a_3, there is at most one such a_j (specifically, if such an a_j exists, then it is $a_1 + 1$ if $a_2 - a_1 = 2$ and it is $a_1 + 2$ if $a_2 - a_1 = 1$). Thus, if $m = 3$, then $k \leq 1$ and $m + k \leq 4$. Since $m \geq k$, we get that if $m \leq 2$, then $k \leq 2$ so that again $m + k \leq 4$. Thus, for $r \geq 2$, the lemma follows. The case $r = 1$ is trivial, and the lemma follows.

The above argument establishes a little more. We can replace $r + 2$ in the statement of the lemma with $\max\{4, r\}$. If there are integers m_1 and m_2 such that $g(m_1) = 1$ and $g(m_2) = -1$, then we can replace $r + 2$ with 4.

We note that in the statements of Theorem 12 and Theorem 13, one can replace "$|f(m)|$ is prime" with "$|f(m)| = 1$ or $|f(m)|$ is prime." Considerably more work has been done in the direction of Ore's Theorem. Prior to Ore's Theorem, Pólya [1] showed that if the degree of $f(x) \in \mathbb{Z}[x]$ is an odd integer $n \geq 17$ and if there are $\geq n$ integers m such that $|f(m)| = p$ for some fixed prime p, then $f(x)$ is irreducible. Ore [1] classified the reducible polynomials $f(x) \in \mathbb{Z}[x]$ for which there are $> \deg f(x)$ integers m for which $|f(m)|$ is prime. Theorem 13 followed as a consequence of Ore's work. As an example of further consequences, we note that Ore showed that if $f(x) \in \mathbb{Z}[x]$ is reducible and is such that there are $\deg(f(x)) + 4$ integers m for which $|f(m)|$ is prime, then $f(x)$ is of degree 4 and has the form $f(x) = g(x)h(x)$ where both $g(x)$ and $h(x)$ are translates of $x(x+1) - 1$. For example, he notes that

$$f(x) = ((x-2)(x-1) - 1)\,((x-6)(x-5) - 1)$$

is such that $|f(m)|$ is prime for $m \in \{0, 1, \ldots, 7\}$. For other results related to Ore's Theorem see Desimirova [1], Dorwart [2], and Schulz [1].

3.4. Observe that one can use Ore's Theorem or Theorem 12 to establish the irreducibility of a polynomial $f(x) \in \mathbb{Z}[x]$ by showing that $|f(m)|$ is prime for a sufficient number of

integers m. The next results we discuss are special cases in which we can deduce the irreducibility of a polynomial $f(x) \in \mathbb{Z}[x]$ based on the fact that $f(m)$ is prime for a single value of m. The next theorem, due to A. Cohn and G. Pólya (Pólya and Szegő [2, pp. 133, 330]), is a particular case of this.

Theorem 14. *Let $d_n d_{n-1} \dots d_0$ be the decimal representation of a prime. Then $f(x) = \sum_{j=0}^{n} d_j x^j$ is irreducible.*

Thus, since 7776589 is prime, $f(x) = 7x^6 + 7x^5 + 7x^4 + 6x^3 + 5x^2 + 8x + 9$ is irreducible. Or to put it another way, we can deduce the irreducibility of $f(x)$ based on the fact that $f(10)$ is prime. For related results see Brillhart, Filaseta, and Odlyzko [1], Filaseta [1,3], and Alexander [1]. In particular, Brillhart, Filaseta, and Odlyzko have shown that if $(d_n d_{n-1} \dots d_0)_b$ is the base b representation of a prime where b is an integer ≥ 2, then $f(x) = \sum_{j=0}^{n} d_j x^j$ is irreducible. Our next result is a consequence of the work by Filaseta [3] and improvements of the result can be found there and in Alexander [1]. In particular, the next result easily implies Theorem 14.

Theorem 15. *If $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ is such that $f(10)$ is prime and $0 \leq a_j \leq 10^{15} a_n$ for $j \in \{0, 1, \dots, n-1\}$, then $f(x)$ is irreducible.*

Lemma. *Let $f(x) \in \mathbb{Z}[x]$ with $f(x) \not\equiv \pm 1$, and let m be an integer such that $|f(m)|$ is 1 or a prime and such that $f(x)$ has no zeroes in $\{z \in \mathbb{C} : |z - m| \leq 1\}$. Then $f(x)$ is irreducible.*

Proof. Assume $f(x) = g(x)h(x)$ where $g(x)$ and $h(x) \in \mathbb{Z}[x]$, with $g(x) \not\equiv \pm 1$ and $h(x) \not\equiv \pm 1$. We will obtain a contradiction by showing that $f(x)$ must have a root in $\{z \in \mathbb{C} : |z - m| \leq 1\}$. Since $|f(m)| = |g(m)||h(m)|$ is 1 or a prime, either $|g(m)| = 1$ or $|h(m)| = 1$. Without loss of generality, say $|g(m)| = 1$. Then $g(x)$ is not a constant function since $g(x) \not\equiv \pm 1$. Hence, we can write $g(x) = b \prod_{j=1}^{r} (x - \beta_j)$, where b is a non-zero integer, r is a positive integer, and $\beta_1, \dots, \beta_r$ are the roots of $g(x)$ (counted to their multiplicity).

Thus,

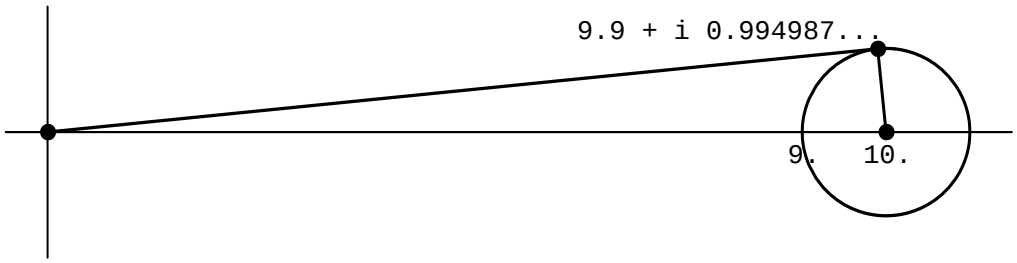
$$1 = |g(m)| = |b| \prod_{j=1}^{r} |m - \beta_j|.$$

Hence, there exists $k \in \{1, ..., r\}$ such that $|m - \beta_k| \leq 1$ and $f(\beta_k) = g(\beta_k)h(\beta_k) = 0$. Therefore, $f(x)$ has a root in $\{z \in \mathbb{C} : |z - m| \leq 1\}$, giving a contradiction and completing the proof. ■

Before continuing we note that the following Corollary is an immediate consequence of the above Lemma (with $m = 0$). The Corollary is due to Brillhart and Constantin [1]. We leave the details of its proof as an exercise (Problem (3.9)).

Corollary. *If $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$, $|a_0|$ is prime, and $|a_0| > |a_1| + |a_2| + \cdots + |a_n|$, then $f(x)$ is irreducible.*

Proof of Theorem 15. By the Lemma, it suffices to show that $f(x)$ has no zeroes in $D = \{z : |z - 10| \leq 1\}$. Let $z \in D$. Then $z = re^{i\theta}$ where $r \geq 9$ and $|\theta| \leq \text{Sin}^{-1}(1/10) = 5.739\ldots^{\circ}$.



Since $|15\theta| < 90^{\circ}$, we get that

$$\Re\left(z^{-1}\right) > 0, \Re\left(z^{-2}\right) > 0, \ldots, \Re\left(z^{-15}\right) > 0.$$

We may assume that $a_n \neq 0$ (so we do so). Thus,

$$\begin{aligned}
\left|\frac{f(z)}{z^n}\right| &= \left|a_n + \frac{a_{n-1}}{z} + \cdots + \frac{a_1}{z^{n-1}} + \frac{a_0}{z^n}\right| \\
&\geq \left|a_n + \frac{a_{n-1}}{z} + \cdots + \frac{a_{n-15}}{z^{15}}\right| - \sum_{j=16}^{n} \frac{|a_j|}{|z|^j} \\
&\geq \Re\left(a_n + \frac{a_{n-1}}{z} + \cdots + \frac{a_{n-15}}{z^{15}}\right) - \sum_{j=16}^{n} \frac{10^{15} a_n}{|z|^j} \\
&\geq a_n - 10^{15} \times \frac{1}{9^{16}} \times \frac{1}{1-(1/9)} \times a_n > 0.39 a_n > 0.
\end{aligned}$$

Thus, for $z \in D$, $f(z) \neq 0$, concluding the proof. ■

Before leaving this chapter, we note that there are many other irreducibility criteria in the literature. In particular, the interested reader may wish to read Dorwart [3] for a survey of some irreducibility results. Several irreducibility results also appear in Pólya and Szegő [2]; in particular, results related to deducing the irreducibility of a polynomial based on the size of non-zero values of the polynomial can be found there.

Problems

(3.1) Let $f(x) \in \mathbb{Z}[x]$. Prove that there are infinitely many integers k such that $f(x)+k$ is irreducible.

(3.2) Let $f(x) \in \mathbb{Z}[x]$. Prove that $x^2 f(x) + kx + 1$ is irreducible provided only that k is a sufficiently large integer. In other words, show that there is a number k_0, possibly depending on $f(x)$, such that if $k \geq k_0$, then $x^2 f(x) + kx + 1$ is irreducible.

(3.3) (a) Let $f(x) \in \mathbb{Z}[x]$, and let a be a non-zero integer. Prove that $f(x)$ is irreducible over the rationals if and only if $f(ax)$ is irreducible over the rationals.

(b) Note that (a) is no longer true if "over the rationals" is replaced by "over the integers." Give an example to justify this comment.

(c) Let $g(x) \in \mathbb{Z}[x]$. Use (a) and Problem (3.2) to show that if a is a fixed non-zero integer and k is a sufficiently large integer, then $f(x) = g(x)x^2 + kx + a$ is irreducible over the rationals.

(3.4) Let $f(x)$ be a quadratic polynomial with non-negative integer coefficients and non-zero constant term. Prove that if there is a positive integer m such that $f(m)$ is prime, then $f(x)$ is irreducible.

(3.5) Let $f(x)$ be a cubic polynomial with non-negative integer coefficients and non-zero constant term. Prove that if there is a positive integer m such that $f(m)$ is prime, then either $f(x)$ is irreducible or $f(x) = x^3 + 1$.

(3.6) Observe that $f(x) = x - 1$ is irreducible but $f(x^2) = x^2 - 1 = (x+1)(x-1)$ is reducible. Suppose that $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ with $n \geq 1$ is such that every coefficient of $f(x)$ is non-negative, $a_n = 1$, $a_0 \neq 0$, and $|a_{n-1}| > 1 + |a_{n-2}| + |a_{n-3}| + \cdots + |a_0|$. Then $f(x)$ is irreducible by Perron's Theorem. Prove that $f(x^2)$ is also irreducible.

(3.7) Let N be a positive integer, and let $f(x) \in \mathbb{Z}[x]$ such that the absolute value of each of its coefficients is $\leq N$. Prove that if there are at least $2N+4$ integers m such that $|f(m)|$ is prime, then $f(x)$ is irreducible.

(3.8) Suppose that $f(x)$ is a polynomial of degree 3 in $\mathbb{Z}[x]$, $f(m) = 1$ for 3 integers m, and $f(m) = -1$ for one integer m. Prove that $f(x)$ is a translate of $x(x-1)(x-3)+1$ or a translate of $-x(x-2)(x-3)+1$.

(3.9) Prove the Corollary to the Lemma for Theorem 15.

(3.10) Let n be a composite number > 1. Prove that there is an integer $b \geq 2$ such that if $n = \sum_{j=0}^{r} d_j b^j$, with $d_j \in \{0, 1, \ldots, b-1\}$, and $f(x) = \sum_{j=0}^{r} d_j x^j$, then $f(x)$ is a reducible polynomial of degree ≥ 2.

(3.11) Recall the remark after Theorem 14 that its analog for an arbitrary base $b \geq 2$ is true. Explain why this implies that if $f(x) \in \mathbb{Z}[x]$ has non-negative coefficients and if for some positive integer k one has that $f(f(k))$ is prime, then $f(x)$ is irreducible.

(3.12) Let $f(x) \in \mathbb{Z}[x]$ of degree n. Suppose that $f(x)$ has non-negative coefficients and $f(10)$ is prime. Prove that if $n \leq 31$, then $f(x)$ is irreducible. (We note that the bound 31 in this problem cannot be replaced by 32.)

(3.13) Prove that if $d_n d_{n-1} \ldots d_0$ is the decimal representation of 5^k for some positive integer k, then $f(x) = \sum_{j=0}^{n} d_j x^j$ is irreducible.

(3.14) Prove that if $d_n d_{n-1} \ldots d_0$ is the decimal representation of 16^k for some positive integer k, then $f(x) = \sum_{j=0}^{n} d_j x^j$ is irreducible.

(3.15) Show that the following more general version of Rouché's Theorem follows from Lemma 2 of Theorem 8.

Let R be a positive real number. Let $f(x)$ and $g(x)$ be polynomials in $\mathbb{C}[x]$, and let $\mathcal{C} =$

$\{z : |z| = R\}$. *If the strict inequality* $|f(z) + g(z)| < |f(z)| + |g(z)|$ *holds for each* $z \in \mathcal{C}$, *then* $f(x)$ *and* $g(x)$ *have the same total number of zeroes (counting multiplicity) inside the circle* $\mathcal{C}$ *(i.e., in the interior of the region bounded by* $\mathcal{C}$*).*

(3.16) (a) Let $f(x) \in \mathbb{Z}[x]$ with $f(x) \not\equiv 0$. Prove that there is a B depending on $f(x)$ such that if b is an integer $\geq B$, then $f(x)(x-b)+1$ is irreducible. (Hint: Let $g(x) = -f(x)(x-b)$ and start by using the previous problem to show that for $b \geq B$, $f(x)(x-b)+1$ has at most one root with absolute value $\geq b/2$.)

(b) Let $f(x) \in \mathbb{Z}[x]$ with $f(x) \not\equiv 0$, and let c be an arbitrary non-zero integer. Prove that there is a B depending on $f(x)$ and c such that if b is an integer $\geq B$, then $f(x)(x-b)+c$ is irreducible over the rationals.

(3.17) For each positive integer n, prove that there is an irreducible $f(x) \in \mathbb{Z}[x]$ with n distinct real roots.

(3.18) Let $f(x)$ be as in equation (3.5) with $n = 2$, with a denoting a positive integer, and with a_1 and a_2 denoting distinct integers. Show that if $f(x)$ is reducible, then $f(x)$ is a translation of $x(x-2)+1$ or a translation of $4x(x-1)+1$.

(3.19) Let $f(x)$ be as in equation (3.5) with $n = 4$, with a denoting a positive integer, and with $a_1, \ldots, a_4$ denoting distinct integers. Show that if $f(x)$ is reducible, then $a = 1$ and $f(x)$ is a translation of $x(x-1)(x-2)(x-3)+1$.

(3.20) In this chapter, we have obtained irreducibility results for $f(x)$ as in equation (3.5) with a denoting a positive integer and with $a_1, \ldots, a_n$ denoting distinct integers. In this problem, we consider the possibility that $a_1, \ldots, a_n$ are not distinct.

(a) A squarefull number a is a positive integer which satisfies $p^2|a$ for each prime divisor p of a. For example, the squares are squarefull as well as the numbers 72 and 108. Show that if a is squarefull, then $a = b^2d^3$ for some positive integers b and d.

(b) Show that there are $O(\sqrt{x})$ squarefull numbers $\leq x$ (in other words, show that there

is an absolute constant c such that the number of squarefull numbers $\leq x$ is $< c\sqrt{x}$ for every $x \geq 1$).

(c) Show that all but $O(\sqrt{t})$ positive integers $a \leq t$ satisfy the property that if $f(x)$ is of the form given in equation (3.5) where n is a positive integer and $a_1, \ldots, a_n$ are arbitrary integers, then $f(x)$ is irreducible.

(d) Show that all but $O(\sqrt{t})$ positive integers $a \leq t$ satisfy the property that if $f(x) = axg(x) \pm 1$ where $g(x)$ is an arbitrary monic polynomial in $\mathbb{Z}[x]$, then $f(x)$ is irreducible.

(3.21) Let S be an arbitrary finite set of integers. Show that there exists an N such that if $f(x)$ is a polynomial with integer coefficients of degree $n \geq N$, then there exist at most n integers m such that $f(m) \in S$.

(3.22) Prove that if $f(x) \in \mathbb{Z}[x]$ is reducible and is such that there are $\deg(f(x)) + 4$ integers m for which $|f(m)|$ is prime, then $f(x)$ is of degree 4 and has the form $f(x) = g(x)h(x)$ where both $g(x)$ and $h(x)$ are translates of $x(x+1) - 1$.

(3.23) Let $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ with $n \geq 1$, $a_n = 1$, and $a_0 \neq 0$. Suppose further that $|a_{n-1}| \geq 1 + |a_{n-2}| + |a_{n-3}| + \cdots + |a_0|$. Then it is possible for $f(x)$ to be reducible (for example, if $f(x) = x^2 - 2x + 1$ or $f(x) = x^2 + 2x + 1$). Show that if $f(1) \neq 0$ and $f(-1) \neq 0$, then $f(x)$ is irreducible. (Hint: Consider the proof of Theorem 8, and use that if $z_1, \ldots, z_n$ are complex numbers such that $|z_1 + \cdots + z_n| = |z_1| + \cdots + |z_n|$, then $z_1, \ldots, z_n$ are on the same ray emanating from the origin.)

CHAPTER 4

MODULO ARITHMETIC

4.1. As we will see, modulo arithmetic aids in testing the irreducibility of polynomials and even in completely factoring polynomials in $\mathbb{Z}[x]$. If we expect a polynomial $f(x)$ is irreducible, for example, it is not unreasonable to try to find a prime p such that $f(x)$ is irreducible modulo p. If we can find such a prime p and p does not divide the leading coefficient of $f(x)$, then $f(x)$ is irreducible in $\mathbb{Z}[x]$ (see Problem (1.6)). It is the case that there exist polynomials which are irreducible in $\mathbb{Z}[x]$ but are reducible modulo every prime (see Problem (4.1)), but as it turns out, one can show that such polynomials are rare and verifying that a polynomial $f(x)$ is irreducible by trying to find a prime p for which $f(x)$ is irreducible modulo p will almost always work rather quickly (see Chapter 6). This is already strong motivation for looking into the idea of using modulo arithmetic, but in this chapter, we plan to explore other aspects of modulo arithmetic as well.

We begin with a definition. Let p be a prime, and let $f(x) \in \mathbb{Z}[x]$. Suppose further that $f(x) \not\equiv 0 \pmod{p}$. We say that $u(x) \equiv v(x) \pmod{p,\ f(x)}$, where $u(x)$ and $v(x)$ are in $\mathbb{Z}[x]$, if there exist $g(x)$ and $h(x)$ in $\mathbb{Z}[x]$ such that $u(x) = v(x) + f(x)g(x) + ph(x)$. (In other words, $u(x) \equiv v(x) \pmod{p,\ f(x)}$ if $u(x) - v(x)$ is in the ideal generated by p and $f(x)$ in the ring $\mathbb{Z}[x]$.) One easily checks that if $u(x) \equiv v(x) \pmod{p,\ f(x)}$ and $v(x) \equiv w(x) \pmod{p,\ f(x)}$, then $u(x) \equiv w(x) \pmod{p,\ f(x)}$. Suppose that $u_1(x) \equiv v_1(x) \pmod{p,\ f(x)}$ and $u_2(x) \equiv v_2(x) \pmod{p,\ f(x)}$. Then $u_1(x) \pm u_2(x) \equiv v_1(x) \pm$

$v_2(x) \pmod{p,\ f(x)}$. Also, using

$$u_1(x)u_2(x) - v_1(x)v_2(x) = u_1(x)\left(u_2(x) - v_2(x)\right) + v_2(x)\left(u_1(x) - v_1(x)\right),$$

we easily see that $u_1(x)u_2(x) \equiv v_1(x)v_2(x) \pmod{p,\ f(x)}$. We note that if $u(x) \equiv v(x) \pmod{p}$, then $u(x) \equiv v(x) \pmod{p,\ f(x)}$ (by taking $g(x) \equiv 0$), and if $u(x) \equiv v(x) \pmod{f(x)}$, then $u(x) \equiv v(x) \pmod{p,\ f(x)}$ (by taking $h(x) \equiv 0$). Also, if $u(x) \equiv 0 \pmod{p,\ f(x)}$, then $f(x)$ is a factor of $u(x)$ modulo p.

Let $f(x)$ be monic. If $u(x)$ and $v(x)$ are in $\mathbb{Z}[x]$ and $u(x) \equiv v(x) \pmod{p,\ f(x)}$, then there are polynomials $g_0(x)$ and $h_0(x)$ in $\mathbb{Z}[x]$ such that $u(x) - v(x) = f(x)g_0(x) + ph_0(x)$. Recall (see the last remarks of Section 1.2) that when dividing a polynomial in $\mathbb{Z}[x]$ by a monic polynomial in $\mathbb{Z}[x]$, the quotient and remainder will be in $\mathbb{Z}[x]$. It follows that there are polynomials $q(x)$ and $r(x)$ in $\mathbb{Z}[x]$ with $r(x) \equiv 0$ or $\deg r < \deg f$ such that $h_0(x) = f(x)q(x) + r(x)$. Taking $g(x) = g_0(x) + pq(x)$ and $h(x) = r(x)$, we deduce that if $u(x) \equiv v(x) \pmod{p,\ f(x)}$, then there are polynomials $g(x)$ and $h(x)$ in $\mathbb{Z}[x]$ with $h(x) \equiv 0$ or $\deg h < \deg f$ such that $u(x) - v(x) = f(x)g(x) + ph(x)$. A simple argument shows further that such a $g(x)$ and $h(x)$ are unique (given $u(x)$, $v(x)$, $f(x)$, and p).

We will also make use of the following convention. Let p be a prime, and suppose $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ (with $f(x) \not\equiv 0 \pmod{p}$). Then we refer to the degree of $f(x)$ modulo p as the largest positive integer $k \leq n$ for which p does not divide a_k. Thus, for example, $2x^3+3x^2+4$ is a polynomial of degree 2 modulo 2. With the added condition that $a_n = 1$, we easily see that any $g(x) \in \mathbb{Z}[x]$ is congruent $(\text{modd } p,\ f(x))$ to one of the p^n polynomials of degree $\leq n-1$ with coefficients from $\{0, 1, \ldots, p-1\}$. Also, each of these p^n polynomials are incongruent $(\text{modd } p,\ f(x))$. In other words, we can view these p^n polynomials as representatives of the p^n distinct residue classes $(\text{modd } p,\ f(x))$. Consider now the possibility that $a_n \neq 1$, and let k denote the degree of $f(x)$ modulo p. Problem (4.7) implies that arithmetic $(\text{modd } p,\ f(x))$ is the same as arithmetic $(\text{modd } p,\ f_1(x))$ where $f_1(x) \equiv f(x) \pmod{p}$ and $\deg f_1(x) = k$. Problem (4.4) further implies that arithmetic $(\text{modd } p,\ f_1(x))$ is the same as arithmetic $(\text{modd } p,\ f_2(x))$ where $f_2(x)$ is monic and

$\deg f_2(x) = k$. It follows that there are precisely p^k distinct residue classes (modd p, $f(x)$) with representatives given by the polynomials of degree $\leq k-1$ with coefficients from $\{0, 1, \ldots, p-1\}$.

Theorem 16. *Let p be a prime. If $f(x) \in \mathbb{Z}[x]$ is of degree n modulo p and $f(x)$ is irreducible modulo p, then*

$$x^{p^n} \equiv x \pmod{p,\ f(x)}.$$

We clarify that in Theorem 16, as is usual,

$$x^{p^n} = x^{(p^n)}.$$

Before we prove this theorem, we consider an example. We show that $f(x) = x^p - x - 1$ is irreducible modulo p (and hence irreducible over $\mathbb{Z}$). Consider $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$, with $u(x)$ irreducible modulo p and with $f(x) \equiv u(x)v(x) \pmod{p}$. Observe that $1 \leq \deg u(x) \leq p$. We further suppose, as we may, that $u(x)$ is monic (for if a is the leading non-zero coefficient modulo p of $u(x)$, then we can consider $f(x) \equiv (a^{-1}u(x))(av(x)) \pmod{p}$). It suffices to show $\deg u(x) = p$. Note that

$$x^p \equiv x + 1 \pmod{p,\ f(x)}.$$

Hence,

$$x^{p^2} \equiv (x^p)^p \equiv (x+1)^p \equiv x^p + 1 \equiv x + 2 \pmod{p,\ f(x)}.$$

For any integer a, Fermat's Little Theorem gives us that $a^p \equiv a \pmod{p}$. An easy induction argument shows that for every positive integer r,

$$x^{p^r} \equiv x + r \pmod{p,\ f(x)}. \tag{4.1}$$

Since $u(x)$ divides $f(x)$ modulo p, we may replace $f(x)$ with $u(x)$ in (4.1). Let $m = \deg u(x)$. Then by Theorem 16 and (4.1),

$$x \equiv x^{p^m} \equiv x + m \pmod{p,\ u(x)}.$$

Hence, $m \equiv 0 \pmod{p, u(x)}$. Recalling that this implies there are polynomials $g(x)$ and $h(x)$ in $\mathbb{Z}[x]$ with $\deg h < \deg u$ such that $m = u(x)g(x) + ph(x)$, we obtain that $g(x) \equiv 0$, $\deg h = 0$, and $p|m$. On the other hand, $1 \leq m \leq p$; thus, $m = p$, implying that $f(x)$ is irreducible modulo p.

We now turn to the proof of Theorem 16.

Lemma. *Let p be a prime, and let $f(x)$ be irreducible modulo p. Let $a(x) \in \mathbb{Z}[x]$ with $a(x) \not\equiv 0 \pmod{p, f(x)}$. Then there exists $b(x) \in \mathbb{Z}[x]$ such that $a(x)b(x) \equiv 1 \pmod{p, f(x)}$.*

Proof. Let $n = \deg f(x)$. Making use of Problems (4.7) and (4.4) as before, we may suppose (and do suppose) that $f(x)$ is monic. Observe that there exists a $w(x) \in \mathbb{Z}[x]$ with $\deg w < n$ such that $a(x) \equiv w(x) \pmod{f(x)}$. Thus, $a(x) \equiv w(x) \pmod{p, f(x)}$. Since $a(x) \not\equiv 0 \pmod{p, f(x)}$, we deduce that $w(x) \not\equiv 0 \pmod{p}$. Hence, there exists an integer m and a monic polynomial $v(x) \in \mathbb{Z}[x]$ such that $w(x)m \equiv v(x) \pmod{p}$ so that $a(x)m \equiv v(x) \pmod{p, f(x)}$. Here, $\deg v \leq \deg w < n$. Fix $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$ with $a(x)u(x) \equiv v(x) \pmod{p, f(x)}$, with $v(x)$ monic, and with $\deg v(x)$ as small as possible. We deduce that $\deg v(x) < n$ and $v(x) \not\equiv 0 \pmod{p, f(x)}$. Since $v(x)$ is monic, there exist $q(x)$ and $r(x)$ in $\mathbb{Z}[x]$ such that

$$f(x) = q(x)v(x) + r(x) \tag{4.2}$$

and such that either $r(x) \equiv 0$ or $\deg r(x) < \deg v(x)$. Observe that

$$a(x)u(x)q(x) \equiv v(x)q(x) \equiv -r(x) \pmod{p, f(x)}.$$

From the minimality of $\deg v(x)$, we deduce $r(x) \equiv 0 \pmod{p}$ (otherwise, we could multiply through by a constant in the above congruence to obtain a monic polynomial on the right-hand side, leading to a contradiction). Since $\deg v(x) < n = \deg f(x)$ and $f(x)$ is irreducible modulo p, we get from (4.2) that $\deg v(x) = 0$. Since $v(x)$ is monic, we deduce that $v(x) \equiv 1$ and the lemma follows. ■

Proof of Theorem 16. As before, using Problem (4.4), we may suppose that $f(x)$ is monic and do so. Suppose $f(x) \equiv x \pmod{p}$. Then $n = 1$ and

$$x^{p^n} \equiv 0 \equiv x \pmod{p,\ f(x)}.$$

Now, suppose that $f(x) \not\equiv x \pmod{p}$. From the lemma, we get that x has an inverse (modd p, $f(x)$). Let $k = p^n - 1$, and let $a_1(x), \ldots, a_k(x)$ denote incongruent non-zero polynomials (modd p, $f(x)$). Then every non-zero polynomial (modd p, $f(x)$) is congruent to one of $a_1(x), \ldots, a_k(x)$. It follows that $xa_1(x), \ldots, xa_k(x)$ are congruent to $a_1(x), \ldots, a_k(x)$ in some order (modd p, $f(x)$). Hence,

$$a_1(x) \cdots a_k(x) \equiv (xa_1(x)) \cdots (xa_k(x)) \equiv x^k a_1(x) \cdots a_k(x) \pmod{p,\ f(x)}.$$

Observe that $a_1(x) \cdots a_k(x) \not\equiv 0$ (modd p, $f(x)$); otherwise, there would exist a $g(x) \in \mathbb{Z}[x]$ such that $f(x)g(x) \equiv a_1(x) \cdots a_k(x) \pmod{p}$, contradicting Theorem 3. Using the lemma with $a(x) = a_1(x) \cdots a_k(x)$, we get that

$$x^{p^n - 1} \equiv x^k \equiv 1 \pmod{p,\ f(x)} \tag{4.3}$$

from which it follows that

$$x^{p^n} \equiv x \pmod{p,\ f(x)},$$

completing the proof. ■

Given the lemma above, it is easy to see that the p^n incongruent representatives (modd p, $f(x)$) together with the operations modulo (modd p, $f(x)$) form a field. Thus, the $p^n - 1$ non-zero elements (modd p, $f(x)$) form a multiplicative group. Theorem 16 (or, more precisely, (4.3)) is merely asserting that in this group (as with any group) an element raised to the order of the group is equal to the identity element in the group.

4.2. In this section, we generalize Theorem 16 and show how we can deduce from the generalization a formula for the number of irreducible polynomials of a given degree n

modulo a prime p. We shall make use of this result later in the book when we discuss the density of $f(x) \in \mathbb{Z}[x]$ which are irreducible modulo some prime. Let p be a prime, and let $f(x) \in \mathbb{Z}[x]$. Suppose that $f(x)$ is of degree n modulo p and that $f(x)$ is irreducible modulo p. We use the concluding remark of the previous section that the p^n incongruent representatives (modd p, $f(x)$) together with addition and multiplication (modd p, $f(x)$) form a field. If we denote this field by F, then we can deduce from Theorem 4 that the polynomial $y^{p^k} - y$ has at most p^k roots in F. We begin by showing that if $k < n$, then x is not a root of $y^{p^k} - y$ in F. Suppose x is a root of $y^{p^k} - y$ in F. Then letting $g(x) = \sum_{j=0}^{r} b_j x^j$ represent an element in F, we get (by applying the multinomial theorem k times)

$$g(x)^{p^k} \equiv \left(\sum_{j=0}^{r} b_j x^j \right)^{p^k} \equiv \sum_{j=0}^{r} b_j^{p^k} x^{p^k j} \equiv \sum_{j=0}^{r} b_j x^j \equiv g(x) \pmod{p,\ f(x)}.$$

Thus, if x is a root of $y^{p^k} - y$ in F, then so is every element of F. Hence, by Theorem 4, $p^k \geq |F| = p^n$ so that $k \geq n$. Therefore, if $k < n$, then x is not a root of $y^{p^k} - y$ in F.

It is easy to see that since $x^{p^n} \equiv x \pmod{p,\ f(x)}$, we can obtain for every non-negative integer m,

$$x^{p^{mn}} \equiv x \pmod{p,\ f(x)}.$$

In other words, if k is a non-negative integer which is divisible by n, then

$$x^{p^k} \equiv x \pmod{p,\ f(x)}. \tag{4.4}$$

We now show that the converse of this statement is also true. In other words, if (4.4) holds, then k is divisible by n. Suppose then that (4.4) holds. By the previous paragraph, we know that $k \geq n$. Write $k = qn + r$, where q and r are non-negative integers with $0 \leq r < n$. Taking $m = q$ above, we see that $x^{p^{qn}} \equiv x \pmod{p,\ f(x)}$. Therefore, by (4.4),

$$x^{p^r} \equiv \left(x^{p^{qn}} \right)^{p^r} \equiv x^{p^{qn+r}} \equiv x^{p^k} \equiv x \pmod{p,\ f(x)}.$$

This implies $r = 0$ by the result of the previous paragraph. Thus, we obtain the following improvement of Theorem 16.

Theorem 17. *Let p be a prime, and let n be a positive integer. Let $f(x)$ be an irreducible polynomial modulo p, and suppose that p does not divide the leading coefficient of $f(x)$. Then*

$$x^{p^n} \equiv x \pmod{p,\ f(x)}$$

holds if and only if $\deg f(x)$ *divides* n.

Observe that $x^{p^n} \equiv x \pmod{p,\ f(x)}$ if and only if $f(x)$ is a factor of $x^{p^n} - x$ modulo p. Derivative considerations easily imply that $x^{p^n} - x$ cannot be divisible by $f(x)^2$ modulo p. When factoring $x^{p^n} - x$ modulo p, we need only consider monic factors. Therefore, by Theorem 17, $x^{p^n} - x$ factors modulo p as the product of all monic irreducible polynomials modulo p of degree dividing n with each irreducible factor occuring once and only once. Hence,

$$x^{p^n} - x \equiv \prod_{k|n} \left(\prod\nolimits^{*} f(x) \right) \pmod{p},$$

where the $*$ indicates that the product (or sum below) is over those $f(x)$ modulo p which are monic, irreducible, and of degree k. Thus,

$$\begin{aligned} p^n &= \sum_{k|n} \left(\sum\nolimits^{*} \deg f(x) \right) = \sum_{k|n} \left(\sum\nolimits^{*} k \right) \\ &= \sum_{k|n} k \sum\nolimits^{*} 1 = \sum_{k|n} k M_k, \end{aligned}$$

where $M_k = M_k(p)$ denotes the number of incongruent monic irreducible polynomials of degree k modulo p. We state this as

Lemma 1. *If M_k denotes the number of monic irreducible polynomials modulo a prime p, then*

$$p^n = \sum_{k|n} k M_k.$$

We now obtain an exact formula for M_n and for the number of incongruent irreducible polynomials of degree n modulo a prime p. We denote this last quantity by $I_n = I_n(p)$

and observe that in fact $I_n = (p-1)M_n$. To obtain a formula for M_n, we introduce the Möbius μ–function which is defined by

$$\mu(n) = \begin{cases} (-1)^r & \text{if } n = p_1 \dots p_r \text{ where the } p_j \text{ are distinct primes} \\ 0 & \text{otherwise,} \end{cases}$$

where we interpret the above to mean that $\mu(1) = 1$. In particular, it is immediate from this definition that

$$\mu(ab) = \mu(a)\mu(b) \quad \text{for } a \text{ and } b \in \mathbb{Z} \text{ with } \gcd(a,b) = 1.$$

In other words, μ is a multiplicative function.

Lemma 2. *Let n be a positive integer. Then*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Proof. If $n = 1$, then $\sum_{d|n} \mu(d) = \mu(1) = 1$. If $n > 1$, then we can write n in the form,

$$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r},$$

where $p_1, \dots, p_r$ are distinct primes with $r \geq 1$ and where $e_1, \dots, e_r$ are positive integers. Observing that $\mu(d) = 0$ if d is not squarefree, we get that

$$\sum_{d|n} \mu(d) = \sum_{d|p_1 \cdots p_r} \mu(d).$$

Recalling that μ is a multiplicative function and that $r \geq 1$, we deduce that if $n > 1$, then

$$\sum_{d|n} \mu(d) = \prod_{j=1}^{r} (1 + \mu(p_j)) = \prod_{j=1}^{r} (1-1) = 0,$$

completing the proof. ■

Observe that

$$\sum_{d|n} \mu(d) = \sum_{d|n} \mu\left(\frac{n}{d}\right)$$

so that we can use the sum on the right above in Lemma 2 rather than the sum on the left. From Lemma 1, we get that

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) p^d = \sum_{d|n} \mu\left(\frac{n}{d}\right) \sum_{k|d} kM_k.$$

For each d and k in this last expression, we have that $d = kd'$ for some integer d'. Thus, rearranging the order of summation and using Lemma 2, we obtain that

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) p^d = \sum_{k|n} \sum_{d'|(n/k)} \mu\left(\frac{n}{kd'}\right) kM_k = \sum_{k|n} kM_k \sum_{d'|(n/k)} \mu\left(\frac{n/k}{d'}\right) = nM_n.$$

Therefore, we have established

Theorem 18. *Let p be a prime, and let n be a positive integer. Then*

$$M_n(p) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d \quad \text{and} \quad I_n(p) = \frac{p-1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d.$$

Example 1. Consider $n = 12$ and $p = 2$. Then

$$\frac{1}{12} \sum_{d|12} \mu\left(\frac{12}{d}\right) 2^d = \frac{1}{12} \left(2^{12} - 2^6 - 2^4 + 2^2\right) = 335.$$

Thus, there are exactly 335 incongruent (monic) irreducible polynomials of degree 12 modulo 2.

Example 2. Consider $n = 3$ and $p = 5$. Then

$$\frac{4}{3} \sum_{d|3} \mu\left(\frac{3}{d}\right) 5^d = \frac{4}{3} \left(5^3 - 5\right) = 160.$$

Thus, there are exactly 160 incongruent irreducible polynomials of degree 3 modulo 5.

The proof above that Theorem 18 follows from Lemma 1 is simply an application of the Möbius inversion formula. The argument presented is based on a derivation of the Möbius inversion formula which can be found in almost every if not every introductory Number Theory text.

If p is a prime and n is a positive integer, then the existence of a finite field of order p^n is a consequence of the fact that $I_n(p) > 0$. The latter follows from Theorem 18. To see this, observe that if $n = k\ell$, where k is the largest squarefree factor of n, then $(1/p^\ell)\sum_{d|n}\mu(n/d)p^d$ is an integer $\equiv \pm 1 \pmod p$. Thus, $\sum_{d|n}\mu(n/d)p^d$ and, hence, $I_n(p)$ are non-zero.

4.3. In this section, we give another approach to establishing Theorem 18. More precisely, we shall establish Lemma 1 of the previous section using formal power series. For this approach, we follow Berlekamp [1]. We begin with a general discussion of formal power series. Formal power series are used to obtain results by manipulating series without concern for their convergence or divergence. In fact, one can discuss these series with their coefficients coming from an arbitrary field so that the concepts of convergence or divergence may not even be defined. For our purposes, the reader may assume that the coefficients are rational. A formal power series is of the form

$$f(z) = a_0 + a_1 z + a_2 z^2 + \cdots .$$

If

$$g(z) = b_0 + b_1 z + b_2 z^2 + \cdots \qquad \text{and} \qquad h(z) = c_0 + c_1 z + c_2 z^2 + \cdots$$

are two formal power series, then we say that $g(z) = h(z)$ if $b_j = c_j$ for every $j \in \{0, 1, 2, \dots\}$. If $f(z)$, $g(z)$, and $h(z)$ are as above, then we say $f(z) = g(z) \pm h(z)$ if $a_k = b_k \pm c_k$ for every $k \in \{0, 1, 2, \dots\}$ and we say $f(z) = g(z)h(z)$ if

$$a_k = \sum_{i+j=k} b_i c_j = \sum_{j=0}^{k} b_{k-j} c_j \qquad \text{for every } k \in \{0, 1, 2, \dots\}.$$

If $g(z)h(z) = 1$, then we will sometimes write $g(z) = 1/h(z)$ and refer to $g(z)$ as an inverse of $h(z)$. In this case, we must have that $b_0 c_0 = 1$. Thus, a formal power series $g(z) = b_0 + b_1 z + \cdots$ does not have an inverse if $b_0 = 0$. If $b_0 \neq 0$, then $g(z)$ does have an inverse (Problem (4.5)). If $g(z)$ and $h(z)$ are non-zero, then the definition of $g(z)h(z)$

above implies that the coefficient of $z^{k+\ell}$ in $g(z)h(z)$ is non-zero where k is the minimal j such that $b_j \neq 0$ and ℓ is the minimal j such that $c_j \neq 0$. Hence, if $g(z)h(z) \equiv 0$, then either $g(z) \equiv 0$ or $h(z) \equiv 0$. If $g_1(z)$, $g_2(z)$, and $h(z)$ are formal power series, then the above definitions imply that

$$(g_1(z) \pm g_2(z))\, h(z) = g_1(z)h(z) \pm g_2(z)h(z).$$

It now follows that the inverse of a formal power series is unique (if it exists). For example, the inverse of $1-z$ as a formal power series with coefficients from any field is $1+z+z^2+z^3+\cdots$. Whenever we use the notation $g(z)/h(z)$, we shall mean that $h(z)$ has an inverse and $g(z)/h(z)$ represents the product of $g(z)$ with the inverse of $h(z)$. It is not difficult to see that addition and multiplication of formal power series are commutative and associative operations. In particular, if $g_1(z), \ldots, g_r(z)$ are formal power series, then what we mean by the product $g_1(z) \cdots g_r(z)$ is understood.

We define the derivative of a formal power series $f(z) = a_0 + a_1 z + a_2 z^2 + \cdots$ as

$$f'(z) = a_1 + 2a_2 z + 3a_3 z^2 + \cdots = \sum_{k=1}^{\infty} k a_k z^{k-1}.$$

It is easy to check that if $g(z)$ and $h(z)$ are formal power series, then

$$(g(z) \pm h(z))' = g'(z) \pm h'(z).$$

Using the notation for $g(z)$ and $h(z)$ above, we see that the derivative of $g(z)h(z)$ is

$$\begin{aligned}
(g(z)h(z))' &= \left(\sum_{k=0}^{\infty} \left(\sum_{j=0}^{k} b_{k-j} c_j \right) z^k \right)' \\
&= \sum_{k=1}^{\infty} k \left(\sum_{j=0}^{k} b_{k-j} c_j \right) z^{k-1} \\
&= \sum_{k=1}^{\infty} \left(\sum_{j=0}^{k} (k-j) b_{k-j} c_j \right) z^{k-1} + \sum_{k=1}^{\infty} \left(\sum_{j=0}^{k} b_{k-j} j c_j \right) z^{k-1} \\
&= g'(z)h(z) + g(z)h'(z).
\end{aligned}$$

If $h(z) = 1/g(z)$, then we get that

$$0 = \frac{g'(z)}{g(z)} + g(z)\left(\frac{1}{g(z)}\right)'$$

so that

$$\left(\frac{1}{g(z)}\right)' = -\frac{g'(z)}{g(z)^2}.$$

If $g_1(z), \ldots, g_r(z)$ are formal power series, then we also get that

$$(g_1(z)\cdots g_r(z))' = \sum_{k=1}^{r} \frac{g_k'(z)}{g_k(z)} \prod_{j=1}^{r} g_j(z)$$

so that

$$\frac{(g_1(z)\cdots g_r(z))'}{g_1(z)\cdots g_r(z)} = \sum_{k=1}^{r} \frac{g_k'(z)}{g_k(z)}.$$

Thus, we get the usual Calculus rules for derivatives of sums (or differences), for derivatives of products, for derivatives of reciprocals, and for logarithmic derivatives of products. All of these hold regardless of the field of coefficients for the formal power series.

We now restrict our attention to formal power series with rational coefficients. We recall the notation $M_n(p)$ of the previous section for the number of monic irreducible polynonmials modulo a prime p. The total number of monic polynomials (including reducible ones) of degree n modulo p is p^n, and each of these by Theorem 3 can be written uniquely as a product of monic irreducible polynomials modulo p (without regard to the order in which the factors appear). This implies that if $n \leq m$, then p^n will be the coefficient of z^n in the formal power series product

$$\prod_{k=1}^{m} \left(1 + z^k + z^{2k} + \cdots\right)^{M_k} = \prod_{k=1}^{m} \left(\frac{1}{1-z^k}\right)^{M_k}.$$

On the other hand, if n is any non-negative integer, then p^n is the coefficient of z^n in $1/(1-pz)$. Hence, we can find a formal power series $g(z)$ such that

$$\frac{1}{1-pz} = \prod_{k=1}^{m} \left(\frac{1}{1-z^k}\right)^{M_k} + z^{m+1} g(z).$$

Let L denote the left-hand side above and R denote the right-hand side. Also, let P denote the product in R. Since inverses are unique, it follows that the inverse of R exists and is $1-pz$. Observe also that P has the inverse $\prod_{k=1}^{m}(1-z^k)^{M_k}$. It follows that we can write the inverse of R as

$$\frac{1-z^{m+1}g(z)(1-pz)}{P}.$$

Since $L=R$, we get that $L'/L = R'/R$. Hence, we get that there is a formal power series $h(z)$ such that

$$\begin{aligned}\frac{p}{1-pz} &= \frac{P'+(m+1)z^m g(z)+z^{m+1}g'(z)}{R}\\ &= \frac{P'}{P}\left(1-z^{m+1}g(z)(1-pz)\right)+\left((m+1)z^m g(z)+z^{m+1}g'(z)\right)(1-pz)\\ &= \frac{P'}{P}+z^m h(z).\end{aligned}$$

Using our previous formula for the logarithmic derivative of a product and multiplying through by z, we obtain that

$$\begin{aligned}\sum_{d=1}^{\infty}p^d z^d &= \frac{pz}{1-pz}\\ &= \sum_{k=1}^{m}\frac{M_k k z^k}{1-z^k} \;+\; z^{m+1}h(z)\\ &= \sum_{k=1}^{m}kM_k\sum_{\substack{d\geq 1\\ k|d}}z^d \;+\; z^{m+1}h(z)\\ &= \sum_{d=1}^{\infty}\left(\sum_{\substack{1\leq k\leq m\\ k|d}}kM_k\right)z^d \;+\; z^{m+1}h(z).\end{aligned}$$

If we consider any positive integer n and take $m=n$ above, we deduce Lemma 1 of the previous section by comparing the coefficients of z^n above.

Problems

(4.1) (a) Let p be an odd prime. Show that if a is a non-zero square modulo p, then a is a root of $x^{(p-1)/2} - 1$ modulo p; and if a is not a square modulo p, then a is a root of $x^{(p-1)/2} + 1$ modulo p.

(b) Prove that if a and b are not squares modulo a prime p, then $a \times b$ is a square modulo p.

(c) From part (b), we know that for every prime p, either -1, 2, or -2 is a square modulo p. Prove that $x^4 + 1$ is reducible modulo every prime p.

(4.2) Let a and b be integers. Prove that $x^4 + ax^2 + b$ is reducible modulo every prime.

(4.3) Let p be a prime, and let a be an integer which is not divisible by p. Prove that $x^p - x - a$ is irreducible modulo p.

(4.4) Let p be a prime, and let $f(x) \in \mathbb{Z}[x]$ with leading coefficient a modulo p (in other words, a is the coefficient of the highest degree term in $f(x)$ which is non-zero modulo p). Then we can write $f(x) \equiv ag(x) \pmod{p}$ for some monic polynomial $g(x) \in \mathbb{Z}[x]$. Let $u(x)$ and $v(x)$ be in $\mathbb{Z}[x]$. Prove that $u(x) \equiv v(x)$ (modd p, $f(x)$) if and only if $u(x) \equiv v(x)$ (modd p, $g(x)$).

(4.5) Let $g(z) = b_0 + b_1 z + \cdots$ represent a formal power series with $b_0 \neq 0$. Prove that $g(z)$ has an inverse.

(4.6) Let $f(x) = ax^2 + bx + c$, where a, b, and c are odd integers. Using arithmetic modulo 2, explain why $f(x)$ is irreducible over the rationals.

(4.7) Let p be a prime, and let $f(x)$ and $g(x)$ be in $\mathbb{Z}[x]$ with $f(x) \equiv g(x) \pmod{p}$. Let $u(x)$ and $v(x)$ be in $\mathbb{Z}[x]$. Prove that $u(x) \equiv v(x)$ (modd p, $f(x)$) if and only if $u(x) \equiv v(x)$ (modd p, $g(x)$).

CHAPTER 6

DENSITY RESULTS

A weaker man might be moved to re-examine his faith,
if in nothing else at least in the law of probability.

– Guildenstern

Rosencrantz and Guildenstern are Dead
by Tom Stoppard

"Let's count our pebbles," said Pooh.
Piglet emptied the sock. He counted very slowly.
Then he said, "One."
Pooh Bear was puzzled. "Are you sure?" he asked.
"Please count them again, Piglet. More slowly this time."
Piglet took a deep breath and counted as slowly as he could.
"One pebble," he said at last. "I counted very slowly."

– Walt Disney's

Winnie-the-Pooh and the Pebble Hunt

6.1. With all the irreducibility criteria at our disposal, we might be surprised to find that there even exists one reducible polynomial. Although such a statement should not be taken seriously, the reader might want to consider some random sequences of polynomials in $\mathbb{Z}[x]$ and test the irreducibility of the polynomials. For example, it is commonly accepted that no particular pattern exists among the digits of π (though the author has on occasion

told his students that he knows all the digits of π ... all 10 of them). Consider

$$P_n(x) = 3 + x + 4x^2 + \cdots,$$

where, for $j \in \{0, \ldots, n\}$, the coefficient of x^j is the $(j+1)$th digit of π. What would be a good estimate for the number of irreducible (or reducible) $P_n(x)$ with $n \leq t$? We may or may not be able to answer such a question in the near future. A quick computational check indicates that $P_n(x)$ is irreducible for $0 \leq n \leq 150$. There is no result in the literature to justify that $P_n(x)$ is usually irreducible or, more generally, that most polynomials with a non-zero constant term and a fixed bound on their coefficients are irreducible. For example, an open problem (due to Odlyzko and Poonen) is to determine whether

$$\lim_{n\to\infty} \frac{|\{f(x) = \sum_{j=0}^{n} \epsilon_j x^j : \epsilon_0 = 1, \epsilon_j \in \{0,1\} \text{ for } j = 1, \ldots, n, \text{ and } f(x) \text{ irreducible}\}|}{2^n} = 1.$$

Simply showing that the limit on the left-hand side above exists or showing that the limit supremum is positive seems to be difficult.

We can, however, obtain some density results if we fix a bound on the degree n of the polynomials we wish to consider and examine what happens as the absolute value of their coefficients are allowed to get large. For the purposes of this chapter, then, we define

$$S_n(B) = \left\{ f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x] : |a_j| \leq B \text{ for } j = 0, 1, \ldots, n \right\}.$$

Thus, $S_n(B)$ is the set of all polynomials in $\mathbb{Z}[x]$ of degree $\leq n$ with coefficients in the interval $[-B, B]$. Note that the total number of polynomials $f(x) \in S_n(B)$ is $(2[B] + 1)^{n+1} \sim (2B)^{n+1}$ as $B \to \infty$. We say that the proportion of polynomials in $\mathbb{Z}[x]$ of degree n satisfying a given property $\mathcal{P}$ is c if

$$\lim_{B\to\infty} \frac{|\{f(x) \in S_n(B) : f(x) \text{ satisfies } \mathcal{P}\}|}{(2B)^{n+1}} = c$$

where c is a constant possibly depending on n. If c does not depend on n and if for every sufficiently large positive integer n, the proportion of the polynomials in $\mathbb{Z}[x]$ of degree n

satisfying $\mathcal{P}$ is c, then we say that the proportion of the polynomials in $\mathbb{Z}[x]$ satisfying $\mathcal{P}$ is c. We will use the terminology "almost all" in the case that $c = 1$. Thus, almost all polynomials satisfy property $\mathcal{P}$ if for all sufficiently large n,

$$\lim_{B\to\infty} \frac{|\{f(x) \in S_n(B) : f(x) \text{ satisfies } \mathcal{P}\}|}{(2B)^{n+1}} = 1.$$

We say that a positive proportion of the polynomials in $\mathbb{Z}[x]$ of degree n have a given property $\mathcal{P}$ (and the proportion is at least c) if

$$\liminf_{B\to\infty} \frac{|\{f(x) \in S_n(B) : f(x) \text{ satisfies } \mathcal{P}\}|}{(2B)^{n+1}} > c$$

for some constant $c > 0$ (possibly depending on n). If for every sufficiently large positive integer n, the proportion of the polynomials in $\mathbb{Z}[x]$ of degree n satisfying $\mathcal{P}$ is at least $c > 0$ where c is independent of n, then we say that a positive proportion of the polynomials in $\mathbb{Z}[x]$ satisfy $\mathcal{P}$.

We are now ready to establish

Theorem 20. *Almost all polynomials in $\mathbb{Z}[x]$ are irreducible over the rationals.*

Proof. Fix a positive integer n. We will show that there are $\ll_n B^n \log^2 B$ reducible $f(x) \in S_n(B)$ over the rationals from which the theorem will follow. Observe that there are $2[B] + 1 \ll B$ constant polynomials in $S_n(B)$, which by definition are not irreducible; we need not concern ourselves with these as $B \ll_n B^n \log^2 B$. Each non-zero polynomial $f(x) \in S_n(B)$ can have at most n roots so that there are at least $n+1$ integers a (depending on $f(x)$) with absolute value $\leq n$ such that $f(a) \neq 0$. Let U be the set of $n+1$ element subsets of $\{-n, -n+1, \ldots, n-1, n\}$. Thus, $|U| = \binom{2n+1}{n+1}$. For each $T \in U$, let $V(T)$ be the set of $f(x) \in S_n(B)$ such that $f(a) \neq 0$ for every $a \in T$. Hence, every non-zero $f(x) \in S_n(B)$ belongs to $V(T)$ for at least one $T \in U$. Fix $T = \{a_0, a_1, \ldots, a_n\} \in U$. We will find an upper bound for the number of $f(x)$ in $V(T)$ which are reducible over the rationals. Let $f(x) \in V(T)$, and suppose that $f(x)$ is reducible over the rationals. Then there are polynomials $g(x)$ and $h(x)$ in $\mathbb{Z}[x]$ such that

$$f(x) = g(x)h(x) \quad \text{and} \quad 1 \leq \deg g(x) \leq \deg h(x) \leq n-1.$$

For every $a \in T$, we get that

$$|g(a)||h(a)| = |f(a)| \leq c_n B \quad \text{where} \quad c_n = n^n + n^{n-1} + \cdots + n + 1. \tag{6.1}$$

Furthermore, $|g(a)||h(a)| \neq 0$. Observe that (6.1) is true for any $f(x) \in V(T)$ and $g(x)$ and $h(x) \in \mathbb{Z}[x]$ with $f(x) = g(x)h(x)$. We get from (6.1) that for each $j \in \{0, \ldots, n\}$, the total number of values for the pair $(g(a_j), h(a_j))$ is bounded by

$$\begin{aligned} 4 \sum_{k \leq c_n B} \sum_{d|k} 1 = 4 \sum_{d \leq c_n B} \sum_{\substack{k \leq c_n B \\ d|k}} 1 &\leq 4 \sum_{d \leq c_n B} \frac{c_n B}{d} \\ &\leq 4 c_n B \left(1 + \int_1^{c_n B} \frac{1}{t}\, dt \right) \ll_n B \log B, \end{aligned}$$

where the 4 appears above since each of $g(a_j)$ and $h(a_j)$ may be either positive or negative. Fix integers r and s with $1 \leq r \leq s \leq n - r$, and consider now those $f(x) \in V(T)$ which factor as a product of a polynomial $g(x)$ of degree r and a polynomial $h(x)$ of degree s. Thus, as $f(x)$ runs through those elements in $V(T)$, there are $\ll_n (B \log B)^{r+1}$ values for $(g(a_0), h(a_0)), (g(a_1), h(a_1)), \ldots, (g(a_r), h(a_r))$. Since $g(x)$ is completely determined by the values of $g(a_0), \ldots, g(a_r)$ and since once $g(x)$ is determined (6.1) implies that each of $h(a_{r+1}), \ldots, h(a_s)$ can have at most $\leq 2c_n B$ different values, we get that there are

$$\ll_n (B \log B)^{r+1} B^{s-r} \ll_n B^{s+1} \log^{r+1} B$$

different possibilities for the pair $(g(x), h(x))$. Therefore, there are $\ll_n B^{s+1} \log^{r+1} B$ polynomials $f(x) \in V(T)$ that factor as a product of a polynomial of degree r times a polynomial of degree s. Observe that this bound is maximized when $r = 1$ and $s = n - 1$ (given that $1 \leq r \leq s \leq n - r$). Since there are $\binom{2n+1}{n+1}$ choices for $T \in U$ and $\leq n^2$ choices for r and s, we get that there are $\ll_n B^n \log^2 B$ polynomials $f(x) \in S_n(B)$ which are reducible over the rationals. The theorem easily follows. ■

Observe that we have actually proven a result stronger than Theorem 20. We have shown that if n is a positive integer, then the number of reducible $f(x) \in S_n(B)$ is $\ll_n B^n \log^2 B$.

It also follows as a consequence of the above proof that the number of $f(x) \in S_n(B)$ which can be written as a product of a polynomial of degree r times a polynomial of degree s with $s \geq r$ is $\ll_n B^{s+1} \log^{r+1} B$.

6.2. Another related theorem is due to Van der Waerden [1]. Van der Waerden's Theorem is the earliest known density theorem in this chapter. We state it as follows:

Theorem 21. *Almost all polynomials in $\mathbb{Z}[x]$ are irreducible modulo some prime.*

Before proving Theorem 21, we make some further remarks. First, it should be noted that Van der Waerden actually established a stronger version of this theorem. He showed that almost all polynomials $f(x) \in \mathbb{Z}[x]$ have their associated Galois group equal to the symmetric group on $\deg f(x)$ letters. He stated his result (in German) by referring to "100 %" of the polynomials rather than "almost all" of the polynomials. This result is mentioned in Van der Waeden's classical *Algebra* [2] (however, not in the earliest editions). The translations of Van der Waerden's *Algebra* into English (cf. [3]) have improperly stated the result as being that all polynomials $f(x) \in \mathbb{Z}[x]$ have their associated Galois group equal to the symmetric group on $\deg f(x)$ letters. The latter would imply that every polynomial in $\mathbb{Z}[x]$ is irreducible over the rationals. (Now is a good time to reread the first sentence of this chapter.)

Observe that Theorem 21 neither implies nor is implied by Theorem 20 (at least not directly); see Problems (1.6) and (4.1). On the other hand, it can be shown that if $f(x)$ is irreducible over $\mathbb{Q}$ and $f(x)$ is of prime degree, then $f(x)$ is irreducible modulo infinitely many primes; thus, Theorem 20 implies Theorem 21 when one considers polynomials of prime degree. In general, from Problem (1.6), we see that Theorem 20 would follow from the assertion that almost all polynomials $f(x)$ in $\mathbb{Z}[x]$ are irreducible modulo some prime not dividing the leading coefficient of $f(x)$. This assertion can in fact be obtained by modifying our argument for Theorem 21.

To prove Theorem 21, we recall Lemma 1 to Theorem 18. Let n be a positive integer.

Define, as in that theorem, $M_n = M_n(p)$ as the number of incongruent monic irreducible polynomials modulo p of degree n and $I_n = I_n(p)$ as the number of incongruent irreducible polynomials of degree n modulo p. Then

$$p^n = \sum_{k|n} kM_k.$$

In the sum above, $M_k \leq p^k$ and if $k \neq n$, then $k \leq n/2$. Thus, we easily get that each term in the sum other than nM_n is $\leq np^{n/2}$. In particular,

$$\sum_{\substack{1\leq k<n \\ k|n}} kM_k \leq \sum_{\substack{1\leq k<n \\ k|n}} np^{n/2} \leq n^2 p^{n/2}.$$

Hence, we get that

$$M_n = \frac{1}{n}\left(p^n - \sum_{\substack{1\leq k<n \\ k|n}} kM_k\right) = \frac{p^n}{n} + O(np^{n/2}).$$

Observe that we could have used Theorem 18 directly to obtain the above formula. Since $I_n = (p-1)M_n$, we deduce

$$I_n(p) = \frac{p^n(p-1)}{n} + O(np^{(n+2)/2}). \tag{6.2}$$

Define

$$I'_n(B,p) = |\{f(x) \in S_n(B) : f(x) \text{ is irreducible mod } p\}|.$$

Next, we obtain an upper bound for $I'_n(B,p)$ as follows. We divide the integers in the interval $[-B,B]$ into $\ell = [(2[B]+1)/p]+1$ disjoint sets (where the last expression involves two uses of the greatest integer function $[\ ]$) with the first $[(2[B]+1)/p]$ sets, say $S_1,\ldots,S_{\ell-1}$, each consisting of p consecutive integers and with the final set, say S_ℓ, consisting of the remaining unspecified number of consecutive integers. In particular, S_ℓ has ≥ 0 elements and $\leq p-1$ elements. There are $\leq (n+1)(p-1)(2[B]+1)^n \ll_n pB^n$ polynomials $f(x) \in S_n(B)$ which have a coefficient in S_ℓ. We consider now the polynomials $f(x) \in S_n(B)$ which have all their coefficients in $S_1 \cup S_2 \cup \cdots \cup S_{\ell-1}$. Fix

$f_0(x) = \sum_{j=0}^{n} a'_j x^j \in \mathbb{Z}[x]$. We count the number of $f(x) = \sum_{j=0}^{n} a_j x^j \in S_n(B)$ with coefficients in $S_1 \cup S_2 \cup \cdots \cup S_{\ell-1}$ and with $f(x) \equiv f_0(x) \pmod{p}$. For each fixed $j \in \{0, \ldots, n\}$ and for each fixed set S_i of p consecutive integers, there is a unique value of $a_j \in S_i$ such that $a_j \equiv a'_j \pmod{p}$. Thus, for each $j \in \{0, \ldots, n\}$, there are $[(2[B]+1)/p]$ values of $a_j \equiv a'_j \pmod{p}$ among the $\ell - 1$ sets $S_1, \ldots, S_{\ell-1}$ (one value for each set). Hence, we get that there are $(\ell-1)^{n+1} = [(2[B]+1)/p]^{n+1}$ polynomials $f(x)$ as above with $f(x) \equiv f_0(x) \pmod{p}$. If $f(x) \in S_n(B)$ is irreducible modulo p, then $f(x)$ has degree $\leq n$ and is congruent to one of the $\sum_{k \leq n} I_k(p)$ different irreducible polynomials modulo p of degree $\leq n$. Recalling our bound on the number of polynomials in $S_n(B)$ which have a coefficient in S_ℓ, we get that

$$I'_n(B,p) = [(2[B]+1)/p]^{n+1} \sum_{k \leq n} I_k(p) \ + O_n\left(pB^n\right).$$

We set

$$c_n(p) = \frac{\sum_{k \leq n} I_k(p)}{p^{n+1}}.$$

Using the trivial bound of $I_k(p) \leq p^{n+1}$ for $k \leq n$, we easily get that

$$I'_n(B,p) = c_n(p)(2B)^{n+1} + O_n\left(p^{n+1}B^n\right). \tag{6.3}$$

There is a generalization of (6.3) that we will want. Let $P = \{p_1, \ldots, p_r\}$ be a set of r primes, and define $I_n(P)$ as the number of incongruent polynomials modulo $p_1 \cdots p_r$ of degree $\leq n$ which are irreducible when considered modulo p for every $p \in P$. Observe that this definition differs from our use of $I_n(p)$ in that the latter only concerns itself with polynomials of degree equal to n. In particular, if p is a prime and $P = \{p\}$, then

$$I_n(P) = I_n(\{p\}) = \sum_{k \leq n} I_k(p).$$

We let

$$I'_n(B,P) = |\{f(x) \in S_n(B) : f(x) \text{ is irreducible mod } p \text{ for every } p \in P\}|.$$

We will make use of the following version of the Chinese Remainder Theorem.

Lemma. *Let $f_1(x), \ldots, f_r(x)$ be polynomials with integer coefficients, and let $p_1, \ldots, p_r$ be r distinct primes. Then there exists a unique polynomial $w(x)$ modulo $p_1 \cdots p_r$ such that*

$$w(x) \equiv f_j(x) \pmod{p_j} \quad \text{for every } j \in \{1, \ldots, r\}. \tag{6.4}$$

Proof. For each $j \in \{1, \ldots, r\}$, let $N_j = \left(\prod_{i=1}^{r} p_i\right)/p_j$ and let N_j' be an integer satisfying $N_j N_j' \equiv 1 \pmod{p_j}$. Consider

$$w(x) = \sum_{j=1}^{r} f_j(x) N_j N_j'.$$

Then it is easily verified that (6.4) holds, and therefore the existence of $w(x)$ as in the lemma is established. If $u(x) \in \mathbb{Z}[x]$ and $u(x) \equiv f_j(x) \pmod{p_j}$ for every $j \in \{1, \ldots, r\}$, then each p_j divides the coefficients of $w(x) - u(x)$ (since $w(x) \equiv f_j(x) \equiv u(x) \pmod{p_j}$) and, hence, $w(x) \equiv u(x) \pmod{p_1 \cdots p_r}$. This proves the uniqueness of $w(x)$ modulo $p_1 \cdots p_r$ and completes the proof. ■

Corollary. $I_n(P) = \prod_{j=1}^{r} \left(\sum_{k \le n} I_k(p_j)\right)$.

Proof. The lemma implies that there is a one-to-one correspondence between the $r-$tuples $(f_1(x), \ldots, f_r(x))$ where $f_j(x)$ is an irreducible polynomial of degree $\le n$ modulo p_j for each $j \in \{1, \ldots, r\}$ and the polynomials $f(x)$ modulo $p_1 \cdots p_r$ of degree $\le n$ which are irreducible when considered modulo each p_j. Thus,

$$I_n(P) = \prod_{j=1}^{r} I_n(\{p_j\}),$$

and the result follows. ■

We can divide the integers in the interval $[-B, B]$ into $[(2[B]+1)/(p_1 \cdots p_r)]+1$ disjoint sets and use the argument given for obtaining (6.3) to get that

$$I_n'(B, P) = \left(\prod_{j=1}^{r} c_n(p_j)\right) (2B)^{n+1} + O_n\left(p_1^{n+1} \cdots p_r^{n+1} B^n\right). \tag{6.5}$$

We are now ready to prove Theorem 21. Fix $n \geq 1$ and define $R(n, B, z)$ as the number of polynomials $f(x)$ in $S_n(B)$ such that $f(x)$ is reducible modulo p for every prime $p \leq z$. Thus, if $f(x)$ is not among the polynomials counted by $R(n, B, z)$, then it is irreducible modulo some prime. Hence, it suffices to show that for every $\epsilon > 0$ and for every $B \geq B_0(n, \epsilon)$ and $z \geq z_0(n, \epsilon, B)$, we have that

$$R(n, B, z) \leq \epsilon B^{n+1}. \tag{6.6}$$

To get such a bound, we can use the method of inclusion and exclusion. If we were to take away from the polynomials in $S_n(B)$ all of those polynomials which are irreducible modulo some prime $\leq z$, then we would be left with

$$|S_n(B)| - \sum_{p \leq z} I'_n(B, \{p\})$$

polynomials except that this last sum over counts the number of polynomials which are irreducible modulo some prime $\leq z$. More specifically, if a polynomial $f(x)$ in $S_n(B)$ is irreducible modulo several primes $\leq z$, then it is counted several times in the last sum (once for each prime $p \leq z$ such that $f(x)$ is irreducible modulo p). Thus, we need to modify the expression above. For this purpose, we consider $f(x) \in S_n(B)$ and define

$$\alpha(f(x)) = 1 - \sum_{p_1 \leq z}^{*} 1 + \sum_{p_1 < p_2 \leq z}^{*} 1 - \sum_{p_1 < p_2 < p_3 \leq z}^{*} 1 + \cdots,$$

where the $*$ in a summation indicates that each prime p_j in the sum is such that $f(x)$ is irreducible modulo p_j. Suppose that there are exactly k primes $p \leq z$ such that $f(x)$ is irreducible modulo p. If $k = 0$, then we get that $\alpha(f(x)) = 1$. If $k > 0$, then we get that

$$\alpha(f(x)) = 1 - \binom{k}{1} + \binom{k}{2} - \binom{k}{3} + \cdots = (1-1)^k = 0.$$

Thus, $\alpha(f(x)) = 0$ if $f(x)$ is irreducible modulo some prime $\leq z$ and otherwise $\alpha(f(x)) = 1$.

We get that

$$R(n,B,z) = \sum_{f(x)\in S_n(B)} \alpha(f(x))$$

$$= \sum_{f(x)\in S_n(B)} \left(1 - \sum_{p_1\le z}^{*} 1 + \sum_{p_1<p_2\le z}^{*} 1 - \sum_{p_1<p_2<p_3\le z}^{*} 1 + \cdots\right)$$

$$= |S_n(B)| - \sum_{f(x)\in S_n(B)} \sum_{p_1\le z}^{*} 1 + \sum_{f(x)\in S_n(B)} \sum_{p_1<p_2\le z}^{*} 1 - \sum_{f(x)\in S_n(B)} \sum_{p_1<p_2<p_3\le z}^{*} 1 + \cdots.$$

Rearranging the summations and using the definition of $I'_n(B,P)$, we get that

$$R(n,B,z) = |S_n(B)| - \sum_{p_1\le z} I'_n(B,\{p_1\}) + \sum_{p_1<p_2\le z} I'_n(B,\{p_1,p_2\}) - \sum_{p_1<p_2<p_3\le z} I'_n(B,\{p_1,p_2,p_3\}) + \cdots.$$

Observe that this gives an exact formula for $R(n,B,z)$ and that there are only a finite number of sums above since $\pi(z)$ (the number of primes $\le z$) is finite. Indeed, there are $\le z$ primes which are $\le z$. Hence, from (6.5), we get that

$$R(n,B,z) = (2B)^{n+1} - \sum_{p_1\le z} c_n(p_1)(2B)^{n+1} + \sum_{p_1<p_2\le z} c_n(p_1)c_n(p_2)(2B)^{n+1} - \sum_{p_1<p_2<p_3\le z} c_n(p_1)c_n(p_2)c_n(p_3)(2B)^{n+1} + \cdots + E$$

$$= (2B)^{n+1} \prod_{p\le z} (1 - c_n(p)) \; + E,$$

where

$$|E| \ll_n B^n \left(1 + \binom{\pi(z)}{1} z^{n+1} + \binom{\pi(z)}{2} z^{2(n+1)} + \binom{\pi(z)}{3} z^{3(n+1)} + \cdots\right)$$

$$\ll_n \left(1 + \binom{\pi(z)}{1} + \binom{\pi(z)}{2} + \binom{\pi(z)}{3} + \cdots\right) z^{z(n+1)} B^n \ll_n 2^z z^{z(n+1)} B^n.$$

Taking $z = \log\log B$, one gets that

$$|E| \ll_n e^z z^{z(n+1)} B^n \ll_n (\log B)(\log\log B)^{(n+1)\log\log B} B^n.$$

For B sufficiently large, we get that

$$|E| \leq \frac{\epsilon}{2} B^{n+1}.$$

From (6.2) and the definition of $c_n(p)$, we get that

$$\begin{aligned} c_n(p) &= \frac{1}{p^{n+1}} \sum_{k \leq n} I_k(p) \\ &\geq \frac{1}{p^{n+1}} I_n(p) = \frac{p-1}{pn} + O(np^{-n/2}) \\ &\geq \frac{1}{2n} + O(np^{-1/2}). \end{aligned}$$

For any constant c' and for $p \geq 16(c')^2 n^4$, we get that

$$c' n p^{-1/2} \leq \frac{1}{4n}.$$

Thus, if p is sufficiently large, then $c_n(p) \geq 1/(4n)$. This easily implies that if B is sufficiently large (so that z consequently is large), then

$$\prod_{p \leq z} (1 - c_n(p)) < \frac{\epsilon}{2^{n+2}}.$$

Combining the above estimates, (6.6) and, hence, Theorem 21 follows.

The technique used in establishing Theorem 21 is a sieve technique, more precisely the sieve of Eratosthenes. A more general consequence of the approach described above is

Theorem 22. *Let T be a set of polynomials in $\mathbb{Z}[x]$ of degree $\leq n$. Let D be a set of positive integers. For each $d \in D$, suppose that we have associated with it a subset $T(d)$ of T. For any $d_1, \ldots, d_r$ in D, define*

$$T(\{d_1, \ldots, d_r\}) = \bigcap_{j=1}^{r} T(d_j).$$

For $d \in D$, let $c(d)$ and $R(d, B)$ (possibly depending on n) be such that

$$|T(d) \cap S_n(B)| = c(d)(2B)^{n+1} + R(d, B).$$

For $d_1, \ldots, d_r$ in D, define $R(\{d_1, \ldots, d_r\}, B)$ by

$$|T(\{d_1, \ldots, d_r\}) \cap S_n(B)| = c(d_1) \cdots c(d_r)(2B)^{n+1} + R(\{d_1, \ldots, d_r\}, B).$$

Then for every $z > 0$,

$$|\{f(x) \in S_n(B) : \text{ for each } d \in D \text{ with } d \leq z, f(x) \notin T(d)\}|$$

$$= \prod_{\substack{d \in D \\ d \leq z}} (1 - c(d))\,(2B)^{n+1} + O\Bigg(\sum_{\substack{D' \subseteq D \\ d \in D' \implies d \leq z}} |R(D', B)| \Bigg) + O\left(B^n\right).$$

The sieve of Eratosthenes has been extended and elaborated on considerably to provide a very powerful and useful tool in Number Theory. We will use sieve methods again later in this book. For an excellent reference on this subject see Halberstam and Richert [1]. In particular, if in trying to apply Theorem 22, the reader unfamiliar with sieve techniques finds the value of z he wishes to use is sufficiently large so that the first error term above exceeds the main term, then he may wish to consider using the Brun sieve or the Selberg sieve instead of the sieve of Eratosthenes. The book by Halberstam and Richert [1] can be consulted for this purpose.

The proof of Theorem 21 implies that not only is almost every $f(x) \in \mathbb{Z}[x]$ irreducible modulo some prime but also that almost every $f(x) \in \mathbb{Z}[x]$ is irreducible modulo some *small* prime. More specifically, it is possible to modify the proof slightly to obtain that if $\psi(t)$ is any function that tends to infinity with t, then for almost all $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$, there is a prime $p \leq \psi(\max_{0 \leq j \leq n}\{|a_j|\})$ such that $f(x)$ is irreducible modulo p. This implies that a fast probabilistic test for irreducibility over the rationals can be formulated which simply tests a given $f(x) \in \mathbb{Z}[x]$ for irreducibility modulo small primes. If $f(x)$ is irreducible modulo a small prime and the prime does not divide the leading coefficient of $f(x)$, then $f(x)$ is irreducible over the rationals; and if $f(x)$ is reducible modulo every small prime used, then the test is inconclusive. If one fixes a function $\psi(t)$ and defines "small" as above, then the test will correctly deduce the irreducibility over the rationals of almost every $f(x) \in \mathbb{Z}[x]$. There is an even quicker algorithm which correctly predicts

the irreducibility over the rationals of almost every polynomial $f(x) \in \mathbb{Z}[x]$. In fact, the second algorithm is so quick that its running time is faster than the running time it takes to input most polynomials. The second algorithm is to disregard the polynomial and simply print a note claiming the polynomial is irreducible over the rationals. By Theorem 20, we know the second algorithm will correctly predict the irreducibility over $\mathbb{Q}$ of almost all $f(x) \in \mathbb{Z}[x]$. The difference, however, in these two irreducibility algorithms is that the first never produces misinformation; in other words, it never claims that a reducible polynomial is irreducible (over $\mathbb{Q}$).

6.3. In this section, we show that if $f(x) \in \mathbb{Z}[x]$ is irreducible over the rationals, then usually the Eisenstein-Schönemann Criterion does not help in determining its irreducibility. To be more precise, we let E denote the set of polynomials in $\mathbb{Z}[x]$ which are Eisenstein. We will prove that e_n approaches 0 as n approaches infinity where

$$e_n = \limsup_{B\to\infty} \frac{|\{f(x) \in S_n(B) : f(x) \in E\}|}{|\{f(x) \in S_n(B) : f(x) \text{ irreducible over } \mathbb{Q}\}|}.$$

Since from Theorem 20

$$\lim_{B\to\infty} \frac{|\{f(x) \in S_n(B) : f(x) \text{ irreducible over } \mathbb{Q}\}|}{(2B)^{n+1}} = 1,$$

we see that

$$e_n = \limsup_{B\to\infty} \frac{|\{f(x) \in S_n(B) : f(x) \in E\}|}{(2B)^{n+1}}.$$

We consider $n \geq 10$. Recall that if $f(x)$ is an Eisenstein polynomial of degree m with respect to some prime p, then there are integers a and b such that $f(x) \equiv b(x-a)^m \pmod{p}$. We let T be the set of all $f(x) \in \mathbb{Z}[x]$ such that $f(x) \equiv b(x-a)^m \pmod{p}$ holds for some prime p and some integers a, b, and m (with $m \geq 0$). Thus, $E \subseteq T$. We set

$$t_n = \limsup_{B\to\infty} \frac{|\{f(x) \in S_n(B) : f(x) \in T\}|}{(2B)^{n+1}}.$$

Thus, $e_n \leq t_n$, and it suffices to show that $\lim_{n\to\infty} t_n = 0$. We use Theorem 22 with D being the set of primes. For each prime p, we set $T(p)$ to be the set $f(x) \in \mathbb{Z}[x]$ such

that $f(x) \equiv b(x-a)^m \pmod{p}$ for some choice of integers a, b, and m (with $m \geq 0$). In particular, if $f(x)$ is a constant modulo p, then $f(x) \in T(p)$. The number of other incongruent $f(x)$ modulo p in $T(p) \cap S_n(B)$ is $(p-1)pn$. Hence, there are a total of $(np-n+1)p$ incongruent $f(x)$ modulo p in $T(p) \cap S_n(B)$. In a manner similar to that used to obtain (6.3) in the previous section, we deduce that

$$|T(p) \cap S_n(B)| = c(p)(2B)^{n+1} + O_n\left(p^2 B^n\right) \tag{6.7}$$

where $c(p) = (np-n+1)/p^n$. Furthermore, if $P = \{p_1, \ldots, p_r\}$ is a set of primes, then

$$|T(P) \cap S_n(B)| = c(p_1) \cdots c(p_r)(2B)^{n+1} + O_n\left(p_1^2 \cdots p_r^2 B^n\right).$$

Thus,

$$R(P,B) \ll p_1^2 \cdots p_r^2 B^n$$

and (along the lines of estimating $|E|$ in the previous section)

$$\sum_{\substack{P=\{p_1,\ldots,p_r\} \\ p_j \leq z \text{ for each } j}} |R(P,B)| \ll 2^z z^{2z} B^n.$$

Taking $z = \log\log B$, we deduce from Theorem 22 that

$$\begin{aligned} &|\{f(x) \in S_n(B) : \text{for each prime } p \leq z, f(x) \notin T(p)\}| \\ &\qquad = \prod_{p \leq z} (1 - c(p))\,(2B)^{n+1} + O_n\left(B^{(2n+1)/2}\right). \end{aligned}$$

Since we are considering $n \geq 10$, the product

$$\prod_p (1 - c(p)) = \prod_p \left(1 - \frac{np-n+1}{p^n}\right)$$

converges. We are almost ready to claim that t_n is no larger than the value of this product; however, T is the union of the sets $T(p)$ as p varies over all the primes, and we have thus far only established an estimate for the number of $f(x) \in S_n(B)$ with $f(x) \notin T(p)$ for $p \leq \log\log B$.

Suppose now that $f(x) \in T(p) \cap S_n(B)$ and $p > z = \log\log B$. We recall Problem (2.7) (a). Although the problem there dealt with Eisenstein polynomials rather than polynomials in T, for the purposes of that problem, the conclusion is the same. In other words, $p^{n-1} | R(f, f')$. On the other hand, if $m = \deg f(x) \geq 1$, then $R(f, f')$ is the determinant of a $(2m-1) \times (2m-1)$ matrix all of whose entries are $\leq mB$. Since $m \leq n$, we easily deduce that $|R(f, f')| = O_n(B^{2n-1})$. If $R(f, f') = 0$, then recall that (2.2) implies that $f(x)$ and $f'(x)$ have a root in common so that one can deduce that $f(x)$ is reducible. We have already shown in the proof of Theorem 20 that there are at most $O_n(B^n \log^2 B)$ such $f(x) \in S_n(B)$. If $R(f, f') \neq 0$, then $p^{n-1} | R(f, f')$ and $|R(f, f')| = O_n(B^{2n-1})$ imply that $p \leq B^3$ (where we consider here, as we may, B to be large compared to n). Therefore, we have $z < p \leq B^3$. For each such p, we use that

$$|T(p) \cap S_n(B)| \leq (np - n + 1)p \left(\frac{2B+1}{p} + 1 \right)^{n+1}.$$

This inequality can be deduced along the lines of (6.7). From this we obtain

$$|T(p) \cap S_n(B)| = O_n\left(c(p) B^{n+1}\right) + O_n\left(p^2\right).$$

We now deduce that the number of $f(x) \in T(p) \cap S_n(B)$ for some $p > z$ is

$$O_n\left(\sum_{z < p \leq B^3} c(p) B^{n+1} \right) + O_n\left(\sum_{z < p \leq B^3} p^2 \right) + O_n\left(B^n \log^2 B\right).$$

Using $c(p) = (np - n + 1)/p^n$ and $n \geq 10$, we conclude that the number of such $f(x)$ is $O_n(B^{n+1}/\log\log B)$.

Combining the above, we obtain

$$|\{f(x) \in S_n(B) : f(x) \notin T\}| = \prod_{p \leq \log\log B} (1 - c(p)) (2B)^{n+1} + O_n\left(B^{n+1}/\log\log B\right).$$

Hence,

$$\lim_{B \to \infty} \frac{|\{f(x) \in S_n(B) : f(x) \notin T\}|}{(2B)^{n+1}} = \prod_p \left(1 - \frac{np - n + 1}{p^n}\right) \geq \prod_p \left(1 - \frac{n}{p^{n-1}}\right).$$

We leave it now to the reader to verify that $\lim_{n \to \infty} t_n = 0$.

Problems

(6.1) Modify the proof of Theorem 20 to show that for every positive integer n, almost all monic polynomials are irreducible. In other words, show that if $n \geq 1$, then

$$\lim_{B\to\infty} \frac{|\{f(x) \in S_n(B) : f(x) \text{ is monic and irreducible}\}|}{(2B)^n} = 1.$$

(6.2) Let n be a positive integer. What proportion of the polynomials of degree n are irreducible over the *integers*? More specifically, evaluate

$$\lim_{B\to\infty} \frac{|\{f(x) \in S_n(B) : f(x) \text{ is irreducible}\}|}{(2B)^{n+1}}.$$

(6.3) Given two properties $\mathcal{P}_1$ and $\mathcal{P}_2$, we say that almost all polynomials $f(x) \in \mathbb{Z}[x]$ which satisfy property $\mathcal{P}_1$ have property $\mathcal{P}_2$ if

$$\lim_{B\to\infty} \frac{|\{f(x) \in S_n(B) : f(x) \text{ satisfies } \mathcal{P}_1 \text{ and } \mathcal{P}_2\}|}{|\{f(x) \in S_n(B) : f(x) \text{ satisfies } \mathcal{P}_1\}|} = 1$$

for every sufficiently large positive integer n.

(a) Using the comments after the proof of Theorem 20, explain why almost all $f(x) \in \mathbb{Z}[x]$ which are reducible over the rationals have a linear factor in $\mathbb{Z}[x]$.

(b) Let k be a positive integer. Consider the $f(x) \in \mathbb{Z}[x]$ which have a factor over the rationals of degree $\geq k$ but which have no factor over the rationals of degree ℓ for $1 \leq \ell < k$. Show that almost all such $f(x)$ have a factor over the rationals of degree exactly k.

(6.4) Observe that both $f(x) = 2x + 2$ and $f(x) = x^2 + x + 2$ have the property that if m is an integer, then $f(m)$ is even. We say that $f(x) \in \mathbb{Z}[x]$ has a fixed prime divisor if for some prime p and every integer m, $f(m)$ is divisible by p. Show that the density of $f(x) \in \mathbb{Z}[x]$ of degree n which do not have a fixed prime divisor is $\prod_{p\leq n}(1 - (1/p^p))$. (Hint: First resolve why the product is only over the primes which are $\leq n$.)

(6.5) (a) Let $f(x) \in \mathbb{Z}[x]$. Suppose that for some integer a, $f(x + a) = \sum_{j=0}^{n} a_j x^j$ with $a_n = 1$, $a_0 \neq 0$, and $|a_{n-1}| > 1 + \sum_{j=0}^{n-2} |a_j|$. By Perron's Theorem (Theorem 8) and

Problem (1.1), we can deduce that $f(x)$ is irreducible. Call such an $f(x)$ irreducible by Perron's Theorem. The argument for establishing Perron's Theorem implies that such an $f(x)$ has $n-1$ roots within 1 of a in the complex plane. Write $f(x) = \sum_{j=0}^{n} b_j x^j$, and suppose that $f(x) \in S_n(B)$. By considering the relations b_0 and b_1 have with the roots of $f(x)$, show that if $B \geq 2$, $n \geq 4$, and $|a| \geq n$, then $|a| \leq 2B^{1/3} + 1$.

(b) With the notation in part (a), show that

$$|b_{n-1}| \leq (n-1)(|a|+1) + \frac{B}{(|a|-1)^{n-1}}.$$

(c) In the above situation, suppose that B is sufficiently large (possibly depending on n). Show that there are at most $4B$ possible values for the pair (a, a_{n-1}). Furthermore, establish that $|a_{n-1}| \leq 2B$.

(d) In part (c), show that there are at most $(6^{n-1}/(n-1)!)B^{n-1}$ possible values for the $(n-1)-$tuple $(a_{n-2}, \ldots, a_1, a_0)$.

(e) Prove that if $f(x) \in \mathbb{Z}[x]$ is a monic irreducible polynomial, then one cannot usually determine its irreducibility by using Perron's Theorem. In other words, establish that if

$$p_n = \limsup_{B \to \infty} \frac{|\{f(x) \in S_n(B) : f(x) \text{ irreducible by Perron's Theorem}\}|}{|\{f(x) \in S_n(B) : f(x) \text{ monic and irreducible}\}|},$$

then $\lim_{n\to\infty} p_n = 0$.

(6.6) Explain how

$$\left| \left\{ f(x) = \sum_{j=0}^{n} \epsilon_j x^j : \epsilon_0 = 1, \epsilon_j \in \{0,1\} \text{ for } j = 1, \ldots, n, \text{ and } f(x) \text{ irreducible} \right\} \right| \gg \frac{2^n}{n}$$

follows as a consequence of a theorem from Chapter 4.

(6.7) Recall the polynomials $P_n(x) = 3 + x + 4x^2 + \cdots$, in Section 6.1. Think of what might likely be a factor of $P_n(x)$ and find (computationally) a positive integer n for which $P_n(x)$ is reducible. (Hint: If one flips a coin patiently for years and years, what is the probability that eventually the number of heads flipped equals the number of tails flipped?)

CHAPTER 7

THE CYCLOTOMIC POLYNOMIALS

7.1. We define the n^{th} cyclotomic polynomial, $\Phi_n(x)$, as the product of the monic irreducible factors of x^n-1 which are not factors of x^k-1 for $k \in \{1,...,n-1\}$. There are other ways one can define $\Phi_n(x)$. This particular definition seems to be the simplest in that it can be explained rather readily to a junior high school or high school student familiar with the rudiments of basic algebra. Observe that every irreducible factor of $x^n - 1$ in $\mathbb{Z}[x]$ necessarily has leading coefficient ± 1. If $w(x)$ is such a factor, then so is $-w(x)$. We have restricted our attention to only the monic irreducible factors of $x^n - 1$ in defining $\Phi_n(x)$; thus, only one of $w(x)$ and $-w(x)$ is considered in the definition. The first 10 values of $\Phi_n(x)$ are:

$$\Phi_1(x) = x - 1, \quad \Phi_2(x) = x + 1, \quad \Phi_3(x) = x^2 + x + 1, \quad \Phi_4(x) = x^2 + 1,$$

$$\Phi_5(x) = x^4+x^3+x^2+x+1, \quad \Phi_6(x) = x^2-x+1, \quad \Phi_7(x) = x^6+x^5+x^4+x^3+x^2+x+1,$$

$$\Phi_8(x) = x^4 + 1, \quad \Phi_9(x) = x^6 + x^3 + 1, \quad \Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1.$$

Our first theorem in this chapter shows that there is only one monic irreducible factor of $x^n - 1$ which is not a factor of $x^k - 1$ for some $k \in \{1,...,n-1\}$. In other words, $\Phi_n(x)$ is irreducible. This result is due to Kronecker [1]. Our proof will be based on a proof of Landau [1]. Note that when n is a prime, the irreducibility of $\Phi_n(x)$ follows by Eisenstein's Criterion (see Problem (7.1)); Gauss [1] first established this particular case of the theorem.

Theorem 23. *$\Phi_n(x)$ is irreducible for all positive integers n.*

Proof. The roots of $x^n - 1$ are $e^{2\pi im/n}$ where $m \in \{0, 1, \ldots, n-1\}$. If $\gcd(m, n) = d > 1$, then there are integers m' and n' such that $m = dm'$ and $n = dn'$ so that $e^{2\pi im/n} = e^{2\pi im'/n'}$ is a root of $x^k - 1$ where $k = n' = n/d < n$. In this case, we get that $e^{2\pi im/n}$ is a root of $\gcd(x^n - 1, x^k - 1)$ and, hence, a root of an irreducible factor of $x^n - 1$ which is not among the irreducible factors defining $\Phi_n(x)$. Thus, the roots of $\Phi_n(x)$ are among the numbers of the form $e^{2\pi im/n}$ where $m \in \{0, 1, \ldots, n-1\}$ and $\gcd(m, n) = 1$. In particular, observe that $e^{2\pi i/n}$ is a root of $\Phi_n(x)$ since it is not a root of $x^k - 1$ for $k \in \{1, \ldots, n-1\}$.

Let $\zeta = e^{2\pi ij/n}$ with j a non-negative integer. Let $f(x) \in \mathbb{Z}[x]$ such that $f(x)$ is monic and $f(\zeta) = 0$. By the above comments, it suffices to show that if $m \in \{0, 1, \ldots, n-1\}$ and $\gcd(m, n) = 1$, then $f(\zeta^m) = 0$ (and, in fact, we only need to establish this for $j = 1$). Since ζ is a root of $x^n - 1$, ζ is a root of a monic irreducible polynomial in $\mathbb{Z}[x]$. Let d be the degree of this monic irreducible polynomial. By Problem (7.7), for each positive integer k, there is a unique element $R_k(x)$ of $\mathbb{Z}[x]$ which is $\equiv 0$ or of degree $< d$ such that $f(\zeta^k) = R_k(\zeta)$; furthermore, if p is a prime, then every coefficient of $R_p(x)$ is divisible by p.

Since $\zeta^n = 1$, we get that for every positive integer k, $R_k(x) = R_{k+n}(x)$. Thus, the set of coefficients of the polynomials $R_1(x), R_2(x), \ldots$ is finite. Let A denote the maximum of the absolute values of these coefficients. By the previous paragraph, if p is a prime $> A$, then we must have that $R_p(x) \equiv 0$ so that $f(\zeta^p) = 0$ for every prime $p > A$. It suffices at this point to use Dirichlet's Theorem concerning primes in arithmetic progressions, but we will avoid the use of Dirichlet's Theorem as follows. The above all held with $\zeta = e^{2\pi ij/n}$ where j is any non-negative integer. By applying the above observations several times while appropriately replacing j by suitable multiples of j, one gets that $f(\zeta^w) = 0$ for every positive integer w which has all of its prime factors $> A$. Let $m \in \{0, 1, \ldots, n-1\}$ such that $\gcd(m, n) = 1$. Since $\zeta^n = 1$, we get that $\zeta^m = \zeta^w$, where

$$w = m + n \prod_{\substack{p \text{ prime} \\ p \le A, p \nmid m}} p.$$

Since $\gcd(m,n)=1$, one gets that w is not divisible by any prime $\leq A$. Hence, $f(\zeta^m) = f(\zeta^w) = 0$. This completes the proof. ■

The following is an easy consequence of the above proof.

Corollary. *Let n be a positive integer. Then*

$$\Phi_n(x) = \prod_{\substack{1\leq j\leq n \\ \gcd(j,n)=1}} \left(x - e^{2\pi ij/n}\right).$$

The Corollary implies that the degree of $\Phi_n(x)$ is the number of positive integers relatively prime to n and $\leq n$. In other words,

$$\deg \Phi_n(x) = \phi(n),$$

where ϕ denotes Euler's $\phi-$function. A different formula for $\Phi_n(x)$ is often useful, and our next goal is to establish such a formula. We make use of Lemma 2 to Theorem 18 in Chapter 4.

Theorem 24. *Let n be a positive integer. Then*

$$\Phi_n(x) = \prod_{d|n} \left(x^d - 1\right)^{\mu(n/d)}.$$

Proof. Whenever d divides n, the linear factors of $x^d - 1$ in $\mathbb{C}[x]$ are all of the form $x - e^{2\pi ij/n}$ for some $j \in \{0, 1, \ldots, n-1\}$. For a fixed $j \in \{0, 1, \ldots, n-1\}$, $x - e^{2\pi ij/n}$ is a factor of $x^d - 1$ if and only if $n/\gcd(j,n)$ divides d or, in other words, if and only if n/d divides $\gcd(j,n)$. Thus, the factor $x - e^{2\pi ij/n}$ appears on the right-hand side above with the exponent

$$\sum_{\substack{d|n \\ (n/d)|\gcd(j,n)}} \mu\left(\frac{n}{d}\right).$$

Observe that as d runs over the divisors of n so does $k = n/d$. Hence,

$$\sum_{\substack{d|n \\ (n/d)|\gcd(j,n)}} \mu\left(\frac{n}{d}\right) = \sum_{k|\gcd(j,n)} \mu(k).$$

By Lemma 2 to Theorem 18, $x - e^{2\pi ij/n}$ is a factor on the right-hand side above if and only if $\gcd(j, n) = 1$ and then $x - e^{2\pi ij/n}$ appears with the exponent 1. By the Corollary to Theorem 23, the result follows. ■

7.2. To illustrate an application of the cyclotomic polynomials, we give the next result first stated by Euler (cf. Dickson [2, Vol. I, p. 415]). It is an "easy" case of Dirichlet's Theorem that if a and b are relatively prime positive integers, then there exist infinitely many primes in the arithmetic progression $a + kb$.

Theorem 25. *Let n be a positive integer. Then there are infinitely many primes p such that $p \equiv 1 \pmod{n}$.*

Proof. By Problem (7.8), it suffices to show that if p is a prime dividing $\Phi_n(a)$ for some integer a, then $p|n$ or $p \equiv 1 \pmod{n}$. Fix an integer a and a prime p dividing $\Phi_n(a)$ with $p \nmid n$. Note that p cannot divide a since otherwise the fact that $p|\Phi_n(a)$ would imply that p divides the constant term in $\Phi_n(x)$; this is impossible since the constant term of $\Phi_n(x)$ divides the constant term of $x^n - 1$ and, hence, 1.

Next, we show that a has order n modulo p. Once this has been established, we will be through since the order of a modulo p must divide $p - 1$ which would imply that $n|(p - 1)$ so that $p \equiv 1 \pmod{n}$.

Observe that since $p|\Phi_n(a)$ and $\Phi_n(a)$ divides $a^n - 1$, we have that $a^n \equiv 1 \pmod{p}$. Assume that there is a positive integer $k < n$ such that $a^k \equiv 1 \pmod{p}$. Let $d = \gcd(k, n)$. Then $d \leq k < n$. There are integers u and v such that $ku + nv = d$. Recalling that p does not divide a (so that a and its powers have inverses modulo p), we get that

$$a^d = a^{ku+nv} = \left(a^k\right)^u \times \left(a^n\right)^v \equiv 1 \pmod{p}.$$

Since $d = \gcd(k, n)$ divides n, we get that $x^d - 1$ divides $x^n - 1$. By the definition of $\Phi_n(x)$,

$$\left(x^d - 1\right) \Phi_n(x) | \left(x^n - 1\right).$$

Since $a^d - 1 \equiv 0 \pmod{p}$ and $\Phi_n(a) \equiv 0 \pmod{p}$, we get that $(x-a)^2$ divides $x^n - 1$ modulo p. This contradicts that a is non-zero modulo p and

$$\frac{d}{d\,x}(x^n - 1) = nx^{n-1}$$

has 0 as its only root modulo p (where here we have used that $p \nmid n$). Hence, a has order n modulo p, and the proof is complete. ■

Note that it is not difficult to modify the above proof to establish that p is a prime with $p \equiv 1 \pmod{n}$ if and only if $p \nmid n$ and p is a prime divisor of $\Phi_n(a)$ for some integer a.

7.3. In this section, we begin with the following result due to Kronecker [2].

Theorem 26. *If $f(x) \in \mathbb{Z}[x]$ is monic, is irreducible, and has all its roots on $\{z : |z| = 1\}$, then $f(x)$ is a cyclotomic polynomial.*

Proof. Let α be such that $f(\alpha) = 0$. If we can establish that α is a root of some cyclotomic polynomial, then since both cyclotomic polynomials and $f(x)$ are irreducible, $f(x)$ will be cyclotomic. Thus, it suffices to show that there exists a positive integer m such that $\alpha^m = 1$.

Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the complete list of roots of $f(x)$ with $\alpha_1 = \alpha$. Using elementary symmetric functions (cf. Uspensky [1]), it is easy to deduce that $(x-\alpha_1^k)(x-\alpha_2^k)\cdots(x-\alpha_n^k)$ is in $\mathbb{Z}[x]$ for every positive integer k. We can avoid the use of elementary symmetric functions, however, by restricting consideration to polynomials of the form

$$f_k(x) = (x - \alpha_1^{2^k})(x - \alpha_2^{2^k})\cdots(x - \alpha_n^{2^k}).$$

Then one easily deduces that

$$f_1(x^2) = (-1)^n f(x) f(-x) \in \mathbb{Z}[x].$$

Since $f_1(x^2)$ is a polynomial in x^2 with integer coefficients, it follows that $f_1(x)$ has integer coefficients. An easy induction argument now implies that $f_k(x) \in \mathbb{Z}[x]$ for every positive integer k.

Since $f_k(x)$ is monic and each root of $f_k(x)$ has absolute value ≤ 1, we conclude that the coefficient of x^j in $f_k(x)$ is $\leq \binom{n}{j}$ (by observing, for example, that the coefficient of x^j in $f_k(x)$ must be less than or equal to the coefficient of x^j in $(x+1)^n$). Since n is fixed, this implies that the set $\{f_k(x) : k \geq 1\}$ is finite. Let $F(x)$ denote the least common multiple of the elements of $\{f_k(x) : k \geq 1\}$. Since $\alpha^2, \alpha^4, \alpha^8, \ldots$ are all roots of $F(x)$, there exist integers r and s with $1 \leq r < s$ and $\alpha^{2^r} = \alpha^{2^s}$. Since $|\alpha| = 1 \neq 0$, we get that $\alpha^m = 1$ with $m = 2^s - 2^r$, completing the proof. ■

Before continuing, we make a comment about what Theorem 26 is *not* saying. Consider the polynomial $f(x) = x^4 - 2x^3 + x^2 - 2x + 1$. It is easy to verify that $f(x)$ is not divisible by a cyclotomic polynomial. Is it possible that $f(x)$ has roots with absolute value 1? Yes, and as we shall see, it does. Theorem 26 asserts that all of its roots cannot have absolute value 1. To see that $f(x)$ has roots on the unit circle in the complex plane, observe that $f(\alpha) = 0$ if and only if

$$\left(\alpha + \frac{1}{\alpha}\right)^2 - 2\left(\alpha + \frac{1}{\alpha}\right) - 1 = 0,$$

from which one can easily deduce that the roots of $f(x)$ are

$$\frac{1 + \sqrt{2} \pm \sqrt{2\sqrt{2} - 1}}{2} \quad \text{and} \quad \frac{1 - \sqrt{2} \pm i\sqrt{2\sqrt{2} + 1}}{2}.$$

The last two roots are imaginary, and a quick check indicates that they have absolute value 1.

There are a variety of results related to Theorem 26 (cf. Cassels [1], Smyth [1], and Lloyd-Smith [1]). In particular, we mention the following result of Dobrowolski [1].

Theorem 27. *Let $\epsilon > 0$, and let n be a sufficiently large integer. If $f(x) \in \mathbb{Z}[x]$ is monic, non-cyclotomic, and irreducible of degree n, then there is a root α of $f(x)$ such that*

$$|\alpha| > 1 + \frac{2 - \epsilon}{n}\left(\frac{\log\log n}{\log n}\right)^3.$$

It has been conjectured by Schinzel and Zassenhaus [2] that the factor $(\log\log n/\log n)^3$ can be replaced by an absolute constant. We will establish

Theorem 28. *Let n be a positive integer, and let $f(x) \in \mathbb{Z}[x]$ be monic, non-cyclotomic, and irreducible of degree n. Furthermore, suppose that $f(0) \neq 0$ and that $f(x)$ has no reciprocal roots (i.e., that $f(\alpha) = 0$ implies $f(1/\alpha) \neq 0$). Then there is a root α of $f(x)$ such that*

$$|\alpha| > 1 + \frac{1}{10n}.$$

In other words, the conjecture of Schinzel and Zassenhaus is true when $f(x)$ has no reciprocal roots. Theorem 28 was stated in such a way as to make its connection to Theorem 27 and the conjecture of Schinzel and Zassenhaus, but observe that the conditions that $f(x)$ is non-cyclotomic and that $f(x)$ is irreducible may be omitted from the theorem without changing the content of the result. Theorem 28 was established by Cassels [1] and is proven below. However, first we deal with some preliminaries.

Lemma 1. *Let $\delta \in (0,1)$, and let x_j, for $j \in \{1, 2, \ldots, m\}$, be real numbers satisfying*

$$0 < x_j \leq 1 + \delta \quad \text{for } j \in \{1, 2, \ldots, m\} \tag{7.1}$$

and

$$\prod_{j=1}^{m} x_j = 1. \tag{7.2}$$

Then

$$\prod_{j=1}^{m} |x_j - 1| < (\delta e)^m. \tag{7.3}$$

Proof. Let $x_1, \ldots, x_m$ be real numbers satisfying (7.1) and (7.2), and assume that (7.3) is not true. For the time being, suppose that there are i and $j \in \{1, 2, \ldots, m\}$ such that $x_i < 1$, $x_j < 1$, and $x_i \neq x_j$. For such an i and j fixed, consider

$$x'_k = \begin{cases} \sqrt{x_i x_j} & \text{if } k = i \text{ or } j \\ x_k & \text{otherwise.} \end{cases}$$

Then

$$0 < x'_k \leq 1 + \delta \quad \text{for } k \in \{1, 2, \ldots, m\},$$

and

$$\prod_{k=1}^{m} x'_k = \prod_{k=1}^{m} x_k = 1.$$

Observe that

$$|x_i - 1|\,|x_j - 1| = (1 - x_i)(1 - x_j) = 1 - (x_i + x_j) + x_i x_j$$

and

$$|x'_i - 1|\,|x'_j - 1| = (1 - \sqrt{x_i x_j})(1 - \sqrt{x_i x_j}) = 1 - 2\sqrt{x_i x_j} + x_i x_j.$$

Since $x_i \neq x_j$, we get that $x_i + x_j > 2\sqrt{x_i x_j}$. Therefore,

$$\prod_{k=1}^{m} |x_k - 1| < \prod_{k=1}^{m} |x'_k - 1|.$$

Since $x_1, \ldots, x_m$ do not satisfy (7.3), we get that $x'_1, \ldots, x'_m$ do not satisfy (7.3). By repeating the above several times if necessary, we get that we can replace the real numbers $x_1, \ldots, x_m$ by a new collection of m real numbers satisfying (7.1) and (7.2) and not (7.3) and having the property that any two elements of the new collection of real numbers which are < 1 are equal. For notational reasons, we assume as we can that $x_1, \ldots, x_m$ already have the latter property.

Observe that if $x_j = 1$ for every $j \in \{1, \ldots, m\}$, then (7.3) would be true, giving a contradiction. Thus, since (7.1) and (7.2) hold, there must be an i and $j \in \{1, \ldots, m\}$ such that

$$x_i < 1 < x_j \leq 1 + \delta.$$

Using an argument similar to the above, one can show that we can further assume that any such $x_j = 1 + \delta$. To do this, note that

$$((1 + \delta) - x_i)\,((1 + \delta) - x_j) > 0 \quad \text{if } x_j \neq 1 + \delta,$$

and set

$$x'_k = \begin{cases} 1 + \delta & \text{if } k = j \\ x_i x_j (1 + \delta)^{-1} & \text{if } k = i \\ x_k & \text{otherwise.} \end{cases}$$

By the above observations, there will be a certain number, say $m - s$, of the x_j equal to $1 + \delta$ and the remaining s will be equal to $1 - \eta$ where

$$(1 - \eta)^s (1 + \delta)^{m-s} = 1.$$

Then

$$-s \log(1 - \eta) \leq m \log(1 + \delta)$$

so that

$$s\eta < s\left(\eta + \frac{\eta^2}{2} + \frac{\eta^3}{3} + \cdots\right) \leq m\left(\delta - \frac{\delta^2}{2} + \frac{\delta^3}{3} - \cdots\right) < m\delta.$$

Thus, $\eta < m\delta/s$, and we get that

$$\prod_{k=1}^{m} |x_k - 1| = \eta^s \delta^{m-s} \leq \left(\frac{m}{s}\right)^s \delta^m.$$

Since $m/s > 1$, we get that

$$\frac{m}{s} < \left(\frac{m}{s}\right)^e \leq e^{m/s}$$

(see Problem (7.10)). Thus, $(m/s)^s < e^m$, and we get that

$$\prod_{k=1}^{m} |x_k - 1| < (e\delta)^m,$$

concluding the proof. ■

We will put off the proof of the next lemma for the moment and discuss first how to obtain a certain Corollary to the lemma and how to establish Theorem 28 from the Corollary.

Lemma 2. *Let m be an integer > 1, and let ρ be a real number > 1 satisfying*

$$\cos\left(\frac{\pi}{m}\right) < \frac{\rho^2}{\rho^4 + 1 - \rho^2}. \tag{7.4}$$

Suppose that $z_1, \ldots, z_m \in \mathbb{C}$ and that

$$|z_j| \leq \rho \quad \text{for all } j \in \{1, \ldots, m\}. \tag{7.5}$$

Then

$$\prod_{\substack{1 \leq j,k \leq m \\ j \neq k}} |z_j \overline{z_k} - 1| \leq \left(\frac{\rho^{2m} - 1}{\rho^2 - 1}\right)^m. \tag{7.6}$$

Corollary. *Let m be an integer > 1, and let*

$$1 < \rho \leq 1 + \frac{1}{10m}. \tag{7.7}$$

Suppose that $z_1, \ldots, z_m \in \mathbb{C}$ satisfying (7.5). Then

$$\prod_{\substack{1 \leq j,k \leq m \\ j \neq k}} |z_j \overline{z_k} - 1| \leq m^m \rho^{2m(m-1)}. \tag{7.8}$$

Proof (assuming Lemma 2). One easily checks that for $x > 1$, $x^2 + x^{-2} - 1$ is increasing so that for $1 < x < 1 + (1/(10m))$, the value of $x^2 + x^{-2} - 1$ is at most

$$\begin{aligned}
&\left(1 + \frac{1}{10m}\right)^2 + \left(1 + \frac{1}{10m}\right)^{-2} - 1 \\
&\qquad = \left(1 + \frac{2}{10m} + \frac{1}{100m^2}\right) + \left(1 - \frac{2}{10m} + \frac{3}{100m^2} - \frac{4}{1000m^3} + \cdots\right) - 1 \\
&\qquad < 1 + \frac{4}{100m^2}.
\end{aligned}$$

Thus, the value of $1/(x^2 + x^{-2} - 1)$ is greater than

$$\frac{1}{1 + \dfrac{1}{25m^2}} > 1 - \frac{1}{25m^2} > 1 - \frac{\pi^2}{2m^2} + \frac{\pi^4}{24m^4} > \cos\left(\frac{\pi}{m}\right).$$

From (7.7), we get that

$$\cos\left(\frac{\pi}{m}\right) < \frac{1}{\rho^2 + \rho^{-2} - 1} = \frac{\rho^2}{\rho^4 + 1 - \rho^2}.$$

Thus, the conditions of Lemma 2 are satisfied. Hence,

$$\begin{aligned}
\prod_{\substack{1 \leq j,k \leq m \\ j \neq k}} |z_j \overline{z_k} - 1| &\leq \left(\frac{\rho^{2m} - 1}{\rho^2 - 1}\right)^m \\
&= \left(\rho^{2m-2} + \rho^{2m-4} + \cdots + \rho^2 + 1\right)^m \\
&\leq \left(\rho^{2m-2} m\right)^m = m^m \rho^{2m(m-1)},
\end{aligned}$$

establishing the corollary. ■

Proof of Theorem 28 (assuming Lemma 2). Let $w(x) = \sum_{j=0}^{m} a_j x^j$ with $a_0 \neq 0$ and $a_m = 1$, and suppose that the roots of $w(x)$ satisfy that

$$|\alpha_j| \leq 1 + \frac{1}{10m} \quad \forall j \in \{1, \ldots, m\}. \tag{7.9}$$

First, we show that $|a_0| = 1$. Assume that $|a_0| \geq 2$. Then observe that

$$\left(1 + \frac{1}{2m}\right)^m = 1 + \frac{1}{2} + \frac{m(m-1)}{2}\frac{1}{4m^2} + \cdots < 1 + \frac{1}{2} + \frac{1}{4} + \cdots = 2.$$

Also,

$$\left|\prod_{j=1}^{m} \alpha_j\right| = |a_0| \geq 2.$$

Therefore, we get that there is a $j \in \{1, \ldots, m\}$ such that

$$|\alpha_j| \geq 2^{1/m} > 1 + \frac{1}{2m},$$

contradicting (7.9). Hence, $|a_0| = 1$. Thus,

$$\prod_{j=1}^{m} |\alpha_j| = 1. \tag{7.10}$$

Consider

$$P = \prod_{1 \leq i,j \leq m} (\alpha_i \alpha_j - 1).$$

If $P = 0$, then $w(x)$ has reciprocal roots, and we are through. We therefore assume $P \neq 0$. By the definition of P, P is a symmetric function of the roots $\alpha_1, \ldots, \alpha_m$ of $w(x)$, and hence $P \in \mathbb{Z} - \{0\}$. Thus,

$$\prod_{1 \leq i,j \leq m} |\alpha_i \alpha_j - 1| \geq 1. \tag{7.11}$$

Observe that

$$\prod_{1 \leq i,j \leq m} |\alpha_i \alpha_j - 1| = \prod_{1 \leq i,j \leq m} |\alpha_i \overline{\alpha_j} - 1| = \Big(\prod_{1 \leq i \leq m} |\alpha_i \overline{\alpha_i} - 1|\Big)\Big(\prod_{\substack{1 \leq i,j \leq m \\ i \neq j}} |\alpha_i \overline{\alpha_j} - 1|\Big).$$

Also,

$$\alpha_i\overline{\alpha_i} = |\alpha_i|^2 \leq \left(1 + \frac{1}{10m}\right)^2 = 1 + \frac{1}{5m} + \frac{1}{100m^2} \leq 1 + \frac{1}{4m}.$$

Therefore, by Lemma 1, with $\delta = 1/(4m)$, we get by (7.10) that

$$\prod_{1\leq i\leq m} |\alpha_i\overline{\alpha_i} - 1| \leq \left(\frac{e}{4m}\right)^m.$$

Also, by the foregoing Corollary, we get that

$$\prod_{\substack{1\leq i,j\leq m \\ i\neq j}} |\alpha_i\overline{\alpha_j} - 1| \leq m^m \left(1 + \frac{1}{10m}\right)^{2m(m-1)}$$

$$= m^m \left(\left(1 + \frac{1}{10m}\right)^{10m}\right)^{(m-1)/5} < m^m e^{m/5}.$$

Combining the above, we get that

$$\prod_{1\leq i,j\leq m} |\alpha_i\alpha_j - 1| < \left(\frac{e}{4m}\right)^m m^m e^{m/5} = \left(\frac{e^{6/5}}{4}\right)^m < 1.$$

This contradicts (7.11); hence, the assumption that $P \neq 0$ is invalid and the proof is complete. ■

To complete this section, we now proceed to prove Lemma 2. To do so, we first make some further preliminaries.

Lemma 3. *Let r, α, and β be real numbers, and set $\lambda = (\alpha + \beta)/2$. Suppose that*

$$r \geq 1, \quad \alpha \geq 0, \quad \beta \geq 0, \quad \lambda < 3\pi/2,$$

and

$$\cos(\lambda) < \frac{r}{r^2 + 1 - r}.$$

Then

$$\left|re^{i\alpha} - 1\right| \left|re^{i\beta} - 1\right| \leq \left|re^{i\lambda} - 1\right|^2, \tag{7.12}$$

with equality if and only if $\alpha = \beta = \lambda$.

Proof. We suppose as we may that $\alpha \geq \beta$. Define $\mu = \alpha - \lambda$, and observe that

$$\alpha = \mu + \lambda \quad \text{and} \quad \beta = \lambda - \mu.$$

Let

$$L = \cos\lambda \quad \text{and} \quad M = \cos\mu.$$

Note that $\mu \geq 0$; and if $\mu = 0$, then $\alpha = \beta = \lambda$ and (7.12) holds. We need only show now that if $\mu > 0$, then (7.12) holds with strict inequality. Therefore, we suppose that $\mu > 0$. Observe that $\mu = \alpha - \lambda \leq \lambda < 3\pi/2$. Also, if $\lambda \geq 0$, then $0 \leq \lambda \leq \pi/2$. We get either

$$L < 0 \quad \text{and} \quad -1 \leq M < 1 \tag{7.13}$$

or

$$0 \leq L \leq M < 1 \quad \text{and} \quad L < \frac{r}{r^2 + 1 - r}. \tag{7.14}$$

Now, squaring the left-hand side of (7.12), we get that

$$\begin{aligned} \left|re^{i\alpha} - 1\right|^2 \left|re^{i\beta} - 1\right|^2 &= \left(re^{i\alpha} - 1\right)\left(re^{-i\alpha} - 1\right)\left(re^{i\beta} - 1\right)\left(re^{-i\beta} - 1\right) \\ &= \left((r^2+1) - 2r\cos(\alpha)\right)\left((r^2+1) - 2r\cos(\beta)\right). \end{aligned}$$

Using this together with

$$\begin{aligned} \cos(\alpha) + \cos(\beta) &= \cos(\lambda+\mu) + \cos(\lambda-\mu) \\ &= (\cos(\lambda)\cos(\mu) - \sin(\lambda)\sin(\mu)) + (\cos(\lambda)\cos(\mu) + \sin(\lambda)\sin(\mu)) \\ &= 2\cos(\lambda)\cos(\mu) = 2LM \end{aligned}$$

and

$$\begin{aligned} \cos(\alpha)\cos(\beta) &= (\cos(\lambda+\mu))\,(\cos(\lambda-\mu)) \\ &= \cos^2(\lambda)\cos^2(\mu) - \sin^2(\lambda)\sin^2(\mu) \\ &= \cos^2(\lambda)\cos^2(\mu) - \left(1 - \cos^2(\lambda)\right)\left(1 - \cos^2(\mu)\right) \\ &= \cos^2(\lambda) + \cos^2(\mu) - 1 = L^2 + M^2 - 1, \end{aligned}$$

we get that the square of the left-hand side of (7.12) is

$$\left(r^2+1\right)^2 - 4r\left(r^2+1\right)LM + 4r^2\left(L^2+M^2-1\right). \tag{7.15}$$

Observe that if we set $\alpha = \lambda$ and $\beta = \lambda$ in the above calculations of the square of the left-hand side of (7.12), we will obtain the square of the right-hand side of (7.12). In other words, we get the latter by setting $M = 1$ in (7.15). Thus, to finish the proof of the lemma, it suffices to show that

$$\left(r^2+1\right)^2 - 4r\left(r^2+1\right)LM + 4r^2\left(L^2+M^2-1\right) < \left(r^2+1\right)^2 - 4r\left(r^2+1\right)L + 4r^2\left(L^2\right).$$

This is the same as establishing that

$$4r^2\left(M^2-1\right) < 4r\left(r^2+1\right)L(M-1)$$

or, upon reducing and noting that $M - 1 < 0$,

$$r(M+1) > \left(r^2+1\right)L.$$

This is clear in the case that (7.13) holds. In the case that (7.14) holds, we rewrite the above as

$$r > \left(r^2+1\right)L - rM.$$

This inequality follows directly from

$$r > \left(r^2+1-r\right)L$$

and

$$\left(r^2+1-r\right)L \geq \left(r^2+1\right)L - rM,$$

completing the proof. ■

Lemma 4. *Let $m > 1$ be an integer, and let $\theta_1, \theta_2, \ldots, \theta_m$ be real numbers satisfying*

$$0 \le \theta_j \le 2\pi \quad \text{for } 1 \le j \le m.$$

Let

$$w = \frac{1}{2m}\left(\theta_1 + \cdots + \theta_m\right).$$

Consider $r > 1$ such that

$$|\cos(w)| < \frac{r}{r^2 + 1 - r}. \tag{7.16}$$

Then

$$\prod_{1 \le j \le m} \left|re^{i\theta_j} - 1\right| \le \left|re^{2iw} - 1\right|^m \tag{7.17}$$

with equality if and only if $\theta_1 = \cdots = \theta_m = 2w$.

Proof. Observe that if $r > 1$, then $r/(r^2 + 1 - r) < 1$. Hence, the lemma vacuously holds if $w = 0$ or π. Also, the lemma follows if $w = \pi/2$ since then we get that

$$\left|re^{i\theta_j} - 1\right| \le r + 1 = \left|re^{2iw} - 1\right|$$

with equality if and only if $\theta_j = \pi = 2w$. If $\pi/2 < w < \pi$, then replace θ_j with $2\pi - \theta_j$ and w by $\pi - w$ to reduce the lemma to a case in which

$$0 < w < \pi/2.$$

Thus, we suppose as we may that the latter holds for w.

For fixed w, by continuity and compactness considerations, the left-hand side of (7.17) obtains its upper bound for some choice of $\theta_1, \ldots, \theta_m$ as in the lemma. We fix $\theta_1, \ldots, \theta_m$ so that this upper bound is obtained and note that now it suffices to prove (7.17) with the θ_j so chosen. If $\theta_1 = \cdots = \theta_m$, then we are through; thus, we suppose as we may that θ_1 and θ_2 satisfy

$$0 \le \theta_1 < 2w < \pi \quad \text{and} \quad 2w < \theta_2 \le 2\pi.$$

Set $\alpha = \theta_1$, $\beta = \theta_2$, and $\lambda = (\alpha + \beta)/2$. Then

$$\lambda = \frac{1}{2}(\theta_1 + \theta_2) < \frac{1}{2}(\pi + 2\pi) = \frac{3}{2}\pi$$

and either $\lambda \geq \pi/2$ so that

$$\cos(\lambda) \leq 0 < \frac{r}{r^2 + 1 - r}$$

or $0 < w < \theta_2/2 < \lambda < \pi/2$ so that from (7.16)

$$\cos(\lambda) \leq \cos(\theta_2/2) < \cos(w) < \frac{r}{r^2 + 1 - r}.$$

Thus, from Lemma 3, we get that

$$\left|re^{i\alpha} - 1\right| \left|re^{i\beta} - 1\right| < \left|re^{i\lambda} - 1\right|^2.$$

By considering $\theta_1' = \theta_2' = \lambda = (\theta_1 + \theta_2)/2$ and $\theta_j' = \theta_j$ for $j \in \{3, \ldots, m\}$, we get that the above inequality contradicts that $\theta_1, \ldots, \theta_m$ were chosen so that the left-hand side of (7.17) was maximal. Hence, for $\theta_1, \ldots, \theta_m$ so chosen, we must have that $\theta_1 = \cdots = \theta_m = 2w$ so that (7.17) holds with equality. This completes the proof. ■

Lemma 5 (The Maximum Modulus Principle). *Let $f(z) \in \mathbb{C}[z]$, and let $\rho \geq 0$. Then*

$$\max\{|f(z)| : |z| \leq \rho\} = \max\{|f(z)| : |z| = \rho\}.$$

Proof. Observe that the maximums exist above since $f(z)$ is continuous. Let z_0 be such that $|z_0| \leq \rho$ and

$$|f(z_0)| = \max\{|f(z)| : |z| \leq \rho\}.$$

Furthermore, suppose that $|z_0|$ is maximal with the above conditions (noting that this is in fact possible). If $|z_0| = \rho$, then we're done. Assume therefore that $|z_0| < \rho$. Let $r = \rho - |z_0|$. Then the average value of $|f(z)|^2$ on the circle $\{z : |z - z_0| = r\}$ is $< |f(z_0)|^2$.

Let $g(z) = f(z + z_0) = \sum_{j=0}^{n} b_j z^j$. Then the above implies that

$$\begin{aligned}\sum_{j=0}^{n} |b_j|^2 r^{2j} &= \frac{1}{2\pi}\int_0^{2\pi} \left(\sum_{j=0}^{n} b_j r^j e^{ji\theta}\right)\left(\sum_{j=0}^{n} \overline{b_j} r^j e^{-ji\theta}\right) d\theta \\ &= \frac{1}{2\pi}\int_0^{2\pi} g\left(re^{i\theta}\right)\overline{g\left(re^{i\theta}\right)}\, d\theta = \frac{1}{2\pi}\int_0^{2\pi} \left|g\left(re^{i\theta}\right)\right|^2 d\theta \\ &= \frac{1}{2\pi}\int_0^{2\pi} \left|f\left(z_0 + re^{i\theta}\right)\right|^2 d\theta < |f(z_0)|^2 = |g(0)|^2 = |b_0|^2,\end{aligned}$$

giving a contradiction. Thus, the result follows. ■

Proof of Lemma 2. Fix $j \in \{1, \ldots, m\}$ and complex numbers $z_1, \ldots, z_{j-1}, z_{j+1}, \ldots, z_m$ as in the lemma. Then

$$\begin{aligned}\prod_{\substack{1\le t,k\le m\\ t\ne k}} |z_t\overline{z_k} - 1| &= \left(\prod_{\substack{1\le t,k\le m\\ t\ne k, t\ne j, k\ne j}} |z_t\overline{z_k} - 1|\right)\prod_{\substack{1\le k\le m\\ k\ne j}} \left(|z_j\overline{z_k} - 1||\overline{z_j}z_k - 1|\right) \\ &= \left(\prod_{\substack{1\le t,k\le m\\ t\ne k, t\ne j, k\ne j}} |z_t\overline{z_k} - 1|\right)\prod_{\substack{1\le k\le m\\ k\ne j}} |z_j\overline{z_k} - 1|^2.\end{aligned}$$

Hence, we may view

$$\prod_{\substack{1\le t,k\le m\\ t\ne k}} |z_t\overline{z_k} - 1| \tag{7.18}$$

as the absolute value of a polynomial in z_j. By Lemma 5, given that $|z_j| \le \rho$, we get that (7.18) obtains its maximum for some z_j with $|z_j| = \rho$. Letting j vary now, we see that to finish the proof, we need only consider the case when

$$|z_1| = |z_2| = \cdots = |z_m| = \rho.$$

By reordering the z_j's if necessary, we suppose as we may that

$$z_j = \rho e^{i\phi_j} \quad \text{for } j \in \{1, \ldots, m\},$$

where

$$0 \leq \phi_1 \leq \phi_2 \leq \cdots \leq \phi_m < 2\pi.$$

Now, (7.18) becomes

$$\prod_{\substack{1 \leq t,k \leq m \\ t \neq k}} |\rho^2 e^{i(\phi_t - \phi_k)} - 1| = \prod_{1 \leq s \leq m-1} P_s,$$

where

$$P_s = \prod_{\substack{1 \leq t,k \leq m \\ t \equiv k+s \pmod m}} |\rho^2 e^{i(\phi_t - \phi_k)} - 1|.$$

Observe that if s and t are known, then k is uniquely determined by the conditions $1 \leq k \leq m$ and $t \equiv k + s \pmod m$. For fixed $s \in \{1, \ldots, m-1\}$ and fixed $t \in \{1, \ldots, m\}$, consider the uniquely determined k as in the product above. Define

$$\theta_t = \theta_t(s) = \begin{cases} \phi_t - \phi_k & \text{if } t > k \\ \phi_t - \phi_k + 2\pi & \text{if } k > t \end{cases}$$

and note that $k > t$ in this definition if and only if $t \in \{1, \ldots, s\}$. Set

$$r = \rho^2$$

and

$$w = s\pi/m.$$

Then, for $s \in \{1, \ldots, m-1\}$,

$$\theta_1 + \cdots + \theta_m = 2\pi s = 2mw$$

and

$$|\cos(w)| = \left|\cos\left(\frac{s\pi}{m}\right)\right| \leq \cos\left(\frac{\pi}{m}\right) < \frac{\rho^2}{\rho^4 + 1 - \rho^2} = \frac{r}{r^2 + 1 - r}.$$

Thus, we may apply Lemma 4 to get that

$$P_s \leq \left|\rho^2 e^{2\pi i s/m} - 1\right|^m$$

so that (7.18) is bounded above by

$$\prod_{1\le s\le m-1}\left|\rho^2 e^{2\pi is/m}-1\right|^m=\left|\frac{\rho^{2m}-1}{\rho^2-1}\right|^m,$$

completing the proof. ■

7.4. In this section, we investigate the size of the coefficients of $\Phi_n(x)$. Recall the values of $\Phi_n(x)$ for $n\in\{1,2,\dots,10\}$ given at the beginning of the chapter. If we continue calculating up to $\Phi_{104}(x)$, the coefficients obtained will remain in the set $\{-1,0,1\}$ suggesting at the very least that the coefficients of $\Phi_n(x)$ do not get very large. This is in fact *not* the case, and it is the purpose of this section to mention two results in this direction. We shall only prove the first. It is a consequence of the second but seemingly much easier to establish. The proof given here is due to I. Schur (cf. E. Lehmer [1], her first mathematical publication).

Theorem 29. *Given B, there exists a positive integer n such that $\Phi_n(x)$ has at least one coefficient with absolute value $> B$.*

Proof. Let $n=p_1p_2\dots p_k$, where k is an odd positive integer and $p_1,p_2,\dots,p_k$ are primes satisfying

$$p_1<p_2<\cdots<p_k<p_1+p_2.$$

Note that there are infinitely many such n for any given k (see problem (AII.1)). To prove the theorem, it is sufficient to prove that the coefficient of x^{p_k} in $\Phi_n(x)$ is $1-k$. Using Theorem 24 and calculating $\Phi_n(x)$ modulo $x^{p_k}+1$, we get that modulo $x^{p_k}+1$

$$\Phi_n(x)\equiv\left(\prod_{j=1}^{k}\left(x^{p_j}-1\right)\right)/(x-1)$$

$$\equiv\left(x^{p_k-1}+x^{p_k-2}+\cdots+x+1\right)\left(x^{p_1}-1\right)\left(x^{p_2}-1\right)\cdots\left(x^{p_{k-1}}-1\right)$$

$$\equiv\left(x^{p_k-1}+x^{p_k-2}+\cdots+x+1\right)\left(-x^{p_{k-1}}-x^{p_{k-2}}-\cdots-x^{p_1}+1\right)$$

The fact that the coefficient of x^{p_k} in $\Phi_n(x)$ is $1-k$ follows, and the proof is complete. ■

The above proof shows that certain positive integers n with sufficiently many distinct prime factors are such that $\Phi_n(x)$ has a coefficient whose absolute value exceeds B for any preassigned B. Migotti (cf. E. Lehmer [1]) showed that if n is the product of 2 primes, then the coefficients of $\Phi_n(x)$ are all from the set $\{0, \pm 1\}$. E. Lehmer [1] showed that as n runs through the positive integers which are the product of 3 distinct primes, the coefficients of $\Phi_n(x)$ get arbitrarily large.

We end this section by stating what is undoubtedly one of the nicest result on the subject. Let M_n denote the maximum of the absolute values of the coefficients of $\Phi_n(x)$. Erdős conjectured that for every constant c, one has that $M_n \geq c$ for almost all n. In other words, the number of $n \leq x$ for which $M_n < c$ is $o(x)$. The conjecture was first resolved by Maier [1] in a much stronger form. He showed the following:

Theorem 30. *Let $\epsilon(n)$ be any function defined for all positive integers and satisfying $\lim_{n\to\infty} \epsilon(n) = 0$. Then*

$$M_n \geq n^{\epsilon(n)}$$

for almost all n.

Thus, the conjecture follows by taking, for example, $\epsilon(n) = 1/\log\log n$. We note that the result of Maier [1] is in fact even stronger than that given by Theorem 30.

7.5. In this section, we discuss the factorization of $\Phi_n(x)$ modulo a prime. We will establish

Theorem 31. *Let n be a positive integer, and let p be a prime. Write $n = p^k m$ where k is a non-negative integer and $\gcd(p, m) = 1$. Let f be the least positive integer such that $p^f \equiv 1 \pmod{m}$. Then $\Phi_n(x)$ factors as a product of $\phi(m)/f$ incongruent irreducible polynomials modulo p of degree f each raised to the $\phi(p^k)$ power.*

Before presenting the proof of Theorem 31, we give two examples. Further examples can be found in the exercises as well as in the Corollaries following the proof.

Example 1. Consider $f(x) = \Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1$. If $p = 2$, then $m = 5$ and $f = 4$ in Theorem 31 so that $f(x)$ is irreducible modulo 2. If $p = 5$, then $m = 2$ and $f = 1$ so that $f(x)$ factors as a linear polynomial raised to the 4th power modulo 5. In fact, we have

$$f(x)(x+1) \equiv x^5 + 1 \equiv (x+1)^5 \pmod 5$$

so that by Theorem 3 (unique factorization in $\mathbb{Z}_5[x]$) we get that $f(x) \equiv (x+1)^4 \pmod 5$. If p is a prime $\equiv 1 \pmod{10}$, then $m = 10$ and $f = 1$ so that $f(x)$ factors as a product of 4 distinct linear polynomials modulo p. If p is a prime $\equiv 3$ or $7 \pmod{10}$, then $m = 10$ and $f = 4$ so that $f(x)$ is irreducible modulo p. Finally, if p is a prime $\equiv 9 \pmod{10}$, then $m = 10$ and $f = 2$ so that $f(x)$ factors as a product of 2 distinct irreducible quadratic polynomials modulo p.

Example 2. Consider $f(x) = \Phi_8(x) = x^4 + 1$. If $p = 2$, then $m = 1$ and $f = 1$ in Theorem 31 so that $f(x)$ factors as a linear polynomial raised to the 4th power modulo 2. Here we have

$$f(x) \equiv x^4 + 1 \equiv (x+1)^4 \pmod 2.$$

If p is a prime $\equiv 1 \pmod 8$, then $m = 8$ and $f = 1$ so that $f(x)$ factors as a product of 4 distinct linear polynomials modulo p. If p is a prime $\equiv 3$, 5, or $7 \pmod 8$, then $m = 8$ and $f = 2$ so that $f(x)$ factors as a product of 2 distinct irreducible quadratic polynomials modulo p. Observe that this implies the result of Problem (4.1) that $x^4 + 1$ is reducible modulo every prime. (Also, see Corollary 1 below.)

These examples demonstrate what is apparent from the statement of the theorem, namely that the factorization of $\Phi_n(x)$ modulo a prime p is completely determined by the residue class to which p belongs modulo n. We also note that Theorem 31 can be used to give an alternative proof of Theorem 25. More specifically, Theorem 31 implies that if p is a prime which does not divide n and is such that $p | \Phi_n(a)$ for some integer a, then $p \equiv 1 \pmod n$.

Proof of Theorem 31. The main tool we use to obtain Theorem 31 is Theorem 17 of Chapter 4. We begin, however, by making use of Problem (7.3). If, in the statement of Theorem 31, $k \geq 1$, then Problem (7.3) (a) implies that

$$\Phi_n(x) = \Phi_{pm}\left(x^{p^{k-1}}\right),$$

and Problem (7.3) (b) implies that

$$\Phi_{pm}\left(x^{p^{k-1}}\right)\Phi_m\left(x^{p^{k-1}}\right) = \Phi_m\left(x^{p^k}\right).$$

On the other hand,

$$\Phi_m\left(x^{p^{k-1}}\right) \equiv \Phi_m(x)^{p^{k-1}} \pmod{p} \quad \text{and} \quad \Phi_m\left(x^{p^k}\right) \equiv \Phi_m(x)^{p^k} \pmod{p}.$$

Hence, we deduce that

$$\Phi_n(x) \equiv \Phi_m(x)^{\phi(p^k)} \pmod{p}.$$

We assumed above that $k \geq 1$, but we note that this last congruence is trivially true in the case that $k = 0$. To establish the theorem, then, it suffices to show $\Phi_m(x)$ factors modulo p as a product of $\phi(m)/f$ incongruent irreducible polynomials of degree f.

By the definition of f, we see that m divides $p^f - 1$. Hence, $x^m - 1$ divides $x^{p^f - 1} - 1$, and we obtain that $\Phi_m(x)$ divides $\left(x^{p^f - 1} - 1\right)x = x^{p^f} - x$. By Theorem 17, each irreducible factor $g(x)$ of $\Phi_m(x)$ modulo p is such that its degree, say r, divides f. We show that for each such $g(x)$, $r = f$. Assume for some such $g(x)$, we have $r < f$. Then by Theorem 16 or Theorem 17, $g(x)$ divides $x^{p^r} - x$ modulo p. In fact, since $\Phi_m(x)$ divides $x^m - 1$, the constant term of $\Phi_m(x)$ is ± 1 and so the constant term of $g(x)$ is non-zero modulo p. Thus, $g(x)$ is not a multiple of x modulo p and $g(x)$ divides $x^{p^r - 1} - 1$ modulo p. In particular, x has an inverse (modd p, $g(x)$). The definition of f implies that m does not divide $p^r - 1$ so that $d = \gcd(m, p^r - 1) < m$. Let u and v be integers satisfying $mu + (p^r - 1)\, v = d$. Then

$$x^d - 1 \equiv x^{mu + (p^r - 1)\, v} - 1 \equiv (x^m)^u \left(x^{p^r - 1}\right)^v - 1 \equiv 0 \pmod{p,\, g(x)}.$$

Therefore, $g(x)$ divides $x^d - 1$ modulo p.

Observe that $d < m$ implies $\Phi_m(x)$ is by definition relatively prime to $x^d - 1$. Therefore, $\Phi_m(x)$ and $x^d - 1$ are relatively prime divisors of $x^{md} - 1$ in $\mathbb{Z}[x]$. Let $h_1(x) \in \mathbb{Z}[x]$ with $x^{md} - 1 = \Phi_m(x)\left(x^d - 1\right) h_1(x)$. Since $g(x)$ is a common divisor of $\Phi_m(x)$ and $x^d - 1$ modulo p, we get that for some $h_2(x) \in \mathbb{Z}[x]$

$$x^{md} - 1 \equiv \Phi_m(x)\left(x^d - 1\right) h_1(x) \equiv g(x)^2 h_2(x) \pmod{p}.$$

Since d divides $p^r - 1$, p does not divide d. The definition of m implies that p does not divide m. Hence, taking derivatives above, we deduce that $g(x)$ is an irreducible factor of x^{md-1} modulo p and yet $g(x)$ is not a multiple of x modulo p. This is a contradiction which implies that $r = f$. Thus, every irreducible factor of $\Phi_m(x)$ modulo p is of degree f.

Since $\deg \Phi_m(x) = \phi(m)$, it remains only to show that if $g(x)$ is an irreducible factor of $\Phi_m(x)$ modulo p, then $g(x)^2$ does not divide $\Phi_m(x)$ modulo p. Assume $g(x)^2$ divides $\Phi_m(x)$ modulo p. Then there is an $h(x) \in \mathbb{Z}[x]$ such that $x^m - 1 \equiv g(x)^2 h(x) \pmod{p}$. Following the argument above, we get in this case that $g(x)$ must be an irreducible factor of x^{m-1} modulo p, resulting in a contradiction and, hence, completing the proof. ■

Let n be a positive integer. Observe that if a prime p does not have order $\phi(n)$ modulo n, then the above theorem implies $\Phi_n(x)$ is reducible modulo p. In particular, if there are no primitive roots modulo n (i.e., no integers a for which the order of a is $\phi(n)$ modulo n), then $\Phi_n(x)$ is reducible modulo every prime. On the other hand, using the above theorem in conjunction with Dirichlet's Theorem on primes in arithmetic progression, one can easily deduce that if there exists a primitive root modulo n, then $\Phi_n(x)$ is irreducible modulo some prime. The n for which a primitive root modulo n exists are 1, 2, 4, and numbers of the form p^k or $2p^k$ where p is an odd prime and k a positive integer; thus, we can summarize the comments here with

Corollary 1. *Let n be a positive integer. Then $\Phi_n(x)$ is reducible modulo every prime p if and only if n is not among the numbers of the form 1, 2, 4, p^k, or $2p^k$ where p denotes an odd prime and k denotes a positive integer.*

We consider now the possibility that $\Phi_n(x)$ is Eisenstein with respect to some prime p. Then $\Phi_n(x)$ would factor modulo p as a constant times a linear polynomial raised to the power $\phi(n)$. Using the notation of Theorem 31, we would necessarily have that $f = 1$ and $\phi(m) = 1$. Therefore, $m = 1$ or 2. This implies that either $n = p^k$ or $n = 2p^k$ for some prime p. In these cases, Theorem 31 can be used to establish that $\Phi_n(x)$ is Eisenstein with respect to p (or see Problem (7.5) and Problem (7.6)). Hence, we get

Corollary 2. *Let n be a positive integer. Then $\Phi_n(x)$ is Eisenstein with respect to a prime p if and only if $n = p^k$ or $n = 2p^k$ for some positive integer k.*

7.6. There are numerous results concerning cyclotomic polynomials and it would be impossible in one chapter to give them a thorough treatment. In this section, we briefly mention a few other results without proofs. The results are classical and can be found in Narkiewicz [1].

The field $\mathbb{Q}(\zeta_n)$ is called a cyclotomic field. All the roots of $x^n - 1$ are in $\mathbb{Q}(\zeta_n)$. Thus, we can refer to the galois group $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ associated with the polynomial $\Phi_n(x)$. The galois group G is isomorphic to $\mathbb{Z}_n^*$ (the multiplicative group of integers modulo n). The elements of G can be described as follows. Let $j \in \{1, \ldots, n-1\}$ with $\gcd(j, n) = 1$. Define σ_j as the automorphism of $\mathbb{Q}(\zeta_n)$ satisfying $\sigma_j(\zeta_n) = \zeta_n^j$ and $\sigma_j(u) = u$ for all $u \in \mathbb{Q}$. Then the σ_j's are precisely the elements of G. Observe that in particular $|G| = \phi(n)$.

The ring of algebraic integers in $\mathbb{Q}(\zeta_n)$ clearly contains $\mathbb{Z}[\zeta_n]$. In fact, the ring of integers can be shown to be $\mathbb{Z}[\zeta_n]$. The units in $\mathbb{Z}[\zeta_n]$ are described in a convenient form by a result known as Kummer's Lemma (which Kummer used to establish his classical result that Fermat's Last Theorem holds for any "regular" prime exponent). It is

Theorem 32. *Every unit in $\mathbb{Z}[\zeta_n]$ can be written in the form $r\zeta_n^k$ where r is real and k is an integer.*

Problems

(7.1) (a) What is the value of $\Phi_p(x)$ when p is a prime?

(b) Expand $\Phi_p(x+1)$ as a polynomial in x, and deduce that $\Phi_p(x)$ is irreducible.

(7.2) Prove that if $\Phi_n(x)$ is Eisenstein with respect to p, then p divides n. (Hint: First show that if $f(x)$ and $g(x)$ are in $\mathbb{Z}[x]$ and each does not have a multiple root, then $R(f,f')R(g,g')$ divides $R(fg,(fg)')$. Be sure to justify that $R(fg,(fg)')/(R(f,f')R(g,g'))$ is an integer.)

(7.3) Let n be a positive integer, and let p be a prime.

(a) Prove that if p divides n, then $\Phi_{pn}(x) = \Phi_n(x^p)$.

(b) Prove that if p does not divide n, then $\Phi_{pn}(x) = \Phi_n(x^p)/\Phi_n(x)$.

(7.4) Prove that if n is an odd integer ≥ 3, then $\Phi_{2n}(x) = \Phi_n(-x)$.

(7.5) Without using any material after Section 7.1 except the problems above, prove that if k is a positive integer and p is a prime, then $\Phi_{p^k}(x)$ is Eisenstein with respect to p.

(7.6) Without using any material after Section 7.1 except the problems above, prove that if k is a positive integer and p is a prime, then $\Phi_{2p^k}(x)$ is Eisenstein with respect to p.

(7.7) Let $f(x)$ be a monic irreducible polynomial of degree n, and let α denote a root of $f(x)$.

(a) Prove that for every positive integer k, there is a unique polynomial $g(x) \in \mathbb{Z}[x]$ which is $\equiv 0$ or of degree $< n$ such that $f(\alpha^k) = g(\alpha)$.

(b) In (a), if $k = p$ where p is a prime, then prove that every coefficient of $g(x)$ is divisible by p. (Hint: Consider $f(x^p) - f(x)^p$.)

(7.8) Let $f(x)$ be a non-constant polynomial with integer coefficients. Prove that there

are infinitely primes p for which p divides $f(m)$ for some integer m.

(7.9) Modify the proof of Kronecker's Theorem in Section 3 to give an easy proof that there is a positive function $\epsilon(n)$ such that if $f(x) \in \mathbb{Z}[x]$ is a monic irreducible polynomial of degree n with all of its roots having absolute value $\leq 1 + \epsilon(n)$, then $f(x)$ is cyclotomic.

(7.10) Prove that if $x > 0$, then $x^e \leq e^x$ (a result used in the proof of Lemma 1 to Theorem 28).

(7.11) (a) Is it possible to load 2 dice in such a way that each face of each die has a rational probability of coming facing up on a roll and such that if both dice are rolled, then the sum of the 2 numbers rolled is equally likely to be each of $2, 3, \ldots, 12$?

(b) Do part (a) with each face of each die having a "real" probability of coming facing up on a roll.

(7.12) Let n and k be positive integers. Prove that $\Phi_n(x^k)$ is a product of distinct cyclotomic polynomials. (Note: The product may consist of just one factor.)

(7.13) Let n and k be positive integers. Prove that $\Phi_n(x^k)$ is irreducible if and only if every prime divisor of k is a prime divisor of n.

(7.14) Prove that for each prime p, $\Phi_{200}(x)$ can be written as a product of at least 4 factors modulo p.

NEWTON POLYGONS

NEWTON POLYGONS

WITH RESPECT TO A PRIME p

$$f(x) \quad = \quad x^6 + \ 24\ x^5 + \ 12\ x^3 - \ 18\ x + \ 36$$

$$f(x) \quad = \quad x^6 + 2^3 3^1 x^5 + \ 12\ x^3 - \ 18\ x + \ 36$$

$$f(x) \quad = \quad x^6 + 2^3 3^1 x^5 + 2^2 3^1 x^3 - \ 18\ x + \ 36$$

$$f(x) \quad = \quad x^6 + 2^3 3^1 x^5 + 2^2 3^1 x^3 - 2^1 3^2 x + \ 36$$

$$f(x) \quad = \quad x^6 + 2^3 3^1 x^5 + 2^2 3^1 x^3 - 2^1 3^2 x + 2^2 3^2$$

$$f(x) = 2^0 3^0 x^6 + 2^3 3^1 x^5 + 2^2 3^1 x^3 - 2^1 3^2 x + 2^2 3^2$$

$$f(x) = 2^0 3^0 x^6 + 2^3 3^1 x^5 + 2^2 3^1 x^3 - 2^1 3^2 x + 2^2 3^2$$

$$p = 2$$

$$f(x) = 2^{0}3^{0}x^{6} + 2^{3}3^{1}x^{5} + 2^{2}3^{1}x^{3} - 2^{1}3^{2}x + 2^{2}3^{2}$$

$$p = 2$$

$$f(x) = 2^{0}3^{0}x^{6} + 2^{3}3^{1}x^{5} + 2^{2}3^{1}x^{3} - 2^{1}3^{2}x + 2^{2}3^{2}$$

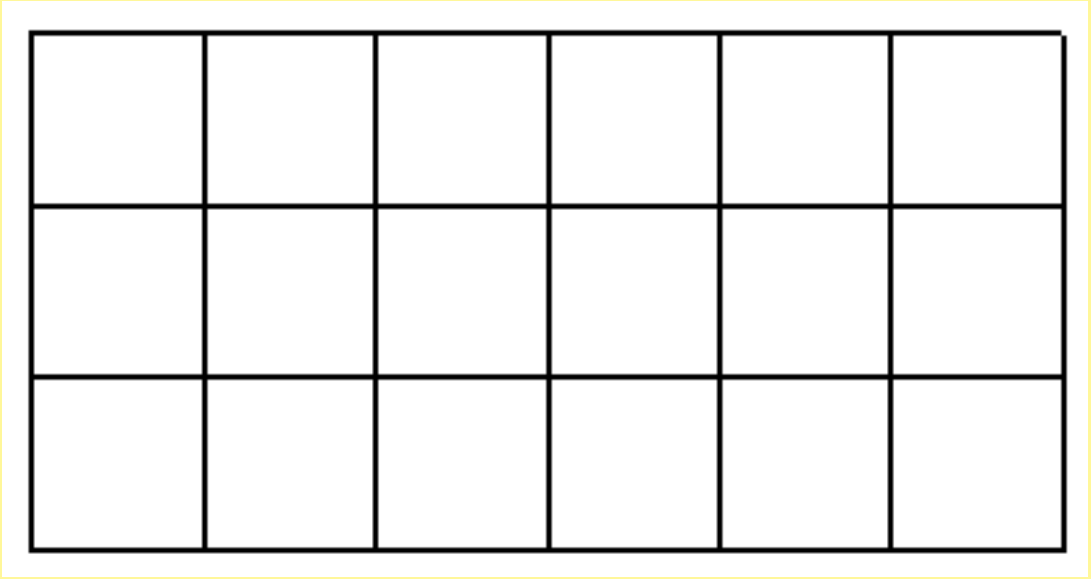
$$p = 2$$

$$f(x) = 2^{0}3^{0}x^{6} + 2^{3}3^{1}x^{5} + 2^{2}3^{1}x^{3} - 2^{1}3^{2}x + 2^{2}3^{2}$$

$$p = 2$$

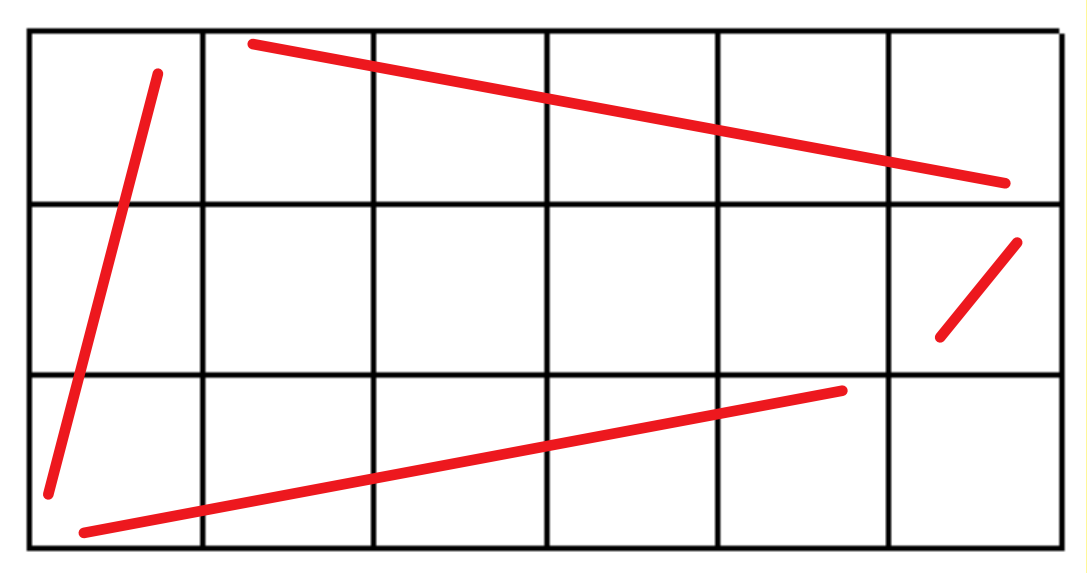
$$f(x) = 2^{0}3^{0}x^{6} + 2^{3}3^{1}x^{5} + 2^{2}3^{1}x^{3} - 2^{1}3^{2}x + 2^{2}3^{2}$$

$$p = 2$$



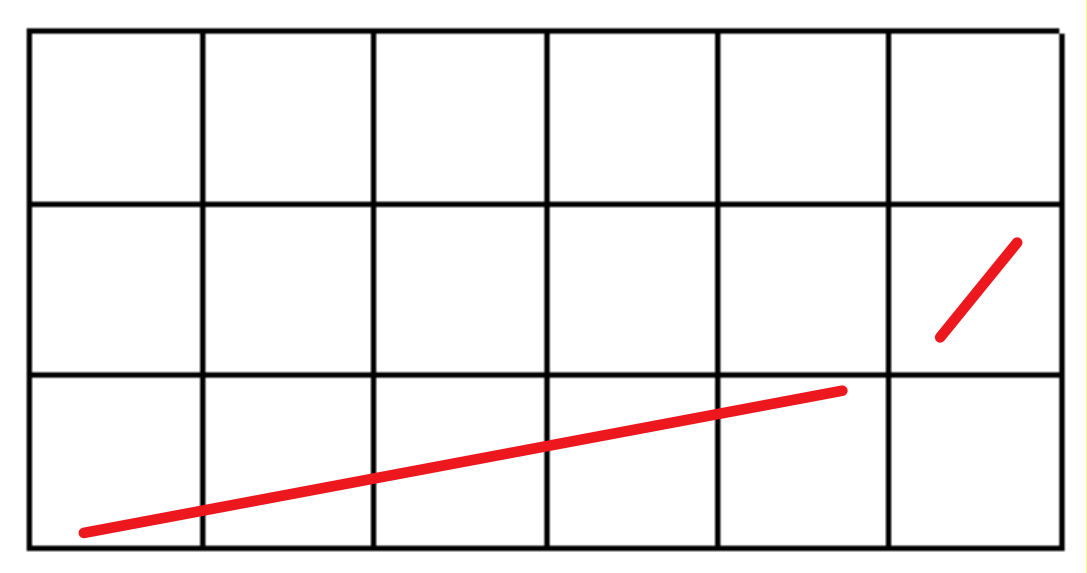
$$f(x) = 2^{0}3^{0}x^{6} + 2^{3}3^{1}x^{5} + 2^{2}3^{1}x^{3} - 2^{1}3^{2}x + 2^{2}3^{2}$$

$$p = 2$$



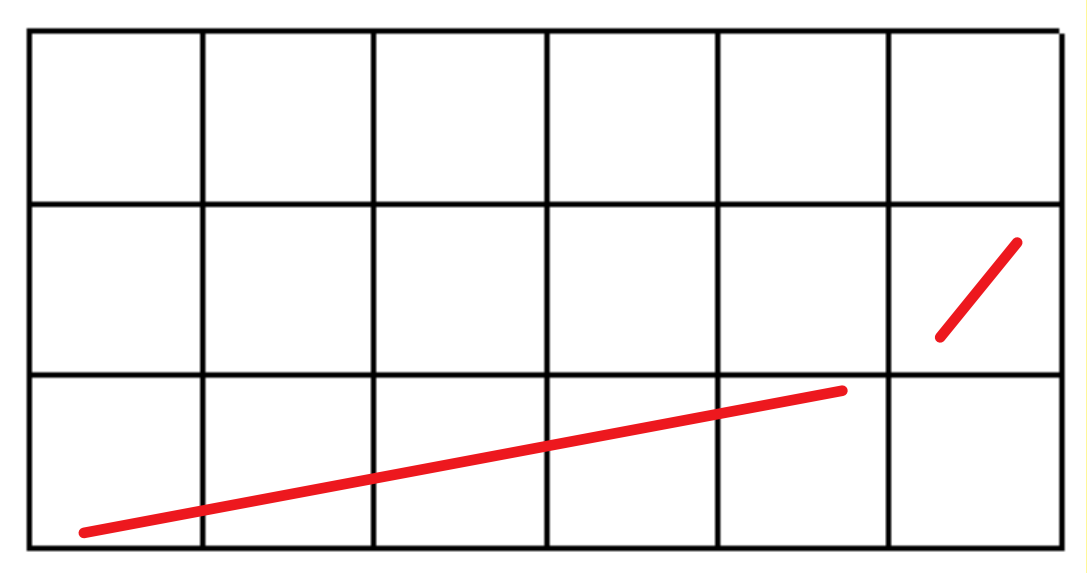
$$f(x) = 2^{0}3^{0}x^{6} + 2^{3}3^{1}x^{5} + 2^{2}3^{1}x^{3} - 2^{1}3^{2}x + 2^{2}3^{2}$$

$$p = 2$$



$$f(x) = 2^{0}3^{0}x^{6} + 2^{3}3^{1}x^{5} + 2^{2}3^{1}x^{3} - 2^{1}3^{2}x + 2^{2}3^{2}$$

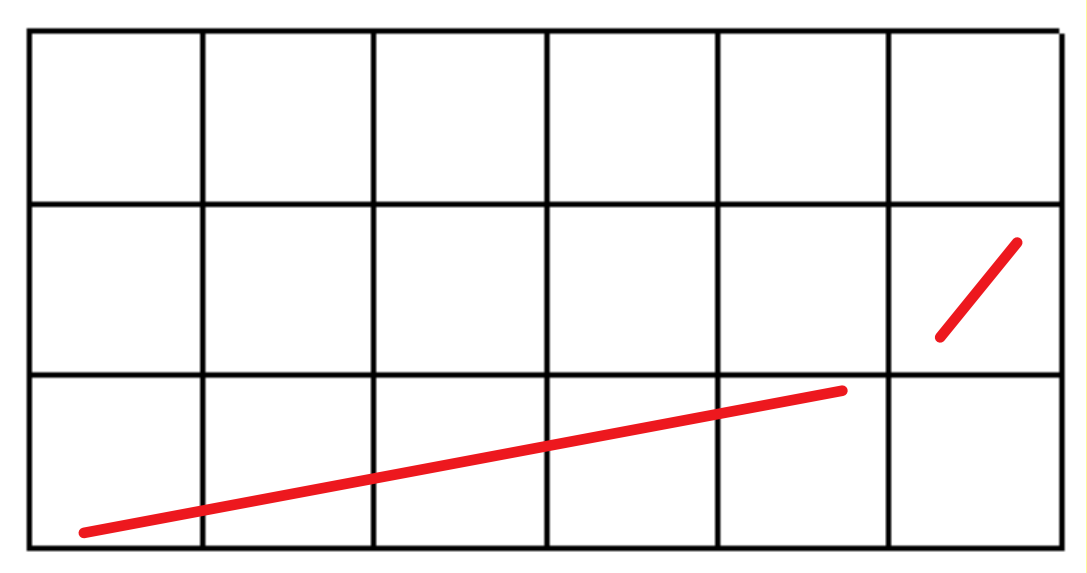
$$p = 2$$



Newton polygon of $f(x)$ with respect to p

$$f(x) = 2^{0}3^{0}x^{6} + 2^{3}3^{1}x^{5} + 2^{2}3^{1}x^{3} - 2^{1}3^{2}x + 2^{2}3^{2}$$

$$p = 2$$



Newton polygon of $f(x)$ with respect to 2

Comment: The slopes of the edges of a Newton polygon increase going from left to right.

$$f(x) = 2^0 3^0 x^6 + 2^3 3^1 x^5 + 2^2 3^1 x^3 - 2^1 3^2 x + 2^2 3^2$$

$$f(x) = 2^0 3^0 x^6 + 2^3 3^1 x^5 + 2^2 3^1 x^3 - 2^1 3^2 x + 2^2 3^2$$

$$p = 3$$

$$f(x) = 2^0 3^0 x^6 + 2^3 3^1 x^5 + 2^2 3^1 x^3 - 2^1 3^2 x + 2^2 3^2$$

$$p = 3$$

$$f(x) = 2^0 3^0 x^6 + 2^3 3^1 x^5 + 2^2 3^1 x^3 - 2^1 3^2 x + 2^2 3^2$$

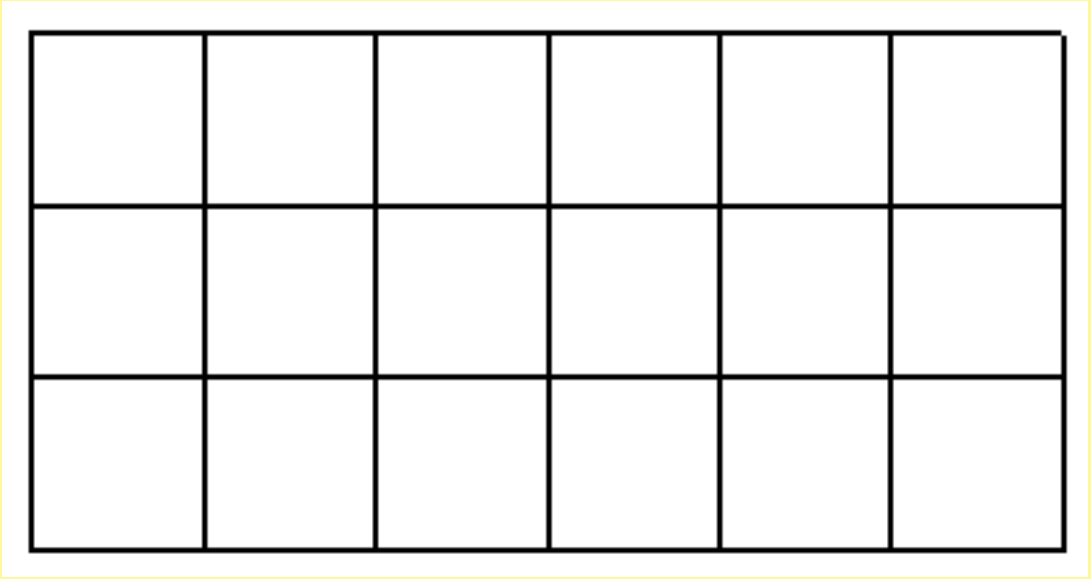
$$p = 3$$

$$f(x) = 2^0 3^0 x^6 + 2^3 3^1 x^5 + 2^2 3^1 x^3 - 2^1 3^2 x + 2^2 3^2$$

$$p = 3$$

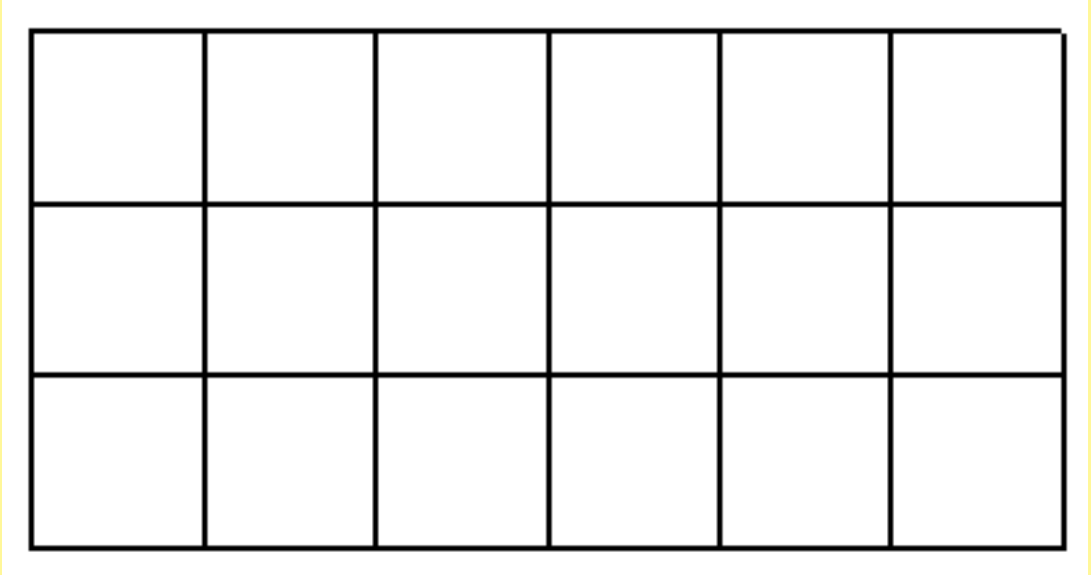
$$f(x) = 2^0 3^0 x^6 + 2^3 3^1 x^5 + 2^2 3^1 x^3 - 2^1 3^2 x + 2^2 3^2$$

$$p = 3$$



$$f(x) = 2^0 3^0 x^6 + 2^3 3^1 x^5 + 2^2 3^1 x^3 - 2^1 3^2 x + 2^2 3^2$$

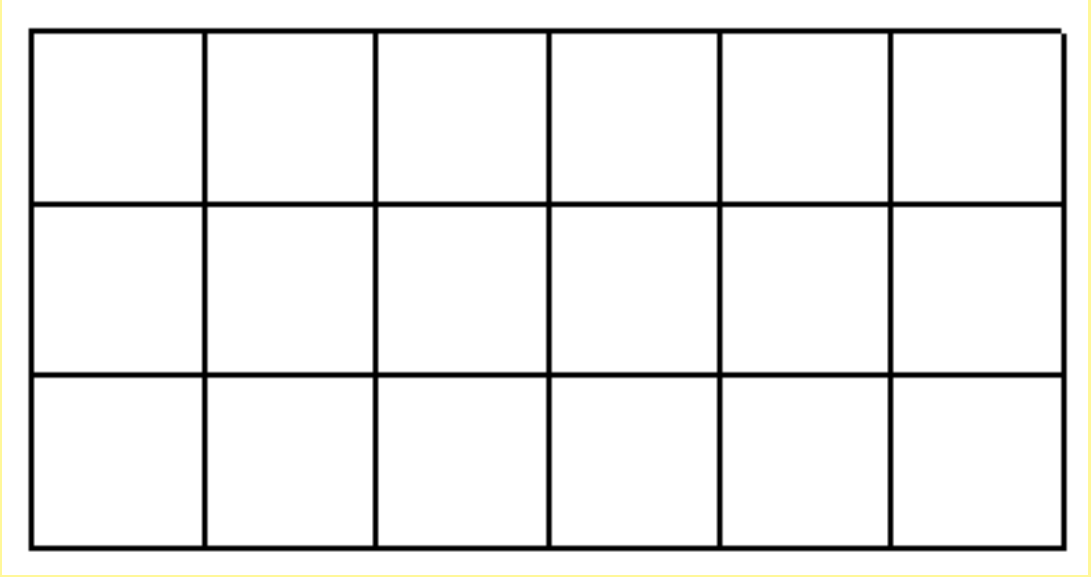
$$p = 3$$



0

$$f(x) = 2^0 3^0 x^6 + 2^3 3^1 x^5 + 2^2 3^1 x^3 - 2^1 3^2 x + 2^2 3^2$$

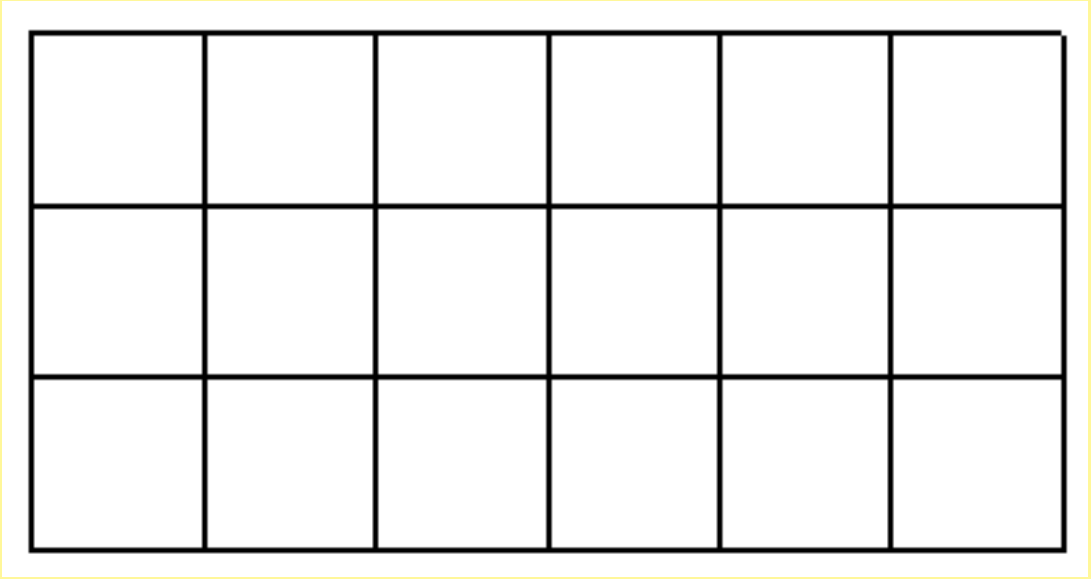
$$p = 3$$



0 1

$$f(x) = 2^0 3^0 x^6 + 2^3 3^1 x^5 + 2^2 3^1 x^3 - 2^1 3^2 x + 2^2 3^2$$

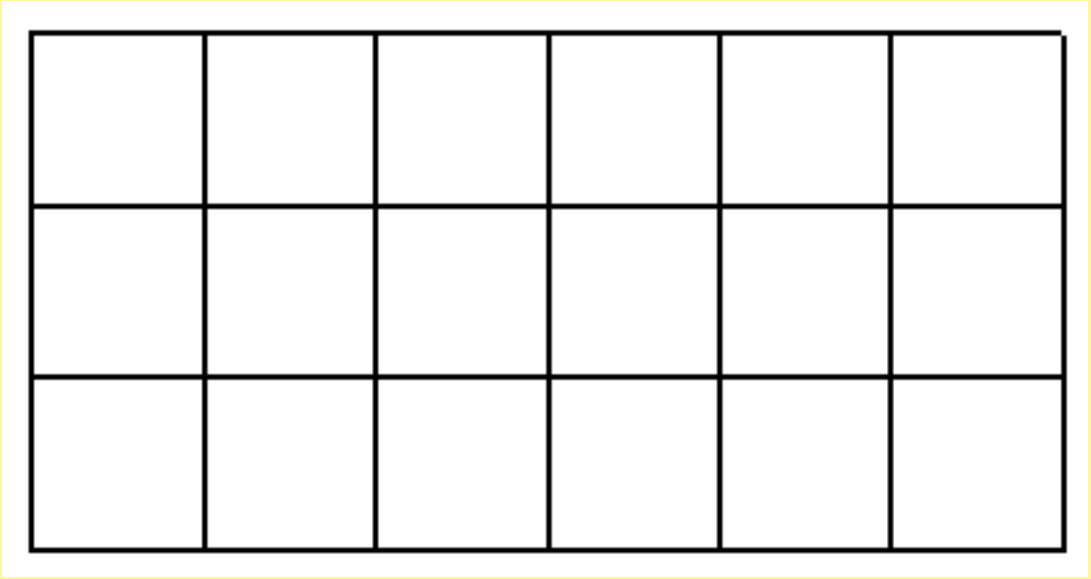
$$p = 3$$



0 1 1

$$f(x) = 2^0 3^0 x^6 + 2^3 3^1 x^5 + 2^2 3^1 x^3 - 2^1 3^2 x + 2^2 3^2$$

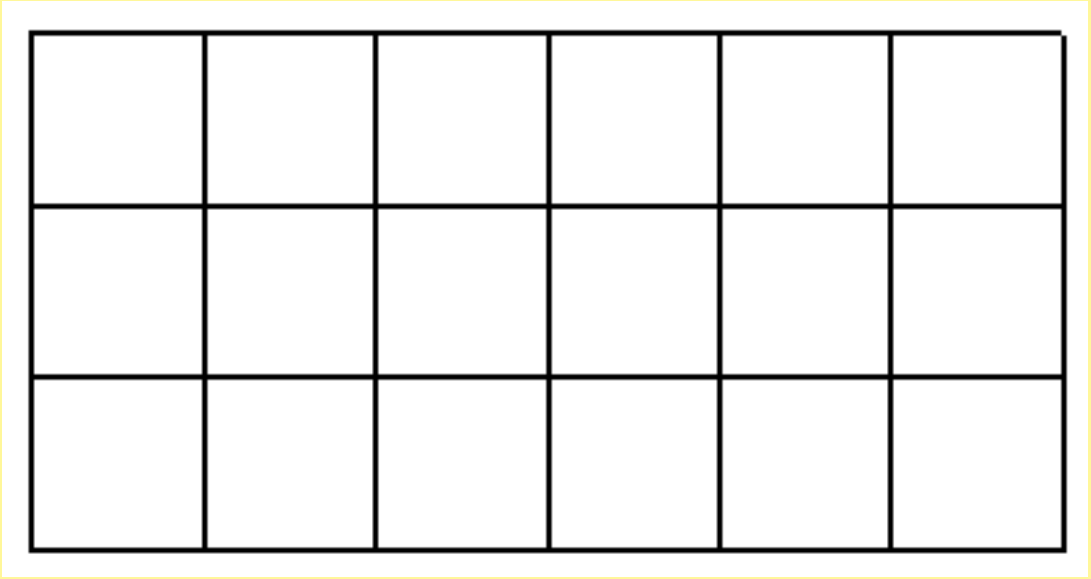
$$p = 3$$



0 1 1 2

$$f(x) = 2^0 3^0 x^6 + 2^3 3^1 x^5 + 2^2 3^1 x^3 - 2^1 3^2 x + 2^2 3^2$$

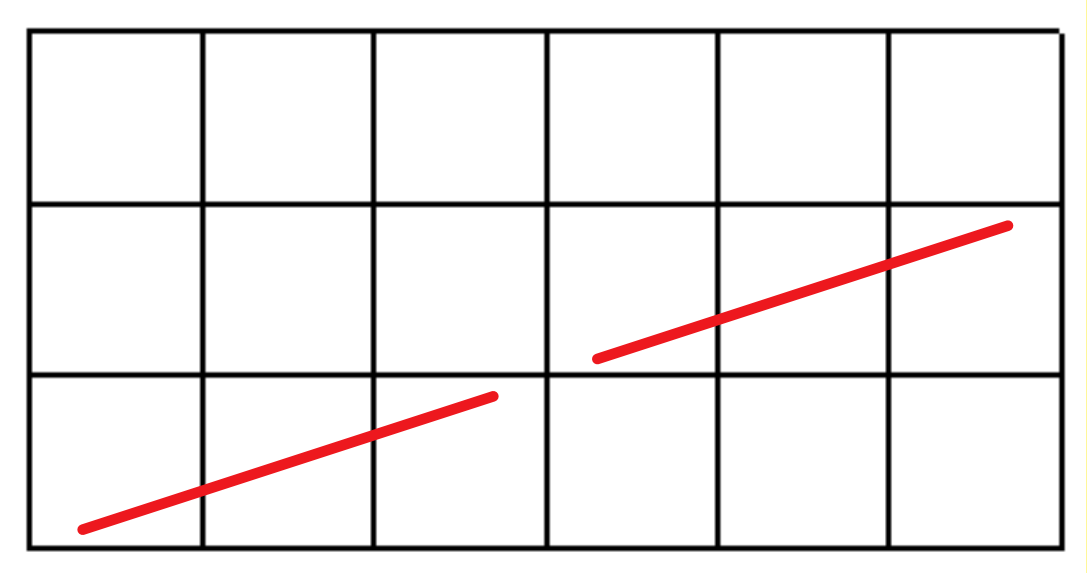
$$p = 3$$



0 1 1 2 2

$$f(x) = 2^0 3^0 x^6 + 2^3 3^1 x^5 + 2^2 3^1 x^3 - 2^1 3^2 x + 2^2 3^2$$

$$p = 3$$



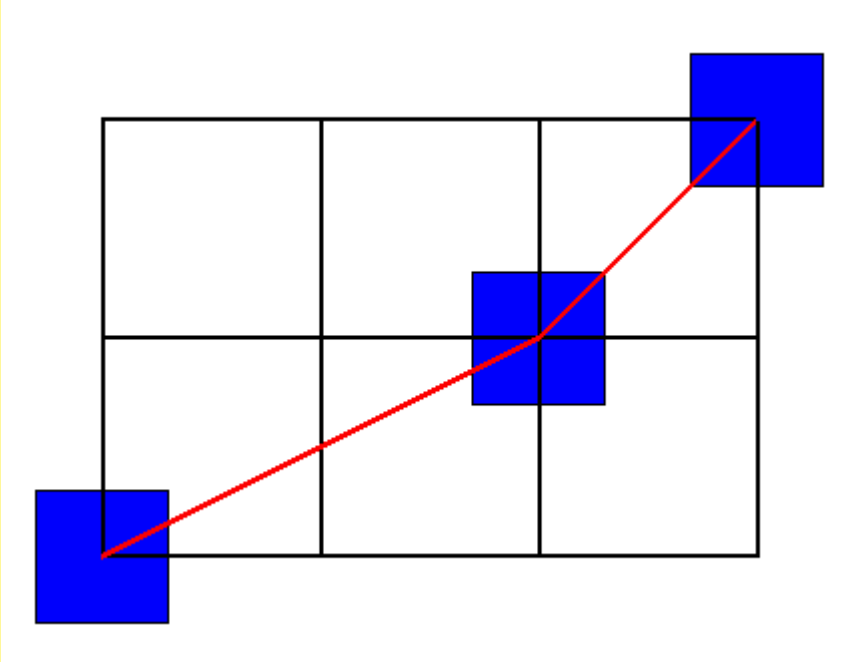
Newton polygon of $f(x)$ with respect to 3

DUMAS' THEOREM

DUMAS' THEOREM . . .

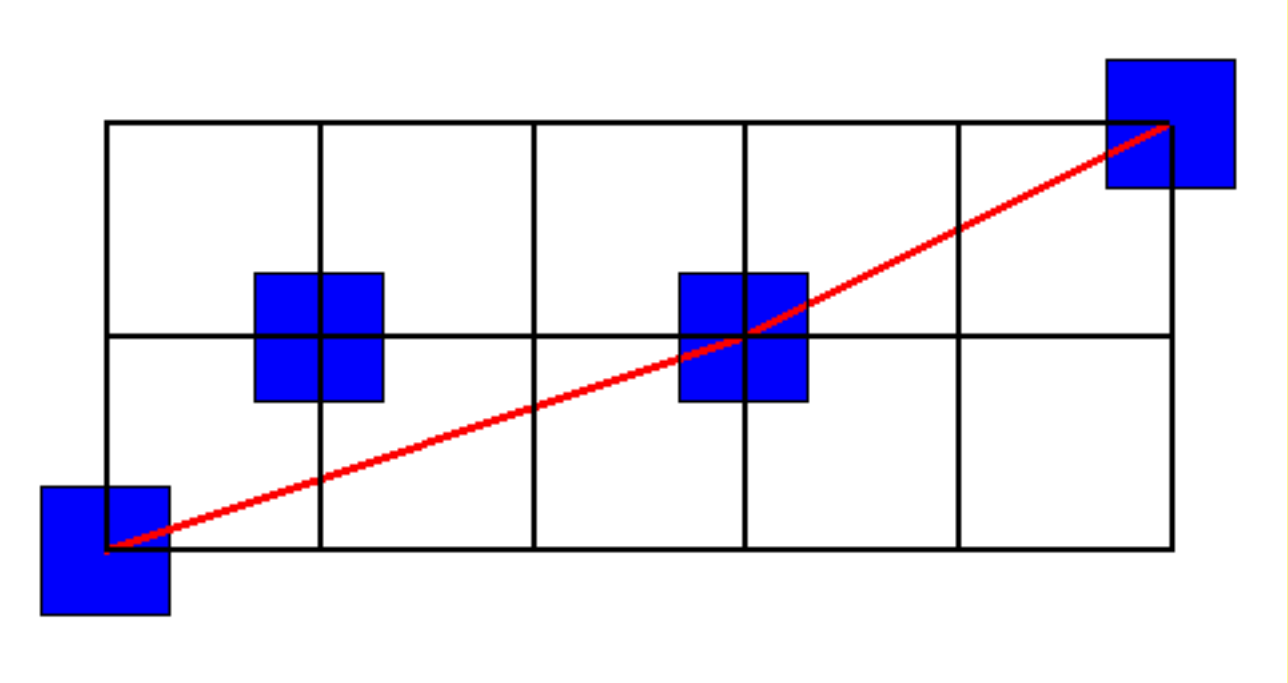
$$g(x) = x^3 + 2x - 4, \;\; h(x) = x^5 - 6x^4 + 2x^2 - 12$$

$$g(x) = x^3 + 2x - 4, \quad h(x) = x^5 - 6x^4 + 2x^2 - 12$$

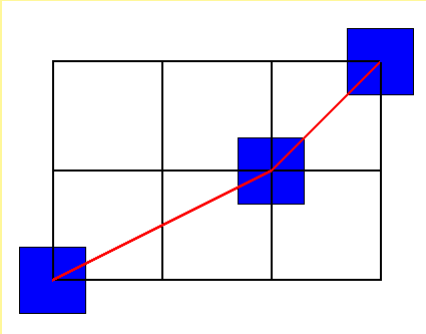


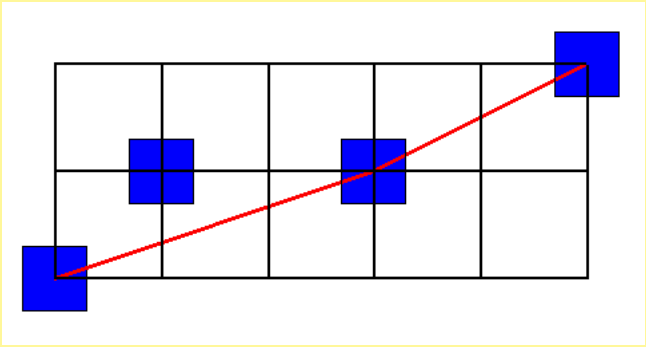
Newton polygon of $g(x)$ with respect to 2

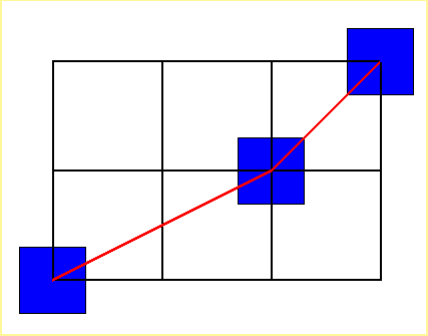
$$g(x) = x^3 + 2x - 4, \;\; h(x) = x^5 - 6x^4 + 2x^2 - 12$$

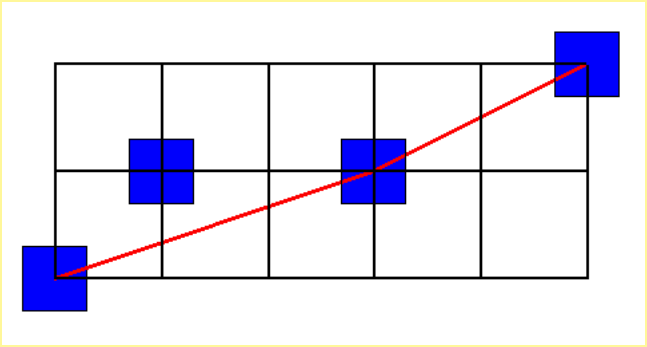


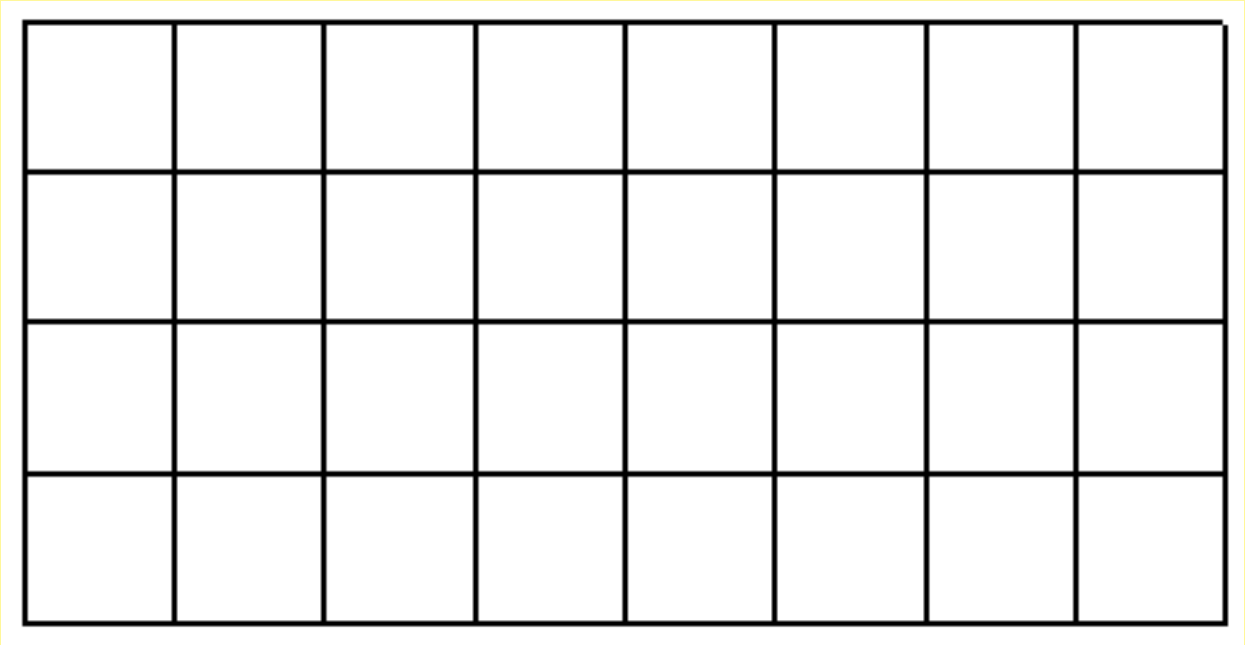
Newton polygon of $h(x)$ with respect to 2



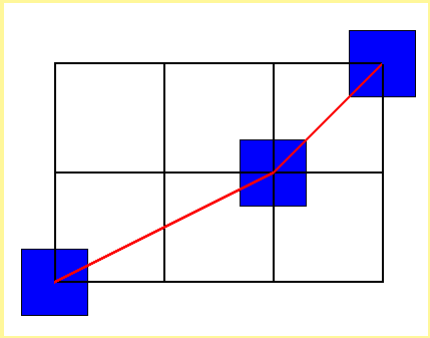


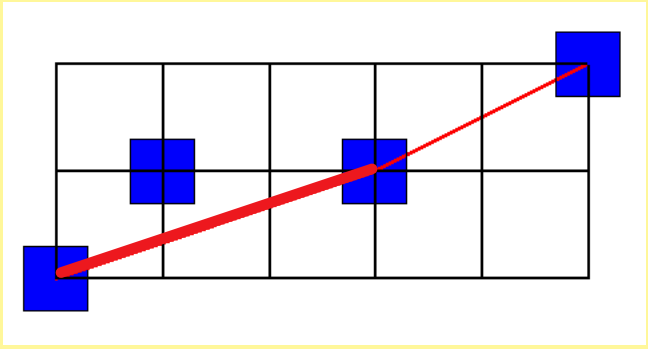


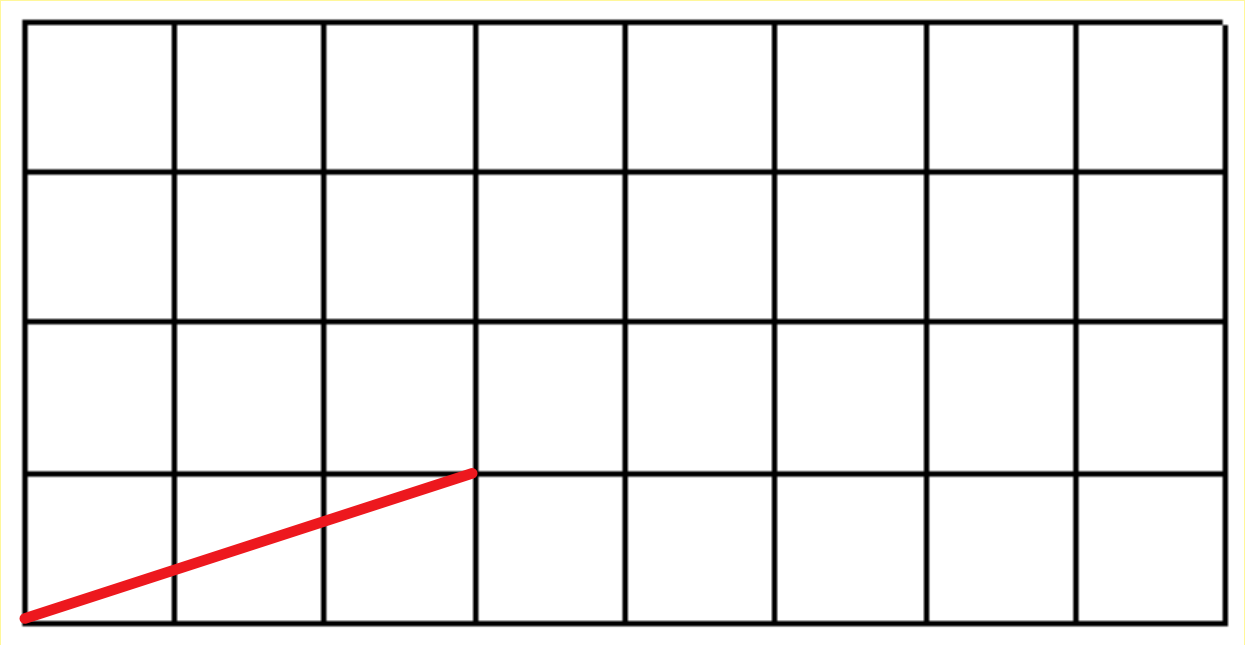




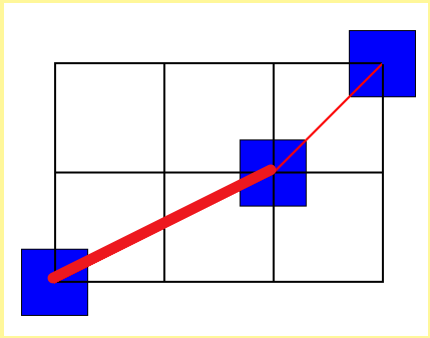
Newton polygon of $g(x)h(x)$ with respect to 2

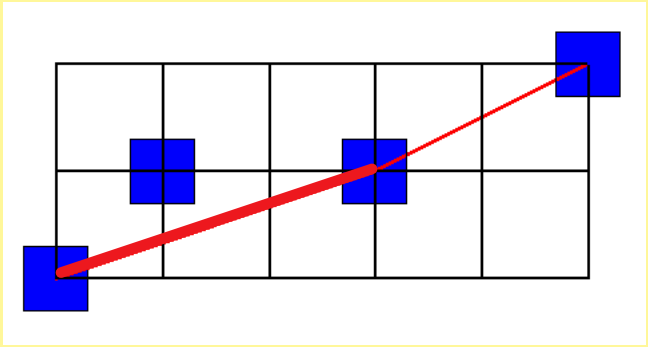


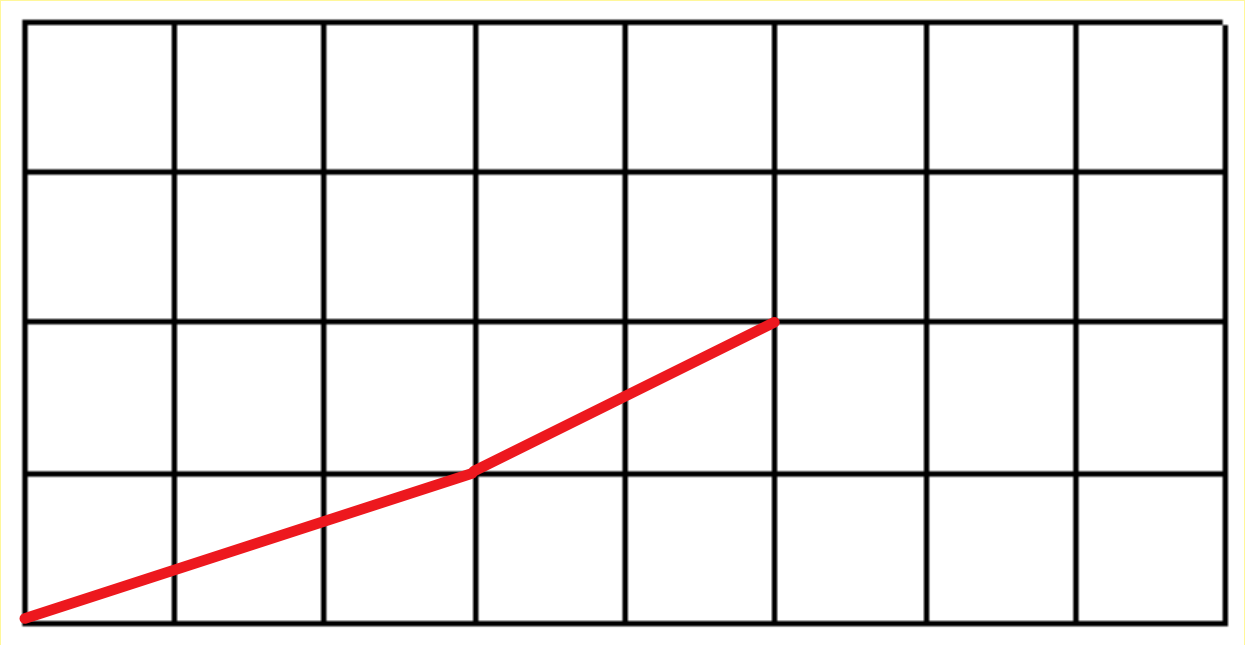




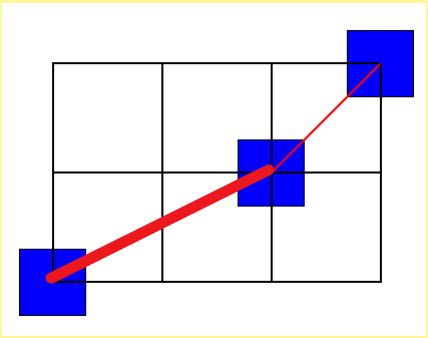
Newton polygon of $g(x)h(x)$ with respect to 2

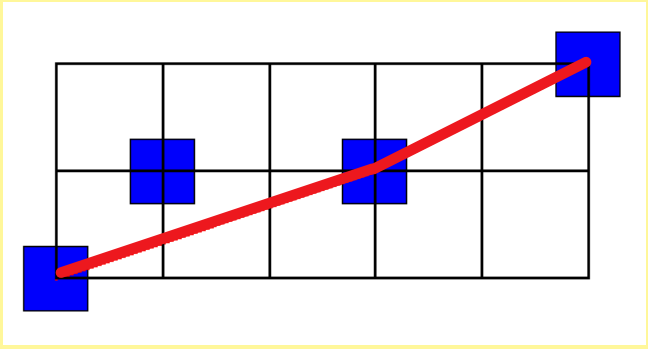


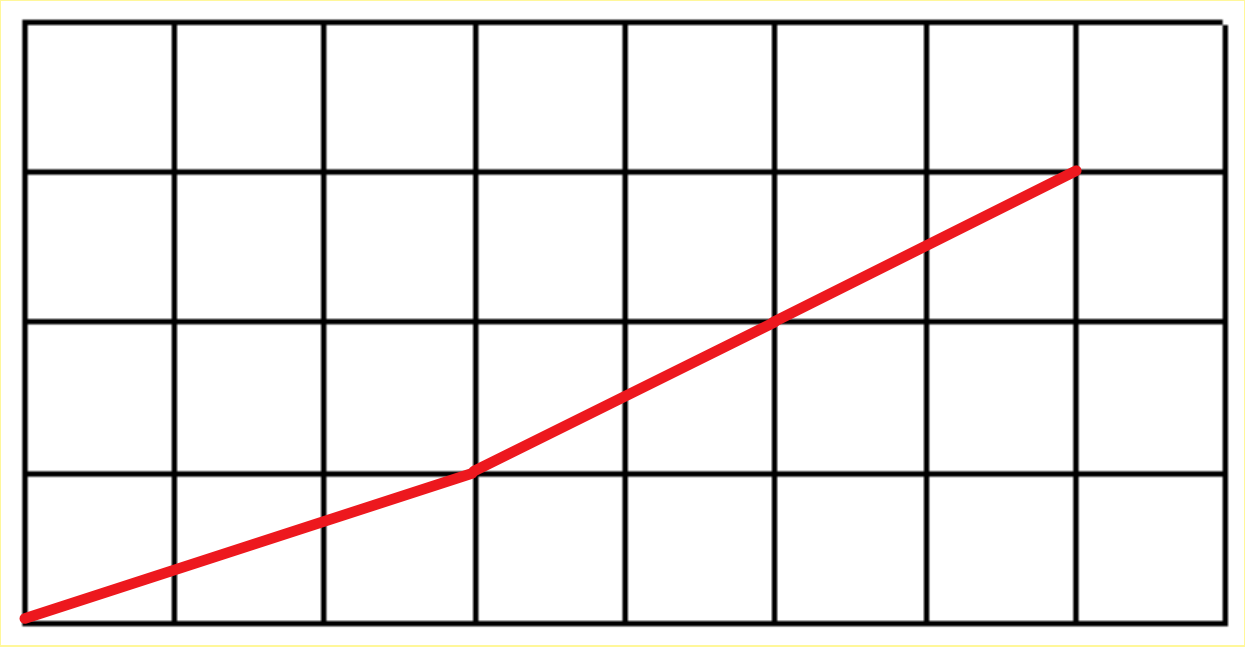




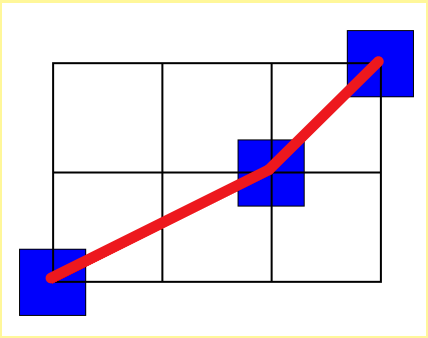
Newton polygon of $g(x)h(x)$ with respect to 2

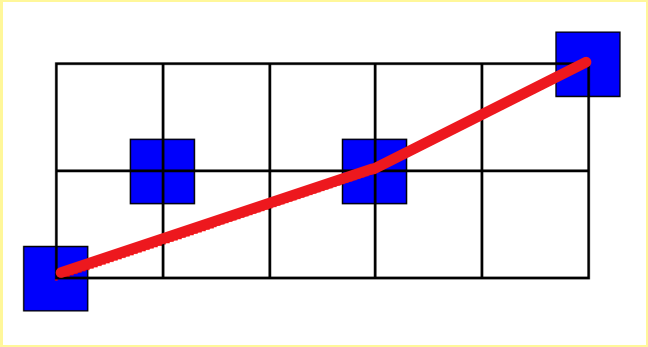


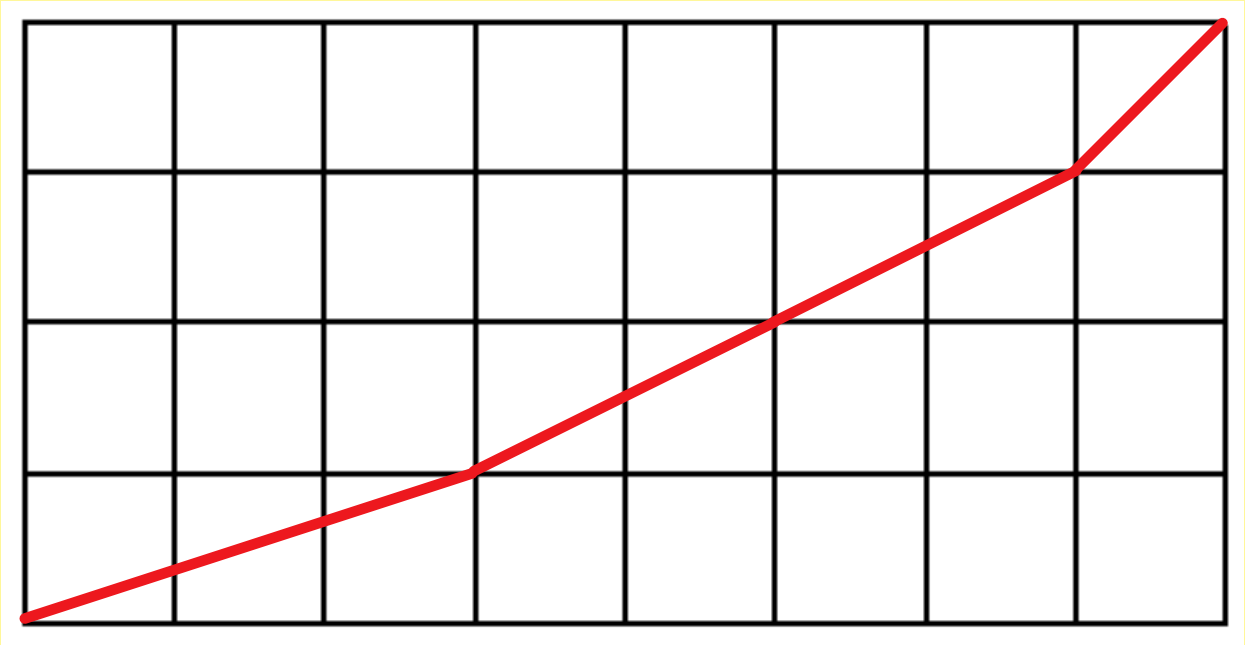




Newton polygon of $g(x)h(x)$ with respect to 2







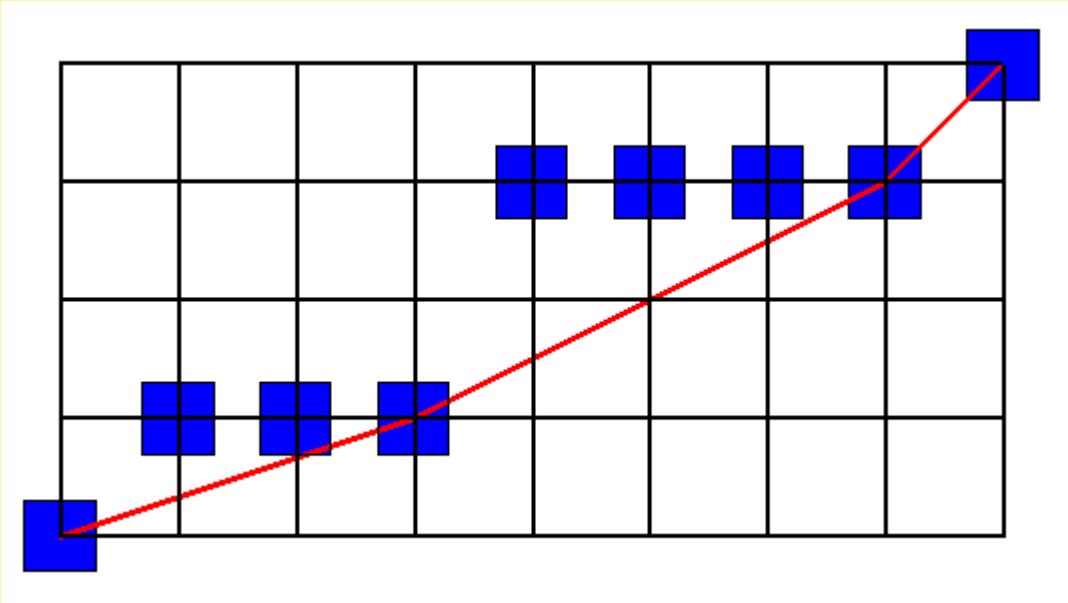
Newton polygon of $g(x)h(x)$ with respect to 2

$$g(x) = x^3 + 2x - 4, \;\; h(x) = x^5 - 6x^4 + 2x^2 - 12$$

$$g(x) = x^3 + 2x - 4, \;\; h(x) = x^5 - 6x^4 + 2x^2 - 12$$

$$f(x) = x^8 - 6x^7 + 2x^6 - 14x^5 + 24x^4 - 8x^3 - 8x^2 - 24x + 48$$

$$f(x) = x^8 - 6x^7 + 2x^6 - 14x^5 + 24x^4 - 8x^3 - 8x^2 - 24x + 48$$



Newton polygon of $f(x)$ with respect to 2

How is Dumas' theorem used to establish irreducibility?

$$f(x) = x^{10} - 7x^8 + 14x^7 - 28x^5 - 49x^2 - 21$$

$$f(x) = x^{10} - 7x^8 + 14x^7 - 28x^5 - 49x^2 - 21$$

Why is $f(x)$ irreducible?

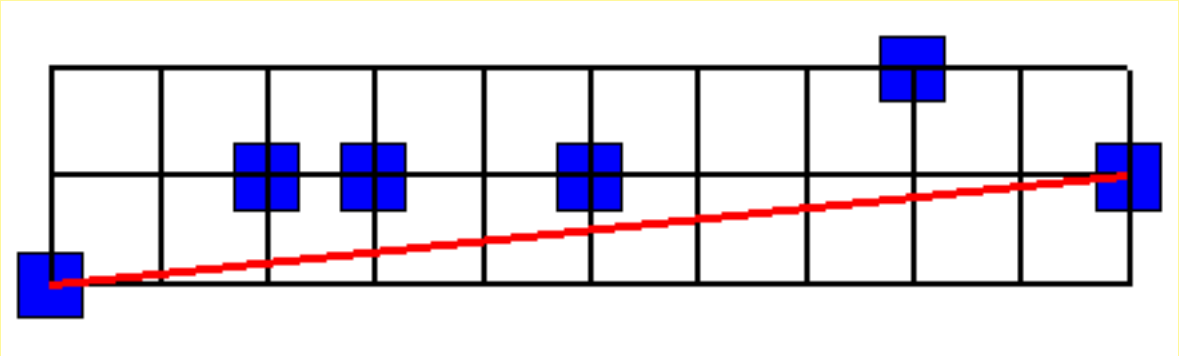
$$f(x) = x^{10} - 7x^8 + 14x^7 - 28x^5 - 49x^2 - 21$$

Why is $f(x)$ irreducible?

Eisenstein's Criterion applies

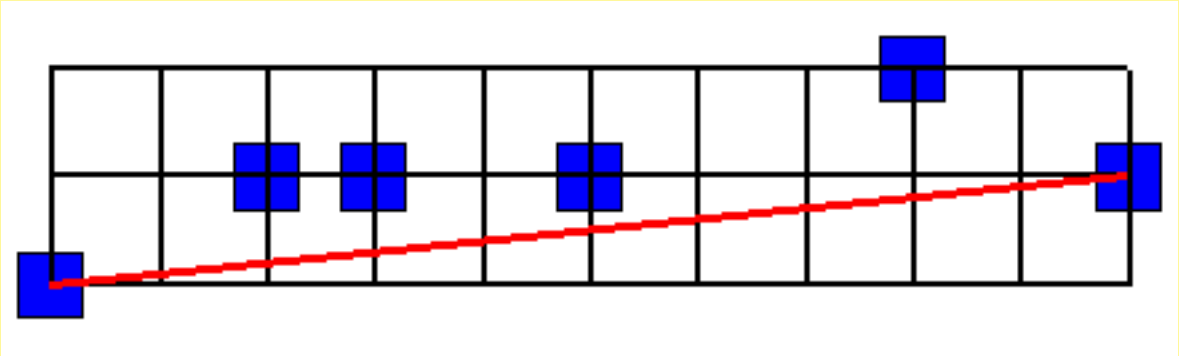
$$f(x) = x^{10} - 7x^8 + 14x^7 - 28x^5 - 49x^2 - 21$$

$$f(x) = x^{10} - 7x^8 + 14x^7 - 28x^5 - 49x^2 - 21$$



Newton polygon of $f(x)$ with respect to 7

$$f(x) = x^{10} - 7x^8 + 14x^7 - 28x^5 - 49x^2 - 21$$

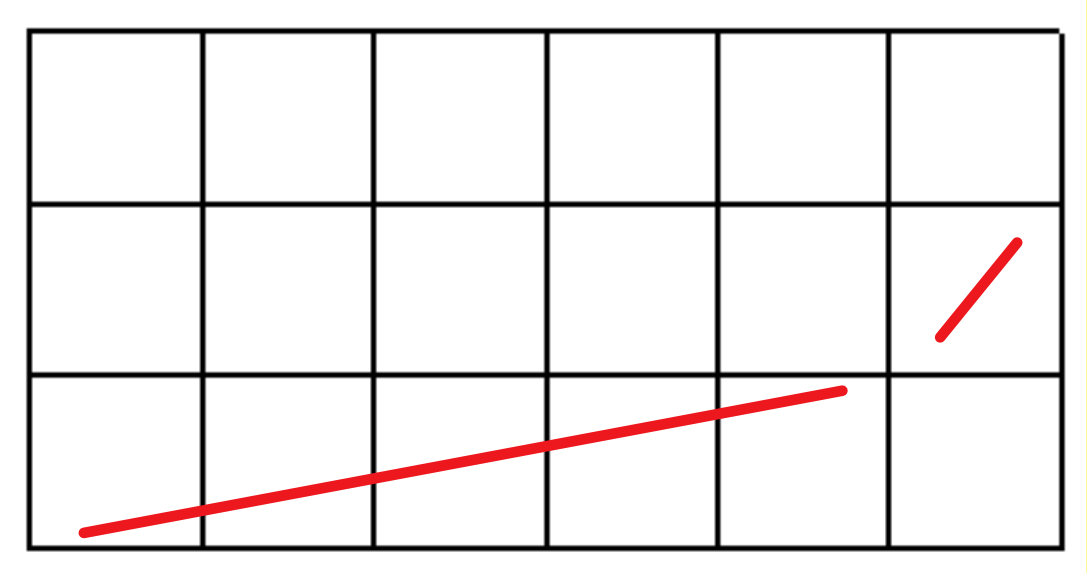


Newton polygon of $f(x)$ with respect to 7

What factors could $f(x)$ have?

$$f(x) = 2^{0}3^{0}x^{6} + 2^{3}3^{1}x^{5} + 2^{2}3^{1}x^{3} - 2^{1}3^{2}x + 2^{2}3^{2}$$

$$p = 2$$

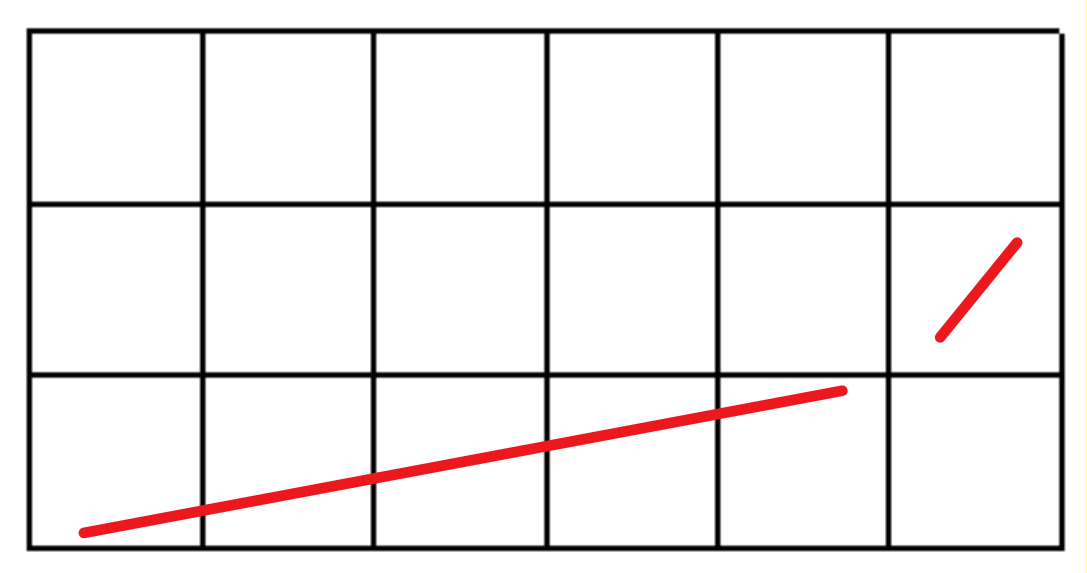


Newton polygon of $f(x)$ with respect to 2

$$f(x) = 2^{0}3^{0}x^{6} + 2^{3}3^{1}x^{5} + 2^{2}3^{1}x^{3} - 2^{1}3^{2}x + 2^{2}3^{2}$$

$$p = 2$$

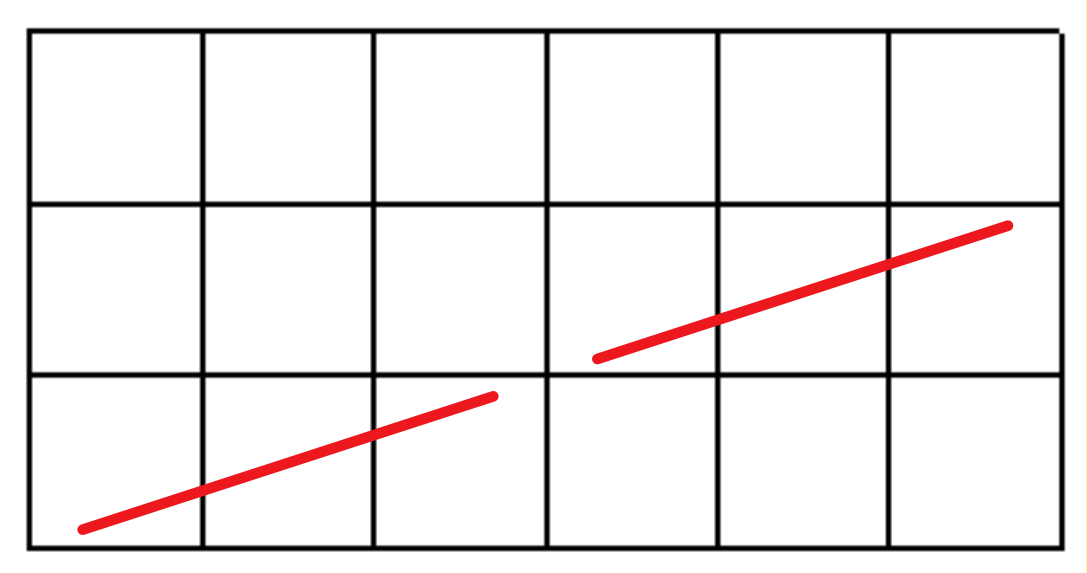
What factors could $f(x)$ have?



Newton polygon of $f(x)$ with respect to 2

$$f(x) = 2^0 3^0 x^6 + 2^3 3^1 x^5 + 2^2 3^1 x^3 - 2^1 3^2 x + 2^2 3^2$$

$$p = 3$$

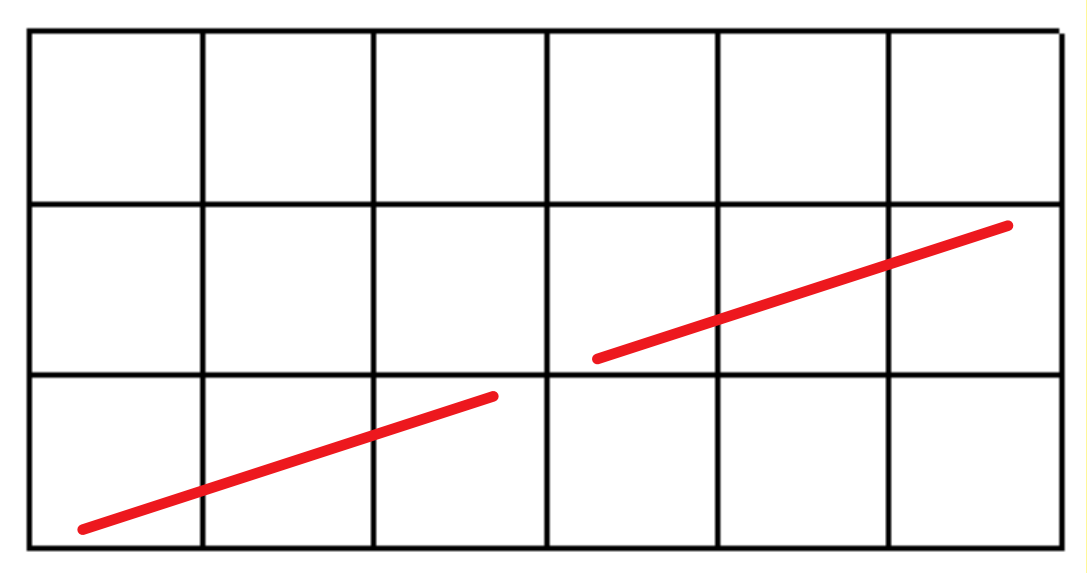


Newton polygon of $f(x)$ with respect to 3

$$f(x) = 2^0 3^0 x^6 + 2^3 3^1 x^5 + 2^2 3^1 x^3 - 2^1 3^2 x + 2^2 3^2$$

$$p = 3$$

What factors could $f(x)$ have?

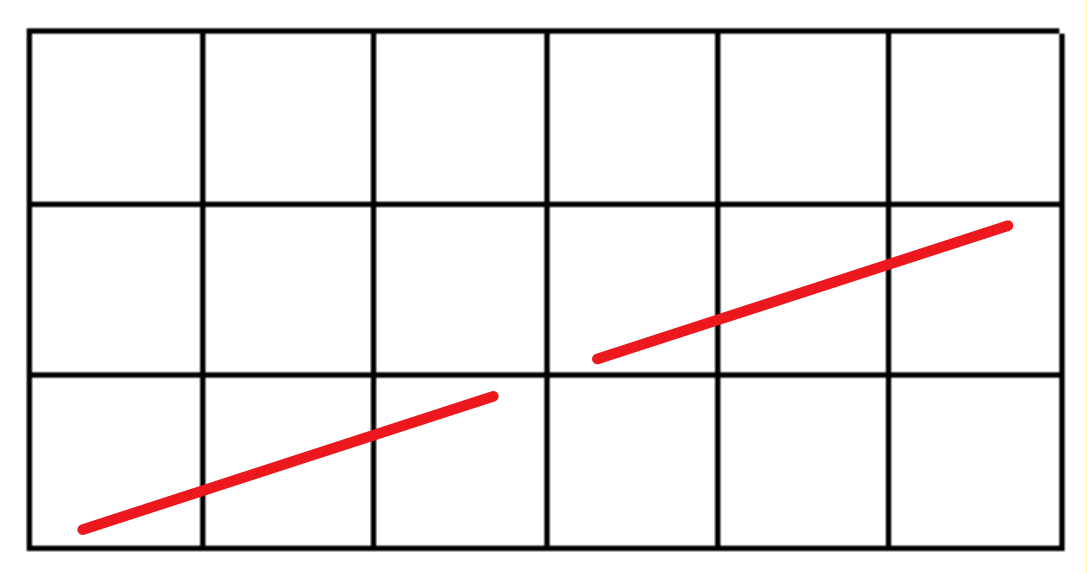


Newton polygon of $f(x)$ with respect to 3

$$f(x) = x^6 + 24\,x^5 + 12\,x^3 - 18\,x + 36$$

$f(x)$ is irreducible

What factors could $f(x)$ have?



Newton polygon of $f(x)$ with respect to 3

MATH 788F

Practice Test Problems

(1) Prove the following:

Let $f(x)$ be a monic polynomial in $\mathbb{Z}[x]$ for which $f(0) \neq 0$. Suppose further that $f(x) = f_1(x)f_2(x)f_3(x)$ where each $f_j(x)$ is irreducible. If

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

where each $\alpha_j \in \mathbb{C}$, then $|\alpha_j| \geq 1$ for at least three values of $j \in \{1, 2, \ldots, n\}$.

(1) Prove the following:

Let $f(x)$ be a monic polynomial in $\mathbb{Z}[x]$ for which $f(0) \neq 0$. Suppose further that $f(x) = f_1(x)f_2(x)f_3(x)$ where each $f_j(x)$ is irreducible. If

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

where each $\alpha_j \in \mathbb{C}$, then $|\alpha_j| \geq 1$ for at least three values of $j \in \{1, 2, \ldots, n\}$.

(1) Prove the following:

Let $f(x)$ be a monic polynomial in $\mathbb{Z}[x]$ for which $f(0) \neq 0$. Suppose further that $f(x) = f_1(x)f_2(x)f_3(x)$ where each $f_j(x)$ is irreducible. If

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

where each $\alpha_j \in \mathbb{C}$, then $|\alpha_j| \geq 1$ for at least three values of $j \in \{1, 2, \ldots, n\}$.

$$f_1(x)f_2(x)f_3(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

(1) Prove the following:

Let $f(x)$ be a monic polynomial in $\mathbb{Z}[x]$ for which $f(0) \neq 0$. Suppose further that $f(x) = f_1(x)f_2(x)f_3(x)$ where each $f_j(x)$ is irreducible. If

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

where each $\alpha_j \in \mathbb{C}$, then $|\alpha_j| \geq 1$ for at least three values of $j \in \{1, 2, \ldots, n\}$.

$$f_1(x)f_2(x)f_3(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

(1) Prove the following:

Let $f(x)$ be a monic polynomial in $\mathbb{Z}[x]$ for which $f(0) \neq 0$. Suppose further that $f(x) = f_1(x)f_2(x)f_3(x)$ where each $f_j(x)$ is irreducible. If

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

where each $\alpha_j \in \mathbb{C}$, then $|\alpha_j| \geq 1$ for at least three values of $j \in \{1, 2, \ldots, n\}$.

Us Too!

$$f_1(x)f_2(x)f_3(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

(1) Prove the following:

Let $f(x)$ be a monic polynomial in $\mathbb{Z}[x]$ for which $f(0) \neq 0$. Suppose further that $f(x) = f_1(x)f_2(x)f_3(x)$ where each $f_j(x)$ is irreducible. If

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

where each $\alpha_j \in \mathbb{C}$, then $|\alpha_j| \geq 1$ for at least three values of $j \in \{1, 2, \ldots, n\}$.

$$f_1(x)f_2(x)f_3(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

(1) Prove the following:

Let $f(x)$ be a monic polynomial in $\mathbb{Z}[x]$ for which $f(0) \neq 0$. Suppose further that $f(x) = f_1(x)f_2(x)f_3(x)$ where each $f_j(x)$ is irreducible. If

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

where each $\alpha_j \in \mathbb{C}$, then $|\alpha_j| \geq 1$ for at least three values of $j \in \{1, 2, \ldots, n\}$.

Us Too!

$f_1(x)f_2(x)f_3(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$

(1) Prove the following:

Let $f(x)$ be a monic polynomial in $\mathbb{Z}[x]$ for which $f(0) \neq 0$. Suppose further that $f(x) = f_1(x)f_2(x)f_3(x)$ where each $f_j(x)$ is irreducible. If

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

where each $\alpha_j \in \mathbb{C}$, then $|\alpha_j| \geq 1$ for at least three values of $j \in \{1, 2, \ldots, n\}$.

Show each $f_j(x)$ has a root with absolute value ≥ 1.

$f_j(x)$ monic in $\mathbb{Z}[x]$, $\quad f_j(0) \neq 0$

$f_j(x)$ monic in $\mathbb{Z}[x]$, $f_j(0) \neq 0$

$$f_j(x) = (x - \alpha'_1)(x - \alpha'_2) \cdots (x - \alpha'_r)$$

$f_j(x)$ monic in $\mathbb{Z}[x]$, $\quad f_j(0) \neq 0$

$$f_j(x) = (x - \alpha'_1)(x - \alpha'_2) \cdots (x - \alpha'_r)$$

$$|f_j(0)| = |\alpha'_1|\,|\alpha'_2| \cdots |\alpha'_r|$$

$f_j(x)$ monic in $\mathbb{Z}[x]$, $\quad f_j(0) \neq 0$

$$f_j(x) = (x - \alpha_1')(x - \alpha_2') \cdots (x - \alpha_r')$$

$$1 \leq |f_j(0)| = |\alpha_1'|\,|\alpha_2'| \cdots |\alpha_r'|$$

$f_j(x)$ monic in $\mathbb{Z}[x]$, $\quad f_j(0) \neq 0$

$$f_j(x) = (x - \alpha'_1)(x - \alpha'_2) \cdots (x - \alpha'_r)$$

$$1 \leq |f_j(0)| = |\alpha'_1|\,|\alpha'_2| \cdots |\alpha'_r|$$

$$\Longrightarrow \quad \text{there exists } j \text{ such that } |\alpha'_j| \geq 1$$

(4) Let

$$f(x) = x^{16} - 8x^{15} - 4x^{14} - 2x^{13} - x^{12} - x^{11} - x^{10} - \cdots - x - 1.$$

(a) Consider $F(x) = (2x - 1)f(x)$. Explain why $F(x)$ has exactly one root α satisfying $|\alpha| \geq 1$.

(b) Explain why this implies that $f(x)$ is irreducible.

(4) Let

$$f(x) = x^{16} - 8x^{15} - 4x^{14} - 2x^{13} - x^{12} - x^{11} - x^{10} - \cdots - x - 1.$$

(a) Consider $F(x) = (2x - 1)f(x)$. Explain why $F(x)$ has exactly one root α satisfying $|\alpha| \geq 1$.

(4) Let

$$f(x) = x^{16} - 8x^{15} - 4x^{14} - 2x^{13} - x^{12} - x^{11} - x^{10} - \cdots - x - 1.$$

$$F(x) = (2x - 1)f(x)$$

(4) Let

$$f(x) = x^{16} - 8x^{15} - 4x^{14} - 2x^{13} - x^{12} - x^{11} - x^{10} - \cdots - x - 1.$$

$$F(x) = (2x - 1)f(x)$$

(4) Let

$$f(x) = x^{16} - 8x^{15} - 4x^{14} - 2x^{13} - x^{12} - x^{11} - x^{10} - \cdots - x - 1.$$

$$F(x) = (2x - 1)f(x) = 2x^{17}$$

(4) Let

$$f(x) = x^{16} - 8x^{15} - 4x^{14} - 2x^{13} - x^{12} - x^{11} - x^{10} - \cdots - x - 1.$$

$$\begin{aligned} F(x) &= (2x-1)f(x) \\ &= 2x^{17} \end{aligned}$$

(4) Let

$$f(x) = x^{16} - 8x^{15} - 4x^{14} - 2x^{13} - x^{12} - x^{11} - x^{10} - \cdots - x - 1.$$

$$F(x) = (2x - 1)f(x)$$
$$= 2x^{17}$$

(4) Let

$$f(x) = x^{16} - 8x^{15} - 4x^{14} - 2x^{13} - x^{12} - x^{11} - x^{10} - \cdots - x - 1.$$

$$F(x) = (2x - 1)f(x)$$
$$= 2x^{17}$$

(4) Let

$$f(x) = x^{16} - 8x^{15} - 4x^{14} - 2x^{13} - x^{12} - x^{11} - x^{10} - \cdots - x - 1.$$

$$\begin{aligned} F(x) &= (2x-1)f(x) \\ &= 2x^{17} - 17x^{16} \end{aligned}$$

(4) Let

$$f(x) = x^{16} - 8x^{15} - 4x^{14} - 2x^{13} - x^{12} - x^{11} - x^{10} - \cdots - x - 1.$$

$$\begin{aligned} F(x) &= (2x-1)f(x) \\ &= 2x^{17} - 17x^{16} - x^{12} \end{aligned}$$

(4) Let

$$f(x) = x^{16} - 8x^{15} - 4x^{14} - 2x^{13} - x^{12} - x^{11} - x^{10} - \cdots - x - 1.$$

$$\begin{aligned} F(x) &= (2x-1)f(x) \\ &= 2x^{17} - 17x^{16} - x^{12} - x^{11} - \cdots - x \end{aligned}$$

(4) Let

$$f(x) = x^{16} - 8x^{15} - 4x^{14} - 2x^{13} - x^{12} - x^{11} - x^{10} - \cdots - x - 1.$$

$$\begin{aligned} F(x) &= (2x-1)f(x) \\ &= 2x^{17} - 17x^{16} - x^{12} - x^{11} - \cdots - x + 1 \end{aligned}$$

$$\begin{aligned} F(x) &= (2x-1)f(x) \\ &= 2x^{17} - 17x^{16} - x^{12} - x^{11} - \cdots - x + 1 \end{aligned}$$

$$\begin{aligned} F(x) &= (2x-1)f(x) \\ &= 2x^{17} - 17x^{16} - x^{12} - x^{11} - \cdots - x + 1 \end{aligned}$$

Lemma 2. Let $f(x)$ and $g(x)$ be polynomials in $\mathbb{C}[x]$, and let $\mathcal{C} = \{z \in \mathbb{C} : |z| = 1\}$. If the strict inequality $|f(z) + g(z)| < |f(z)| + |g(z)|$ holds for each $z \in \mathcal{C}$, then $f(x)$ and $g(x)$ have the same total number of zeroes (counting multiplicity) inside the circle $\mathcal{C}$ (i.e., in the interior of the region bounded by $\mathcal{C}$).

$$
\begin{aligned}
F(x) &= (2x-1)f(x) \\
&= 2x^{17} - 17x^{16} - x^{12} - x^{11} - \cdots - x + 1 \\
G(x) &= 17x^{16}
\end{aligned}
$$

$$F(x) = (2x-1)f(x)$$
$$= 2x^{17} - 17x^{16} - x^{12} - x^{11} - \cdots - x + 1$$

$$G(x) = 17x^{16}$$

$$|F(z) + G(z)|$$

$$F(x) = (2x-1)f(x)$$
$$= 2x^{17} - 17x^{16} - x^{12} - x^{11} - \cdots - x + 1$$

$$G(x) = 17x^{16}$$

$$|F(z) + G(z)| = |2z^{17} - z^{12} - \cdots - z + 1|$$

$$
\begin{aligned}
F(x) &= (2x-1)f(x) \\
&= 2x^{17} - 17x^{16} - x^{12} - x^{11} - \cdots - x + 1 \\
G(x) &= 17x^{16}
\end{aligned}
$$

$$
\begin{aligned}
|F(z) + G(z)| &= |2z^{17} - z^{12} - \cdots - z + 1| \\
&\leq 2|z|^{17} + |z|^{12} + \cdots + |z| + 1
\end{aligned}
$$

$$
\begin{aligned}
F(x) &= (2x-1)f(x) \\
&= 2x^{17} - 17x^{16} - x^{12} - x^{11} - \cdots - x + 1 \\
G(x) &= 17x^{16}
\end{aligned}
$$

$$
\begin{aligned}
|F(z) + G(z)| &= |2z^{17} - z^{12} - \cdots - z + 1| \\
&\le 2|z|^{17} + |z|^{12} + \cdots + |z| + 1 \\
&\le 2 + 1 + \cdots + 1 + 1
\end{aligned}
$$

$$
\begin{aligned}
F(x) &= (2x-1)f(x) \\
&= 2x^{17} - 17x^{16} - x^{12} - x^{11} - \cdots - x + 1 \\
G(x) &= 17x^{16}
\end{aligned}
$$

$$
\begin{aligned}
|F(z) + G(z)| &= |2z^{17} - z^{12} - \cdots - z + 1| \\
&\le 2|z|^{17} + |z|^{12} + \cdots + |z| + 1 \\
&\le 2 + 1 + \cdots + 1 + 1 = 15
\end{aligned}
$$

$$
\begin{aligned}
F(x) &= (2x-1)f(x) \\
&= 2x^{17} - 17x^{16} - x^{12} - x^{11} - \cdots - x + 1 \\
G(x) &= 17x^{16}
\end{aligned}
$$

$$
\begin{aligned}
|F(z) + G(z)| &= |2z^{17} - z^{12} - \cdots - z + 1| \\
&\le 2|z|^{17} + |z|^{12} + \cdots + |z| + 1 \\
&\le 2 + 1 + \cdots + 1 + 1 = 15 \\
&< 17|z|^{17}
\end{aligned}
$$

$$
\begin{aligned}
F(x) &= (2x-1)f(x) \\
&= 2x^{17} - 17x^{16} - x^{12} - x^{11} - \cdots - x + 1 \\
G(x) &= 17x^{16}
\end{aligned}
$$

$$
\begin{aligned}
|F(z) + G(z)| &= |2z^{17} - z^{12} - \cdots - z + 1| \\
&\le 2|z|^{17} + |z|^{12} + \cdots + |z| + 1 \\
&\le 2 + 1 + \cdots + 1 + 1 = 15 \\
&< 17|z|^{17} \\
&= |G(z)|
\end{aligned}
$$

$$F(x) = (2x-1)f(x)$$
$$= 2x^{17} - 17x^{16} - x^{12} - x^{11} - \cdots - x + 1$$

$$G(x) = 17x^{16}$$

$$\begin{aligned} |F(z) + G(z)| &= |2z^{17} - z^{12} - \cdots - z + 1| \\ &\le 2|z|^{17} + |z|^{12} + \cdots + |z| + 1 \\ &\le 2 + 1 + \cdots + 1 + 1 = 15 \\ &< 17|z|^{17} \\ &= |G(z)| \le |F(z)| + |G(z)| \end{aligned}$$

$$F(x) = (2x-1)f(x)$$
$$= 2x^{17} - 17x^{16} - x^{12} - x^{11} - \cdots - x + 1$$

$$G(x) = 17x^{16}$$

$$\begin{aligned} |F(z) + G(z)| &= |2z^{17} - z^{12} - \cdots - z + 1| \\ &\le 2|z|^{17} + |z|^{12} + \cdots + |z| + 1 \\ &\le 2 + 1 + \cdots + 1 + 1 = 15 \\ &< 17|z|^{17} \\ &= |G(z)| \le |F(z)| + |G(z)| \end{aligned}$$

$$F(x) = (2x-1)f(x)$$
$$= 2x^{17} - 17x^{16} - x^{12} - x^{11} - \cdots - x + 1$$
$$G(x) = 17x^{16}$$

Since $G(x)$ has exactly 16 zeroes in

$$\mathcal{C} = \{z \in \mathbb{C} : |z| = 1\},$$

so does $F(x)$.

$$F(x) = (2x-1)f(x)$$
$$= 2x^{17} - 17x^{16} - x^{12} - x^{11} - \cdots - x + 1$$

$$G(x) = 17x^{16}$$

Since $G(x)$ has exactly 16 zeroes in

$$\mathcal{C} = \{z \in \mathbb{C} : |z| = 1\},$$

so does $F(x)$. Hence, $F(x)$ has exactly one root with absolute value ≥ 1.

$$F(x) = (2x-1)f(x)$$
$$= 2x^{17} - 17x^{16} - x^{12} - x^{11} - \cdots - x + 1$$

$$G(x) = 17x^{16}$$

Since $G(x)$ has exactly 16 zeroes in

$$\mathcal{C} = \{z \in \mathbb{C} : |z| = 1\},$$

so does $F(x)$. Hence, $F(x)$ has exactly one root with absolute value ≥ 1.

$$F(x) = (2x-1)f(x)$$
$$= 2x^{17} - 17x^{16} - x^{12} - x^{11} - \cdots - x + 1$$

$$G(x) = 17x^{16}$$

Since $G(x)$ has exactly 16 zeroes in

$$\mathcal{C} = \{z \in \mathbb{C} : |z| = 1\},$$

so does $F(x)$. Hence, $f(x)$ has exactly one root with absolute value ≥ 1.

So why is $f(x)$ irreducible?

So why is $f(x)$ irreducible?

Lemma 1. Let $f(x)$ be a monic polynomial in $\mathbb{Z}[x]$ for which $f(0) \neq 0$. Suppose further that $f(x)$ has exactly 1 root α (with multiplicity 1) such that $|\alpha| \geq 1$. Then $f(x)$ is irreducible.

So why is $f(x)$ irreducible?

Lemma 1. Let $f(x)$ be a monic polynomial in $\mathbb{Z}[x]$ for which $f(0) \neq 0$. Suppose further that $f(x)$ has exactly 1 root α (with multiplicity 1) such that $|\alpha| \geq 1$. Then $f(x)$ is irreducible.

$$f(x) = x^{16} - 8x^{15} - 4x^{14} - 2x^{13} \\ - x^{12} - x^{11} - x^{10} - \cdots - x - 1$$

So why is $f(x)$ irreducible?

Lemma 1. Let $f(x)$ be a monic polynomial in $\mathbb{Z}[x]$ for which $f(0) \neq 0$. Suppose further that $f(x)$ has exactly 1 root α (with multiplicity 1) such that $|\alpha| \geq 1$. Then $f(x)$ is irreducible.

$$f(x) = x^{16} - 8x^{15} - 4x^{14} - 2x^{13} \\ - x^{12} - x^{11} - x^{10} - \cdots - x - 1$$

So why is $f(x)$ irreducible?

Lemma 1. Let $f(x)$ be a monic polynomial in $\mathbb{Z}[x]$ for which $f(0) \neq 0$. Suppose further that $f(x)$ has exactly 1 root α (with multiplicity 1) such that $|\alpha| \geq 1$. Then $f(x)$ is irreducible.

$$f(x) = x^{16} - 8x^{15} - 4x^{14} - 2x^{13} \\ - x^{12} - x^{11} - x^{10} - \cdots - x - 1$$

So why is $f(x)$ irreducible?

Lemma 1. Let $f(x)$ be a monic polynomial in $\mathbb{Z}[x]$ for which $f(0) \neq 0$. Suppose further that $f(x)$ has exactly 1 root α (with multiplicity 1) such that $|\alpha| \geq 1$. Then $f(x)$ is irreducible.

$$f(x) = x^{16} - 8x^{15} - 4x^{14} - 2x^{13} \\ - x^{12} - x^{11} - x^{10} - \cdots - x - 1$$

So why is $f(x)$ irreducible?

Lemma 1. Let $f(x)$ be a monic polynomial in $\mathbb{Z}[x]$ for which $f(0) \neq 0$. Suppose further that $f(x)$ has exactly 1 root α (with multiplicity 1) such that $|\alpha| \geq 1$. Then $f(x)$ is irreducible.

$$f(x) = x^{16} - 8x^{15} - 4x^{14} - 2x^{13} \\ - x^{12} - x^{11} - x^{10} - \cdots - x - 1$$

(5) For p a prime, prove that the Bernoulli polynomial $B_{(2p-1)(p-1)}(x)$ is irreducible.

(5) For p a prime, prove that the Bernoulli polynomial $B_{(2p-1)(p-1)}(x)$ is irreducible.

Idea: Take $m = (2p-1)(p-1)$, and show that

$$p\widetilde{B}_m(x) = \sum_{j=0}^{m} pB_j \binom{m}{j} x^j$$

is a rational number times a polynomial in Eisenstein form with respect to p.

$$m = (2p-1)(p-1), \quad f(x) = \sum_{j=0}^{m} pB_j \binom{m}{j} x^j$$

$$m = (2p-1)(p-1), \quad f(x) = \sum_{j=0}^{m} pB_j \binom{m}{j} x^j$$

The Leading Coefficient is $\boxed{}$.

$$m = (2p-1)(p-1), \quad f(x) = \sum_{j=0}^{m} pB_j \binom{m}{j} x^j$$

The Leading Coefficient is $\boxed{pB_m}$.

$$m = (2p-1)(p-1), \quad f(x) = \sum_{j=0}^{m} pB_j \binom{m}{j} x^j$$

The Leading Coefficient is $\boxed{pB_m}$.

Use that $(p-1)|m$ implies B_m is a rational number which when reduced has denominator divisible by p but not by p^2.

$$m = (2p-1)(p-1), \quad f(x) = \sum_{j=0}^{m} pB_j \binom{m}{j} x^j$$

The Leading Coefficient is $\boxed{pB_m}$.

Use that $(p-1)|m$ implies B_m is a rational number which when reduced has denominator divisible by p but not by p^2.

The Constant Term is $\boxed{}$.

$$m = (2p-1)(p-1), \quad f(x) = \sum_{j=0}^{m} pB_j \binom{m}{j} x^j$$

The Leading Coefficient is $\boxed{pB_m}$.

Use that $(p-1)|m$ implies B_m is a rational number which when reduced has denominator divisible by p but not by p^2.

The Constant Term is $\boxed{p}$.

$$m = (2p-1)(p-1), \quad f(x) = \sum_{j=0}^{m} pB_j \binom{m}{j} x^j$$

The Leading Coefficient is $\boxed{pB_m}$.

Use that $(p-1)|m$ implies B_m is a rational number which when reduced has denominator divisible by p but not by p^2.

The Constant Term is $\boxed{p}$.

So p divides the constant term and p^2 does not.

$$m = (2p-1)(p-1), \quad f(x) = \sum_{j=0}^{m} pB_j \binom{m}{j} x^j$$

Other Terms where $(p-1) \nmid j$:

$$m = (2p-1)(p-1), \quad f(x) = \sum_{j=0}^{m} pB_j \binom{m}{j} x^j$$

Other Terms where $(p-1) \nmid j$:

Use that B_j is a rational number which when reduced has both numerator and denominator *not* divisible by p.

$$m = (2p-1)(p-1), \quad f(x) = \sum_{j=0}^{m} pB_j \binom{m}{j} x^j$$

Other Terms where $(p-1) \nmid j$:

Use that B_j is a rational number which when reduced has both numerator and denominator *not* divisible by p.

Other Terms where $(p-1)|j$:

$$m = (2p-1)(p-1), \quad f(x) = \sum_{j=0}^{m} pB_j \binom{m}{j} x^j$$

Other Terms where $(p-1) \nmid j$:

Use that B_j is a rational number which when reduced has both numerator and denominator *not* divisible by p.

Other Terms where $(p-1)|j$:

Panic and hope for partial credit.

$$m = (2p-1)(p-1), \quad f(x) = \sum_{j=0}^{m} pB_j \binom{m}{j} x^j$$

Other Terms where $(p-1) \nmid j$:

Use that B_j is a rational number which when reduced has both numerator and denominator *not* divisible by p.

Other Terms where $(p-1)|j$:

Panic and hope for partial credit or use the lemma on the power of p dividing a factorial.

$$m = (2p-1)(p-1), \quad f(x) = \sum_{j=0}^{m} pB_j \binom{m}{j} x^j$$

Other Terms where $(p-1)|j$:

$$m = (2p-1)(p-1), \quad f(x) = \sum_{j=0}^{m} pB_j \binom{m}{j} x^j$$

Other Terms where $(p-1)|j$:

$$m = 2p^2 - 3p + 1$$

$$m = (2p-1)(p-1), \quad f(x) = \sum_{j=0}^{m} pB_j \binom{m}{j} x^j$$

Other Terms where $(p-1)|j$:

$$m = 2p^2 - 3p + 1 = p^2 + (p-3)p + 1$$

$$m = (2p-1)(p-1), \quad f(x) = \sum_{j=0}^{m} pB_j \binom{m}{j} x^j$$

Other Terms where $(p-1)|j$:

$$m = 2p^2 - 3p + 1 = p^2 + (p-3)p + 1$$

$s(m) = p-1$

$$m = (2p-1)(p-1), \quad f(x) = \sum_{j=0}^{m} pB_j \binom{m}{j} x^j$$

Other Terms where $(p-1)|j$:

$$m = 2p^2 - 3p + 1 = p^2 + (p-3)p + 1$$

$$s(m) = p-1 \implies \nu_p(m!) =$$

$$m = (2p-1)(p-1), \quad f(x) = \sum_{j=0}^{m} pB_j \binom{m}{j} x^j$$

Other Terms where $(p-1)|j$:

$$m = 2p^2 - 3p + 1 = p^2 + (p-3)p + 1$$

$$s(m) = p-1 \implies \nu_p(m!) = \frac{m - s(m)}{p-1}$$

$$m = (2p-1)(p-1), \quad f(x) = \sum_{j=0}^{m} pB_j \binom{m}{j} x^j$$

Other Terms where $(p-1)|j$:

$$m = 2p^2 - 3p + 1 = p^2 + (p-3)p + 1$$

$$s(m) = p-1 \implies \nu_p(m!) = \frac{m - s(m)}{p-1} = 2p-2$$

$$m = (2p-1)(p-1), \quad f(x) = \sum_{j=0}^{m} pB_j \binom{m}{j} x^j$$

Other Terms where $(p-1)|j$:

$$\nu_p(m!) = 2p-2$$

$$m = (2p-1)(p-1), \quad f(x) = \sum_{j=0}^{m} pB_j \binom{m}{j} x^j$$

Other Terms where $(p-1)|j$:

$$\nu_p(m!) = 2p-2$$

$$\nu_p(j!) = \frac{j - s(j)}{p-1}$$

$$m = (2p-1)(p-1), \quad f(x) = \sum_{j=0}^{m} pB_j \binom{m}{j} x^j$$

Other Terms where $(p-1)|j$:

$$\nu_p(m!) = 2p-2$$

$$\nu_p(j!) = \frac{j - s(j)}{p-1} < \frac{j}{p-1}$$

$$m = (2p-1)(p-1), \quad f(x) = \sum_{j=0}^{m} pB_j \binom{m}{j} x^j$$

Other Terms where $(p-1)|j$:

$$\nu_p(m!) = 2p-2$$

$$\nu_p(j!) = \frac{j - s(j)}{p-1} < \frac{j}{p-1} \implies \nu_p(j!) \leq$$

$$m = (2p-1)(p-1), \quad f(x) = \sum_{j=0}^{m} pB_j \binom{m}{j} x^j$$

Other Terms where $(p-1)|j$:

$$\nu_p(m!) = 2p-2$$

$$\nu_p(j!) = \frac{j - s(j)}{p-1} < \frac{j}{p-1} \implies \nu_p(j!) \leq \frac{j}{p-1} - 1$$

$$m = (2p-1)(p-1), \quad f(x) = \sum_{j=0}^{m} pB_j \binom{m}{j} x^j$$

Other Terms where $(p-1)|j$:

$$\nu_p(m!) = 2p-2, \quad \nu_p(j!) \leq \frac{j}{p-1} - 1$$

$$m = (2p-1)(p-1), \quad f(x) = \sum_{j=0}^{m} pB_j \binom{m}{j} x^j$$

Other Terms where $(p-1)|j$:

$$\nu_p(m!) = 2p-2, \quad \nu_p(j!) \leq \frac{j}{p-1} - 1$$

$$\nu_p\big((m-j)!\big) \leq \frac{m-j}{p-1} - 1$$

$$\nu_p(m!) = 2p-2, \quad \nu_p(j!) \le \frac{j}{p-1} - 1$$

$$\nu_p\big((m-j)!\big) \le \frac{m-j}{p-1} - 1$$

$$\nu_p(m!) = 2p-2, \quad \nu_p(j!) \le \frac{j}{p-1} - 1$$

$$\nu_p\big((m-j)!\big) \le \frac{m-j}{p-1} - 1$$

$$\nu_p\left(\binom{m}{j}\right) =$$

$$\nu_p(m!) = 2p-2, \quad \nu_p(j!) \le \frac{j}{p-1} - 1$$

$$\nu_p\big((m-j)!\big) \le \frac{m-j}{p-1} - 1$$

$$\nu_p\left(\binom{m}{j}\right) = \nu_p(m!) - \nu_p(j!) - \nu_p\big((m-j)!\big)$$

$$\nu_p(m!) = 2p-2, \quad \nu_p(j!) \le \frac{j}{p-1} - 1$$

$$\nu_p\big((m-j)!\big) \le \frac{m-j}{p-1} - 1$$

$$\nu_p\left(\binom{m}{j}\right) = \nu_p(m!) - \nu_p(j!) - \nu_p\big((m-j)!\big)$$

$$\ge 2p - 2 - \frac{j}{p-1} - \frac{m-j}{p-1} + 2$$

$$\nu_p(m!) = 2p-2, \quad \nu_p(j!) \le \frac{j}{p-1} - 1$$

$$\nu_p\big((m-j)!\big) \le \frac{m-j}{p-1} - 1$$

$$\nu_p\left(\binom{m}{j}\right) = \nu_p(m!) - \nu_p(j!) - \nu_p\big((m-j)!\big)$$

$$\ge 2p - 2 - \frac{j}{p-1} - \frac{m-j}{p-1} + 2$$

$$\nu_p(m!) = 2p-2, \quad \nu_p(j!) \le \frac{j}{p-1} - 1$$

$$\nu_p\big((m-j)!\big) \le \frac{m-j}{p-1} - 1$$

$$\nu_p\left(\binom{m}{j}\right) = \nu_p(m!) - \nu_p(j!) - \nu_p\big((m-j)!\big)$$

$$\ge 2p - 2 - \frac{j}{p-1} - \frac{m-j}{p-1} + 2$$

$$\nu_p(m!) = 2p-2, \quad \nu_p(j!) \le \frac{j}{p-1} - 1$$

$$\nu_p\big((m-j)!\big) \le \frac{m-j}{p-1} - 1$$

$$\nu_p\left(\binom{m}{j}\right) = \nu_p(m!) - \nu_p(j!) - \nu_p\big((m-j)!\big)$$

$$\ge 2p - \frac{m}{p-1}$$

$$\nu_p(m!) = 2p-2, \quad \nu_p(j!) \le \frac{j}{p-1} - 1$$

$$\nu_p\big((m-j)!\big) \le \frac{m-j}{p-1} - 1$$

$$\nu_p\left(\binom{m}{j}\right) = \nu_p(m!) - \nu_p(j!) - \nu_p\big((m-j)!\big)$$

$$\ge 2p - \frac{(2p-1)(p-1)}{p-1}$$

$$\nu_p(m!) = 2p-2, \quad \nu_p(j!) \le \frac{j}{p-1} - 1$$

$$\nu_p\big((m-j)!\big) \le \frac{m-j}{p-1} - 1$$

$$\nu_p\left(\binom{m}{j}\right) = \nu_p(m!) - \nu_p(j!) - \nu_p\big((m-j)!\big)$$

$$\ge 2p - \frac{(2p-1)(p-1)}{p-1} \ge 1$$

MATH 788F: PRACTICE TEST

(1) Prove the following:

> Let $f(x)$ be a monic polynomial in $\mathbb{Z}[x]$ for which $f(0) \neq 0$. Suppose further that $f(x) = f_1(x)f_2(x)f_3(x)$ where each $f_j(x)$ is irreducible. If
>
> $$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$
>
> where each $\alpha_j \in \mathbb{C}$, then $|\alpha_j| \geq 1$ for at least three values of $j \in \{1, 2, \ldots, n\}$.

(2) Let $f(x) = x^3 + 22$. Determine with proof all primes p for which $f(x)$ is Eisenstein with respect to p. For each such p, find a value of a for which $f(x + a)$ is in Eisenstein form with respect to p.

(3) Let

$$f(x) = x^7 + 21x^6 - 30x^4 - 90x^3 + 1350x + 2700.$$

Using Newton polygons, explain why $f(x)$ is irreducible. (Be careful, and indicate as clearly as possible what information you are obtaining from each Newton polygon you use in your argument.)

(4) Let

$$f(x) = x^{16} - 8x^{15} - 4x^{14} - 2x^{13} - x^{12} - x^{11} - x^{10} - \cdots - x - 1.$$

For each part below, give all details of your solution. Do NOT refer to any theorems from class (in particular, do not refer to Perron's Theorem or its proof). You may however use the following lemmas from class:

Lemma 1. Let $f(x)$ be a monic polynomial in $\mathbb{Z}[x]$ for which $f(0) \neq 0$. Suppose further that $f(x)$ has exactly 1 root α (with multiplicity 1) such that $|\alpha| \geq 1$. Then $f(x)$ is irreducible.

Lemma 2. Let $f(x)$ and $g(x)$ be polynomials in $\mathbb{C}[x]$, and let $\mathcal{C} = \{z \in \mathbb{C} : |z| = 1\}$. If the strict inequality $|f(z) + g(z)| < |f(z)| + |g(z)|$ holds for each $z \in \mathcal{C}$, then $f(x)$ and $g(x)$ have the same total number of zeroes (counting multiplicity) inside the circle $\mathcal{C}$ (i.e., in the interior of the region bounded by $\mathcal{C}$).

(a) Consider $F(x) = (2x - 1)f(x)$. Explain why $F(x)$ has exactly one root α satisfying $|\alpha| \geq 1$. (Hint: Expand the product $(2x - 1)f(x)$.)

(b) Explain why this implies that $f(x)$ is irreducible.

(5) For p a prime, prove that the Bernoulli polynomial $B_{(2p-1)(p-1)}(x)$ is irreducible.

MATERIAL TO STUDY FOR MATH 788F

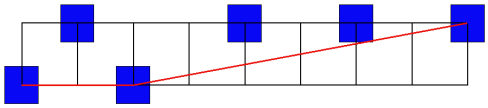
- Difference between irreducibility over $\mathbb{Z}$ and over $\mathbb{Q}$
- Gauss' Theorem connecting irreducibility over $\mathbb{Q}$ with irreducibility over $\mathbb{Z}$ (know proof)
- Computing the greatest common divisor of two polynomials
- The Schönemann-Eisenstein Criterion (know a proof)
- Determining if a polynomial is Eisenstein
- Newton polygons (definitely on test)
- Do not concern yourselves with the last section of Chapter 2 (Schur's theorem)
- Perron's Theorem (know proof given the second lemma, that is given Rouché's theorem)
- A. Cohn's and G. Pólya's Theorem concerning $f(10)$ being prime (know proof of the theorem and the lemma to the theorem)
- Bernoulli polynomials (know proof of Theorem 4.2.2)
- Be able to do the exercises at the end of the chapters

MATH 788F TEST

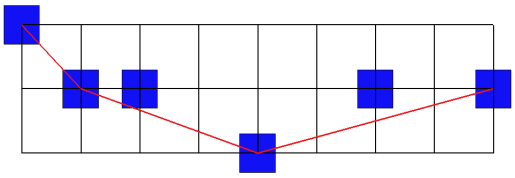
(1) Let

$$f(x) = 45x^8 - 30x^7 - 15x^6 - 2x^4 + 30x^2 + 150.$$

Using Newton polygons, explain why $f(x)$ is irreducible. Below are two Newton polygons to get you started. You may want to use others.



Newton polygon of $f(x)$ with respect to 2



Newton polygon of $f(x)$ with respect to 3

(2) Let $f(x) = x^3 + k$ where k is an arbitrary integer. Suppose that $f(x)$ is Eisenstein with respect to a prime p. Prove that either $p = 3$ or p is a divisor of k.

(3) Let $m = p^2 + p - 2$. Recall that $p\widetilde{B}_m(x) = \sum_{j=0}^{m} pB_j \binom{m}{j}$. Explain why each of the coefficients $pB_j\binom{m}{j}$ for $1 \leq j \leq m-1$ is a rational number which, when reduced, has its numerator divisible by p. (I am *not* asking you to prove $p\widetilde{B}_m(x)$ is a rational number times an Eisenstein polynomial. I am, however, asking you to give part of a proof that $p\widetilde{B}_m(x)$ is a rational number times an Eisenstein polynomial.)

(4) Let $d_n d_{n-1} \dots d_0$ be the decimal representation of a product of three primes. Let $f(x) = \sum_{j=0}^{n} d_j x^j$. Prove that $f(x)$ is the product of at most three irreducible polynomials. In other words, show that if $f(x) = f_1(x)f_2(x)f_3(x)f_4(x)$ where each $f_j(x) \in \mathbb{Z}[x]$, then $f_j(x) \equiv \pm 1$ for at least one $j \in \{1, 2, 3, 4\}$. Prove any lemmas from class you use except you may use Lemma 5, without proof, given in the handout.

(5) Let $f(x) = \sum_{j=0}^{n} a_j x^j$ where $a_n = 1$, $a_{n-1} = 0$, and

$$a_{n-2} > 1 + |a_{n-3}| + |a_{n-4}| + \cdots + |a_1| + |a_0|.$$

Note that the coefficients should be integers and the constant term non-zero.

Thus, a_{n-2} is positive and greater than the sum of the absolute values of the other coefficients.

(a) Show that $f(x)$ has exactly two roots (counting multiplicity) with absolute values ≥ 1.

(b) Show that $f(x)$ has no real roots with absolute value ≥ 1. (Hint: If $z \in \mathbb{R}$, then the terms $a_n z^n$ and $a_{n-2}z^{n-2}$ have the same sign. Also, the inequality in this problem is mighty strong.)

(c) Explain why $f(x)$ is irreducible.

Last Lecture

of

Math 788F

Final Exam:

Final Exam: Thursday, December 12, 2:00 p.m.

Final Exam: Thursday, December 12, 2:00 p.m.
The Final will be in this room.

Final Exam: Thursday, December 12, 2:00 p.m.
The Final will be in this room.
The Final is optional.

Final Exam: Thursday, December 12, 2:00 p.m.
The Final will be in this room.
The Final is optional.
It can only help your grade.

Final Exam: Thursday, December 12, 2:00 p.m.
The Final will be in this room.
The Final is optional.
It can only help your grade.

Material to Know:

Final Exam: Thursday, December 12, 2:00 p.m.
The Final will be in this room.
The Final is optional.
It can only help your grade.

Material to Know: Same as what you needed to know for the test.

Final Exam: Thursday, December 12, 2:00 p.m.
The Final will be in this room.
The Final is optional.
It can only help your grade.

Material to Know: Same as what you needed to know for the test.

Will I be Around?

Final Exam: Thursday, December 12, 2:00 p.m.
The Final will be in this room.
The Final is optional.
It can only help your grade.

Material to Know: Same as what you needed to know for the test.

Will I be Around? Can be

Final Exam: Thursday, December 12, 2:00 p.m.
The Final will be in this room.
The Final is optional.
It can only help your grade.

Material to Know: Same as what you needed to know for the test.

Will I be Around? Can be (maybe will be).

Final Exam: Thursday, December 12, 2:00 p.m.
The Final will be in this room.
The Final is optional.
It can only help your grade.

Material to Know: Same as what you needed to know for the test.

Will I be Around? Can be (maybe will be). Please send me email if you would like to get together (or if you have questions).

What were we discussing before our test?

What were we discussing before our test?

Laguerre Polynomials

What were we discussing before our test?

Laguerre Polynomials

Really? What are they?

WHAT WERE WE DISCUSSING BEFORE OUR TEST?

Laguerre Polynomials

REALLY? WHAT ARE THEY?

$$\sum_{j=0}^{m} \frac{(m+\alpha)(m-1+\alpha)\cdots(j+1+\alpha)(-x)^j}{(m-j)!j!}$$

$$\sum_{j=0}^{m} \frac{(m+\alpha)(m-1+\alpha)\cdots(j+1+\alpha)(-x)^j}{(m-j)!j!}$$

$$\sum_{j=0}^{m} \frac{(m+\alpha)(m-1+\alpha)\cdots(j+1+\alpha)(-x)^j}{(m-j)!j!}$$

We denote this $L_m^{(\alpha)}(x)$.

$$\sum_{j=0}^{m} \frac{(m+\alpha)(m-1+\alpha)\cdots(j+1+\alpha)(-x)^j}{(m-j)!j!}$$

We denote this $L_m^{(\alpha)}(x)$.

THEOREM 7.7.2. $\forall \alpha \in \mathbb{Q} - \mathbb{Z}^-$, $\exists$ finitely many $m \in \mathbb{Z}^+$ such that $L_m^{(\alpha)}(x)$ is reducible.

$$\alpha = \frac{u}{v} \notin \mathbb{Z}^-, \quad v > 0, \quad \gcd(u, v) = 1$$

$$\alpha = \frac{u}{v} \notin \mathbb{Z}^-, \quad v > 0, \quad \gcd(u, v) = 1$$

$$b_j = \binom{m}{j}(m+\alpha)(m-1+\alpha)\cdots(j+1+\alpha)$$

$$\alpha = \frac{u}{v} \notin \mathbb{Z}^-, \quad v > 0, \quad \gcd(u, v) = 1$$

$$b_j = \binom{m}{j}(m+\alpha)(m-1+\alpha)\cdots(j+1+\alpha)$$

$$= \binom{m}{j}\frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$\alpha = \frac{u}{v} \notin \mathbb{Z}^-, \quad v > 0, \quad \gcd(u, v) = 1$$

$$b_j = \binom{m}{j}(m+\alpha)(m-1+\alpha)\cdots(j+1+\alpha)$$

$$= \binom{m}{j}\frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

Let $g(x) = \sum_{j=0}^{m} b_j x^j$ and $f(x) = \sum_{j=0}^{m} a_j b_j x^j$.

$$\alpha = \frac{u}{v} \notin \mathbb{Z}^-, \quad v > 0, \quad \gcd(u, v) = 1$$

$$b_j = \binom{m}{j}(m+\alpha)(m-1+\alpha)\cdots(j+1+\alpha)$$

$$= \binom{m}{j}\frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

Let $g(x) = \sum_{j=0}^{m} b_j x^j$ and $f(x) = \sum_{j=0}^{m} a_j b_j x^j$. Then $g(x)$ is monic.

$$\alpha = \frac{u}{v} \notin \mathbb{Z}^-, \quad v > 0, \quad \gcd(u, v) = 1$$

$$b_j = \binom{m}{j}(m+\alpha)(m-1+\alpha)\cdots(j+1+\alpha)$$

$$= \binom{m}{j}\frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

Let $g(x) = \sum_{j=0}^{m} b_j x^j$ and $f(x) = \sum_{j=0}^{m} a_j b_j x^j$. Then $g(x)$ is monic. Assume $f(x)$ has a factor of degree k in $[1, m/2]$.

$$\alpha = \frac{u}{v} \notin \mathbb{Z}^-, \quad v > 0, \quad \gcd(u, v) = 1$$

$$b_j = \binom{m}{j}(m+\alpha)(m-1+\alpha)\cdots(j+1+\alpha)$$

$$= \binom{m}{j}\frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

Let $g(x) = \sum_{j=0}^{m} b_j x^j$ and $f(x) = \sum_{j=0}^{m} a_j b_j x^j$. Then $g(x)$ is monic. Assume $f(x)$ has a factor of degree k in $[1, m/2]$. Use Lemma 2.4.2 to obtain a contradiction.

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

Let $g(x) = \sum_{j=0}^{m} b_j x^j$ and $f(x) = \sum_{j=0}^{m} a_j b_j x^j$. Then $g(x)$ is monic. Assume $f(x)$ has a factor of degree k in $[1, m/2]$. Use Lemma 2.4.2 to obtain a contradiction.

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

Let $g(x) = \sum_{j=0}^{m} b_j x^j$ and $f(x) = \sum_{j=0}^{m} a_j b_j x^j$. Then $g(x)$ is monic. Assume $f(x)$ has a factor of degree k in $[1, m/2]$. Use Lemma 2.4.2 to obtain a contradiction.

We want a prime p that satisfies certain conditions with $g(x)$.

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

Let $g(x) = \sum_{j=0}^{m} b_j x^j$ and $f(x) = \sum_{j=0}^{m} a_j b_j x^j$. Then $g(x)$ is monic. Assume $f(x)$ has a factor of degree k in $[1, m/2]$. Use Lemma 2.4.2 to obtain a contradiction.

We want a prime p that satisfies certain conditions with $g(x)$. One of them is that p does not divide the leading coefficient of $g(x)$.

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

Let $g(x) = \sum_{j=0}^{m} b_j x^j$ and $f(x) = \sum_{j=0}^{m} a_j b_j x^j$. Then $g(x)$ is monic. Assume $f(x)$ has a factor of degree k in $[1, m/2]$. Use Lemma 2.4.2 to obtain a contradiction.

We want a prime p that satisfies certain conditions with $g(x)$. One of them is that p does not divide the leading coefficient of $g(x)$. This is clear.

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$g(x) = \sum_{j=0}^{m} b_j x^j, \quad k \in [1, m/2], \quad p \text{ prime}$$

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$g(x) = \sum_{j=0}^{m} b_j x^j, \quad k \in [1, m/2], \quad p \text{ prime}$$

CASES:

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$g(x) = \sum_{j=0}^{m} b_j x^j, \quad k \in [1, m/2], \quad p \text{ prime}$$

CASES:

- $k > m/\log^2 m$
- $k_0 \le k \le m/\log^2 m$
- $2 \le k < k_0$
- $k = 1$

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$g(x) = \sum_{j=0}^{m} b_j x^j, \quad k \in [1, m/2], \quad p \text{ prime}$$

CASES:

- $k > m/\log^2 m$
- $k_0 \le k \le m/\log^2 m$
- $2 \le k < k_0$
- $k = 1$

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$g(x) = \sum_{j=0}^{m} b_j x^j, \quad k \in [1, m/2], \quad p \text{ prime}$$

BASIC IDEA IN EACH CASE:

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$g(x) = \sum_{j=0}^{m} b_j x^j, \quad k \in [1, m/2], \quad p \text{ prime}$$

BASIC IDEA IN EACH CASE:

- Want $p|(v(m-j)+u)$ for some $j \in \{0, 1, ..., k-1\}$.

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$g(x) = \sum_{j=0}^{m} b_j x^j, \quad k \in [1, m/2], \quad p \text{ prime}$$

BASIC IDEA IN EACH CASE:

- Want $p|(v(m-j)+u)$ for some $j \in \{0, 1, ..., k-1\}$.
- Want $p > v$.

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$g(x) = \sum_{j=0}^{m} b_j x^j, \quad k \in [1, m/2], \quad p \text{ prime}$$

BASIC IDEA IN EACH CASE:

- Want $p|(v(m-j)+u)$ for some $j \in \{0, 1, ..., k-1\}$.
- Want $p > v$.
- Then $\nu_p(b_j) \geq 1$ for all $j \in \{0, 1, ..., m-k\}$.

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$g(x) = \sum_{j=0}^{m} b_j x^j, \quad k \in [1, m/2], \quad p \text{ prime}$$

BASIC IDEA IN EACH CASE:

- Want $p|(v(m-j)+u)$ for some $j \in \{0, 1, ..., k-1\}$.
- Want $p > v$.
- Then $\nu_p(b_j) \geq 1$ for all $j \in \{0, 1, ..., m-k\}$.
- Show slope of right-most edge of N. P. of $g(x)$ is $< \frac{1}{k}$.

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$g(x) = \sum_{j=0}^{m} b_j x^j, \quad k \in [1, m/2], \quad p \text{ prime}$$

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$g(x) = \sum_{j=0}^{m} b_j x^j, \quad k \in [1, m/2], \quad p > (v + |u|)k$$

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$g(x) = \sum_{j=0}^{m} b_j x^j, \quad k \in [1, m/2], \quad p > (v + |u|)k$$

Slope of right-most edge is $\max\limits_{1 \le j \le m} \left\{ \dfrac{\nu(b_0) - \nu(b_j)}{j} \right\}$.

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$g(x) = \sum_{j=0}^{m} b_j x^j, \quad k \in [1, m/2], \quad p > (v + |u|)k$$

Slope of right-most edge is $\max\limits_{1 \le j \le m} \left\{ \dfrac{\nu(b_0) - \nu(b_j)}{j} \right\}$.

$\nu(b_0) - \nu(b_j)$

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$g(x) = \sum_{j=0}^{m} b_j x^j, \quad k \in [1, m/2], \quad p > (v+|u|)k$$

Slope of right-most edge is $\max\limits_{1\le j\le m} \left\{ \dfrac{\nu(b_0)-\nu(b_j)}{j} \right\}$.

$$\nu(b_0)-\nu(b_j) \le \nu((vj+u)(v(j-1)+u)\cdots(v+u))$$

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$g(x) = \sum_{j=0}^{m} b_j x^j, \quad k \in [1, m/2], \quad p > (v+|u|)k$$

Slope of right-most edge is $\max\limits_{1\le j\le m} \left\{ \dfrac{\nu(b_0)-\nu(b_j)}{j} \right\}$.

$$\nu(b_0)-\nu(b_j) \le \nu((vj+u)(v(j-1)+u)\cdots(v+u))$$

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$g(x) = \sum_{j=0}^{m} b_j x^j, \quad k \in [1, m/2], \quad p > (v+|u|)k$$

Slope of right-most edge is $\max\limits_{1\le j\le m} \left\{ \dfrac{\nu(b_0)-\nu(b_j)}{j} \right\}$.

$$\nu(b_0)-\nu(b_j) \le \nu((vj+u)(v(j-1)+u)\cdots(v+u))$$

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$g(x) = \sum_{j=0}^{m} b_j x^j, \quad k \in [1, m/2], \quad p > (v+|u|)k$$

Slope of right-most edge is $\max\limits_{1\le j\le m} \left\{ \dfrac{\nu(b_0)-\nu(b_j)}{j} \right\}$.

$$\nu(b_0)-\nu(b_j) \le \nu((vj+u)(v(j-1)+u)\cdots(v+u))$$

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$g(x) = \sum_{j=0}^{m} b_j x^j, \quad k \in [1, m/2], \quad p > (v+|u|)k$$

Slope of right-most edge is $\max\limits_{1\le j\le m} \left\{ \dfrac{\nu(b_0)-\nu(b_j)}{j} \right\}$.

$$\begin{aligned} \nu(b_0)-\nu(b_j) &\le \nu((vj+u)(v(j-1)+u)\cdots(v+u)) \\ &\le \nu((vj+|u|)!) \end{aligned}$$

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$g(x) = \sum_{j=0}^{m} b_j x^j, \quad k \in [1, m/2], \quad p > (v+|u|)k$$

Slope of right-most edge is $\max\limits_{1\le j\le m} \left\{ \dfrac{\nu(b_0)-\nu(b_j)}{j} \right\}$.

$$\begin{aligned} \nu(b_0)-\nu(b_j) &\le \nu((vj+u)(v(j-1)+u)\cdots(v+u)) \\ &\le \nu((vj+|u|)!) < \frac{vj+|u|}{p-1} \end{aligned}$$

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$g(x) = \sum_{j=0}^{m} b_j x^j, \quad k \in [1, m/2], \quad p > (v+|u|)k$$

Slope of right-most edge is $\max\limits_{1\le j\le m} \left\{ \dfrac{\nu(b_0)-\nu(b_j)}{j} \right\}$.

$$\begin{aligned} \nu(b_0)-\nu(b_j) &\le \nu((vj+u)(v(j-1)+u)\cdots(v+u)) \\ &\le \nu((vj+|u|)!) < \frac{vj+|u|}{p-1} \end{aligned}$$

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$g(x) = \sum_{j=0}^{m} b_j x^j, \quad k \in [1, m/2], \quad p > (v+|u|)k$$

Slope of right-most edge is $\max\limits_{1\le j\le m} \left\{ \dfrac{\nu(b_0)-\nu(b_j)}{j} \right\}$.

$$\begin{aligned} \nu(b_0)-\nu(b_j) &\le \nu((vj+u)(v(j-1)+u)\cdots(v+u)) \\ &\le \nu((vj+|u|)!) < \frac{vj+|u|}{(v+|u|)k} \end{aligned}$$

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$g(x) = \sum_{j=0}^{m} b_j x^j, \quad k \in [1, m/2], \quad p > (v+|u|)k$$

Slope of right-most edge is $\max\limits_{1\le j\le m} \left\{ \dfrac{\nu(b_0)-\nu(b_j)}{j} \right\}$.

$$\begin{aligned} \nu(b_0)-\nu(b_j) &\le \nu((vj+u)(v(j-1)+u)\cdots(v+u)) \\ &\le \nu((vj+|u|)!) < \frac{(v+|u|)j}{(v+|u|)k} \end{aligned}$$

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$g(x) = \sum_{j=0}^{m} b_j x^j, \quad k \in [1, m/2], \quad p > (v+|u|)k$$

Slope of right-most edge is $\max\limits_{1\le j\le m} \left\{ \dfrac{\nu(b_0)-\nu(b_j)}{j} \right\}$.

$$\begin{aligned} \nu(b_0)-\nu(b_j) &\le \nu((vj+u)(v(j-1)+u)\cdots(v+u)) \\ &\le \nu((vj+|u|)!) < \frac{j}{k} \end{aligned}$$

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$g(x) = \sum_{j=0}^{m} b_j x^j, \quad k \in [1, m/2], \quad p > (v+|u|)k$$

Slope of right-most edge is $\max\limits_{1\le j\le m} \left\{ \dfrac{\nu(b_0)-\nu(b_j)}{j} \right\}$.

$$\begin{aligned} \nu(b_0)-\nu(b_j) &\le \nu((vj+u)(v(j-1)+u)\cdots(v+u)) \\ &\le \nu((vj+|u|)!) < \frac{j}{k} \end{aligned}$$

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$g(x) = \sum_{j=0}^{m} b_j x^j, \quad k \in [1, m/2], \quad p > (v + |u|)k$$

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$g(x) = \sum_{j=0}^{m} b_j x^j, \quad k \in [1, m/2], \quad p > (v + |u|)k$$

Cases:

- $k > m/\log^2 m$
- $k_0 \le k \le m/\log^2 m$
- $2 \le k < k_0$
- $k = 1$

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$g(x) = \sum_{j=0}^{m} b_j x^j, \quad k \in [1, m/2], \quad p > (v + |u|)k$$

Cases:
- $2 \le k < k_0$
- $k = 1$

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$g(x) = \sum_{j=0}^{m} b_j x^j, \quad k \in [1, m/2], \quad p > (v + |u|)k$$

CASES:
- $2 \le k < k_0$
- $k = 1$

BASIC IDEA IN EACH CASE:

- Want $p|(v(m-j)+u)$ for some $j \in \{0, 1, ..., k-1\}$.

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$g(x) = \sum_{j=0}^{m} b_j x^j, \quad k \in [1, m/2], \quad p > (v+|u|)k$$

CASES:
- $2 \le k < k_0$, $p|(vm+u)(v(m-1)+u)$
- $k = 1$

BASIC IDEA IN EACH CASE:

- Want $p|(v(m-j)+u)$ for some $j \in \{0, 1, ..., k-1\}$.

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$g(x) = \sum_{j=0}^{m} b_j x^j, \quad k \in [1, m/2], \quad p > (v+|u|)k$$

CASES: • $2 \le k < k_0$, $p|(vm+u)(v(m-1)+u)$

• $k = 1$, $p|(vm+u)$

BASIC IDEA IN EACH CASE:

• Want $p|(v(m-j)+u)$ for some $j \in \{0, 1, ..., k-1\}$.

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$g(x) = \sum_{j=0}^{m} b_j x^j, \quad k \in [1, m/2], \quad p > (v+|u|)k$$

CASES: • $2 \le k < k_0$, $p|(vm+u)(v(m-1)+u)$
• $k = 1$, $p|(vm+u)$

LEMMA 7.7.7. If $a, b, c, d \in \mathbb{Z}$ with $ad-bc \neq 0$, then the largest prime factor of $(am+b)(cm+d)$ tends to infinity with m.

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$g(x) = \sum_{j=0}^{m} b_j x^j, \quad k \in [1, m/2], \quad p > (v+|u|)k$$

CASES:
- $2 \le k < k_0$, $p | (vm+u)(v(m-1)+u)$
- $k = 1$, $p | (vm+u)$

LEMMA 7.7.7. If $a, b, c, d \in \mathbb{Z}$ with $ad - bc \neq 0$, then the largest prime factor of $(am+b)(cm+d)$ tends to infinity with m.

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$g(x) = \sum_{j=0}^{m} b_j x^j, \quad k \in [1, m/2], \quad p > (v+|u|)k$$

Cases: • $k = 1,\ p|(vm+u)$

Lemma 7.7.7. If $a, b, c, d \in \mathbb{Z}$ with $ad - bc \neq 0$, then the largest prime factor of $(am + b)(cm + d)$ tends to infinity with m.

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$g(x) = \sum_{j=0}^{m} b_j x^j, \quad k \in [1, m/2], \quad p > (v + |u|)k$$

Cases: • $k = 1$, $p|(vm+u)$

Lemma 7.7.7. If $a, b, c, d \in \mathbb{Z}$ with $ad - bc \neq 0$, then the largest prime factor of $(am + b)(cm + d)$ tends to infinity with m.

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$g(x) = \sum_{j=0}^{m} b_j x^j, \quad k \in [1, m/2], \quad p > (v+|u|)k$$

Cases: • $k = 1$, $p | m(vm+u)$

Lemma 7.7.7. If $a, b, c, d \in \mathbb{Z}$ with $ad - bc \neq 0$, then the largest prime factor of $(am + b)(cm + d)$ tends to infinity with m.

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$g(x) = \sum_{j=0}^{m} b_j x^j, \quad k \in [1, m/2], \quad p > (v+|u|)k$$

Cases: • $k = 1,\ p | m(vm+u)$

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$g(x) = \sum_{j=0}^{m} b_j x^j, \quad k \in [1, m/2], \quad p > (v + |u|)k$$

CASES: • $k = 1,\ p | m(vm+u)$

BASIC IDEA IN EACH CASE:

• Want $p | (v(m-j)+u)$ for some $j \in \{0, 1, ..., k-1\}$.

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$g(x) = \sum_{j=0}^{m} b_j x^j, \quad k \in [1, m/2], \quad p > (v + |u|)k$$

CASES: • $k = 1,\ p | m(vm+u)$

BASIC IDEA IN EACH CASE:

• Want $p | (v(m-j)+u)$ for some $j \in \{0, 1, ..., k-1\}$.

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$g(x) = \sum_{j=0}^{m} b_j x^j, \quad k \in [1, m/2], \quad p > (v + |u|)k$$

CASES: • $k = 1,\ p | m(vm+u)$

BASIC IDEA IN EACH CASE:

• Want $p | (v(m-j)+u)$ for some $j \in \{0, 1, ..., k-1\}$.

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$g(x) = \sum_{j=0}^{m} b_j x^j, \quad k \in [1, m/2], \quad p > (v + |u|)k$$

Cases: • $k = 1,\ p | m(vm+u)$

Basic Idea in Case $k = 1$:

$$b_j = \binom{m}{j} \frac{(vm+u)(v(m-1)+u)\cdots(v(j+1)+u)}{v^{m-j}}$$

$$g(x) = \sum_{j=0}^{m} b_j x^j, \quad k \in [1, m/2], \quad p > (v+|u|)k$$

CASES: • $k = 1$, $p | m(vm+u)$

BASIC IDEA IN CASE $k = 1$:

- Use that if $p|m$ and p is large, then $p|\binom{m}{j}$ for small j and the numerator above for large j.