# Course 311: Michaelmas Term 2001
# Part I: Topics in Number Theory

D. R. Wilkins

## Contents

**1 Topics in Number Theory** **2**
1.1 Subgroups of the Integers . . . . . 2
1.2 Greatest Common Divisors . . . . . 2
1.3 The Euclidean Algorithm . . . . . 3
1.4 Prime Numbers . . . . . 4
1.5 The Fundamental Theorem of Arithmetic . . . . . 5
1.6 The Infinitude of Primes . . . . . 6
1.7 Congruences . . . . . 6
1.8 The Chinese Remainder Theorem . . . . . 8
1.9 The Euler Totient Function . . . . . 9
1.10 The Theorems of Fermat, Wilson and Euler . . . . . 11
1.11 Solutions of Polynomial Congruences . . . . . 13
1.12 Primitive Roots . . . . . 14
1.13 Quadratic Residues . . . . . 16
1.14 Quadratic Reciprocity . . . . . 21
1.15 The Jacobi Symbol . . . . . 22

# 1 Topics in Number Theory

## 1.1 Subgroups of the Integers

A subset $S$ of the set $\mathbb{Z}$ of integers is a *subgroup* of $\mathbb{Z}$ if $0 \in S$, $-x \in S$ and $x + y \in S$ for all $x \in S$ and $y \in S$.

It is easy to see that a non-empty subset $S$ of $\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ if and only if $x - y \in S$ for all $x \in S$ and $y \in S$.

Let $m$ be an integer, and let $m\mathbb{Z} = \{mn : n \in \mathbb{Z}\}$. Then $m\mathbb{Z}$ (the set of integer multiples of $m$) is a subgroup of $\mathbb{Z}$.

**Theorem 1.1** *Let $S$ be a subgroup of $\mathbb{Z}$. Then $S = m\mathbb{Z}$ for some non-negative integer $m$.*

**Proof** If $S = \{0\}$ then $S = m\mathbb{Z}$ with $m = 0$. Suppose that $S \neq \{0\}$. Then $S$ contains a non-zero integer, and therefore $S$ contains a positive integer (since $-x \in S$ for all $x \in S$). Let $m$ be the smallest positive integer belonging to $S$. A positive integer $n$ belonging to $S$ can be written in the form $n = qm + r$, where $q$ is a positive integer and $r$ is an integer satisfying $0 \leq r < m$. Then $qm \in S$ (because $qm = m + m + \cdots + m$). But then $r \in S$, since $r = n - qm$. It follows that $r = 0$, since $m$ is the smallest positive integer in $S$. Therefore $n = qm$, and thus $n \in m\mathbb{Z}$. It follows that $S = m\mathbb{Z}$, as required. ∎

## 1.2 Greatest Common Divisors

**Definition** Let $a_1, a_2, \ldots, a_r$ be integers, not all zero. A *common divisor* of $a_1, a_2, \ldots, a_r$ is an integer that divides each of $a_1, a_2, \ldots, a_r$. The *greatest common divisor* of $a_1, a_2, \ldots, a_r$ is the greatest positive integer that divides each of $a_1, a_2, \ldots, a_r$. The greatest common divisor of $a_1, a_2, \ldots, a_r$ is denoted by $(a_1, a_2, \ldots, a_r)$.

**Theorem 1.2** *Let $a_1, a_2, \ldots, a_r$ be integers, not all zero. Then there exist integers $u_1, u_2, \ldots, u_r$ such that*

$$(a_1, a_2, \ldots, a_r) = u_1 a_1 + u_2 a_2 + \cdots + u_r a_r.$$

*where $(a_1, a_2, \ldots, a_r)$ is the greatest common divisor of $a_1, a_2, \ldots, a_r$.*

**Proof** Let $S$ be the set of all integers that are of the form

$$n_1 a_1 + n_2 a_2 + \cdots + n_r a_r$$

for some $n_1, n_2, \ldots, n_r \in \mathbb{Z}$. Then $S$ is a subgroup of $\mathbb{Z}$. It follows that $S = m\mathbb{Z}$ for some non-negative integer $m$ (Theorem 1.1). Then $m$ is a

common divisor of $a_1, a_2, \ldots, a_r$, (since $a_i \in S$ for $i = 1, 2, \ldots, r$). Moreover any common divisor of $a_1, a_2, \ldots, a_r$ is a divisor of each element of $S$ and is therefore a divisor of $m$. It follows that $m$ is the greatest common divisor of $a_1, a_2, \ldots, a_r$. But $m \in S$, and therefore there exist integers $u_1, u_2, \ldots, u_r$ such that

$$(a_1, a_2, \ldots, a_r) = u_1 a_1 + u_2 a_2 + \cdots + u_r a_r,$$

as required. ∎

**Definition** Let $a_1, a_2, \ldots, a_r$ be integers, not all zero. If the greatest common divisor of $a_1, a_2, \ldots, a_r$ is 1 then these integers are said to be *coprime*. If integers $a$ and $b$ are coprime then $a$ is said to be coprime to $b$. (Thus $a$ is coprime to $b$ if and only if $b$ is coprime to $a$.)

**Corollary 1.3** *Let $a_1, a_2, \ldots, a_r$ be integers, not all zero, Then $a_1, a_2, \ldots, a_r$ are coprime if and only if there exist integers $u_1, u_2, \ldots, u_r$ such that*

$$1 = u_1 a_1 + u_2 a_2 + \cdots + u_r a_r.$$

**Proof** If $a_1, a_2, \ldots, a_r$ are coprime then the existence of the required integers $u_1, u_2, \ldots, u_r$ follows from Theorem 1.2. On the other hand, if there exist integers $u_1, u_2, \ldots, u_r$ with the required property then any common divisor of $a_1, a_2, \ldots, a_r$ must be a divisor of 1, and therefore $a_1, a_2, \ldots, a_r$ must be coprime. ∎

## 1.3 The Euclidean Algorithm

Let $a$ and $b$ be positive integers with $a > b$. Let $r_0 = a$ and $r_1 = b$. If $b$ does not divide $a$ then let $r_2$ be the remainder on dividing $a$ by $b$. Then $a = q_1 b + r_2$, where $q_1$ and $r_2$ are positive integers and $0 < r_2 < b$. If $r_2$ does not divide $b$ then let $r_3$ be the remainder on dividing $b$ by $r_2$. Then $b = q_2 r_2 + r_3$, where $q_2$ and $r_3$ are positive integers and $0 < r_3 < r_2$. If $r_3$ does not divide $r_2$ then let $r_4$ be the remainder on dividing $r_2$ by $r_3$. Then $r_2 = q_3 r_3 + r_4$, where $q_3$ and $r_4$ are positive integers and $0 < r_4 < r_3$. Continuing in this fashion, we construct positive integers $r_0, r_1, \ldots, r_n$ such that $r_0 = a$, $r_1 = b$ and $r_i$ is the remainder on dividing $r_{i-2}$ by $r_{i-1}$ for $i = 2, 3, \ldots, n$. Then $r_{i-2} = q_{i-1} r_{i-1} + r_i$, where $q_{i-1}$ and $r_i$ are positive integers and $0 < r_i < r_{i-1}$. The algorithm for constructing the positive integers $r_0, r_1, \ldots, r_n$ terminates when $r_n$ divides $r_{n-1}$. Then $r_{n-1} = q_n r_n$ for some positive integer $q_n$. (The algorithm must clearly terminate in a finite number of steps, since $r_0 > r_1 > r_2 > \cdots > r_n$.) We claim that $r_n$ is the greatest common divisor of $a$ and $b$.

Any divisor of $r_n$ is a divisor of $r_{n-1}$, because $r_{n-1} = q_n r_n$. Moreover if $2 \leq i \leq n$ then any common divisor of $r_i$ and $r_{i-1}$ is a divisor of $r_{i-2}$, because $r_{i-2} = q_{i-1}r_{i-1} + r_i$. If follows that every divisor of $r_n$ is a divisor of all the integers $r_0, r_1, \ldots, r_n$. In particular, any divisor of $r_n$ is a common divisor of $a$ and $b$. In particular, $r_n$ is itself a common divisor of $a$ and $b$.

If $2 \leq i \leq n$ then any common divisor of $r_{i-2}$ and $r_{i-1}$ is a divisor of $r_i$, because $r_i = r_{i-2} - q_{i-1}r_{i-1}$. It follows that every common divisor of $a$ and $b$ is a divisor of all the integers $r_0, r_1, \ldots, r_n$. In particular any common divisor of $a$ and $b$ is a divisor of $r_n$. It follows that $r_n$ is the greatest common divisor of $a$ and $b$.

There exist integers $u_i$ and $v_i$ such that $r_i = u_i a + v_i b$ for $i = 1, 2, \ldots, n$. Indeed $u_i = u_{i-2} - q_{i-1}u_{i-1}$ and $v_i = v_{i-2} - q_{i-1}v_{i-1}$ for each integer $i$ between 2 and $n$, where $u_0 = 1$, $v_0 = 0$, $u_1 = 0$ and $v_1 = 1$. In particular $r_n = u_n a + v_n b$.

The algorithm described above for calculating the greatest common divisor $(a, b)$ of two positive integers $a$ and $b$ is referred to as the *Euclidean algorithm*. It also enables one to calculate integers $u$ and $v$ such that $(a, b) = ua + vb$.

**Example** We calculate the greatest common divisor of 425 and 119. Now

$$\begin{aligned} 425 &= 3 \times 119 + 68 \\ 119 &= 68 + 51 \\ 68 &= 51 + 17 \\ 51 &= 3 \times 17. \end{aligned}$$

It follows that 17 is the greatest common divisor of 425 and 119. Moreover

$$\begin{aligned} 17 &= 68 - 51 = 68 - (119 - 68) \\ &= 2 \times 68 - 119 = 2 \times (425 - 3 \times 119) - 119 \\ &= 2 \times 425 - 7 \times 119. \end{aligned}$$

## 1.4 Prime Numbers

**Definition** A *prime number* is an integer $p$ greater than one with the property that 1 and $p$ are the only positive integers that divide $p$.

Let $p$ be a prime number, and let $x$ be an integer. Then the greatest common divisor $(p, x)$ of $p$ and $x$ is a divisor of $p$, and therefore either $(p, x) = p$ or else $(p, x) = 1$. It follows that either $x$ is divisible by $p$ or else $x$ is coprime to $p$.

**Theorem 1.4** *Let $p$ be a prime number, and let $x$ and $y$ be integers. If $p$ divides $xy$ then either $p$ divides $x$ or else $p$ divides $y$.*

**Proof** Suppose that $p$ divides $xy$ but $p$ does not divide $x$. Then $p$ and $x$ are coprime, and hence there exist integers $u$ and $v$ such that $1 = up + vx$ (Corollary 1.3). Then $y = upy + vxy$. It then follows that $p$ divides $y$, as required. ∎

**Corollary 1.5** *Let $p$ be a prime number. If $p$ divides a product of integers then $p$ divides at least one of the factors of the product.*

**Proof** Let $a_1, a_2, \ldots, a_k$ be integers, where $k > 1$. Suppose that $p$ divides $a_1 a_2 \cdots a_k$. Then either $p$ divides $a_k$ or else $p$ divides $a_1 a_2 \cdots a_{k-1}$. The required result therefore follows by induction on the number $k$ of factors in the product. ∎

## 1.5 The Fundamental Theorem of Arithmetic

**Lemma 1.6** *Every integer greater than one is a prime number or factors as a product of prime numbers.*

**Proof** Let $n$ be an integer greater than one. Suppose that every integer $m$ satisfying $1 < m < n$ is a prime number or factors as a product of prime numbers. If $n$ is not a prime number then $n = ab$ for some integers $a$ and $b$ satisfying $1 < a < n$ and $1 < b < n$. Then $a$ and $b$ are prime numbers or products of prime numbers. Thus if $n$ is not itself a prime number then $n$ must be a product of prime numbers. The required result therefore follows by induction on $n$. ∎

An integer greater than one that is not a prime number is said to be a *composite number*.

Let $n$ be an composite number. We say that $n$ factors uniquely as a product of prime numbers if, given prime numbers $p_1, p_2, \ldots, p_r$ and $q_1, q_2, \ldots, q_s$ such that

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \ldots, q_s,$$

the number of times a prime number occurs in the list $p_1, p_2, \ldots, p_r$ is equal to the number of times it occurs in the list $q_1, q_2, \ldots, q_s$. (Note that this implies that $r = s$.)

**Theorem 1.7** (The Fundamental Theorem of Arithmetic) *Every composite number greater than one factors uniquely as a product of prime numbers.*

**Proof** Let $n$ be a composite number greater than one. Suppose that every composite number greater than one and less than $n$ factors uniquely as a product of prime numbers. We show that $n$ then factors uniquely as a product of prime numbers. Suppose therefore that

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \ldots, q_s,$$

where $p_1, p_2, \ldots, p_r$ and $q_1, q_2, \ldots, q_s$ are prime numbers, $p_1 \leq p_2 \leq \cdots \leq p_r$ and $q_1 \leq q_2 \leq \cdots \leq q_s$. We must prove that $r = s$ and $p_i = q_i$ for all integers $i$ between 1 and $r$.

Let $p$ be the smallest prime number that divides $n$. If a prime number divides a product of integers then it must divide at least one of the factors (Corollary 1.5). It follows that $p$ must divide $p_i$ and thus $p = p_i$ for some integer $i$ between 1 and $r$. But then $p = p_1$, since $p_1$ is the smallest of the prime numbers $p_1, p_2, \ldots, p_r$. Similarly $p = q_1$. Therefore $p = p_1 = q_1$. Let $m = n/p$. Then

$$m = p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s.$$

But then $r = s$ and $p_i = q_i$ for all integers $i$ between 2 and $r$, because every composite number greater than one and less than $n$ factors uniquely as a product of prime numbers. It follows that $n$ factors uniquely as a product of prime numbers. The required result now follows by induction on $n$. (We have shown that if all composite numbers $m$ satisfying $1 < m < n$ factor uniquely as a product of prime numbers, then so do all composite numbers $m$ satisfying $1 < m < n + 1$.) ∎

## 1.6 The Infinitude of Primes

**Theorem 1.8** (Euclid) *The number of prime numbers is infinite.*

**Proof** Let $p_1, p_2, \ldots, p_r$ be prime numbers, let $m = p_1 p_2 \cdots p_r + 1$. Now $p_i$ does not divide $m$ for $i = 1, 2, \ldots, r$, since if $p_i$ were to divide $m$ then it would divide $m - p_1 p_2 \cdots p_r$ and thus would divide 1. Let $p$ be a prime factor of $m$. Then $p$ must be distinct from $p_1, p_2, \ldots, p_r$. Thus no finite set $\{p_1, p_2, \ldots, p_r\}$ of prime numbers can include all prime numbers. ∎

## 1.7 Congruences

Let $m$ be a positive integer. Integers $x$ and $y$ are said to be *congruent* modulo $m$ if $x - y$ is divisible by $m$. If $x$ and $y$ are congruent modulo $m$ then we denote this by writing $x \equiv y \pmod{m}$.

The *congruence class* of an integer $x$ modulo $m$ is the set of all integers that are congruent to $x$ modulo $m$.

Let $x$, $y$ and $z$ be integers. Then $x \equiv x \pmod{m}$. Also $x \equiv y \pmod{m}$ if and only if $y \equiv x \pmod{m}$. If $x \equiv y \pmod{m}$ and $y \equiv z \pmod{m}$ then $x \equiv z \pmod{m}$. Thus congruence modulo $m$ is an equivalence relation on the set of integers.

**Lemma 1.9** *Let $m$ be a positive integer, and let $x$, $x'$, $y$ and $y'$ be integers. Suppose that $x \equiv x' \pmod{m}$ and $y \equiv y' \pmod{m}$. Then $x + y \equiv x' + y' \pmod{m}$ and $xy \equiv x'y' \pmod{m}$.*

**Proof** The result follows immediately from the identities

$$\begin{aligned}(x+y)-(x'+y') &= (x-x')+(y-y'),\\ xy - x'y' &= (x-x')y + x'(y-y').\end{aligned}$$ ∎

**Lemma 1.10** *Let $x$, $y$ and $m$ be integers with $m \neq 0$. Suppose that $m$ divides $xy$ and that $m$ and $x$ are coprime. Then $m$ divides $y$.*

**Proof** There exist integers $a$ and $b$ such that $1 = am + bx$, since $m$ and $x$ are coprime (Corollary 1.3). Then $y = amy + bxy$, and $m$ divides $xy$, and therefore $m$ divides $y$, as required. ∎

**Lemma 1.11** *Let $m$ be a positive integer, and let $a$, $x$ and $y$ be integers with $ax \equiv ay \pmod{m}$. Suppose that $m$ and $a$ are coprime. Then $x \equiv y \pmod{m}$.*

**Proof** If $ax \equiv ay \pmod{m}$ then $a(x-y)$ is divisible by $m$. But $m$ and $a$ are coprime. It therefore follows from Lemma 1.10 that $x - y$ is divisible by $m$, and thus $x \equiv y \pmod{m}$, as required. ∎

**Lemma 1.12** *Let $x$ and $m$ be non-zero integers. Suppose that $x$ is coprime to $m$. Then there exists an integer $y$ such that $xy \equiv 1 \pmod{m}$. Moreover $y$ is coprime to $m$.*

**Proof** There exist integers $y$ and $k$ such that $xy + mk = 1$, since $x$ and $m$ are coprime (Corollary 1.3). Then $xy \equiv 1 \pmod{m}$. Moreover any common divisor of $y$ and $m$ must divide $xy$ and therefore must divide 1. Thus $y$ is coprime to $m$, as required. ∎

**Lemma 1.13** *Let $m$ be a positive integer, and let $a$ and $b$ be integers, where $a$ is coprime to $m$. Then there exist integers $x$ that satisfy the congruence $ax \equiv b \pmod{m}$. Moreover if $x$ and $x'$ are integers such that $ax \equiv b \pmod{m}$ and $ax' \equiv b \pmod{m}$ then $x \equiv x' \pmod{m}$.*

**Proof** There exists an integer $c$ such that $ac \equiv 1 \pmod{m}$, since $a$ is coprime to $m$ (Lemma 1.12). Then $ax \equiv b \pmod{m}$ if and only if $x \equiv cb \pmod{m}$. The result follows. ∎

**Lemma 1.14** *Let $a_1, a_2, \ldots, a_r$ be integers, and let $x$ be an integer that is coprime to $a_i$ for $i = 1, 2, \ldots, r$. Then $x$ is coprime to the product $a_1 a_2 \cdots a_r$ of the integers $a_1, a_2, \ldots, a_r$.*

**Proof** Let $p$ be a prime number which divides the product $a_1 a_2 \cdots a_r$. Then $p$ divides one of the factors $a_1, a_2, \ldots, a_r$ (Corollary 1.5). It follows that $p$ cannot divide $x$, since $x$ and $a_i$ are coprime for $i = 1, 2, \ldots, r$. Thus no prime number is a common divisor of $x$ and the product $a_1 a_2 \cdots a_r$. It follows that the greatest common divisor of $x$ and $a_1 a_2 \cdots a_r$ is 1, since this greatest common divisor cannot have any prime factors. Thus $x$ and $a_1 a_2 \cdots a_r$ are coprime, as required. ∎

Let $m$ be a positive integer. For each integer $x$, let $[x]$ denote the congruence class of $x$ modulo $m$. If $x$, $x'$, $y$ and $y'$ are integers and if $x \equiv x' \pmod{m}$ and $y \equiv y' \pmod{m}$ then $xy \equiv x'y' \pmod{m}$. It follows that there is a well-defined operation of multiplication defined on congruence classes of integers modulo $m$, where $[x][y] = [xy]$ for all integers $x$ and $y$. This operation is commutative and associative, and $[x][1] = [x]$ for all integers $x$. If $x$ is an integer coprime to $m$, then it follows from Lemma 1.12 that there exists an integer $y$ coprime to $m$ such that $xy \equiv 1 \pmod{m}$. Then $[x][y] = [1]$. Therefore the set $\mathbb{Z}_m^*$ of congruence classes modulo $m$ of integers coprime to $m$ is an Abelian group (with multiplication of congruence classes defined as above).

## 1.8 The Chinese Remainder Theorem

Let $I$ be a set of integers. The integers belonging to $I$ are said to be *pairwise coprime* if any two distinct integers belonging to $I$ are coprime.

**Proposition 1.15** *Let $m_1, m_2, \ldots, m_r$ be non-zero integers that are pairwise coprime. Let $x$ be an integer that is divisible by $m_i$ for $i = 1, 2, \ldots, r$. Then $x$ is divisible by the product $m_1 m_2 \cdots m_r$ of the integers $m_1, m_2, \ldots, m_r$.*

**Proof** For each integer $k$ between 1 and $r$ let $P_k$ be the product of the integers $m_i$ with $1 \leq i \leq k$. Then $P_1 = m_1$ and $P_k = P_{k-1} m_k$ for $k = 2, 3, \ldots, r$. Let $x$ be a positive integer that is divisible by $m_i$ for $i = 1, 2, \ldots, r$. We must show that $P_r$ divides $x$. Suppose that $P_{k-1}$ divides $x$ for some integer $k$ between 2 and $r$. Let $y = x/P_{k-1}$. Then $m_k$ and $P_{k-1}$ are coprime

(Lemma 1.14) and $m_k$ divides $P_{k-1}y$. It follows from Lemma 1.10 that $m_k$ divides $y$. But then $P_k$ divides $x$, since $P_k = P_{k-1}m_k$ and $x = P_{k-1}y$. On successively applying this result with $k = 2, 3, \ldots, r$ we conclude that $P_r$ divides $x$, as required. ∎

**Theorem 1.16** (Chinese Remainder Theorem) *Let $m_1, m_2, \ldots, m_r$ be pairwise coprime positive integers. Then, given any integers $x_1, x_2, \ldots, x_r$, there exists an integer $z$ such that $z \equiv x_i \pmod{m_i}$ for $i = 1, 2, \ldots, r$. Moreover if $z'$ is any integer satisfying $z' \equiv x_i \pmod{m_i}$ for $i = 1, 2, \ldots, r$ then $z' \equiv z \pmod{m}$, where $m = m_1 m_2 \cdots m_r$.*

**Proof** Let $m = m_1 m_2 \cdots m_r$, and let $s_i = m/m_i$ for $i = 1, 2, \ldots, r$. Note that $s_i$ is the product of the integers $m_j$ with $j \neq i$, and is thus a product of integers coprime to $m_i$. It follows from Lemma 1.14 that $m_i$ and $s_i$ are coprime for $i = 1, 2, \ldots, r$. Therefore there exist integers $a_i$ and $b_i$ such that $a_i m_i + b_i s_i = 1$ for $i = 1, 2, \ldots, r$ (Corollary 1.3). Let $u_i = b_i s_i$ for $i = 1, 2, \ldots, r$. Then $u_i \equiv 1 \pmod{m_i}$, and $u_i \equiv 0 \pmod{m_j}$ when $j \neq i$. Thus if

$$z = x_1 u_1 + x_2 u_2 + \cdots x_r u_r$$

then $z \equiv x_i \pmod{m_i}$ for $i = 1, 2, \ldots, r$.

Now let $z'$ be an integer with $z' \equiv x_i \pmod{m_i}$ for $i = 1, 2, \ldots, r$. Then $z' - z$ is divisible by $m_i$ for $i = 1, 2, \ldots, r$. It follows from Proposition 1.15 that $z' - z$ is divisible by the product $m$ of the integers $m_1, m_2, \ldots, m_r$. Then $z' \equiv z \pmod{m}$, as required. ∎

## 1.9 The Euler Totient Function

Let $n$ be a positive integer. We define $\varphi(n)$ to be the number of integers $x$ satisfying $0 \leq x < n$ that are coprime to $n$. The function $\varphi$ on the set of positive integers is referred to as the *Euler totient function*.

Every integer (including zero) is coprime to 1, and therefore $\varphi(1) = 1$.

Let $p$ be a prime number. Then $\varphi(p) = p - 1$, since every positive integer less than $p$ is coprime to $p$. Moreover $\varphi(p^k) = p^k - p^{k-1}$ for all positive integers $k$, since there are $p^{k-1}$ integers $x$ satisfying $0 \leq x < p^k$ that are divisible by $p$, and the integers coprime to $p^k$ are those that are not divisible by $p$.

**Theorem 1.17** *Let $m_1$ and $m_2$ be positive integers. Suppose that $m_1$ and $m_2$ are coprime. Then $\varphi(m_1 m_2) = \varphi(m_1)\varphi(m_2)$.*

**Proof** Let $x$ be an integer satisfying $0 \leq x < m_1$ that is coprime to $m_1$, and let $y$ be an integer satisfying $0 \leq y < m_2$ that is coprime to $m_2$. It follows from the Chinese Remainder Theorem (Theorem 1.16) that there exists exactly one integer $z$ satisfying $0 \leq z < m_1 m_2$ such that $z \equiv x \pmod{m_1}$ and $z \equiv y \pmod{m_2}$. Moreover $z$ must then be coprime to $m_1$ and to $m_2$, and must therefore be coprime to $m_1 m_2$. Thus every integer $z$ satisfing $0 \leq z < m_1 m_2$ that is coprime to $m_1 m_2$ is uniquely determined by its congruence classes modulo $m_1$ and $m_2$, and the congruence classes of $z$ modulo $m_1$ and $m_2$ contain integers coprime to $m_1$ and $m_2$ respectively. Thus the number $\varphi(m_1 m_2)$ of integers $z$ satisfying $0 \leq z < m_1 m_2$ that are coprime to $m_1 m_2$ is equal to $\varphi(m_1)\varphi(m_2)$, since $\varphi(m_1)$ is the number of integers $x$ satisfying $0 \leq x < m_1$ that are coprime to $m_1$ and $\varphi(m_2)$ is the number of integers $y$ satisfying $0 \leq y < m_2$ that are coprime to $m_2$. ∎

**Corollary 1.18** $\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$, *for all positive integers* $n$, *where* $\prod_{p|n} \left(1 - \frac{1}{p}\right)$ *denotes the product of* $1 - \frac{1}{p}$ *taken over all prime numbers* $p$ *that divide* $n$.

**Proof** Let $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$, where $p_1, p_2, \ldots, p_m$ are prime numbers and $k_1, k_2, \ldots, k_m$ are positive integers. Then $\varphi(n) = \varphi(p_1^{k_1})\varphi(p_2^{k_2}) \cdots \varphi(p_m^{k_m})$, and $\varphi(p_i^{k_i}) = p_i^{k_i}(1 - (1/p_i))$ for $i = 1, 2, \ldots, m$. Thus $\varphi(n) = n \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right)$, as required. ∎

Let $f$ be any function defined on the set of positive integers, and let $n$ be a positive integer. We denote the sum of the values of $f(d)$ over all divisors $d$ of $n$ by $\sum_{d|n} f(d)$.

**Lemma 1.19** *Let* $n$ *be a positive integer. Then* $\sum_{d|n} \varphi(d) = n$.

**Proof** If $x$ is an integer satisfying $0 \leq x < n$ then $(x, n) = n/d$ for some divisor $d$ of $n$. It follows that $n = \sum_{d|n} n_d$, where $n_d$ is the number of integers $x$ satisfying $0 \leq x < n$ for which $(x, n) = n/d$. Thus it suffices to show that $n_d = \varphi(d)$ for each divisor $d$ of $n$.

Let $d$ be a divisor of $n$, and let $a = n/d$. Given any integer $x$ satisfying $0 \leq x < n$ that is divisible by $a$, there exists an integer $y$ satisfying $0 \leq y < d$

such that $x = ay$. Then $(x, n)$ is a multiple of $a$. Moreover a multiple $ae$ of $a$ divides both $x$ and $n$ if and only if $e$ divides both $y$ and $d$. Therefore $(x, n) = a(y, d)$. It follows that the integers $x$ satisfying $0 \leq x < n$ for which $(x, n) = a$ are those of the form $ay$, where $y$ is an integer, $0 \leq y < d$ and $(y, d) = 1$. It follows that there are exactly $\varphi(d)$ integers $x$ satisfying $0 \leq x < n$ for which $(x, n) = n/d$, and thus $n_d = \varphi(d)$ and $n = \sum_{d|n} \varphi(d)$, as required. ∎

## 1.10 The Theorems of Fermat, Wilson and Euler

**Theorem 1.20** (Fermat) *Let $p$ be a prime number. Then $x^p \equiv x \pmod{p}$ for all integers $x$. Moreover if $x$ is coprime to $p$ then $x^{p-1} \equiv 1 \pmod{p}$.*

We shall give three proofs of this theorem below.

**Lemma 1.21** *Let $p$ be a prime number. Then the binomial coefficient $\binom{p}{k}$ is divisible by $p$ for all integers $k$ satisfying $0 < k < p$.*

**Proof** The binomial coefficient is given by the formula $\binom{p}{k} = \dfrac{p!}{(p-k)!k!}$. Thus if $0 < k < p$ then $\binom{p}{k} = \dfrac{pm}{k!}$, where $m = \dfrac{(p-1)!}{(p-k)!}$. Thus if $0 < k < p$ then $k!$ divides $pm$. Also $k!$ is coprime to $p$. It follows that $k!$ divides $m$ (Lemma 1.10), and therefore the binomial coefficient $\binom{p}{k}$ is a multiple of $p$. ∎

**First Proof of Theorem 1.20** Let $p$ be prime number. Then

$$(x+1)^p = \sum_{k=0}^{p} \binom{p}{k} x^k.$$

It then follows from Lemma 1.21 that $(x+1)^p \equiv x^p + 1 \pmod{p}$. Thus if $f(x) = x^p - x$ then $f(x+1) \equiv f(x) \pmod{p}$ for all integers $x$, since $f(x+1) - f(x) = (x+1)^p - x^p - 1$. But $f(0) \equiv 0 \pmod{p}$. It follows by induction on $|x|$ that $f(x) \equiv 0 \pmod{p}$ for all integers $x$. Thus $x^p \equiv x \pmod{p}$ for all integers $x$. Moreover if $x$ is coprime to $p$ then it follows from Lemma 1.11 that $x^{p-1} \equiv 1 \pmod{p}$, as required. ∎

**Second Proof of Theorem 1.20** Let $x$ be an integer. If $x$ is divisible by $p$ then $x \equiv 0 \pmod{p}$ and $x^p \equiv 0 \pmod{p}$.

Suppose that $x$ is coprime to $p$. If $j$ is an integer satisfying $1 \leq j \leq p-1$ then $j$ is coprime to $p$ and hence $xj$ is coprime to $p$. It follows that there exists a unique integer $u_j$ such that $1 \leq u_j \leq p-1$ and $xj \equiv u_j \pmod{p}$. If $j$ and $k$ are integers between 1 and $p-1$ and if $j \neq k$ then $u_j \neq u_k$. It follows that each integer between 1 and $p-1$ occurs exactly once in the list $u_1, u_2, \ldots, u_{p-1}$, and therefore $u_1 u_2 \cdots u_{p-1} = (p-1)!$. Thus if we multiply together the left hand sides and right hand sides of the congruences $xj \equiv u_j \pmod{p}$ for $j = 1, 2, \ldots, p-1$ we obtain the congruence $x^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$. But then $x^{p-1} \equiv 1 \pmod{p}$ by Lemma 1.11, since $(p-1)!$ is coprime to $p$. But then $x^p \equiv x \pmod{p}$, as required. ∎

**Third Proof of Theorem 1.20** Let $p$ be a prime number. The congruence classes modulo $p$ of integers coprime to $p$ constitute a group of order $p-1$, where the group operation is multiplication of congruence classes. Now it follows from Lagrange's Theorem that that order of any element of a finite group divides the order of the group. If we apply this result to the group of congruence classes modulo $p$ of integers coprime to $p$ we find that if an integer $x$ is not divisible by $p$ then $x^{p-1} \equiv 1 \pmod{p}$. It follows that $x^p \equiv x \pmod{p}$ for all integers $x$ that are not divisible by $p$. This congruence also holds for all integers $x$ that are divisible by $p$. ∎

**Theorem 1.22** (Wilson's Theorem) $(p-1)!+1$ *is divisible by* $p$ *for all prime numbers* $p$.

**Proof** Let $p$ be a prime number. If $x$ is an integer satisfying $x^2 \equiv 1 \pmod{p}$ then $p$ divides $(x-1)(x+1)$ and hence either $p$ divides either $x-1$ or $x+1$. Thus if $1 \leq x \leq p-1$ and $x^2 \equiv 1 \pmod{p}$ then either $x = 1$ or $x = p-1$.

For each integer $x$ satisfying $1 \leq x \leq p-1$, there exists exactly one integer $y$ satisfying $1 \leq y \leq p-1$ such that $xy \equiv 1 \pmod{p}$. Moreover $y \neq x$ when $2 \leq x \leq p-2$. It follows that $(p-2)!$ is a product of numbers of the form $xy$, where $x$ and $y$ are distinct integers between 2 and $p-2$ and $xy \equiv 1 \pmod{p}$. It follows that $(p-2)! \equiv 1 \pmod{p}$. But then $(p-1)! \equiv p-1 \pmod{p}$, and hence $(p-1)!+1 \equiv 0 \pmod{p}$, as required. ∎

The following theorem of Euler generalizes Fermat's Theorem (Theorem 1.20).

**Theorem 1.23** (Euler) *Let* $m$ *be a positive integer, and let* $x$ *be an integer coprime to* $m$. *Then* $x^{\varphi(m)} \equiv 1 \pmod{m}$.

**First Proof of Theorem 1.23** The result is trivially true when $m = 1$. Suppose that $m > 1$. Let $I$ be the set of all positive integers less than $m$ that are coprime to $m$. Then $\varphi(m)$ is by definition the number of integers in $I$. If $y$ is an integer coprime to $m$ then so is $xy$. It follows that, to each integer $j$ in $I$ there exists a unique integer $u_j$ in $I$ such that $xj \equiv u_j \pmod{m}$. Moreover if $j \in I$ and $k \in I$ and $j \neq k$ then $u_j \not\equiv u_k$. Therefore $I = \{u_j : j \in I\}$. Thus if we multiply the left hand sides and right hand sides of the congruences $xj \equiv u_j \pmod{m}$ for all $j \in I$ we obtain the congruence $x^{\varphi(m)}z \equiv z \pmod{m}$, where $z$ is the product of all the integers in $I$. But $z$ is coprime to $m$, since a product of integers coprime to $m$ is itself coprime to $m$. It follows from Lemma 1.11 that $x^{\varphi(m)} \equiv 1 \pmod{m}$, as required. ∎

**2nd Proof of Theorem 1.23** Let $m$ be a positive integer. Then the congruence classes modulo $m$ of integers coprime to $m$ constitute a group of order $\varphi(m)$, where the group operation is multiplication of congruence classes. Now it follows from Lagrange's Theorem that that order of any element of a finite group divides the order of the group. If we apply this result to the group of congruence classes modulo $m$ of integers coprime to $m$ we find that $x^{\varphi(m)} \equiv 1 \pmod{m}$, as required. ∎

## 1.11 Solutions of Polynomial Congruences

Let $f$ be a polynomial with integer coefficients, and let $m$ be a positive integer. If $x$ and $x'$ are integers, and if $x \equiv x' \pmod{m}$, then $f(x) \equiv f(x') \pmod{m}$. It follows that the set consisting of those integers $x$ which satisfy the congruence $f(x) \equiv 0 \pmod{m}$ is a union of congruence classes modulo $m$. The *number of solutions modulo* $m$ of the congruence $f(x) \equiv 0 \pmod{m}$ is defined to be the number of congruence classes of integers modulo $m$ such that an integer $x$ satisfies the congruence $f(x) \equiv 0 \pmod{m}$ if and only if it belongs to one of those congruence classes. Thus a congruence $f(x) \equiv 0 \pmod{m}$ has $n$ solutions modulo $m$ if and only if there exist $n$ integers $a_1, a_2, \ldots, a_n$ satisfying the congruence such that every solution of the congruence $f(x) \equiv 0 \pmod{m}$ is congruent modulo $m$ to exactly one of the integers $a_1, a_2, \ldots, a_n$.

Note that the number of solutions of the congruence $f(x) \equiv 0 \pmod{m}$ is equal to the number of integers $x$ satisfying $0 \leq x < m$ for which $f(x) \equiv 0 \pmod{m}$. This follows immediately from the fact that each congruence class of integers modulo $m$ contains exactly one integer $x$ satisfying $0 \leq x < m$.

**Theorem 1.24** *Let $f$ be a polynomial with integer coefficients, and let $p$ be a prime number. Suppose that the coefficients of $f$ are not all divisible by $p$.*

*Then the number of solutions modulo $p$ of the congruence $f(x) \equiv 0 \pmod{p}$ is at most the degree of the polynomial $f$.*

**Proof** The result is clearly true when $f$ is a constant polynomial. We can prove the result for non-constant polynomials by induction on the degree of the polynomial.

First we observe that, given any integer $a$, there exists a polynomial $g$ with integer coefficients such that $f(x) = f(a) + (x-a)g(x)$. Indeed $f(y+a)$ is a polynomial in $y$ with integer coefficients, and therefore $f(y+a) = f(a)+yh(y)$ for some polynomial $h$ with integer coefficients. Thus if $g(x) = h(x-a)$ then $g$ is a polynomial with integer coefficients and $f(x) = f(a) + (x-a)g(x)$.

Suppose that $f(a) \equiv 0 \pmod{p}$ and $f(b) \equiv 0 \pmod{p}$. Let $f(x) = f(a) + (x-a)g(x)$, where $g$ is a polynomial with integer coefficients. The coefficients of $f$ are not all divisible by $p$, but $f(a)$ is divisible by $p$, and therefore the coefficients of $g$ cannot all be divisible by $p$.

Now $f(a)$ and $f(b)$ are both divisible by the prime number $p$, and therefore $(b-a)g(b)$ is divisible by $p$. But a prime number divides a product of integers if and only if it divides one of the factors. Therefore either $b-a$ is divisible by $p$ or else $g(b)$ is divisible by $p$. Thus either $b \equiv a \pmod{p}$ or else $g(b) \equiv 0 \pmod{p}$. The required result now follows easily by induction on the degree of the polynomial $f$. ∎

## 1.12 Primitive Roots

**Lemma 1.25** *Let $m$ be a positive integer, and let $x$ be an integer coprime to $m$. Then there exists a positive integer $n$ such that $x^n \equiv 1 \pmod{m}$.*

**Proof** There are only finitely many congruence classes modulo $m$. Therefore there exist positive integers $j$ and $k$ with $j < k$ such that $x^j \equiv x^k \pmod{m}$. Let $n = k - j$. Then $x^j x^n \equiv x^j \pmod{m}$. But $x^j$ is coprime to $m$. It follows from Lemma 1.11 that $x^n \equiv 1 \pmod{m}$. ∎

**Remark** The above lemma also follows directly from Euler's Theorem (Theorem 1.23).

Let $m$ be a positive integer, and let $x$ be an integer coprime to $m$. The order of the congruence class of $x$ modulo $m$ is by definition the smallest positive integer $d$ such that $x^d \equiv 1 \pmod{m}$.

**Lemma 1.26** *Let $m$ be a positive integer, let $x$ be an integer coprime to $m$, and let $j$ and $k$ be positive integers. Then $x^j \equiv x^k \pmod{m}$ if and only if $j \equiv k \pmod{d}$, where $d$ is the order of the congruence class of $x$ modulo $m$.*

**Proof** We may suppose without loss of generality that $j < k$. If $j \equiv k \pmod{d}$ then $k - j$ is divisible by $d$, and hence $x^{k-j} \equiv 1 \pmod{m}$. But then $x^k \equiv x^j x^{k-j} \equiv x^j \pmod{m}$. Conversely suppose that $x^j \equiv x^k \pmod{m}$ and $j < k$. Then $x^j x^{k-j} \equiv x^j \pmod{m}$. But $x^j$ is coprime to $m$. It follows from Lemma 1.11 that $x^{k-j} \equiv 1 \pmod{m}$. Thus if $k - j = qd + r$, where $q$ and $r$ are integers and $0 \leq r < d$, then $x^r \equiv 1 \pmod{m}$. But then $r = 0$, since $d$ is the smallest positive integer for which $x^d \equiv 1 \pmod{m}$. Therefore $k - j$ is divisible by $d$, and thus $j \equiv k \pmod{d}$. ∎

**Lemma 1.27** *Let $p$ be a prime number, and let $x$ and $y$ be integers coprime to $p$. Suppose that the congruence classes of $x$ and $y$ modulo $p$ have the same order. Then there exists a non-negative integer $k$, coprime to the order of the congruence classes of $x$ and $y$, such that $y \equiv x^k \pmod{p}$.*

**Proof** Let $d$ be the order of the congruence class of $x$ modulo $p$. The solutions of the congruence $x^d \equiv 1 \pmod{p}$ include $x^j$ with $0 \leq j < d$. But the congruence $x^d \equiv 1 \pmod{p}$ has at most $d$ solutions modulo $p$, since $p$ is prime (Theorem 1.24), and the congruence classes of $1, x, x^2, \ldots, x^{d-1}$ modulo $p$ are distinct (Lemma 1.26). It follows that any solution of the congruence $x^d \equiv 1 \pmod{p}$ is congruent to $x^k$ for some positive integer $k$. Thus if $y$ is an integer coprime to $p$ whose congruence class is of order $d$ then $y \equiv x^k \pmod{p}$ for some positive integer $k$. Moreover $k$ is coprime to $d$, for if $e$ is a common divisor of $k$ and $d$ then $y^{d/e} \equiv x^{d(k/e)} \equiv 1 \pmod{p}$, and hence $e = 1$. ∎

Let $m$ be a positive integer. An integer $g$ is said to be a *primitive root* modulo $m$ if, given any integer $x$ coprime to $m$, there exists an integer $j$ such that $x \equiv g^j \pmod{m}$.

A primitive root modulo $m$ is necessarily coprime to $m$. For if $g$ is a primitive root modulo $m$ then there exists an integer $n$ such that $g^n \equiv 1 \pmod{m}$. But then any common divisor of $g$ and $m$ must divide 1, and thus $g$ and $m$ are coprime.

**Theorem 1.28** *Let $p$ be a prime number. Then there exists a primitive root modulo $p$.*

**Proof** If $x$ is an integer coprime to $p$ then it follows from Fermat's Theorem (Theorem 1.20) that $x^{p-1} \equiv 1 \pmod{p}$. It then follows from Lemma 1.26 that the order of the congruence class of $x$ modulo $p$ divides $p - 1$. For each divisor $d$ of $p-1$, let $\psi(d)$ denote the number of congruence classes modulo $p$ of integers coprime to $p$ that are of order $d$. Clearly $\sum_{d|p-1} \psi(d) = p - 1$.

Let $x$ be an integer coprime to $p$ whose congruence class is of order $d$, where $d$ is a divisor of $p-1$. If $k$ is coprime to $d$ then the congruence class of $x^k$ is also of order $d$, for if $(x^k)^n \equiv 1 \pmod{p}$ then $d$ divides $kn$ and hence $d$ divides $n$ (Lemma 1.10). Let $y$ be an integer coprime to $p$ whose congruence class is also of order $d$. It follows from Lemma 1.27 that there exists a non-negative integer $k$ coprime to $d$ such that $y \equiv x^k \pmod{p}$. It then follows from Lemma 1.26 that there exists a unique integer $k$ coprime to $d$ such that $0 \leq k < d$ and $y \equiv x^k \pmod{p}$. Thus if there exists at least one integer $x$ coprime to $p$ whose congruence class modulo $p$ is of order $d$ then the congruence classes modulo $p$ of integers coprime to $p$ that are of order $d$ are the congruence classes of $x^k$ for those integers $k$ satisfying $0 \leq k < d$ that are coprime to $d$. Thus if $\psi(d) > 0$ then $\psi(d) = \varphi(d)$, where $\varphi(d)$ is the number of integers $k$ satisfying $0 \leq k < d$ that are coprime to $d$.

Now $0 \leq \psi(d) \leq \varphi(d)$ for each divisor $d$ of $p-1$. But $\sum_{d|p-1} \psi(d) = p-1$ and $\sum_{d|p-1} \varphi(d) = p-1$ (Lemma 1.19). Therefore $\psi(d) = \varphi(d)$ for each divisor $d$ of $p-1$. In particular $\psi(p-1) = \varphi(p-1) \geq 1$. Thus there exists an integer $g$ whose congruence class modulo $p$ is of order $p-1$. The congruence classes of $1, g, g^2, \ldots g^{p-2}$ modulo $p$ are then distinct. But there are exactly $p-1$ congruence classes modulo $p$ of integers coprime to $p$. It follows that any integer that is coprime to $p$ must be congruent to $g^j$ for some non-negative integer $j$. Thus $g$ is a primitive root modulo $p$. ∎

**Corollary 1.29** *Let $p$ be a prime number. Then the group of congruence classes modulo $p$ of integers coprime to $p$ is a cyclic group of order $p-1$.*

**Remark** It can be shown that there exists a primitive root modulo $m$ if $m = 1$, 2 or 4, if $m = p^k$ or if $m = 2p^k$, where $p$ is some odd prime number and $k$ is a positive integer. In all other cases there is no primitive root modulo $m$.

## 1.13 Quadratic Residues

**Definition** Let $p$ be a prime number, and let $x$ be an integer coprime to $p$. The integer $x$ is said to be a *quadratic residue* of $p$ if there exists an integer $y$ such that $x \equiv y^2 \pmod{p}$. If $x$ is not a quadratic residue of $p$ then $x$ is said to be a *quadratic non-residue* of $p$.

**Proposition 1.30** *Let $p$ be an odd prime number, and let $a$, $b$ and $c$ be integers, where $a$ is coprime to $p$. Then there exist integers $x$ satisfying the*

*congruence* $ax^2 + bx + c \equiv 0 \pmod{p}$ *if and only if either* $b^2 - 4ac$ *is a quadratic residue of* $p$ *or else* $b^2 - 4ac \equiv 0 \pmod{p}$.

**Proof** Let $x$ be an integer. Then $ax^2 + bx + c \equiv 0 \pmod{p}$ if and only if $4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{p}$, since $4a$ is coprime to $p$ (Lemma 1.11). But $4a^2x^2 + 4abx + 4ac = (2ax + b)^2 - (b^2 - 4ac)$. It follows that $ax^2 + bx + c \equiv 0 \pmod{p}$ if and only if $(2ax + b)^2 \equiv b^2 - 4ac \pmod{p}$. Thus if there exist integers $x$ satisfying the congruence $ax^2 + bx + c \equiv 0 \pmod{p}$ then either $b^2 - 4ac$ is a quadratic residue of $p$ or else $b^2 - 4ac \equiv 0 \pmod{p}$. Conversely suppose that either $b^2 - 4ac$ is a quadratic residue of $p$ or $b^2 - 4ac \equiv 0 \pmod{p}$. Then there exists an integer $y$ such that $y^2 \equiv b^2 - 4ac \pmod{p}$. Also there exists an integer $d$ such that $2ad \equiv 1 \pmod{p}$, since $2a$ is coprime to $p$ (Lemma 1.12). If $x \equiv d(y - b) \pmod{p}$ then $2ax + b \equiv y \pmod{p}$, and hence $(2ax + b)^2 \equiv b^2 - 4ac \pmod{p}$. But then $ax^2 + bx + c \equiv 0 \pmod{p}$, as required. ∎

**Lemma 1.31** *Let* $p$ *be an odd prime number, and let* $x$ *and* $y$ *be integers. Suppose that* $x^2 \equiv y^2 \pmod{p}$. *Then either* $x \equiv y \pmod{p}$ *or else* $x \equiv -y \pmod{p}$.

**Proof** $x^2 - y^2$ is divisible by $p$, since $x^2 \equiv y^2 \pmod{p}$. But $x^2 - y^2 = (x - y)(x + y)$, and a prime number divides a product of integers if and only if it divides at least one of the factors. Therefore either $x - y$ is divisible by $p$ or else $x + y$ is divisible by $p$. Thus either $x \equiv y \pmod{p}$ or else $x \equiv -y \pmod{p}$.

**Lemma 1.32** *Let* $p$ *be an odd prime number, and let* $m = (p - 1)/2$. *Then there are exactly* $m$ *congruence classes of integers coprime to* $p$ *that are quadratic residues of* $p$. *Also there are exactly* $m$ *congruence classes of integers coprime to* $p$ *that are quadratic non-residues of* $p$.

**Proof** If $i$ and $j$ are integers between 1 and $m$, and if $i \neq j$ then $i \not\equiv j \pmod{p}$ and $i \not\equiv -j \pmod{p}$. It follows from Lemma 1.31 that if $i$ and $j$ are integers between 1 and $m$, and if $i \neq j$ then $i^2 \not\equiv j^2$. Thus the congruence classes of $1^2, 2^2, \ldots, m^2$ modulo $p$ are distinct. But, given any integer $x$ coprime to $p$, there is an integer $i$ such that $1 \leq i \leq m$ and either $x \equiv i \pmod{p}$ or $x \equiv -i \pmod{p}$, and therefore $x^2 \equiv i^2 \pmod{p}$. Thus every quadratic residue of $p$ is congruent to $i^2$ for exactly one integer $i$ betweeen 1 and $m$. Thus there are $m$ congruence classes of quadratic residues of $p$.

There are $2m$ congruence classes of integers modulo $p$ that are coprime to $p$. It follows that there are $m$ congruence classes of quadratic non-residues of $p$, as required. ∎

**Theorem 1.33** *Let $p$ be an odd prime number, let $R$ be the set of all integers coprime to $p$ that are quadratic residues of $p$, and let $N$ be the set of all integers coprime to $p$ that are quadratic non-residues of $p$. If $x \in R$ and $y \in R$ then $xy \in R$. If $x \in R$ and $y \in N$ then $xy \in N$. If $x \in N$ and $y \in N$ then $xy \in R$.*

**Proof** Let $m = (p-1)/2$. Then there are exactly $m$ congruence classes of integers coprime to $p$ that are quadratic residues of $p$. Let these congruence classes be represented by the integers $r_1, r_2, \ldots, r_m$, where $r_i \not\equiv r_j \pmod{p}$ when $i \neq j$. Also there are exactly $m$ congruence classes of integers coprime to $p$ that are quadratic non-residules modulo $p$.

The product of two quadratic residues of $p$ is itself a quadratic residue of $p$. Therefore $xy \in R$ for all $x \in R$ and $y \in R$.

Suppose that $x \in R$. Then $xr_i \in R$ for $i = 1, 2, \ldots, m$, and $xr_i \not\equiv xr_j$ when $i \neq j$. It follows that the congruence classes of $xr_1, xr_2, \ldots, xr_m$ are distinct, and consist of quadratic residues of $p$. But there are exactly $m$ congruence classes of quadratic residues of $p$. It follows that every quadratic residue of $p$ is congruent to exactly one of the integers $xr_1, xr_2, \ldots, xr_m$. But if $y \in N$ then $y \not\equiv r_i$ and hence $xy \not\equiv xr_i$ for $i = 1, 2, \ldots, m$. It follows that $xy \in N$ for all $x \in R$ and $y \in N$.

Now suppose that $x \in N$. Then $xr_i \in N$ for $i = 1, 2, \ldots, m$, and $xr_i \not\equiv xr_j$ when $i \neq j$. It follows that the congruence classes of $xr_1, xr_2, \ldots, xr_m$ are distinct, and consist of quadratic non-residues modulo $p$. But there are exactly $m$ congruence classes of quadratic non-residues modulo $p$. It follows that every quadratic non-residue of $p$ is congruent to exactly one of the integers $xr_1, xr_2, \ldots, xr_m$. But if $y \in N$ then $y \not\equiv r_i$ and hence $xy \not\equiv xr_i$ for $i = 1, 2, \ldots, m$. It follows that $xy \in R$ for all $x \in N$ and $y \in N$. ∎

Let $p$ be an odd prime number. The *Legendre symbol* $\left(\frac{x}{p}\right)$ is defined for integers $x$ as follows: if $x$ is coprime to $p$ and $x$ is a quadratic residue of $p$ then $\left(\frac{x}{p}\right) = +1$; if $x$ is coprime to $p$ and $x$ is a quadratic non-residue of $p$ then $\left(\frac{x}{p}\right) = -1$; if $x$ is divisible by $p$ then $\left(\frac{x}{p}\right) = 0$.

The following result follows directly from Theorem 1.33.

**Corollary 1.34** *Let $p$ be an odd prime number. Then*

$$\left(\frac{x}{p}\right)\left(\frac{y}{p}\right) = \left(\frac{xy}{p}\right)$$

*for all integers $x$ and $y$.*

**Lemma 1.35** (Euler) *Let $p$ be an odd prime number, and let $x$ be an integer coprime to $p$. Then $x$ is a quadratic residue of $p$ if and only if $x^{(p-1)/2} \equiv 1 \pmod{p}$. Also $x$ is a quadratic non-residue of $p$ if and only if $x^{(p-1)/2} \equiv -1 \pmod{p}$.*

**Proof** Let $m = (p-1)/2$. If $x$ is a quadratic residue of $p$ then $x \equiv y^2 \pmod{p}$ for some integer $y$ coprime to $p$. Then $x^m = y^{p-1}$, and $y^{p-1} \equiv 1 \pmod{p}$ by Fermat's Theorem (Theorem 1.20), and thus $x^m \equiv 1 \pmod{p}$.

It follows from Theorem 1.24 that there are at most $m$ congruence classes of integers $x$ satisfying $x^m \equiv 1 \pmod{p}$. However all quadratic residues modulo $p$ satisfy this congruence, and there are exactly $m$ congruence classes of quadratic residues modulo $p$. It follows that an integer $x$ coprime to $p$ satisfies the congruence $x^m \equiv 1 \pmod{p}$ if and only if $x$ is a quadratic residue of $p$.

Now let $x$ be a quadratic non-residue of $p$ and let $u = x^m$. Then $u^2 \equiv 1 \pmod{p}$ but $u \not\equiv 1 \pmod{p}$. It follows from Lemma 1.31 that $u \equiv -1 \pmod{p}$. It follows that an integer $x$ coprime to $p$ is a quadratic non-residue of $p$ if and only if $x^m \equiv -1 \pmod{p}$. ∎

**Corollary 1.36** *Let $p$ be an odd prime number. Then*

$$x^{(p-1)/2} \equiv \left(\frac{x}{p}\right) \pmod{p}$$

*for all integers $x$.*

**Proof** If $x$ is coprime to $p$ then the result follows from Lemma 1.35. If $x$ is divisible by $p$ then so is $x^{(p-1)/2}$. In that case $x^{(p-1)/2} \equiv 0 \pmod{p}$ and $\left(\frac{x}{p}\right) = 0 \pmod{p}$. ∎

**Corollary 1.37** $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ *for all odd prime numbers $p$.*

**Proof** It follows from Corollary 1.36 that $\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \pmod{p}$ for all odd prime numbers $p$. But $\left(\frac{-1}{p}\right) = \pm 1$, by the definition of the Legendre symbol. Therefore $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$, as required. ∎

**Remark** Let $p$ be an odd prime number. It follows from Theorem 1.28 that there exists a primitive root $g$ modulo $p$. Moreover the congruence class of

$g$ modulo $p$ is of order $p-1$. It follows that $g^j \equiv g^k \pmod{p}$, where $j$ and $k$ are positive integers, if and only if $j-k$ is divisible by $p-1$. But $p-1$ is even. Thus if $g^j \equiv g^k$ then $j-k$ is even. It follows easily from this that an integer $x$ is a quadratic residue of $p$ if and only if $x \equiv g^k \pmod{p}$ for some even integer $k$. The results of Theorem 1.33 and Lemma 1.35 follow easily from this fact.

Let $p$ be an odd prime number, and let $m = (p-1)/2$. Then each integer not divisible by $p$ is congruent to exactly one of the integers $\pm 1, \pm 2, \ldots, \pm m$.

The following lemma was proved by Gauss.

**Lemma 1.38** *Let $p$ be an odd prime number, let $m = (p-1)/2$, and let $x$ be an integer that is not divisible by $p$. Then $\left(\frac{x}{p}\right) = (-1)^r$, where $r$ is the number of pairs $(j,u)$ of integers satisfying $1 \leq j \leq m$ and $1 \leq u \leq m$ for which $xj \equiv -u \pmod{p}$.*

**Proof** For each integer $j$ satisfying $1 \leq j \leq m$ there is a unique integer $u_j$ satisfying $1 \leq u_j \leq m$ such that $xj \equiv e_j u_j \pmod{p}$ with $e_j = \pm 1$. Then $e_1 e_2 \cdots e_m = (-1)^r$.

If $j$ and $k$ are integers between 1 and $m$ and if $j \neq k$, then $j \not\equiv k \pmod{p}$ and $j \not\equiv -k \pmod{p}$. But then $xj \not\equiv xk \pmod{p}$ and $xj \not\equiv -xk \pmod{p}$ since $x$ is not divisible by $p$. Thus if $1 \leq j \leq m$, $1 \leq k \leq m$ and $j \neq k$ then $u_j \neq u_k$. It follows that each integer between 1 and $m$ occurs exactly once in the list $u_1, u_2, \ldots, u_m$, and therefore $u_1 u_2 \cdots u_m = m!$. Thus if we multiply the congruences $xj \equiv e_j u_j \pmod{p}$ for $j = 1, 2, \ldots, m$ we obtain the congruence $x^m m! \equiv (-1)^r m! \pmod{p}$. But $m!$ is not divisible by $p$, since $p$ is prime and $m < p$. It follows that $x^m \equiv (-1)^r \pmod{p}$. But $x^m \equiv \left(\frac{x}{p}\right) \pmod{p}$ by Lemma 1.35. Therefore $\left(\frac{x}{p}\right) \equiv (-1)^r \pmod{p}$, and hence $\left(\frac{x}{p}\right) = (-1)^r$, as required. ∎

Let $n$ be an odd integer. Then $n = 2k+1$ for some integer $k$. Then $n^2 = 4(k^2+k)+1$, and $k^2+k$ is an even integer. It follows that if $n$ is an odd integer then $n^2 \equiv 1 \pmod{8}$, and hence $(-1)^{(n^2-1)/8} = \pm 1$.

**Theorem 1.39** *Let $p$ be an odd prime number. Then $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.*

**Proof** The value of $(-1)^{(p^2-1)/8}$ is determined by the congruence class of $p$ modulo 8. Indeed $(-1)^{(p^2-1)/8} = 1$ when $p \equiv 1 \pmod{8}$ or $p \equiv -1 \pmod{8}$, and $(-1)^{(p^2-1)/8} = -1$ when $p \equiv 3 \pmod{8}$ or $p \equiv -3 \pmod{8}$.

Let $m = (p-1)/2$. It follows from Lemma 1.38 that $\left(\frac{2}{p}\right) = (-1)^r$, where $r$ is the number of integers $x$ between 1 and $m$ for which $2x$ is not congruent modulo $p$ to any integer between 1 and $m$. But the integers $x$ with this property are those for which $m/2 < x \leq m$. Thus $r = m/2$ if $m$ is even, and $r = (m+1)/2$ if $m$ is odd.

If $p \equiv 1 \pmod 8$ then $m$ is divisible by 4 and hence $r$ is even. If $p \equiv 3 \pmod 8$ then $m \equiv 1 \pmod 4$ and hence $r$ is odd. If $p \equiv 5 \pmod 8$ then $m \equiv 2 \pmod 4$ and hence $r$ is odd. If $p \equiv 7 \pmod 8$ then $m \equiv 3 \pmod 4$ and hence $r$ is even. Therefore $\left(\frac{2}{p}\right) = 1$ when $p \equiv 1 \pmod 8$ and when $p \equiv 7 \pmod 8$, and $\left(\frac{2}{p}\right) = -1$ when $p \equiv 3 \pmod 8$ and $p \equiv 5 \pmod 8$. Thus $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$ for all odd prime numbers $p$, as required. ∎

## 1.14 Quadratic Reciprocity

**Theorem 1.40** (Quadratic Reciprocity Law) *Let $p$ and $q$ be distinct odd prime numbers. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$$

**Proof** Let $S$ be the set of all ordered pairs $(x, y)$ of integers $x$ and $y$ satisfying $1 \leq x \leq m$ and $1 \leq y \leq n$, where $p = 2m+1$ and $q = 2n+1$. We must prove that $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{mn}$.

First we show that $\left(\frac{p}{q}\right) = (-1)^a$, where $a$ is the number of pairs $(x, y)$ of integers in $S$ satisfying $-n \leq py - qx \leq -1$. If $(x, y)$ is a pair of integers in $S$ satisfying $-n \leq py - qx \leq -1$, and if $z = qx - py$, then $1 \leq y \leq n$, $1 \leq z \leq n$ and $py \equiv -z \pmod q$. On the other hand, if $(y, z)$ is a pair of integers such that $1 \leq y \leq n$, $1 \leq z \leq n$ and $py \equiv -z \pmod q$ then there is a unique positive integer $x$ such that $z = qx - py$. Moreover $qx = py + z \leq (p+1)n = 2n(m+1)$ and $q > 2n$, and therefore $x < m+1$. It follows that the pair $(x, y)$ of integers is in $S$, and $-n \leq py - qx \leq -1$. We deduce that the number $a$ of pairs $(x, y)$ of integers in $S$ satisfying $-n \leq py - qx \leq -1$ is equal to the number of pairs $(y, z)$ of integers satisfying $1 \leq y \leq n$, $1 \leq z \leq n$ and $py \equiv -z \pmod q$. It now follows from Lemma 1.38 that $\left(\frac{p}{q}\right) = (-1)^a$. Similarly $\left(\frac{q}{p}\right) = (-1)^b$, where $b$ is the number of pairs $(x, y)$ in $S$ satisfying $1 \leq py - qx \leq m$.

If $x$ and $y$ are integers satisfying $py - qx = 0$ then $x$ is divisible by $p$ and $y$ is divisible by $q$. It follows from this that $py - qx \neq 0$ for all pairs $(x, y)$ in $S$. The total number of pairs $(x, y)$ in $S$ is $mn$. Therefore $mn = a+b+c+d$, where $c$ is the number of pairs $(x, y)$ in $S$ satisfying $py - qx < -n$ and $d$ is the number of pairs $(x, y)$ in $S$ satisfying $py - qx > m$.

Let $(x, y)$ be a pair of integers in $S$, and let and let $x' = m + 1 - x$ and $y' = n + 1 - y$. Then the pair $(x', y')$ also belongs to $S$, and $py' - qx' = m - n - (py - qx)$. It follows that $py - qx > m$ if and only if $py' - qx' < -n$. Thus there is a one-to-one correspondence between pairs $(x, y)$ in $S$ satisfying $py - qx > m$ and pairs $(x', y')$ in $S$ satisfying $py' - qx' < -n$, where $(x', y') = (m + 1 - x,\ n + 1 - y)$ and $(x, y) = (m + 1 - x',\ n + 1 - y')$. Therefore $c = d$, and thus $mn = a + b + 2c$. But then $(-1)^{mn} = (-1)^a(-1)^b = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right)$, as required. ∎

**Corollary 1.41** *Let $p$ and $q$ be distinct odd prime numbers. If $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$ then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$. If $p \equiv 3 \pmod 4$ and $q \equiv 3 \pmod 4$ then $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.*

**Example** We wish to determine whether or not 654 is a quadratic residue modulo the prime number 239. Now $654 = 2 \times 239 + 176$ and thus $654 \equiv 176 \pmod{239}$. Also $176 = 16 \times 11$. Therefore

$$\left(\frac{654}{239}\right) = \left(\frac{176}{239}\right) = \left(\frac{16}{239}\right)\left(\frac{11}{239}\right) = \left(\frac{4}{239}\right)^2\left(\frac{11}{239}\right) = \left(\frac{11}{239}\right)$$

But $\left(\frac{11}{239}\right) = -\left(\frac{239}{11}\right)$ by the Law of Quadratic Reciprocity. Also $239 \equiv 8 \pmod{11}$. Therefore

$$\left(\frac{239}{11}\right) = \left(\frac{8}{11}\right) = \left(\frac{2}{11}\right)^3 = (-1)^3 = -1$$

It follows that $\left(\frac{654}{239}\right) = +1$ and thus 654 is a quadratic residue of 239, as required. ∎

## 1.15 The Jacobi Symbol

Let $s$ be an odd positive integer. If $s > 1$ then $s = p_1 p_2 \cdots p_m$, where $p_1, p_2, \ldots, p_m$ are odd prime numbers. For each integer $x$ we define the *Jacobi*

*symbol* $\left(\frac{x}{s}\right)$ by

$$\left(\frac{x}{s}\right) = \prod_{i=1}^{m} \left(\frac{x}{p_i}\right)$$

(i.e., $\left(\frac{x}{s}\right)$ is the product of the Legendre symbols $\left(\frac{x}{p_i}\right)$ for $i = 1, 2, \ldots, m$.) We define $\left(\frac{x}{1}\right) = 1$.

Note that the Jacobi symbol can have the values 0, +1 and −1.

**Lemma 1.42** *Let $s$ be an odd positive integer, and let $x$ be an integer. Then $\left(\frac{x}{s}\right) \neq 0$ if and only if $x$ is coprime to $s$.*

**Proof** Let $s = p_1 p_2 \cdots p_m$, where $p_1, p_2, \ldots, p_m$ are odd prime numbers. Suppose that $x$ is coprime to $s$. Then $x$ is coprime to each prime factor of $s$, and hence $\left(\frac{x}{p_i}\right) = \pm 1$ for $i = 1, 2, \ldots, m$. It follows that $\left(\frac{x}{s}\right) = \pm 1$ and thus $\left(\frac{x}{s}\right) \neq 0$.

Next suppose that $x$ is not coprime to $s$. Let $p$ be a prime factor of the greatest common divisor of $x$ and $s$. Then $p = p_i$, and hence $\left(\frac{x}{p_i}\right) = 0$ for some integer $i$ between 1 and $m$. But then $\left(\frac{x}{s}\right) = 0$. ∎

**Lemma 1.43** *Let $s$ be an odd positive integer, and let $x$ and $x'$ be integers. Suppose that $x \equiv x' \pmod{s}$. Then $\left(\frac{x}{s}\right) = \left(\frac{x'}{s}\right)$.*

**Proof** If $x \equiv x' \pmod{s}$ then $x \equiv x' \pmod{p}$ for each prime factor $p$ of $s$, and therefore $\left(\frac{x}{p}\right) = \left(\frac{x'}{p}\right)$ for each prime factor of $s$. Therefore $\left(\frac{x}{s}\right) = \left(\frac{x'}{s}\right)$. ∎

**Lemma 1.44** *Let $x$ and $y$ be integers, and let $s$ and $t$ be odd positive integers. Then $\left(\frac{xy}{s}\right) = \left(\frac{x}{s}\right)\left(\frac{y}{s}\right)$ and $\left(\frac{x}{st}\right) = \left(\frac{x}{s}\right)\left(\frac{x}{t}\right)$.*

**Proof** $\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$ for all prime numbers $p$ (Corollary 1.34). The required result therefore follows from the definition of the Jacobi symbol. ∎

**Lemma 1.45** $\left(\frac{x^2}{s}\right) = 1$ *and* $\left(\frac{x}{s^2}\right) = 1$ *for for all odd positive integers $s$ and all integers $x$ that are coprime to $s$.*

**Proof** This follows directly from Lemma 1.44 and Lemma 1.42. ∎

**Theorem 1.46** $\left(\frac{-1}{s}\right) = (-1)^{(s-1)/2}$ *for all odd positive integers* $s$.

**Proof** Let $f(s) = (-1)^{(s-1)/2}\left(\frac{-1}{s}\right)$. for each odd positive integer $s$. We must prove that $f(s) = 1$ for all odd positive integers $s$. If $s$ and $t$ are odd positive integers then

$$(st-1)-(s-1)-(t-1) = st-s-t+1 = (s-1)(t-1)$$

But $(s-1)(t-1)$ is divisible by 4, since $s$ and $t$ are odd positive integers. Therefore $(st-1)/2 \equiv (s-1)/2+(t-1)/2 \pmod 2$, and hence $(-1)^{(st-1)/2} = (-1)^{(s-1)/2}(-1)^{(t-1)/2}$. It now follows from Lemma 1.44 that $f(st) = f(s)f(t)$ for all odd numbers $s$ and $t$. But $f(p) = 1$ for all prime numbers $p$, since $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ (Lemma 1.37). It follows that $f(s) = 1$ for all odd positive integers $s$. as required. ∎

**Theorem 1.47** $\left(\frac{2}{s}\right) = (-1)^{(s^2-1)/8}$ *for all odd positive integers* $s$.

**Proof** Let $g(s) = (-1)^{(s^2-1)/8}\left(\frac{2}{s}\right)$. for each odd positive integer $s$. We must prove that $g(s) = 1$ for all odd positive integers $s$. If $s$ and $t$ are odd positive integers then

$$(s^2t^2-1)-(s^2-1)-(t^2-1) = s^2t^2-s^2-t^2+1 = (s^2-1)(t^2-1).$$

But $(s^2-1)(t^2-1)$ is divisible by 64, since $s^2 \equiv 1 \pmod 8$ and $t^2 \equiv 1 \pmod 8$. Therefore $(s^2t^2-1)/8 \equiv (s^2-1)/8+(t^2-1)/8 \pmod 8$, and hence $(-1)^{(s^2t^2-1)/8} = (-1)^{(s^2-1)/8}(-1)^{(t^2-1)/8}$. It now follows from Lemma 1.44 that $g(st) = g(s)g(t)$ for all odd numbers $s$ and $t$. But $g(p) = 1$ for all prime numbers $p$, since $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$ (Lemma 1.39). It follows that $g(s) = 1$ for all odd positive integers, as required. ∎

**Theorem 1.48** $\left(\frac{s}{t}\right)\left(\frac{t}{s}\right) = (-1)^{(s-1)(t-1)/4}$ *for all odd positive integers* $s$ *and* $t$.

**Proof** Let $h(s,t) = (-1)^{(s-1)(t-1)/4}\left(\frac{s}{t}\right)\left(\frac{t}{s}\right)$. We must prove that $h(s,t) = 1$ for all odd positive integers $s$ and $t$. Now $h(s_1s_2,t) = h(s_1,t)h(s_2,t)$ and $h(s,t_1)h(s,t_2) = h(s,t_1t_2)$ for all odd positive integers $s$, $s_1$, $s_2$, $t$, $t_1$ and $t_2$.

Also $h(s,t) = 1$ when $s$ and $t$ are prime numbers by the Law of Quadratic Reciprocity (Theorem 1.40). It follows from this that $h(s,t) = 1$ when $s$ is an odd positive integer and $t$ is a prime number, since any odd positive integer is a product of odd prime numbers. But then $h(s,t) = 1$ for all odd positive integers $s$ and $t$, as required. ∎

The results proved above can be used to calculate Jacobi symbols, as in the following example.

**Example** We wish to determine whether or not 442 is a quadratic residue modulo the prime number 751. Now $\left(\frac{442}{751}\right) = \left(\frac{2}{751}\right)\left(\frac{221}{751}\right)$. Also $\left(\frac{2}{751}\right) = 1$, since $751 \equiv 7 \pmod 8$ (Theorem 1.39). Also $\left(\frac{221}{751}\right) = \left(\frac{751}{221}\right)$ (Theorem 1.48), and $751 \equiv 88 \pmod{221}$. Thus

$$\left(\frac{442}{751}\right) = \left(\frac{751}{221}\right) = \left(\frac{88}{221}\right) = \left(\frac{2}{221}\right)^3\left(\frac{11}{221}\right).$$

Now $\left(\frac{2}{221}\right) = -1$, since $221 \equiv 5 \pmod 8$ (Theorem 1.47). Also it follows from Theorem 1.48 that

$$\left(\frac{11}{221}\right) = \left(\frac{221}{11}\right) = \left(\frac{1}{11}\right) = 1,$$

since $221 \equiv 1 \pmod 4$ and $221 \equiv 1 \pmod{11}$. Therefore $\left(\frac{442}{751}\right) = -1$, and thus 442 is a quadratic non-residue of 751. The number 221 is not prime, since $221 = 13 \times 17$. Thus the above calculation made use of Jacobi symbols that are not Legendre symbols.