Projects on elliptic curves and modular forms

Math 480, Spring 2010

In the following are 11 projects for this course. Some of the projects are rather ambitious and may very well be the topic of a master thesis. Your report/presentation do *not* need to carry the project(s) all the way through. Rather you want to understand an interesting part of the project and present it in your own words. Some projects can be shared among two or three people, with each person doing a different part.

1. **Nagell-Lutz Theorem on torsion points of an elliptic curve**

   Theorem. Let $y^2 = f(x)$ be the Weierstrass form of an elliptic curve over $\mathbb{Q}$, where $f(x) = x^3 + a\,x^2 + b\,x + c \in \mathbb{Z}[x]$ is a cubic polynomial with integer coefficients, whose discriminant D is non-zero. Let $P = (u, v)$ be a $\mathbb{Q}$-rational *torsion* point of E, i.e. P is a point of *finite* order. Then either $v = 0$ or u, v are both integers and v divides D.

   References:

   1. J. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Chapter 2.
   2. E. Lutz, Sur l'equation $y^2 = x^3 - Ax - B$ dans les corps p-adic, J. Reine Angew. Math. **177** (1937), 237–247;
   3. T. Nagell, Solution de quelque problèmes dans la théorie arithmétiques des cubique planes du permiere genre. Wid. Akad. Skrifter Oslo I (1935), Nr. 1.

2. **Functional equations for the theta function**

   The theta function $\theta(\tau) = \sum_{n \in bbZ} e^{\pi\sqrt{-1}\,n^2\tau}$ is a modular form of weight $1/2$ for a congruence subgroup same for the related function $\Theta(\tau) = \theta(2\tau) = \sum_{n \in bbZ} e^{2\pi\sqrt{-1}\,n^2\tau}$. The functional equation relates $\theta(-\frac{1}{\tau})$ to $\theta(\tau)$. The standard proof uses the Poisson summation formula, applied to the function $e^{\pi\sqrt{-1}\tau x^2}$ on $\mathbb{R}$. This proof can be found in a variety of books, and is an exercise as an application of the Poisson summation formula. Getting from the function equation for the element $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ to the whole modular group is an exercise in group theory; the result of the exercise is an explicit formula which

relates $\theta(\gamma \cdot \tau)$ to $\theta(\tau)$ for an arbitrary element $\gamma \in \Gamma(1)$ with a formula for an explicit "factor of automorphy" on $\Gamma(1)$.

On the other hand, the theta function in two variables

$$\theta(\tau, z) = \sum_{n \in \mathbb{Z}} e^{\pi\sqrt{-1}\, n^2 \tau} + e^{2\pi\sqrt{-1}\, nz} \qquad \tau \in \mathfrak{H},\ z \in \mathbb{C}$$

satisfies the heat equation, a partial differential equation. It also satisfies a functional equation for the discrete group $\Gamma(1) \rtimes \mathbb{Z}^2$ acting on $\mathfrak{H} \times \mathbb{C}$. The Poisson summation formula then gives *Riemann's theta relations*; it is a (collection of) quadratic equation(s) with a fixed τ.

A good reference is D. Mumford, *Tata Lectures on Theta I*, Chapter 1.

3. **Proof of quadratic reciprocity using theta function.**

The Jacobi theta function $\theta(\tau)$ is a modular form of weight $\frac{1}{2}$. The coefficient of the leading term of its asymptotic expansion near a cusp $\frac{a}{b} \in \mathbb{Q} \subset \mathbb{P}^1(\mathbb{Q}))$ determines the quadratic Gauss sum

$$G(a, b) := \frac{1}{\sqrt{b}} \sum_{i=1}^{b} e^{\pi\sqrt{-1}\, i^2}\ .$$

Here $a, b \in \mathbb{Z}$ are positive integers with $\gcd(a, b) = 1$. The functional equation for $\theta(\tau)$ gives a *reciprocity law for Gauss sums* which relates $G(a, b)$ and $G(-b, a)$. The reciprocity law for the Legendre symbol follows.

This method is due to Cauchy and Kronecker and is classical. A good reference is pages 46–56 of C. L. Siegel, *Analytische Zahlentheorie*, 2. Teil, Vorlesung WS 1963/64, Mathematisches Institut, Göttingen. An account of the reciprocity law for Gauss sums, in English, can also be found in § 29 of Bellman, *A Brief Introduction to Theta functions*. Chapter 8 of E. Hecke, *Lectures on the Theory of Algebraic Numbers* extends this method to treat quadratic reciprocity for general algebraic number fields.

4. **Binary quadratic forms**

Binary quadratic forms over $\mathbb{Z}$ was treated in Gauss's *Disquisitions Arithmeticae*. The set of equivalence classes of integral binary quadratic

forms modulo $\mathrm{SL}_2(\mathbb{Z})$ with a fixed discriminant D is finite; its cardinality is denoted by $h(D)$ and called the *class number* with discriminant D. The reduction of definite quadratic forms is closely related to the fundamental domain of the action of the modular group $\Gamma(1)$ on the upper-half plane $\mathfrak{H}$; it is often more natural to consider the action of $\mathrm{GL}_2(\mathbb{Z})$ on $\mathfrak{H}^{\pm}$.

For any *fundamental discriminant* D (i.e. D cannot be written as $D' \cdot r^2$ with $r > 1$ and $D' \equiv 0$ or $1 \pmod 4$), there is a natural bijection between the set of all equivalence classes of binary quadratic forms D and the set of all ideal classes in the quadratic field $\mathbb{Q}(\sqrt{D})$. The class number $h(D)$ is closely related to the value $L(\chi_D, 1)$ of the L-function attached to the Dirichlet character χ_D, and there is a classical formula for this L-value.

For a fixed fundamental discriminant $D < 0$ and let χ be either the trivial character or the Dirichlet character with discriminant D, one can form a weight-1 modular form

$$f_{\chi,D}(\tau) = \frac{1}{w_{\mathbb{Q}(\sqrt{D})}} \sum_I \chi(I) \Theta_I(\tau) = \frac{1}{w_{\mathbb{Q}(\sqrt{D})}} \sum_I \chi(I) \sum_{n \geq 0} r_I(n) q^n \,,$$

where $w_{\mathbb{Q}(\sqrt{D})}$ is the number of roots of unity in the imaginary quadratic field $\mathbb{Q}(\sqrt{D})$ and $r_I(n)$ is the number of elements of norm n in the ideal I of the ring $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ of all algebraic integers in the quadratic field $\mathbb{Q}(\sqrt{D})$. In the case when one has another formula for the modular form $f_{\chi,D}$, for instance an infinite product expansion coming from the Dedekind η-function, one gets an explicit formula for the representation numbers $r_I(n)$.

References.

- David Cox, *Primes of the form $ax^2 + by^2$*; Chapter 1, §2 and §3 is a good reference of the more basic part of the theory.
- E. Landau, *Elementary Number Theory*. It is a classic; with nice treatment of the algebraic (genus theory) and analytic theory of binary quadratic forms.
- D. Zagier, Elliptic modular forms and their applications; in *The 1-2-3 of Modular Forms*, pp. 42–43 gives a rapid indication of the case of binary quadratic forms with discriminant -23.

5. **Mordell's theorem**

   The statement of Mordell's theorem is simple and elegant: *The group of rational points of any elliptic curve over $\mathbb{Q}$ is finitely generated.* Weil generalized this statement to *abelian varieties*, so this theorem is usually called the "Mordell-Weil theorem".

   An exposition of Mordell's theorem at an elementary level can be found in Chapter 3 of Silverman-Tate. An essential related concept is the notion of the *height* of a rational point.

   References. J. Silverman and J. Tate, *Rational Points on Elliptic Curves.*

6. **Elliptic curves over $\mathbb{Q}$ with no rational point of infinite order**

   According to Mordell's theorem, the group of rational points of any elliptic curve over $\mathbb{Q}$ is finitely generated. There are some elliptic curves over $\mathbb{Q}$ whose group of rational points is finite. As of now there is no algorithm which determines whether a given elliptic curve over $\mathbb{Q}$ has a rational point of infinite order; the congruent number problem is a special case of this more general problem.

   This project, in general terms, is to give explicit examples of elliptic curves over $\mathbb{Q}$ with no rational points of infinite order. One such example, due to Fermat, is the curve $y^2 = x^3 - x$. (In other words $n = 1$ is not a congruent number.)

   An interesting example, due to Selmer, is the curve $3\,X^3+4\,Y^3+5\,Z^3$. This curve has no non-trivial rational point, while for every integer $m > 1$ the congruence equation $3\,X^3 + 4\,Y^3 + 5\,Z^3 \equiv 0 \pmod{m}$ has a non-trial solution. (One says that the *Hasse principle* does *not* hold for this example.) A reference for this example is Selmer's famous paper in *Acta Math.* **85** (1951), 203–362.

   For quadratic equations the Hasse principle holds. A good reference is Chapter 4 of Serre's *A course in Arithmetic.*

7. **Product formula for the discriminant function.**

   The product formula $\Delta(\tau) = (2\pi)^1 2\,q \prod_{n\geq 1} q^n$ for the discriminant function Δ can be proved in a number of ways. The "most natural" proof uses elliptic functions; see Chapter 18 of Lang's book on elliptic functions.

An account of Hurwitz's proof is sketched in Chapter 7, 4.4 of Serre's book, which will be explained in class. This proof goes by way of the functional equation for the weight 2 Eisenstein series $G_2(\tau)$; a proof of this functional equation using "Hecke's trick" can be found in 2.3 of Zagier's article.

There is also an "elementary proof" of Siegel, based on residue calculus and is quite short. The good part is that it is quite straight forward. Its drawback is that the proof gives no additional insight or better understanding.

References.

- S. Lang, *Elliptic Functions*. A proof of the product expansion of the discriminant function can be found in Chapter 18, § 4.
- J.-P. Serre, *A Course in Arithmetic*.
- D. Zagier, Elliptic modular forms and their applications; in *The 1-2-3 of Modular Forms*, pp. 42–43 gives a rapid indication of the case of binary quadratic forms with discriminant -23.
- C. L. Siegel, Gesamm. Abh. no. 62.

8. **Complex multiplication of elliptic curves.**

An elliptic curve E over $\mathbb{C}$ is said to have *complex multiplication* if it has an endomorphism which is not multiplication by an integer; if this is the case $\mathrm{End}_{\mathbb{C}}(E)$ is a subring of an imaginary quadratic field K which is strictly bigger than $\mathbb{Z}$.

The j-invariant of a CM elliptic curve E as above is an algebraic *integer*. Mover $K(j(E))$ is an *abelian extension* of K; it is a *ring class field* for K. Using a CM elliptic curve E with CM by an imaginary quadratic field K, one can use this curve E and values of special functions related to E (e.g. its j-invariant and the values of the Weierstrass $\wp$-function for E on torsion points of E) to generate abelian extensions of K.

An interesting related phenomenon is that the exponential of certain numbers of the form $\pi\, a$, where a belongs to a real quadratic field, are very close to an integer. One such example is $e^{\pi\sqrt{163}}$. The key facts for this example is the q-expansion of the j-function (a general fact), and the fact that the imaginary quadratic field $\mathbb{Q}(\sqrt{-163}$ has class number one.

References.

- D. Cox, *Primes of the form* $a\,x^2 + b\,y^2$, Chapter 3.
- J. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Chapter 6.

9. **Product formula for theta functions.**

This is a product expansion of $\theta(\tau, z) = \sum_{n\in\mathbb{Z}} e^{\pi\sqrt{-1}\,n^2\tau} + e^{2\pi\sqrt{-1}\,nz}$ In two variables $\tau \in \mathfrak{H},\ z \in \mathbb{C}$, due to Jacobi:

$$\theta(\tau, z) = \prod_{m\in\mathbb{N}} (1-e^{2\pi\sqrt{-1}\,\tau}) \cdot \prod_{m\in\mathbb{N}_{>0}} \left[(1 + e^{\pi\sqrt{-1}\,(2m+1)\tau - 2\pi\sqrt{-1}\,z})\,(1 + e^{\pi\sqrt{-1}\,(2m+1)\tau + 2\pi\sqrt{-1}\,z})\right]$$

The above formula specializes to many product formulas for theta functions in one variable τ.

A good reference is Chapter 1, § 14 of Mumford's *Tata Lectures on Theta I*. A "more elementary" proof of Jacobi's product formula can be found in 19.6 of Hardy and Wright, *The Theory of Numbers*, as theorem 352. One can also find many applications in Chapter 19–20 of Hardy and Wright.

10. **Representation of an integer of sum of squares.**

A typical theorem in this direction is Jacobi's formula for the number $r_4(n)$ of ways a positive integer n can be written as $x^2 + y^2$ with $(x, y) \in \mathbb{Z}^2$:

$$r_4(n) = \begin{cases} 8 \sum_{d|n} d & \text{if } n \equiv 1 \pmod 2 \\ 24 \sum_{\substack{d|n \\ d \text{ odd}}} d & \text{if } n \equiv 0 \pmod 2 \end{cases}$$

Such results are typically proved using theta functions, which by definition have q-expansions with *representation numbers* as coefficients. Then one establishes an equality with another modular form, typically an Eisenstein series, which yields the formula by comparing coefficients.

An interesting application is *examples of drums whose shape you cannot hear*. This refers to examples of two non-equivalent unimodular integral quadratic forms in 16 variables with the same *spectrum*, i.e. they have the same representation numbers.

References.

- D. Mumford, *Tata Lectures on Theta I*, § 15.
- J.-P. Serre, *A Course in Arithmetic*, Chapter 7, §6 and Chapter 5.

11. **Hecke operators for congruence subgroups.**

We will explain the basics about Hecke operators for the full modular group $\Gamma(1)$ in class, along the lines as in Chapter 7 § 5 of Serre's *A Course in Arithmetic*. These *Hecke symmetries* are what we are left with after taking the quotient of $\mathfrak{H}$ by a discrete subgroup such as $\Gamma(1)$: the group $\mathrm{GL}_2(\mathbb{Q})$ does not operate on the quotient, but there are still some group-like symmetry left. These Hecke symmetries give rise to intricate algebraic structures for modular forms.

The goal of this project is to extend the basic theory of Hecke operators to congruence subgroups.

References.

- A. Ogg, *Modular Forms and Dirichlet Series.*
- J.-P. Serre, *A Course in Arithmetic.*
- G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions.*, Chapter 3.