

Ma 105: Elliptic Curves
California Institute of Technology

Edray Herber Goins

October 2002 - December 2002

Contents

1	Lecture 1: Monday, September 30	7
1.1	Course Information	7
1.1.1	Instructor	7
1.1.2	Meeting Times	7
1.1.3	Suggested Textbook	7
1.1.4	Homework	7
1.1.5	Grading Policy	7
1.1.6	Course Topics	8
1.2	Diophantine Equations	8
1.2.1	Chord-Tangent Construction	8
1.2.2	Quartic and Cubic Equations	9
1.3	Elliptic Curves	10
1.3.1	Weierstrass Form	10
1.3.2	What is an Elliptic Curve?	10
2	Lecture 2: Wednesday, October 2	11
2.1	Elliptic Curves over \mathbb{C}	11
2.1.1	Relation with Ellipses	11
2.1.2	Relation with the Torus	12
2.1.3	Weierstrass \wp -Function	13
2.2	Group Law	13
2.2.1	Addition	13
2.2.2	Multiplication by m Maps	15
2.2.3	Associativity	15
3	Homework Assignment #1	16
4	Lecture 3: Monday, October 7	18
4.1	Modular Functions	18
4.1.1	Action on the Upper-Half Plane	18
4.1.2	The Fundamental Region	19
4.1.3	Modular Forms and Modular Functions	19
4.1.4	Weierstrass Function Again	20
4.2	Points of Finite Order	21

4.2.1	Torsion Points	21
4.2.2	Torsion Subgroup	22
5	Lecture 4: Wednesday, October 9	23
5.1	The Modular Group	23
5.1.1	Congruence Subgroups	23
5.1.2	Relation with the Special Linear Group	24
5.2	Galois Groups	24
5.2.1	Galois Representations	24
5.2.2	$N = 2$ Case	25
5.2.3	$N = 3$ Case	25
5.3	Subfields of $\mathbb{Q}(E[N])$	26
5.3.1	Subgroups of $GL_2(\mathbb{Z}/N\mathbb{Z})$	26
5.3.2	$N = 3$ Case Revisited	26
6	Homework Assignment #2	27
7	Lecture 5: Monday, October 14	29
7.1	Modular Curves	29
7.1.1	Notation	29
7.1.2	Curves of level N	30
7.1.3	N Isogenies	30
7.2	Subgroups of Order p	30
7.2.1	General Theory	30
7.2.2	Atkin-Lehner Theory	31
7.2.3	Galois Theory	31
7.2.4	$p = 2$ Case	32
7.2.5	$p = 3$ Case	32
7.2.6	$p = 5$ Case	33
8	Lecture 6: Wednesday, October 16	34
8.1	Points of Order p	34
8.1.1	Normal Forms	34
8.1.2	$p = 2$ Case	35
8.1.3	Points of Order 3	35
8.1.4	$p = 5$ Case	35
8.2	Basis for p -Torsion	36
8.2.1	Genus of $X(p)$	36
8.2.2	$p = 2$ Case	36
8.2.3	$p = 3$ Case	36
8.2.4	$p = 5$ Case	37
9	Homework Assignment #3	38

10 Lecture 7: Monday, October 21	40
10.1 My Favorite Elliptic Curve	40
10.1.1 Basic Properties	40
10.1.2 Rational Points	40
10.1.3 Mordell-Weil Group	41
10.2 Triangles with Concurrent Cevians	41
10.2.1 Triangles to Elliptic Curves	41
10.2.2 Elliptic Curves to Triangles	42
10.3 Period Maps and Elliptic Logarithms	42
10.3.1 The Real Lattice	42
10.3.2 Approximations at Infinity	43
11 Lecture 8: Wednesday, October 23	44
11.1 Period Maps and Elliptic Logarithms (continued)	44
11.1.1 Elliptic Curves Over \mathbb{R}	44
11.1.2 Relation with the Circle	45
11.1.3 Approximations at Infinity	46
11.2 Heron Triangles	47
11.2.1 Basic Formulas	47
11.2.2 Relation with Rectangles	47
12 Homework Assignment #4	49
13 Lecture 9: Monday, October 28	51
13.1 Congruent Numbers	51
13.1.1 Right Heron Triangles	51
13.1.2 Congruent Numbers	51
13.1.3 Tunnell's Theorem	52
13.1.4 Elliptic Curves	52
13.2 The Elliptic Curve $E^{(n)}$	53
13.2.1 Torsion Points	53
13.2.2 Ranks of Twists of Curves	54
14 Lecture 10: Wednesday, October 30	56
14.1 Heron Triangles	56
14.1.1 Motivation	56
14.1.2 Elliptic Curves	57
14.2 The Elliptic Curve $E_r^{(n)}$	58
14.2.1 2-Torsion	58
14.2.2 3-Torsion	58
14.2.3 4-Torsion	59
14.2.4 Mazur's Theorem	60
14.3 Main Theorem	61
14.3.1 Points of Infinite Order	61
14.3.2 Examples	61

15 Homework Assignment #5	63
16 Lecture 11: Monday, November 4	65
16.1 Solvability of the Quintic	65
16.1.1 History	65
16.1.2 Solvable by Radicals?	65
16.1.3 Frobenius Group	66
16.1.4 Bring-Jerrard Form	66
16.1.5 Tschirnhausen Transformations	66
16.2 Klein's Work	67
16.2.1 Motivation	67
16.2.2 Sketch of Discussion	68
16.2.3 Geometry of the Icosahedron	68
17 Lecture 12: Wednesday, November 6	70
17.1 Klein's Work (continued)	70
17.1.1 Stereographic Projection	70
17.1.2 Invariant Polynomials	71
17.1.3 Klein's Results	72
17.1.4 Modular Functions	72
17.1.5 Klein's Results Revisited	73
17.1.6 Applications	74
18 Homework Assignment #6	75
19 Lecture 13: Monday, November 11	77
19.1 Factoring Integers	77
19.1.1 Motivation	77
19.1.2 Pollard's $p - 1$ Algorithm	78
20 Lecture 14: Wednesday, November 13	80
20.1 Elliptic Curves Over Finite Fields	80
20.1.1 Reduction Modulo Primes	80
20.1.2 Gauss's Theorem	81
20.1.3 Hasse-Weil Inequality	82
21 Homework Assignment #7	83
22 Lecture 15: Monday, November 18	85
22.1 Elliptic Curves Over Finite Fields (continued)	85
22.1.1 Reduction Modulo p Theorem	85
22.1.2 Elliptic Curves over $\mathbb{Z}/n\mathbb{Z}$	86
22.2 Elliptic Curve Factoring Method	87
22.2.1 Motivation	87

23 Lecture 16: Wednesday, November 20	88
23.1 Elliptic Curve Factoring Method (continued)	88
23.1.1 Lenstra's Elliptic Curve Algorithm	88
23.1.2 Worked Example	89
23.1.3 Actual Implementations	90
23.2 Elliptic Curve Primality Proving	91
23.2.1 Motivation	91
23.2.2 Primality Proving for Pollard's Algorithm	91
24 Homework Assignment #8	92
25 Lecture 17: Monday, November 25	93
25.1 Elliptic Curve Primality Proving (continued)	93
25.1.1 Primality Proving for Pollard's Algorithm	93
25.1.2 Lucas's Test	93
25.1.3 Primality Proving for Elliptic Curves	94
25.2 Fermat's Last Theorem	94
25.2.1 Fermat's Conjecture	94
25.2.2 Case-by-Case Analysis	94
25.2.3 General Remarks	95
25.2.4 The Frey Curve	96
26 Lecture 18: Wednesday, November 27	97
26.1 Modular Forms	97
26.1.1 Cusp Forms of Weight 2	97
26.1.2 q -Expansions	98
26.1.3 Relation with Modular Curves	98
26.1.4 Dimension of Space of Cusp Forms	98
26.1.5 Examples of Cusp Forms	99
26.1.6 Hecke Operators	99
26.1.7 Petersson Pairing	100
27 Homework Assignment #9	101
28 Lecture 19: Monday, December 2	103
28.1 Modular Forms (continued)	103
28.1.1 Normalized Eigenform	103
28.1.2 Functional Equation	104
28.2 Modular Elliptic Curves	104
28.2.1 Jacobians of Modular Curves	104
28.2.2 Action by the Hecke Algebra	105
28.2.3 Shimura's Construction	105
28.3 Elliptic Curves	106
28.3.1 Isogenies	106
28.3.2 Conductor	107
28.3.3 L -Series	107

28.3.4	Taniyama-Shimura Conjecture	108
29	Lecture 20: Wednesday, December 4	109
29.1	Proof of Fermat's Conjecture	109
29.1.1	Relation with Frey's Curve	109
29.1.2	Conductor of the Frey Curve	110
29.1.3	Galois Representations	110
29.1.4	Wiles' Approach	111
29.1.5	Universal Deformation Ring	112
29.1.6	The " $R = \mathbb{T}$ " Argument	112
30	Homework Assignment #10	114

Chapter 1

Lecture 1: Monday, September 30

1.1 Course Information

1.1.1 Instructor

Edray Herber Goins. Office: 276 Sloan. Phone: (626) 395-4347. E-Mail: goins@caltech.edu.

1.1.2 Meeting Times

Mondays and Wednesdays from 12:30 PM through 2:00 PM in 257 Sloan.

1.1.3 Suggested Textbook

We will a variety of research papers (which will be posted on the course web site), but the text which will explain concepts in more detail will be Joseph Silverman's *The Arithmetic of Elliptic Curves* as published by Springer Verlag. Copies may be purchased at the Caltech bookstore for around \$60.

1.1.4 Homework

There will be four (4) problems a week, due on Monday morning at the start of lecture. If you do not plan to attend lecture, homework must be placed in instructors mailbox *before* lecture begins. Late homework will be penalized at 10% each day.

1.1.5 Grading Policy

There will only be weekly homework.

1.1.6 Course Topics

We'll cover the following:

Week	Dates	Topics
Week 1	9/30/02 - 10/4/02	Elliptic Curves and the Group Law
Week 2	10/7/02 - 10/11/02	Points of Finite Order
Week 3	10/14/02 - 10/18/02	Elliptic Curves and Geometry
Week 4	10/21/02 - 10/25/02	Congruent Numbers
Week 5	10/28/02 - 11/1/02	Factorization Methods
Week 6	11/4/02 - 11/8/02	Primality Proving
Week 7	11/11/02 - 11/15/02	Application to Nonsolvable Quintics
Week 8	11/18/02 - 11/22/02	Galois Representations
Week 9	11/25/02 - 11/27/02	Modular Forms
Week 10	12/2/02 - 12/6/02	Fermat's Last Theorem

1.2 Diophantine Equations

1.2.1 Chord-Tangent Construction

Say that we wish to find rational points on the unit circle $x^2 + y^2 = 1$. Since this curve involves quadratic polynomials, once we have one rational point on the curve, we can draw a line through this point to find a second rational point. For example, $P = (-1, 0)$ is one rational point, so draw a line having rational slope going through this point:

$$\begin{aligned} x + ty = 1 \\ x^2 + y^2 = 1 \end{aligned} \implies x = \frac{1-t^2}{1+t^2}, \quad y = \frac{2t}{1+t^2}. \quad (1.1)$$

Hence, all points (x, y) different from P must be in this form for some rational t . (We recover the original point P again if we let $t \mapsto \infty$.)

We'll try to generalize this trick to other curves, following the Greek mathematician Diophantus (150 AD - 350 AD?). Say that we have the cubic curve

$$y^2 = x^3 - 3x^2 + 3x + 1. \quad (1.2)$$

One point on this curve is $P = (0, 1)$. To find a second point, we consider now the line tangent to the curve at this point; then counting multiplicities, there would be two rational points on the curve, so the line must intersect at a third rational point Q . To find the slope of the line tangent to a curve $f(x, y) = 0$ at $P = (x_0, y_0)$, recall that

$$f(x, y) = 0 \implies \frac{\partial f}{\partial x}(P) dx + \frac{\partial f}{\partial y}(P) dy = 0 \implies y = -\frac{\partial_x f(P)}{\partial_y f(P)}(x - x_0) + y_0. \quad (1.3)$$

For example, the line tangent to the curve above through $P = (0, 1)$ is $y = \frac{3}{2}x + 1$, so this line will intersect at the point $Q = (\frac{21}{4}, \frac{71}{8})$. We can do this

a second time: The line tangent at Q is $y = \frac{867}{284}x - \frac{8125}{1136}$ so upon substituting this value for y into the original function $f(x, y) = x^3 - 3x^2 + 3x + 1 - y^2$ we find a cubic:

$$f\left(x, \frac{867}{284}x - \frac{8125}{1136}\right) = \left(x - \frac{21}{4}\right)^2 \left(x - \frac{146769}{80656}\right). \quad (1.4)$$

Hence, this tangent line now intersects at the point

$$R = \left(\frac{146769}{284^2}, -\frac{36583777}{284^3}\right). \quad (1.5)$$

1.2.2 Quartic and Cubic Equations

While Diophantus was the first to show the existence of rational solutions to certain polynomial equations, French mathematician Pierre de Fermat (1600's) was the first to show the nonexistence of rational solutions to certain polynomial equations. For example, he showed that the equations

$$a^4 + b^4 = c^2, \quad a^4 - b^4 = c^2, \quad \text{and} \quad a^4 + b^4 = c^4 \quad (1.6)$$

each have no nontrivial integer solutions. In particular, this shows that the cubic curve

$$y^2 = 4x^3 - 6x^2 + 4x - 1 \quad (1.7)$$

has no rational points. Here's why: First I claim the curve $Y^2 = 1 - X^4$ has no rational solutions other than $(\pm 1, 0)$. If not, write this solution (X, Y) as

$$\begin{aligned} X = p/r & \implies r^4 - p^4 = q^2 r^2 \implies a^4 - b^4 = c^2 & \text{where} & \begin{aligned} a &= r \\ b &= p \\ c &= qr. \end{aligned} \end{aligned} \quad (1.8)$$

contradicting Fermat's results. Now if we make the substitution

$$x = \frac{1}{X-1}, \quad y = \frac{Y}{(X-1)^2} \implies y^2 = 4x^3 - 6x^2 + 4x - 1. \quad (1.9)$$

Hence, the curves $y^2 = 4x^3 - 6x^2 + 4x - 1$ and $Y^2 = 1 - X^4$ are equivalent, so this cubic has no rational points.

This motivates studying quartic equations. Say that we have $Y^2 = f(X)$ where $f(X)$ is a degree 4 polynomial. We factor this polynomial as

$$\begin{aligned} f(X) &= a_4 X^4 + a_3 X^3 + a_2 X^2 + a_1 X + a_0 \\ &= a_4 (X - \alpha)(X - \beta)(X - \gamma)(X - \delta); \end{aligned} \quad (1.10)$$

where $\alpha, \beta, \gamma,$ and δ are complex numbers. Now divide $Y^2 = f(X)$ on both sides by $(X - \alpha)^4$:

$$\left(\frac{Y}{(X - \alpha)^2}\right)^2 = a_4 \left(\frac{X - \beta}{X - \alpha}\right) \left(\frac{X - \gamma}{X - \alpha}\right) \left(\frac{X - \delta}{X - \alpha}\right). \quad (1.11)$$

We make the substitution $x = 1/(X - \alpha)$ and $y = Y/(X - \alpha)^2$ to find

$$y^2 = a_4(1 - (\beta - \alpha)x)(1 - (\gamma - \alpha)x)(1 - (\delta - \alpha)x). \quad (1.12)$$

Hence we can always reduce a quartic equation into a cubic equation.

1.3 Elliptic Curves

1.3.1 Weierstrass Form

Isaac Newton (1700's) showed that any equation in the form

$$Y^2 = \text{quartic or cubic in } X \quad (1.13)$$

can be transformed into the equation $y^2 = x^3 + Ax + B$. This is called Weierstrass form, after Karl Weierstrass (1800's).

Here's an example of this: Say that we have the curve

$$Y^2 = (1 - X^2)(1 - k^2 X^2) \quad (1.14)$$

in terms of some $k \in \mathbb{C}$. Following ideas in the previous section, make the substitution

$$\frac{x + (1 - 5k^2)}{6(k^2 - 1)} = \frac{1}{X - 1} \quad \text{and} \quad \frac{y}{6\sqrt{3}(k^2 - 1)} = \frac{Y}{(X - 1)^2}. \quad (1.15)$$

This yields the cubic curve

$$y^2 = x^3 + Ax + B \quad \text{where} \quad \begin{aligned} A &= -3(k^4 + 14k^2 + 1) \\ B &= -2(k^6 - 33k^4 - 33k^2 + 1). \end{aligned} \quad (1.16)$$

1.3.2 What is an Elliptic Curve?

Consider now the equation $y^2 = x^3 + Ax + B$, and say that the cubic on the right has the three roots e_1, e_2 , and e_3 . If all three roots are distinct, we call this curve an elliptic curve. Note this is equivalent to saying $4A^3 + 27B^2 \neq 0$. Otherwise, if any of the roots are repeated, we say the curve is a singular cubic curve. Specifically, if all three roots are equal i.e. $e_1 = e_2 = e_3$, we say the curve has a cusp; but if at least one of the roots is different i.e. $e_1 = e_2 \neq e_3$, we say the curve has a node.

As examples, $y^2 = x^3 - x$ is an elliptic curve. However, $y^2 = x^3 - x^2$ has a node while $y^2 = x^3$ has a cusp. The latter two cubic curves are not elliptic curves.

Chapter 2

Lecture 2: Wednesday, October 2

2.1 Elliptic Curves over \mathbb{C}

2.1.1 Relation with Ellipses

Before, we saw that if we define a function $s(z)$ implicitly by the integral equation

$$z = \int_0^{s(z)} \frac{dx}{\sqrt{1-x^2}} \implies s(z) = \sin z \quad (2.1)$$

then the point $(x, y) = (s(z), s'(z))$ is on the unit circle $x^2 + y^2 = 1$. We generalize this to considering the integral

$$\begin{aligned} z &= \int_0^{\varphi(z)} \frac{dx}{\sqrt{x^3 + Ax + B}} \\ \implies (x, y) &= (\varphi(z), \varphi'(z)) \quad \text{satisfies} \quad y^2 = x^3 + Ax + B. \end{aligned} \quad (2.2)$$

I wish to motivate why one would consider such an integral.

Say that we have an ellipse $x^2/a^2 + y^2/b^2 = 1$ and we wish to compute its arc length. This would be given by

$$T(a, b) = \int_0^{2\pi} \|\vec{r}'(t)\| dt \quad \text{where} \quad \vec{r}(t) = (a \sin t, b \cos t). \quad (2.3)$$

Assume $b \leq a$. This can be computed to be

$$\begin{aligned} T(a, b) &= \int_0^{2\pi} \sqrt{a^2 \cos^2 t + b^2 \sin^2 t} dt \\ &= 4a \int_0^{\pi/2} \sqrt{1 - k^2 \sin^2 t} dt \quad \text{where} \quad k = \frac{\sqrt{a^2 - b^2}}{a}. \end{aligned} \quad (2.4)$$

The number k is the eccentricity of the ellipse. Also, the integral on the left is known as a complete elliptic integral of the second kind:

$$E(k) = \int_0^{\pi/2} \sqrt{1 - k^2 \sin^2 t} dt = \int_0^1 \sqrt{\frac{1 - k^2 X^2}{1 - X^2}} dX, \quad 0 \leq k < 1. \quad (2.5)$$

We also define the complete elliptic integral of the first kind as

$$K(k) = \int_0^{\pi/2} \frac{dt}{\sqrt{1 - k^2 \sin^2 t}} = \int_0^1 \frac{dX}{\sqrt{(1 - X^2)(1 - k^2 X^2)}}, \quad 0 \leq k < 1. \quad (2.6)$$

Note that $E(0) = K(0) = \frac{\pi}{2}$ so that the arc length of a circle of radius a is $T(a, a) = 2\pi a$ as expected. Hence if we consider the incomplete elliptic integral of the first kind

$$K(k; \wp) = \int_0^{\wp} \frac{dX}{\sqrt{(1 - X^2)(1 - k^2 X^2)}}, \quad 0 \leq k < 1; \quad (2.7)$$

we find elliptic curves.

2.1.2 Relation with the Torus

With the circle, the integral

$$\int_0^s \frac{dx}{\sqrt{1 - x^2}} \quad (2.8)$$

has problems in its integrand when $x = \pm 1$, so we must draw a branch cut in the complex plane that avoids these singularities. Hence, the integral

$$\omega_0 = 2 \int_{-1}^1 \frac{dx}{\sqrt{1 - x^2}} = 2\pi \quad (2.9)$$

is a period which comes into play when integrating around various paths in the complex plane. This means the function $s = s(z)$ is periodic i.e. $s(z + \omega_0) = s(z)$.

On the other have, the integral

$$\int_0^{\wp} \frac{dx}{\sqrt{x^3 + Ax + B}} \quad (2.10)$$

has problems in its integrand when $x = e_1, e_2, e_3$ i.e. the three complex roots of $x^3 + Ax + B$. Using a similar argument to above, we have two integrals to consider:

$$\omega_1 = 2 \int_{e_1}^{e_2} \frac{dx}{\sqrt{x^3 + Ax + B}} \quad \text{and} \quad \omega_2 = 2 \int_{e_3}^{infty} \frac{dx}{\sqrt{x^3 + Ax + B}}. \quad (2.11)$$

Both of these complex numbers are periods, and $\wp = \wp(z)$ is now doubly-periodic i.e. $\wp(z + \omega_1) = \wp(z + \omega_2) = \wp(z)$. Denote

$$\Lambda = \mathbb{Z}\langle \omega_1, \omega_2 \rangle = \{\omega = m\omega_1 + n\omega_2 \mid m, n \in \mathbb{Z}\} \subset \mathbb{C} \quad (2.12)$$

as a lattice in \mathbb{C} , and

$$E(\mathbb{C}) = \{(x, y) \in \mathbb{C} \times \mathbb{C} \mid y^2 = x^3 + Ax + B\} \quad (2.13)$$

as the elliptic curve considered over \mathbb{C} . We have a map $E(\mathbb{C}) \rightarrow \mathbb{C}/\Lambda$ given by

$$P_0 = (x_0, y_0) \mapsto \int_0^{x_0} \frac{dx}{\sqrt{x^3 + Ax + B}} \quad (2.14)$$

and an inverse map $\mathbb{C}/\Lambda \rightarrow E(\mathbb{C})$ defined by $z \mapsto (\wp(z), \wp'(z))$. This shows $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$. Hence we think of the elliptic curve as being the complex plane modulo a lattice.

2.1.3 Weierstrass \wp -Function

Following Weierstrass, we construct elliptic curves without using integrals at all. Fix a lattice $\Lambda \subset \mathbb{C}$ and define the function

$$\wp(z; \Lambda) = 4 \left(\frac{1}{z^2} + \sum_{\omega \in \Lambda - \{0\}} \left(\frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right) \right). \quad (2.15)$$

(This is not quite the usual Weierstrass wp -function because there is a nonstandard factor of 4.) Note that this is an even function in z , so that its derivative

$$\wp'(z; \Lambda) = 4 \left(-2 \sum_{\omega \in \Lambda} \frac{1}{(z - \omega)^3} \right) \quad (2.16)$$

is an odd function. We also define the constants

$$A(\Lambda) = -4 \cdot 60 \sum_{\omega \in \Lambda - \{0\}} \frac{1}{\omega^4} \quad \text{and} \quad B(\Lambda) = -4^2 \cdot 140 \sum_{\omega \in \Lambda - \{0\}} \frac{1}{\omega^6}. \quad (2.17)$$

Weierstrass showed (by considering the Laurent expansions above) the relation

$$\wp'(z; \Lambda)^2 = \wp(z; \Lambda)^3 + A(\Lambda) \wp(z; \Lambda) + B(\Lambda). \quad (2.18)$$

The celebrated Uniformization Theorem states that given $A, B \in \mathbb{C}$ such that $4A^3 + 27B^2 \neq 0$, there exists a lattice $\Lambda \subset \mathbb{C}$ such that $A = A(\Lambda)$ and $B = B(\Lambda)$. Hence, any elliptic curve may truly be associated with a Weierstrass \wp -function relative to some lattice.

2.2 Group Law

2.2.1 Addition

Fix a lattice $\Lambda \subset \mathbb{C}$. Given two complex numbers $z_1, z_2 \in \mathbb{C}/\Lambda$, the sum $z_1 + z_2 \in \mathbb{C}/\Lambda$. Can we express $\wp(z_1 + z_2)$ in terms of $\wp(z_1)$ and $\wp(z_2)$? The answer is

yes, and was first discovered by Euler. We'll use this to define "addition" on the curve $y^2 = x^3 + Ax + B$.

We make a few simple definitions first. Say that $P = (\wp(z), \wp'(z))$ is a point on $E(\mathbb{C})$. We will define the "zero point" to be $\mathcal{O} = (\wp(0), \wp'(0))$. Note that $\wp(z)$ has a pole at $z = 0$ so we often call this the point at infinity. We also define $[-1]P = (\wp(-z), \wp'(-z))$ as the inverse of P . Since $\wp(z)$ is even and $\wp'(z)$ is odd, we have $[-1]P = (\wp(z), -\wp'(z))$.

To define "addition" of two points

$$P = (\wp(z_1), \wp'(z_1)) \quad \text{and} \quad Q = (\wp(z_2), \wp'(z_2)) \quad (2.19)$$

on $E(\mathbb{C})$, we perform two steps:

Step 1: Draw a line through P and Q . (If $P = Q$, just draw the line tangent to P .) Call $P * Q = (\wp(z_3), \wp'(z_3))$ the third point on $E(\mathbb{C})$ where this line intersects the curve.

Step 2: Draw a line through this point and \mathcal{O} i.e. consider the inverse. Denote $P \oplus Q = (\wp(z_3), -\wp'(z_3))$ as the desired point.

We present explicit formulas for $P \oplus Q$. Say that $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ are two points on $y^2 = x^3 + Ax + B$, and denote $P * Q = (x_3, y_3)$. If we draw a line through P and Q , say $y = \lambda x + \nu$, then we can choose the slope λ to be

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } x_1 \neq x_2; \\ \frac{3x^2 + A}{2y} & \text{if } P = Q. \end{cases} \quad (2.20)$$

We then consider the equation

$$(x - x_1)(x - x_2)(x - x_3) = x^3 + Ax + B - (\lambda x + \nu)^2 = 0. \quad (2.21)$$

Upon comparing the x^2 terms, we find

$$x_1 + x_2 + x_3 = \lambda^2 \implies \begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 \\ y_3 &= \lambda x_3 + \nu. \end{aligned} \quad (2.22)$$

Then $P \oplus Q = (x_3, -y_3)$.

Let's work out an example. Consider the curve $y^2 = x^3 + 17$. Two rational points are $P = (-1, 4)$ and $Q = (2, 5)$. To compute $P \oplus Q$, we note that the line through P and Q is $y = \frac{1}{3}x + \frac{13}{3}$. Hence we find

$$\begin{aligned} x_3 &= \left(\frac{1}{3}\right)^2 - (-1) - 2 = -\frac{8}{9}, \implies P \oplus Q = \left(-\frac{8}{9}, -\frac{109}{27}\right). \\ y_3 &= \frac{1}{3}x_3 + \frac{13}{3} = \frac{109}{27} \end{aligned} \quad (2.23)$$

On the other hand, to compute $P \oplus P$, we note that the tangent line at P is $y = \frac{3}{8}x + \frac{35}{8}$. Hence we find

$$\begin{aligned} x_3 &= \left(\frac{3}{8}\right)^2 - 2 \cdot (-1) = \frac{137}{64}, & \implies P \oplus P &= \left(\frac{137}{64}, -\frac{2651}{512}\right). \\ y_3 &= \frac{3}{8}x_3 + \frac{35}{8} = \frac{2651}{512} \end{aligned} \quad (2.24)$$

2.2.2 Multiplication by m Maps

We denote $[2]P = P \oplus P$. In general, given an integer m , we denote

$$[m]P = \begin{cases} \mathcal{O} & \text{if } m = 0; \\ P \oplus P \oplus \dots \oplus P \text{ (} m \text{ times)} & \text{if } m > 0; \\ [|m|]([-1]P) & \text{if } m < 0. \end{cases} \quad (2.25)$$

The symbol $[m]$ is known as the multiplication by m map.

2.2.3 Associativity

It's easy to check that $P \oplus Q = Q \oplus P$ i.e. the order of drawing lines doesn't matter, $\mathcal{O} \oplus P = P$ because $P * \mathcal{O} = [-1]P$, and $P \oplus [-1]P = \mathcal{O}$ because $P * [-1]P = \mathcal{O}$. However, it is not so easy to show that

$$(P \oplus Q) \oplus R = P \oplus (Q \oplus R). \quad (2.26)$$

We explain why this holds true. By drawing lines, we have 11 points on the cubic:

$$P, Q, R, P * Q, Q * R, P \oplus Q, Q \oplus R, P * (Q \oplus R), (P \oplus Q) * R; \quad (2.27)$$

and $P \oplus (Q \oplus R)$ and $(P \oplus Q) \oplus R$. However, the most general cubic equation in two variables

$$f(x, y) = \sum_{k=0}^3 \sum_{i+j=k} \alpha_{ij} x^i y^j, \quad \alpha_{ij} \in \mathbb{C} \quad (2.28)$$

has 10 coefficients α_{ij} . Hence, a cubic in two variables cannot have 11 distinct points, so at least two of the 11 points above must be equal. This forces $P \oplus (Q \oplus R) = (P \oplus Q) \oplus R$.

Chapter 3

Homework Assignment #1

Due Monday, October 7 at the start of lecture.

Problem 1. Say that (x, y) is a rational point on the quadratic curve

$$ax^2 + bxy + cy^2 + dx + ey + f = 0.$$

(We assume all coefficients are integers, and not all of a , b , and c are zero.) Show that if (X, Y) is any other rational solution, there exists a rational number t such that

$$\begin{aligned} X &= x - \frac{d+et}{a+bt+ct^2} - \frac{2a+bt}{a+bt+ct^2}x - \frac{b+2ct}{a+bt+ct^2}y; \\ Y &= y - \frac{d+et}{a+bt+ct^2}t - \frac{2a+bt}{a+bt+ct^2}tx - \frac{b+2ct}{a+bt+ct^2}ty. \end{aligned}$$

In particular, conclude that if a quadratic curve has *one* rational solution, then it has *infinitely many* rational solutions.

Problem 2. Say that (x, y) is a rational point on the cubic curve

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

(We assume all coefficients are integers.) Show that there exist integers u , v , and w such that

$$x = \frac{u}{w^2} \quad \text{and} \quad y = \frac{v}{w^3} \quad \text{where} \quad GCD(u, w) = GCD(v, w) = 1.$$

Problem 3. Say that (x, y) is a rational point on the generalized Pell equation

$$x^3 - dy^3 = 1.$$

(We assume d is a nonzero integer.) Using the Chord-Tangent construction, show that another rational point is

$$\left(x \frac{x^3 - 2dy^3}{x^3 + dy^3}, -y \frac{2x^3 - dy^3}{x^3 + dy^3} \right).$$

Use this to find three rational solutions to the equation when $d = 7$.

Problem 4. Show that a nonzero integer d is the discriminant of a cubic polynomial with rational coefficients if and only if the elliptic curve

$$y^2 = x^3 - 432d$$

has a rational point. In particular, find a cubic polynomial with discriminant $d = 5$.

Chapter 4

Lecture 3: Monday, October 7

4.1 Modular Functions

4.1.1 Action on the Upper-Half Plane

Fix a lattice $\Lambda = \mathbb{Z}\langle\omega_1, \omega_2\rangle$. We saw before that an elliptic curve E may be constructed out of Λ via the maps $z \mapsto (\wp(z), \wp'(z))$ where $\wp'(z)^2 = \wp(z)^3 + A(\Lambda)\wp(z) + B(\Lambda)$ in terms of the function

$$\wp(z) = \wp(z; \Lambda) = 4 \left(\frac{1}{z^2} + \sum_{\omega \in \Lambda - \{0\}} \frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right) \quad (4.1)$$

and the constants

$$A(\Lambda) = -4 \cdot 60 \sum_{\omega \in \Lambda - \{0\}} \frac{1}{\omega^4} \quad \text{and} \quad B(\Lambda) = -4^2 \cdot 140 \sum_{\omega \in \Lambda - \{0\}} \frac{1}{\omega^6}. \quad (4.2)$$

Note that $\text{Mat}_{2 \times 2}(\mathbb{Z})$, the 2×2 matrices with integer coefficients, acts on the lattice Λ :

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{Mat}_{2 \times 2}(\mathbb{Z}) \implies \begin{aligned} \gamma \omega_1 &= a \omega_1 + b \omega_2 \\ \gamma \omega_2 &= c \omega_1 + d \omega_2 \end{aligned} \quad (4.3)$$

In particular, $\gamma \omega_1, \gamma \omega_2 \in \Lambda$ as well. In general, if $\alpha \in \mathbb{C}$ satisfies $\alpha \Lambda \subseteq \Lambda$, then we denote

$$[\alpha]P = (\wp(\alpha z), \wp'(\alpha z)) \quad \text{whenever} \quad P = (\wp(z), \wp'(z)). \quad (4.4)$$

We define $\text{End}(E) = \{[\alpha] \mid \alpha \in \mathbb{C} \text{ such that } \alpha \Lambda \subseteq \Lambda\}$ as the endomorphism ring of the elliptic curve $y^2 = x^3 + A(\Lambda)x + B(\Lambda)$. We say E has complex multiplication if there exists $[\alpha] \in \text{End}(E)$ where $[\alpha] \neq [m]$ is not a multiplication by m map.

For example, consider the lattice $\Lambda = \mathbb{Z}\langle 1, \sqrt{-1} \rangle$. Then E is the curve $y^2 = x^3 - x$. The endomorphism ring is $\text{End}(E) = \mathbb{Z}\langle 1, \sqrt{-1} \rangle$ where

$$[\sqrt{-1}](x, y) = (-x, -\sqrt{-1}y). \quad (4.5)$$

4.1.2 The Fundamental Region

Denote $\tau = \omega_1/\omega_2 \in \mathbb{C}$. Then we have an action by $SL_2(\mathbb{Z})$:

$$\gamma\tau = \frac{\gamma\omega_1}{\gamma\omega_2} = \frac{a\omega_1 + b\omega_2}{c\omega_1 + d\omega_2} = \frac{a\tau + b}{c\tau + d} \quad \text{where } ad - bc = 1. \quad (4.6)$$

I claim that I can always choose a basis ω_1, ω_2 such that (1) $\text{Im}\tau > 0$; (2) $|\text{Re}\tau| \leq \frac{1}{2}$; and (3) $|\tau| \geq 1$. Replace ω_2 by $-\omega_2$ if necessary so that $\text{Im}\tau > 0$. (The region of the complex plane satisfying these properties is called the Fundamental Region.) Using the relation

$$\text{Im}\left(\frac{a\tau + b}{c\tau + d}\right) = \frac{ad - bc}{|c\tau + d|^2} \cdot \text{Im}\tau; \quad (4.7)$$

we will act by matrices $\gamma \in SL_2(\mathbb{Z})$ to keep property (1). Consider the matrices

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \implies S\tau = -\frac{1}{\tau}, \quad T\tau = \tau + 1. \quad (4.8)$$

Choose an integer m such that $|\text{Re}T^m\tau| \leq 12$. If $\tau' = T^m\tau$ satisfies $|\tau'| \geq 1$ then we are done. Otherwise, $|S\tau'| < 1$, so now choose an integer n such that $|\text{Re}T^n S\tau'| \leq 12$. Then $\tau'' = T^n S T^m \tau$ is the desired ratio. In particular, we have also showed that any $\gamma \in SL_2(\mathbb{Z})$ can be expressed as a product of S and T i.e. $SL_2(\mathbb{Z})$ is generated by S and T .

4.1.3 Modular Forms and Modular Functions

We make a few substitutions: fix $\tau \in \mathcal{H}$ in the upper-half plane as above, and consider

$$\begin{aligned} A(\Lambda) &= -\frac{3}{12^2} \left(\frac{4\pi}{\omega_2}\right)^4 c_4(\tau) & c_4(\tau) &= \frac{45}{2\pi^4} \sum_{(m,n) \neq (0,0)} \frac{1}{(m\tau + n)^4} \\ B(\Lambda) &= -\frac{2}{12^3} \left(\frac{4\pi}{\omega_2}\right)^6 c_6(\tau) & c_6(\tau) &= \frac{945}{2\pi^6} \sum_{(m,n) \neq (0,0)} \frac{1}{(m\tau + n)^6} \end{aligned} \quad \text{in terms of} \quad (4.9)$$

These functions satisfy the properties

$$c_4(\gamma\tau) = (c\tau + d)^4 c_4(\tau) \quad \text{and} \quad c_6(\gamma\tau) = (c\tau + d)^6 c_6(\tau). \quad (4.10)$$

They are usually called modular function of weight 4 and 6, respectively. A modular function $f(\tau)$ of weight k is one which satisfies the functional equation

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k f(\tau). \quad (4.11)$$

In fact, one computes that

$$\begin{aligned} c_4(\tau) &= 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n & \sigma_\alpha(n) &= \sum_{d|n} d^\alpha \\ c_6(\tau) &= 1 - 504 \sum_{n=1}^{\infty} \sigma_5(n) q^n & q &= e^{2\pi i \tau} \end{aligned} \quad \text{where} \quad (4.12)$$

With these substitutions we have

$$16 \cdot \text{Disc}(x^3 + Ax + B) = -16(4A^3 + 27B^2) = \left(\frac{4\pi}{\omega_2}\right)^6 \frac{c_4^3 - c_6^2}{1728} \quad (4.13)$$

and so we define

$$\Delta(\tau) = \frac{c_4(\tau)^3 - c_6(\tau)^2}{1728} = \eta(\tau)^{24} \quad \text{where} \quad \eta(\tau) = q^{1/24} \prod_{n \geq 1} (1 - q^n). \quad (4.14)$$

The former function is a modular function of weight 12, while the latter function is, Dedekind Eta function, is a modular function of weight 1/2. Actually,

$$\eta\left(-\frac{1}{\tau}\right) = \sqrt{-i\tau} \eta(\tau) \quad \text{and} \quad \eta(\tau + 1) = e^{2\pi i/24} \eta(\tau). \quad (4.15)$$

Finally, we define the j -invariant as the following modular function of weight 0:

$$j(\tau) = \frac{c_4(\tau)^3}{\Delta(\tau)} = 1728 \frac{c_4(\tau)^3}{c_4(\tau)^3 - c_6(\tau)^2} = \frac{1}{q} + 744 + 196884q + \dots \quad (4.16)$$

That is, the j -invariant satisfies

$$j\left(\frac{a\tau + b}{c\tau + d}\right) = j(\tau). \quad (4.17)$$

4.1.4 Weierstrass Function Again

Using these substitutions, we make the substitutions

$$\begin{aligned} x(\mathfrak{z}, \tau) &= \left(\frac{\omega_2}{4\pi}\right)^2 \wp(\omega_2 \mathfrak{z}) \\ &= \frac{1}{(2\pi)^2} \left[\frac{1}{\mathfrak{z}^2} + \sum_{(m,n) \neq (0,0)} \frac{1}{(\mathfrak{z} - m\tau - n)^2} - \frac{1}{(m\tau + n)^2} \right] \\ y(\mathfrak{z}, \tau) &= \left(\frac{\omega_2}{4\pi}\right)^3 \wp'(\omega_2 \mathfrak{z}) \\ &= -\frac{1}{(2\pi)^3} \sum_{(m,n) \neq (0,0)} \frac{1}{(\mathfrak{z} - m\tau - n)^3}. \end{aligned} \quad (4.18)$$

so that we have the elliptic curve

$$y(\mathfrak{z})^2 = x(\mathfrak{z})^3 - \frac{3}{12^2} c_4(\tau) x(\mathfrak{z}) - \frac{2}{12^3} c_6(\tau). \quad (4.19)$$

As an example, consider the substitution

$$\frac{x + (1 - 5k^2)}{6(k^2 - 1)} = \frac{1}{X - 1} \quad \text{and} \quad \frac{y}{6\sqrt{3}(k^2 - 1)} = \frac{Y}{(X - 1)^2}. \quad (4.20)$$

The curve $Y^2 = (1 - X^2)(1 - k^2 X^2)$ then transforms into the cubic curve

$$y^2 = x^3 - \frac{3}{12^2} c_4 x - \frac{2}{12^3} c_6 \quad \text{where} \quad \begin{aligned} c_4 &= 12^2 (k^4 + 14k^2 + 1) \\ c_6 &= 12^3 (k^6 - 33k^4 - 33k^2 + 1). \end{aligned} \quad (4.21)$$

The discriminant and j -invariant are

$$\Delta(E) = 186624 k^2 (k^2 - 1)^4; \quad j(E) = 16 \frac{(k^4 + 14k^2 + 1)^3}{k^2 (k^2 - 1)^4}. \quad (4.22)$$

4.2 Points of Finite Order

4.2.1 Torsion Points

Let N be a positive integer, and fix an elliptic curve $E : y^2 = x^3 + Ax + B$. Denote

$$E[N] = \{(x, y) \in \mathbb{C} \times \mathbb{C} \mid [N](x, y) = \mathcal{O}\} \cup \{\mathcal{O}\} \quad (4.23)$$

as the points of order N . We wish to describe this as a group. Fix a lattice $\Lambda = \mathbb{Z}(\omega_1, \omega_2)$ such that $\tau = \omega_1/\omega_2 \in \mathcal{H}$ and $A = A(\Lambda)$ and $B = B(\Lambda)$. Define the points

$$P = \left(\wp \left(\frac{\omega_1}{N}, \Lambda \right), \wp' \left(\frac{\omega_1}{N}, \Lambda \right) \right) \quad \text{and} \quad Q = \left(\wp \left(\frac{\omega_2}{N}, \Lambda \right), \wp' \left(\frac{\omega_2}{N}, \Lambda \right) \right) \quad (4.24)$$

Then for integers m and n we have

$$[m]P \oplus [n]Q = \left(\wp \left(\frac{m\omega_1 + n\omega_2}{N}, \Lambda \right), \wp' \left(\frac{m\omega_1 + n\omega_2}{N}, \Lambda \right) \right). \quad (4.25)$$

In particular, $R = [m]P \oplus [n]Q$ is a point of order N . Conversely, say R is a point of order N . Then we can find $z \in \mathbb{C}$ such that $R = (\wp(z), \wp'(z))$ where

$$Nz \in \Lambda \implies z = \frac{m\omega_1 + n\omega_2}{N} \implies R = [m]P \oplus [n]Q. \quad (4.26)$$

This shows that $E[N]$ is generated by two points P and Q , and in fact

$$E[N] \simeq \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}. \quad (4.27)$$

Notice in particular that $E[N]$ is a finite group of order N^2 .

4.2.2 Torsion Subgroup

Now say that $A, B \in \mathbb{Q}$, and consider the curve

$$E(\mathbb{Q}) = \{(x, y) \in \mathbb{Q} \times \mathbb{Q} \mid y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}. \quad (4.28)$$

A theorem of L. J. Mordell (1922), which was later extended by Andre Weil (1930), states that $E(\mathbb{Q})$ is a finitely generated abelian group. Hence, we have

$$E(\mathbb{Q}) \simeq \text{Tor}(E) \oplus \mathbb{Z}^r \quad (4.29)$$

for some finite group $\text{Tor}(E)$ and a (possibly) infinite group \mathbb{Z}^r . The first is known as the torsion subgroup of the elliptic curve, while r is known as the rank of the elliptic curve.

Much is known about the torsion subgroup $\text{Tor}(E)$. For example, a theorem of Barry Mazur (1978) states that there are only fifteen possibilities for this subgroup:

$$\text{Tor}(E) \simeq \begin{cases} \mathbb{Z}/N\mathbb{Z} & \text{for } 1 \leq N \leq 10 \text{ or } N = 12; \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z} & \text{for } 1 \leq N \leq 4. \end{cases} \quad (4.30)$$

On the other hand, not much is known about the rank r . The largest known rank is $r \geq 24$, but it is not even known if this is an equality! This was found in 2000 by Martin and McMillen.

For example, consider the elliptic curve $E : y^2 = x^3 - x$. The rank is $r = 0$, whereas the torsion subgroup is

$$\text{Tor}(E) = \{\mathcal{O}, (0, 0), (1, 0), (-1, 0)\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}. \quad (4.31)$$

Chapter 5

Lecture 4: Wednesday, October 9

5.1 The Modular Group

5.1.1 Congruence Subgroups

As usual, fix a positive integer N . (We will only focus on the case where $N = p$ is a prime.) Denote $\Gamma(1) = SL_2(\mathbb{Z})$, and set

$$\begin{aligned}\Gamma_0(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) \mid c \equiv 0(N) \right\} \\ \Gamma_1(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) \mid c \equiv 0(N), a \equiv d \equiv 1(p) \right\} \\ \Gamma(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) \mid b \equiv c \equiv 0(p), a \equiv d \equiv 1(N) \right\}\end{aligned}\tag{5.1}$$

These various subgroups of $\Gamma(1)$ act on the upper-half plane as described in the previous lecture. Note that the matrices ± 1 always have trivial action, so we will only concern ourselves with the various subgroups of the quotient $\bar{\Gamma}(1) = \Gamma(1)/\{\pm 1\}$. This is usually called the modular group.

5.1.2 Relation with the Special Linear Group

There is a simple relation with various subgroups of $SL_2(\mathbb{Z}/N\mathbb{Z})$ which can be seen by considering the diagram

$$\begin{array}{ccccccc}
\{1\} & \longrightarrow & \bar{\Gamma}(N) & \longrightarrow & \bar{\Gamma}(1) & \longrightarrow & \frac{SL_2}{Z \cap SL_2} & \longrightarrow & \{1\} \\
& & \downarrow & & \downarrow & & \downarrow & & \\
\{1\} & \longrightarrow & \bar{\Gamma}_1(N) & \longrightarrow & \bar{\Gamma}(1) & \longrightarrow & \frac{SL_2}{Z \cdot U \cap SL_2} & \longrightarrow & \{1\} \\
& & \downarrow & & \downarrow & & \downarrow & & \\
\{1\} & \longrightarrow & \bar{\Gamma}_0(N) & \longrightarrow & \bar{\Gamma}(1) & \longrightarrow & \frac{SL_2}{B \cap SL_2} & \longrightarrow & \{1\}
\end{array} \quad (5.2)$$

where $B = B(\mathbb{Z}/N\mathbb{Z})$, $Z = Z(\mathbb{Z}/N\mathbb{Z})$, and $U = U(\mathbb{Z}/N\mathbb{Z})$ are the subgroups of $GL_2 = GL_2(\mathbb{Z}/N\mathbb{Z})$ corresponding to the upper triangular, diagonal, and strictly upper triangular matrices, respectively. That is,

$$\begin{aligned}
B &= \left\{ \begin{pmatrix} a & b \\ & d \end{pmatrix} \in GL_2 \mid a, d \in (\mathbb{Z}/N\mathbb{Z})^\times, b \in \mathbb{Z}/N\mathbb{Z} \right\} \\
Z &= \left\{ \begin{pmatrix} a & \\ & a \end{pmatrix} \in GL_2 \mid a \in (\mathbb{Z}/N\mathbb{Z})^\times \right\} \\
U &= \left\{ \begin{pmatrix} 1 & b \\ & 1 \end{pmatrix} \in GL_2 \mid b \in \mathbb{Z}/N\mathbb{Z} \right\}
\end{aligned} \quad (5.3)$$

5.2 Galois Groups

5.2.1 Galois Representations

We know that $E[N] \simeq \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$, so in general we'll have

$$\text{Aut}(E[N]) \simeq GL_2(\mathbb{Z}/N\mathbb{Z}). \quad (5.4)$$

Explicitly, if $E[N]$ is generated by P and Q , then

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \implies \begin{cases} \gamma P = [a]P \oplus [b]Q \\ \gamma Q = [c]P \oplus [d]Q \end{cases} \quad (5.5)$$

There is a second way to act on $E[N]$. Let $G_{\mathbb{Q}}$ denote the compositum over all Galois groups $\text{Gal}(K/\mathbb{Q})$; this is called the absolute Galois group of \mathbb{Q} . If the elliptic curve E is defined over \mathbb{Q} i.e. $A, B \in \mathbb{Q}$ then the group law \oplus is also defined over \mathbb{Q} . Hence the points of order N are permuted by the Galois group since they just involve roots of polynomials. We then have a map

$$\bar{\rho}_{E,N} : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{Z}/N\mathbb{Z}), \quad \sigma \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{if} \quad \begin{cases} \sigma(P) = [a]P \oplus [b]Q \\ \sigma(Q) = [c]P \oplus [d]Q \end{cases} \quad (5.6)$$

This is known as the mod N Galois representation.

There is an extension $\mathbb{Q}(E[N])$ such that

$$G_{\mathbb{Q}} / \text{Ker } \bar{\rho}_{E,N} \simeq \text{Gal}(\mathbb{Q}(E[N])/\mathbb{Q}). \quad (5.7)$$

This extension is the field generated by the x - and y -coordinates of the N torsion points $[a]P \oplus [b]Q$. In general, note that

$$\text{Gal}(\mathbb{Q}(E[N])/\mathbb{Q}) \simeq G_{\mathbb{Q}} / \text{Ker } \bar{\rho}_{E,N} \simeq \text{Im } \bar{\rho}_{E,N} \simeq GL_2(\mathbb{Z}/N\mathbb{Z}). \quad (5.8)$$

5.2.2 $N = 2$ Case

Say that $E : y^2 = x^3 + Ax + B$. If the cubic has roots e_1, e_2 , and e_3 then the 2-torsion points are

$$E[2] = \{\mathcal{O}, (e_1, 0), (e_2, 0), (e_3, 0)\}. \quad (5.9)$$

Hence $\mathbb{Q}(E[2])$ is just the splitting field of the cubic $x^3 + Ax + B$. Note that in the most general case,

$$\text{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \simeq S_3 \simeq GL_2(\mathbb{F}_2). \quad (5.10)$$

5.2.3 $N = 3$ Case

Let's consider the elliptic curve $E : y^2 = x^3 + Ax + B$ again. A point P on E has order 3 if and only if $[2]P = [-1]P$. Considering the x -coordinates we have

$$\frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)} = x([2]P) = x([-1]P) = x. \quad (5.11)$$

That is, we seek the roots of the 3-division polynomial

$$\psi_3(x) = 3x^4 + 6Ax^2 + 12Bx - A^2. \quad (5.12)$$

This polynomial has four roots, say x_1, x_2, x_3 , and x_4 . The equation $y^2 = x^3 + Ax + B$ has two solutions for y , so the 9 points of order 3 are

$$E[3] = \{\mathcal{O}, (x_1, \pm y_1), (x_2, \pm y_2), (x_3, \pm y_3), (x_4, \pm y_4)\}. \quad (5.13)$$

If we consider just the field generated by the x -coordinates, then

$$\mathbb{Q}(E[3]_x) = \mathbb{Q}(x_1, x_2, x_3, x_4) \implies \text{Gal}(\mathbb{Q}(E[3]_x)/\mathbb{Q}) \simeq GL_2(\mathbb{F}_3)/\langle \pm 1_2 \rangle \simeq S_4. \quad (5.14)$$

We present a couple of ways to see that $\psi_3(x)$ has no repeated roots. It is easy to check that $\frac{d}{dx} \psi_3(x) = 12(x^3 + Ax + B)$, so any repeated root would also correspond to a 2-torsion point. Alternatively, the discriminant of ψ_3 is $\text{Disc}(\psi_3) = -3^3 \Delta(E)^2$. The discriminant of the elliptic curve $\Delta(E)$ is nonzero by assumption so the discriminant of the polynomial is nonzero as well. Note in particular that $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\sqrt{\Delta(E)}) \subset \mathbb{Q}(E[3]_x)$, so that $\zeta_3 \in \mathbb{Q}(E[3])$.

5.3 Subfields of $\mathbb{Q}(E[N])$

5.3.1 Subgroups of $GL_2(\mathbb{Z}/N\mathbb{Z})$

For simplicity say $N = p$ is an odd prime. We consider only the most general class of elliptic curves E defined over \mathbb{Q} such that the Galois action on the p -torsion induces a surjective map $\bar{\rho}_{E,p} : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{F}_p)$.

Since $B(\mathbb{F}_p)$ and $Z(\mathbb{F}_p) \cdot U(\mathbb{F}_p)$ are subgroups of $GL_2(\mathbb{F}_p)$, we define K and L as corresponding fields, respectively. These fields are related by the diagram

$$\mathbb{Q}(\zeta_p) \xrightarrow{p+1} K \xrightarrow{(p-1)/2} L \xrightarrow{p} \mathbb{Q}(E[p]_x) \xrightarrow{2} \mathbb{Q}(E[p]) \quad (5.15)$$

which correspond to the Galois groups

$$SL_2 \xrightarrow{p+1} B \cap SL_2 \xrightarrow{(p-1)/2} Z \cdot U \cap SL_2 \xrightarrow{p} Z \cap SL_2 \xrightarrow{2} \{1\} \quad (5.16)$$

There is a theorem due to Andre Weil which states $\zeta_p \in \mathbb{Q}(E[p])$. The proof uses the Weil Pairing. Note that in the diagrams above, the fields K and L are not Galois – and are not even unique – since $B = B(\mathbb{F}_p)$ and $Z \cdot U = Z(\mathbb{F}_p) \cdot U(\mathbb{F}_p)$ are not normal subgroups of $GL_2(\mathbb{F}_p)$.

5.3.2 $N = 3$ Case Revisited

Let's consider the elliptic curve $E : y^2 = x^3 + Ax + B$ once more. Say that we have the factorization $\psi_3(x) = 3 \prod_i (x - x_i)$, and consider the roots

$$\begin{aligned} \theta_1 &= 2A - 3(x_1 x_2 + x_3 x_4), \\ \theta_2 &= 2A - 3(x_1 x_3 + x_2 x_4), \\ \theta_3 &= 2A - 3(x_1 x_4 + x_2 x_3). \end{aligned} \quad (5.17)$$

One verifies that $\prod_i (x - \theta_i) = x^3 - \Delta(E)$. This shows that both $\sqrt[3]{\Delta(E)}$ and ζ_3 are contained in the splitting field. In fact, we can use this to explicitly work out the roots x_i .

Note that ψ_3 is a degree 4 polynomial whose discriminant $\text{Disc}(\psi_3) = -3^3 \Delta(E)^2$ is a square in $\mathbb{Q}(\zeta_3)$. The Galois group is

$$\text{Gal}(\mathbb{Q}(E[3]_x)/\mathbb{Q}(\zeta_3)) \simeq PSL_2(\mathbb{F}_3) \simeq A_4 = D_4 \rtimes Z_3, \quad (5.18)$$

which has order $12 = 4 \times 3$. The irreducibility of ψ_3 contributes the factor of 4 while the irreducibility of $x^3 - \Delta(E)$ contributes the factor of 3.

Chapter 6

Homework Assignment #2

Due Monday, October 14 at the start of lecture.

Problem 1. Consider the cubic curve

$$y^2 + a_1 x y + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6, \quad a_i \in \mathbb{Q}.$$

- Show that there is a linear change of variables such that the curve may be expressed in the form $y^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6$. Moreover, express the b_i 's in terms of the a_i 's.
- Show that there is a linear change of variables such that the curve may be expressed in the form $y^2 = x^3 - (3c_4/12^2)x - (2c_6/12^3)$. Moreover, express the c_i 's in terms of the b_i 's.

Problem 2. Relative to the elliptic curve $y^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6$, consider the 2-division polynomial $\psi_2(x) = 4x^3 + b_2 x^2 + 2b_4 x + b_6$.

- Show that the discriminant of this polynomial is $16\Delta(E)$, where

$$\Delta(E) = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6 \quad \text{where} \quad b_8 = \frac{b_2 b_6 - b_4^2}{4}.$$

- Show that the points of order 2 are $(e_1, 0)$, $(e_2, 0)$, and $(e_3, 0)$ where

$$e_i = \frac{1}{12} \left(-b_2 + \sqrt[3]{c_6 + \sqrt{c_6^2 - c_4^3}} \zeta_3^i + \sqrt[3]{c_6 - \sqrt{c_6^2 - c_4^3}} \zeta_3^{2i} \right).$$

Problem 3. With notation as above, consider the 3-division polynomial $\psi_3(x) = 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8$. Denote the roots of $\psi_3(x)$ by x_1, x_2, x_3 , and x_4 ; and define the resolvent roots

$$\theta_1 = b_4 - 3(x_1x_2 + x_3x_4), \theta_2 = b_4 - 3(x_1x_3 + x_2x_4), \theta_3 = b_4 - 3(x_1x_4 + x_2x_3).$$

- a. Show that these resolvents are roots of the cubic $x^3 - \Delta(E)$.
- b. Show that the discriminant of ψ_3 is $-3^3 \Delta(E)^2$.

Problem 4. With notation as above, show that the x -coordinates of the 3-division are

$$x_i = \frac{1}{12} \left(-b_2 + \sum_{j=1}^3 (-1)^{\lfloor \frac{ij}{2} \rfloor} \sqrt{c_4 + \zeta_3^{j-1} \sqrt[3]{c_6^2 - c_4^3}} \right), \quad i = 1, 2, 3, 4;$$

where ζ_3 is a cube root of unity and $\lfloor \cdot \rfloor$ is the greatest integer function.

Chapter 7

Lecture 5: Monday, October 14

7.1 Modular Curves

7.1.1 Notation

Recall that the group

$$GL_2(\mathbb{Q})^+ = \left\{ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - bc > 0 \right\} \quad (7.1)$$

acts on the extended upper-half plane

$$\mathcal{H}^* = \{ \tau = x + iy \in \mathbb{C} \mid y > 0 \} \cup \{ \infty \} \quad \text{by} \quad \gamma \tau = \frac{a\tau + b}{c\tau + d}. \quad (7.2)$$

In particular, $\Gamma(1) = SL_2(\mathbb{Z}) \subset GL_2(\mathbb{Q})^+$ acts trivially on the j -invariant

$$j(\tau) = \frac{c_4(\tau)^3}{\Delta(\tau)} = \frac{(1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n)^3}{q \prod_{n \geq 1} (1 - q^n)^{24}} = \frac{1}{q} + 744 + 196884q + \dots \quad (7.3)$$

(Recall that $q = e^{2\pi i \tau}$.) Recall the Dedekind eta function defined by

$$\eta(\tau) = q^{1/24} \prod_{n \geq 1} (1 - q^n), \quad \eta\left(-\frac{1}{\tau}\right) = \sqrt{-i\tau} \eta(\tau), \quad \eta(\tau + 1) = e^{2\pi i/24} \eta(\tau). \quad (7.4)$$

We denote $X(1)$ as the collection of pairs (E, \mathcal{O}) of elliptic curves E with a fixed point \mathcal{O} . We have the map $\mathcal{H}^*/\Gamma(1) \rightarrow X(1)$ defined by $\tau \mapsto (E_\tau, \mathcal{O}_\tau)$ where

$$E_\tau : y^2 = x^3 - \frac{3j(\tau)}{j(\tau) - 1728} x - \frac{2j(\tau)}{j(\tau) - 1728}, \quad \mathcal{O}_\tau = (\infty, \infty). \quad (7.5)$$

By the Uniformization Theorem, this map is actually an isomorphism.

7.1.2 Curves of level N

Fix a prime p , and denote

$$\begin{aligned} X_0(N) &= \{(E, C) \mid C \text{ is a subgroup of order } N\} / \sim \\ X_1(N) &= \{(E, P) \mid P \text{ is a point of order } N\} / \sim \\ X(N) &= \{(E, P, Q) \mid P, Q \text{ have order } p, e_N(P, Q) = \zeta_N\} / \sim \end{aligned} \quad (7.6)$$

where \sim is equivalence defined as a bijective map $E_1 \rightarrow E_2$ which takes $C_1 \mapsto C_2$, $P_1 \mapsto P_2$, or $(P_1, Q_1) \mapsto (P_2, Q_2)$, respectively. ($e_N : E[N] \times E[N] \rightarrow \mu_N$ is the Weil pairing, which we will ignore for now.) These are known as the modular curves of level N . For $N = 2, 3, 5$, we will exhibit isomorphisms

$$\mathcal{H}^*/\Gamma_0(N) \rightarrow X_0(N), \quad \mathcal{H}^*/\Gamma_1(N) \rightarrow X_1(N), \quad \mathcal{H}^*/\Gamma(N) \rightarrow X(N). \quad (7.7)$$

7.1.3 N Isogenies

A matrix $\gamma \in GL_2(\mathbb{Q})^+$ can be expressed in the form

$$\gamma = \lambda \psi \quad \text{where} \quad \lambda \in \mathbb{Q}^\times, \quad \psi = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{Mat}_{2 \times 2}(\mathbb{Z}). \quad (7.8)$$

Say that $N = \det \psi \in \mathbb{Z}$. Fix a lattice $\Lambda = \mathbb{Z}\langle \omega_1, \omega_2 \rangle$ such that $E = \mathbb{C}/\Lambda$ is an elliptic curve. We find a new lattice

$$\Lambda' = \mathbb{Z}\langle \omega'_1, \omega'_2 \rangle \quad \text{defined implicitly by} \quad \begin{aligned} \omega_1 &= a\omega'_1 + b\omega'_2; \\ \omega_2 &= c\omega'_1 + d\omega'_2. \end{aligned} \quad (7.9)$$

The new elliptic curve $E' = \mathbb{C}/\Lambda'$ is said to be N -isogeneous to E , and we write $\psi : E \rightarrow E'$. Note that $C = \Lambda'/\Lambda = \ker \psi$ is a subgroup of E of order N , and that $E' \simeq E/C$. There is a dual isogeny $\hat{\psi}$ given by

$$\hat{\psi} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \implies \hat{\psi} \circ \psi = \begin{pmatrix} N & 0 \\ 0 & N \end{pmatrix} = [N] \quad (7.10)$$

is the multiplication by N map. Hence, we will identify N -isogenies as integer matrices with determinant N , and the cyclic subgroup C of order N with the kernel of some N -isogeny.

7.2 Subgroups of Order p

We assume from now on that $N = p$ is a prime.

7.2.1 General Theory

For $p = 2, 3, 5$, we study the composite map

$$\mathcal{H}^*/\Gamma_0(p) \rightarrow V_0(p) \rightarrow X_0(p) \quad \text{defined by} \quad \tau \mapsto j_{p,0}(\tau) \mapsto (E_\tau, C_\tau) \quad (7.11)$$

in terms of

$$r = j_{p,0}(\tau) = \left(\frac{\eta(\tau)}{\eta(p\tau)} \right)^{2m} = \frac{1}{q} + \dots, \quad m = \frac{12}{\gcd(p-1, 12)}. \quad (7.12)$$

such that $(X, Y) = (j(\tau), j(p\tau))$ is a point on some curve $V_0(p) : F_p(X, Y) = 0$. (More precisely, r parametrizes points $(X(r), Y(r))$ on $V_0(p)$.) This polynomial, called the modular polynomial, classifies when two elliptic curves are p -isogenous. Both $j(\tau)$ and $j_{p,0}(\tau)$ are maps onto the complex projective line, so j will be a rational function in $j_{p,0}$ of degree

$$[\bar{\Gamma}(1) : \bar{\Gamma}_0(p)] = [SL_2(\mathbb{F}_p) : B(\mathbb{F}_p) \cap SL_2(\mathbb{F}_p)] = p + 1. \quad (7.13)$$

These maps are related by the diagram

$$\begin{array}{ccc} \mathcal{H}^*/\Gamma_0(p) & \longrightarrow & \mathcal{H}^*/\Gamma(1) \\ \downarrow j_{p,0} & & \downarrow j \\ \mathbb{C} \cup \{i\infty\} & \longrightarrow & \mathbb{C} \cup \{i\infty\} \end{array} \quad (7.14)$$

7.2.2 Atkin-Lehner Theory

Let's consider the action of $\Gamma_0(p)$ in more detail. The subgroup is normalized by the Atkin-Lehner involution:

$$w_p \begin{pmatrix} a & b \\ c & d \end{pmatrix} w_p^{-1} = \begin{pmatrix} d & -c/p \\ -pb & a \end{pmatrix} \quad \text{where} \quad w_p = \begin{pmatrix} & 1 \\ -p & \end{pmatrix}; \quad (7.15)$$

which acts on both $j(\tau)$ and $j_{p,0}(\tau)$. The former is a modular function for the full linear group so that $j(-1/p\tau) = j(p\tau)$, whereas the latter transforms as

$$j_{p,0} \left(-\frac{1}{p\tau} \right) = \left(\frac{\eta \left(-\frac{1}{p\tau} \right)}{\eta \left(-\frac{1}{\tau} \right)} \right)^{2m} = \left(\frac{\sqrt{-i p \tau} \eta(p\tau)}{\sqrt{-i \tau} \eta(\tau)} \right)^{2m} = \frac{p^m}{j_{p,0}(\tau)}. \quad (7.16)$$

The Atkin-Lehner involution acts as a p -isogeny i.e. if an elliptic curve E has j -invariant $j(\tau)$, then a p -isogenous curve E' has j -invariant $j(p\tau)$.

7.2.3 Galois Theory

Let E be a suitably general elliptic curve, and denote K as the subfield of $\mathbb{Q}(E[p])$ which is the field fixed by the Borel subgroup $B(\mathbb{F}_p)$. Then $K = k(j_{p,0}(\tau))$ is the extension of $k = \mathbb{Q}(j(\tau), \zeta_p)$ found by adjoining $j_{p,0}(\tau)$. Moreover, if two elliptic curves E and E' are p -isogenous then $E' \simeq E/C$ is defined over K . Note that $j_{p,0}(\tau)$ is the root of a degree $(p+1)$ polynomial so it defines an extension of degree $(p+1)$. The Galois action on this extension is $\bar{\Gamma}(1)/\bar{\Gamma}_0(p) \simeq SL_2(\mathbb{F}_p)/B(\mathbb{F}_p)$, so the extension $K = k(j_{p,0}(\tau))$ must be the field fixed by $B(\mathbb{F}_p)$.

7.2.4 $p = 2$ Case

We have

$$r = j_{2,0}(\tau) = \left(\frac{\eta(\tau)}{\eta(2\tau)} \right)^{24} = \frac{1}{q \cdot \prod_{n \geq 1} (1 + q^n)^{24}} \quad (7.17)$$

By comparing q -expansions, it is easy to verify

$$j(\tau) = \frac{(r + 256)^3}{r^2}, \quad j(2\tau) = \frac{(r + 16)^3}{r}. \quad (7.18)$$

Then $K = \mathbb{Q}(r)$ where r is a root of $(r + 256)^3 - j r^2$ is the smallest extension where a 2-isogeny can be defined. Upon eliminating r from both expressions we find the polynomial

$$F_2(X, Y) = -(X Y)^2 + 1485(X + Y + 27675) X Y + (X + Y - 54000)^3 \quad (7.19)$$

in terms of $X = j(\tau)$ and $Y = j(2\tau)$. We also have the map $r \mapsto (E_r, C_r)$ where

$$E_r : y^2 = x^3 + 2 \frac{r + 64}{r^2} x^2 + \frac{r + 64}{r^3} x, \quad C_r = \langle (0, 0) \rangle. \quad (7.20)$$

7.2.5 $p = 3$ Case

We have

$$r = j_{3,0}(\tau) = \left(\frac{\eta(\tau)}{\eta(3\tau)} \right)^{12} = \frac{1}{q \cdot \prod_{n \geq 1} (1 + q^n + q^{2n})^{12}}; \quad (7.21)$$

which gives the rational functions

$$j(\tau) = \frac{(r + 27)(r + 243)^3}{r^3}, \quad j(3\tau) = \frac{(r + 27)(r + 3)^3}{r}. \quad (7.22)$$

Then $K = \mathbb{Q}(\zeta_3, r)$ where r is a root of $(r + 27)(r + 243)^3 - j r^3$. Upon eliminating r we find

$$\begin{aligned} F_3(X, Y) = & -(X Y)^3 + 8(279(X + Y) + 323757250)(X Y)^2 \\ & - 920(1163(X + Y)^2 - 9674035200(X + Y) + 838860800000000) X Y \\ & + (X + Y + 12288000)^3(X + Y) \end{aligned} \quad (7.23)$$

in terms of $X = j(\tau)$ and $Y = j(3\tau)$. We have a map $r \mapsto (E_r, C_r)$ where

$$E_r : y^2 + 3 \frac{r + 27}{r} x y + \frac{(r + 27)^2}{r^2} y = x^3, \quad C_r = \langle (0, 0) \rangle. \quad (7.24)$$

7.2.6 $p = 5$ Case

We have

$$r = j_{5,0}(\tau) = \left(\frac{\eta(\tau)}{\eta(5\tau)} \right)^6 = \frac{1}{q \cdot \prod_{n \geq 1} (1 + q^n + q^{2n} + q^{3n} + q^{4n})^6}; \quad (7.25)$$

which gives the rational functions

$$j(\tau) = \frac{(r^2 + 250r + 3125)^3}{r^5}, \quad j(5\tau) = \frac{(r^2 + 10r + 5)^3}{r}. \quad (7.26)$$

Then $K = \mathbb{Q}(\zeta_5, r)$ where r is a root of $(r^2 + 250r + 3125)^3 - jr^5$. We have a map $r \mapsto (E_r, C_r)$ where

$$E_r : \quad y^2 + 2 \frac{2r + 25}{r} xy + \frac{r^2 + 22r + 125}{r^2} y = x^3 + \frac{r + 10}{r} x^2 \quad (7.27)$$

and $C_r = \langle (x, y) \rangle$ is the group of order 5 generated by the the roots of

$$\psi_{5,0}(x) = 5x^2 - 4 \frac{r^2 + 22r + 125}{r^2}. \quad (7.28)$$

Chapter 8

Lecture 6: Wednesday, October 16

8.1 Points of Order p

8.1.1 Normal Forms

To describe the modular curve $X_1(p)$, we must consider elliptic curves with prescribed p -torsion point P . To this end, we will consider the class of normal forms

$$E : y^2 + uxy + vy = x^3 + vx^2, \quad P = (0, 0); \quad (8.1)$$

when $p > 3$. (We use a similar class of normal forms when $p = 2, 3$.) The assumption that P has order p will place conditions on u and v . We wish to exhibit maps

$$\mathcal{H}^*/\Gamma_1(p) \rightarrow V_1(p) \rightarrow X_1(p) \quad \text{defined by} \quad \tau \mapsto j_{p,1}(\tau) \mapsto (E_t, C_t) \quad (8.2)$$

in terms of some hauptmodul $t = j_{p,1}(\tau)$ and some curve $V_1(p)$. (Actually, we won't exhibit equations for $V_1(p)$; we'll just assume $V_1(p) \simeq \mathbb{C} \cup \{\infty\} \simeq \mathbb{P}^1(\mathbb{C})$.)

Let E be a suitably general elliptic curve, and denote L as the subfield of $\mathbb{Q}(E[p])$ which is the field fixed by the subgroup $Z(\mathbb{F}_p) \cdot U(\mathbb{F}_p)$ in terms of the center $Z(\mathbb{F}_p)$ and strictly upper triangular matrices $U(\mathbb{F}_p)$ in $GL_2(\mathbb{F}_p)$. Then $L = k(j_{p,1}(\tau))$ is the extension of $k = \mathbb{Q}(j(\tau), \zeta_p)$ found by adjoining $j_{p,1}(\tau)$. When p is odd, $j_{p,1}(\tau)$ defines an extension of degree $\frac{p-1}{2}$ since $V_1(p)$ gives a cover of $V_0(p)$ of degree

$$[\bar{\Gamma}_0(1) : \bar{\Gamma}_1(p)] = [B(\mathbb{F}_p) \cap SL_2(\mathbb{F}_p) : Z(\mathbb{F}_p) \cdot U(\mathbb{F}_p) \cap SL_2(\mathbb{F}_p)] = \frac{p-1}{2}. \quad (8.3)$$

The Galois action on this extension is

$$\bar{\Gamma}_0(p)/\bar{\Gamma}_1(p) \simeq B(\mathbb{F}_p) \cap SL_2(\mathbb{F}_p) / Z(\mathbb{F}_p) \cdot U(\mathbb{F}_p) \cap SL_2(\mathbb{F}_p); \quad (8.4)$$

so the extension $k(j_{p,1}(\tau))$ must be the field fixed by $Z(\mathbb{F}_p) \cdot U(\mathbb{F}_p)$.

8.1.2 $p = 2$ Case

I claim that an elliptic curve admits a 2-isogeny if and only if it has a rational point of order 2. Indeed, the variety $V_1(2)$ is a trivial covering space for $V_0(2)$ because the Borel subgroup $B \cap SL_2 = Z \cdot U \cap SL_2$ in $SL_2(\mathbb{F}_2)$; hence $X_1(2) \simeq X_0(2)$. Another way to say this is that $j_{2,1}$ is a fractional linear transformation of $j_{2,0}$, so choose $j_{2,1}(\tau)$ by the linear relation

$$j_{2,0}(\tau) = \frac{64t}{1-t} \quad \text{where} \quad t = j_{2,1}(\tau). \quad (8.5)$$

Upon moving the point to the origin we have the moduli space consisting of curves in the form

$$\begin{aligned} E_t : \quad y^2 &= x^3 + 2x^2 + tx, & P_t &= (0, 0); \\ E'_t : \quad y^2 &= x^3 + 2x^2 + sx, & s &= 1 - t. \end{aligned} \quad (8.6)$$

8.1.3 Points of Order 3

Again, the modular curve $X_1(3)$ is a trivial cover for $X_0(3)$ because $B \cap SL_2 = Z \cdot U \cap SL_2$ in $SL_2(\mathbb{F}_3)$. That is, an elliptic curve over $\mathbb{Q}(\zeta_3)$ admits a 3-isogeny if and only if it has a rational point of order 3. Moreover, an elliptic curve over \mathbb{Q} admits a 3-isogeny if and only if the 3-division polynomial has a rational root. We define $j_{3,1}(\tau)$ by the fractional linear transformation

$$j_{3,0}(\tau) = \frac{27t}{1-t} \quad \text{where} \quad t = j_{3,1}(\tau). \quad (8.7)$$

Upon moving the point to the origin we have the moduli space consisting of curves expressed in Deuring normal form:

$$\begin{aligned} E_t : \quad y^2 + 3xy + ty &= x^3, & P_t &= (0, 0); \\ E'_t : \quad y^2 + 3xy + sy &= x^3, & s &= 1 - t. \end{aligned} \quad (8.8)$$

8.1.4 $p = 5$ Case

The modular curve $X_1(5)$ is a 2-fold cover for $X_0(5)$ because the quotient $B \cap SL_2 / Z \cdot U \cap SL_2$ has order 2. We define $j_{5,1}(\tau)$ by the quadratic relation

$$j_{5,0}(\tau) = \frac{125t}{1 - 11t - t^2} \quad \text{where} \quad t = j_{5,1}(\tau). \quad (8.9)$$

The moduli space consists of pairs (E_t, P_t) in the form

$$\begin{aligned} E_t : \quad y^2 + (1+t)xy + ty &= x^3 + tx^2, & P_t &= (0, 0); \\ E'_t : \quad y^2 + (1+s)xy + sy &= x^3 + sx^2, & s &= \frac{\varepsilon^5 - t}{1 + \varepsilon^5 t}. \end{aligned} \quad (8.10)$$

where $\varepsilon = \zeta_5 + \zeta_5^{-1}$ is a root of the quadratic $\varepsilon^2 + \varepsilon - 1$. (There are two choices of s as above; the other comes about by choosing $\varepsilon = \zeta_5^2 + \zeta_5^{-2}$.)

8.2 Basis for p -Torsion

8.2.1 Genus of $X(p)$

By the Hurwitz formula,

$$\text{genus of } X(p) = 1 + \frac{1}{12} [\bar{\Gamma}(1) : \bar{\Gamma}(p)] \cdot \frac{p-6}{p} = \frac{(p+2)(p-3)(p-5)}{24} \quad (8.11)$$

When $p = 2, 3, 5$ the curve has genus 0, but when $p = 7, p = 11$, and $p = 13$ the curve has genus 3, 26, and 8, respectively. In general, $X(p)$ gives a cover of $X_1(p)$ of degree

$$[\bar{\Gamma}_1(p) : \bar{\Gamma}(p)] = [Z(\mathbb{F}_p) \cdot U(\mathbb{F}_p) \cap SL_2(\mathbb{F}_p) : Z(\mathbb{F}_p) \cap SL_2(\mathbb{F}_p)] = p. \quad (8.12)$$

8.2.2 $p = 2$ Case

The modular curve $X(2)$ is a 2-fold cover for $X_1(2)$ so we define $j_2(\tau)$ by the quadratic relation

$$1 - j_{2,1}(\tau) = \left(\frac{1 - \lambda}{1 + \lambda} \right)^2 \quad \text{where} \quad \lambda = j_2(\tau). \quad (8.13)$$

The moduli space consisting of curves in Legendre normal form:

$$E_\lambda : y^2 = x(x-1)(x-\lambda), \quad P_\lambda = (0,0), \quad Q_\lambda = (\lambda,0); \quad (8.14)$$

where $\mathbb{Q}(E[2]_x) = \mathbb{Q}(\lambda)$ is a degree 6 extension characterized by the polynomial $256(1-\lambda+\lambda^2)^3 - j(1-\lambda)^2\lambda^2$. The standard coefficients of the elliptic curve are the polynomials

$$\begin{aligned} c_4(E_\lambda) &= 2^4 (1 - \lambda + \lambda^2) \\ c_6(E_\lambda) &= 2^5 (2 - 3\lambda - 3\lambda^2 + 2\lambda^3) \\ \Delta(E_\lambda) &= 2^4 \lambda^2 (1 - \lambda)^2 \end{aligned} \quad (8.15)$$

The map $\lambda \rightarrow j(E_\lambda)$ is six-to-one because $X(2)$ is a six-fold cover of $X(1)$. In fact, the Galois action on this cover is $PSL_2(\mathbb{F}_2) \simeq S_3$.

8.2.3 $p = 3$ Case

The modular curve $X(3)$ is a 3-fold cover of $X_1(3)$ so define $j_3(\tau)$ by the cubic relation

$$1 - j_{3,1}(\tau) = \lambda^3 \quad \text{where} \quad \lambda = j_3(\tau). \quad (8.16)$$

We have the moduli space consisting of curves in the form:

$$E_\lambda : y^2 + 3xy + (1 - \lambda^3)y = x^3 \quad \begin{aligned} P_\lambda &= (0,0) \\ Q_\lambda &= \left(-\frac{1 - \lambda^3}{1 - \lambda}, (1 - \zeta_3 \lambda) \frac{1 - \lambda^3}{1 - \lambda} \right) \end{aligned} \quad (8.17)$$

where $\mathbb{Q}(E[3]_x) = \mathbb{Q}(\lambda)$ is a degree 12 extension of $\mathbb{Q}(\zeta_3)$ with Galois group $\text{Gal}(L/\mathbb{Q}(\zeta_3)) \simeq PSL_2(\mathbb{F}_3)$. The standard coefficients of the elliptic curve are the polynomials

$$\begin{aligned} c_4(E_\lambda) &= 3^2 (1 + 8\lambda^3) \\ c_6(E_\lambda) &= 3^3 (1 - 20\lambda^3 - 8\lambda^6) \\ \Delta(E_\lambda) &= 3^3 \lambda^3 (1 - \lambda^3)^3 \end{aligned} \tag{8.18}$$

The map $\lambda \rightarrow j(E_\lambda)$ is 12-to-one because $X(3)$ is a 12-fold cover of $X(1)$. The Galois action on this cover is $PSL_2(\mathbb{F}_3) \simeq A_4$.

8.2.4 $p = 5$ Case

The modular curve $X(5)$ is a 5-fold cover of $X_1(5)$. We define $j_5(\tau)$ by the quintic relation

$$\frac{\varepsilon^5 - j_{5,1}(\tau)}{1 + \varepsilon^5 j_{5,1}(\tau)} = \left(\frac{\varepsilon - \lambda}{1 + \varepsilon\lambda} \right)^5 \quad \text{where} \quad \lambda = j_5(\tau). \tag{8.19}$$

Elliptic curves E_λ have the associated the polynomials

$$\begin{aligned} c_4(E_\lambda) &= \lambda^{20} - 228\lambda^{15} + 494\lambda^{10} + 228\lambda^5 + 1 \\ c_6(E_\lambda) &= \lambda^{30} + 522\lambda^{25} - 10005\lambda^{20} - 10005\lambda^{10} - 522\lambda^5 + 1 \\ \Delta(E_\lambda) &= \lambda^5 (1 - 11\lambda^5 - \lambda^{10})^5 \end{aligned} \tag{8.20}$$

where the field of definition $\mathbb{Q}(E[5]_x) = \mathbb{Q}(\lambda)$ is a degree 60 extension characterized by the polynomial $c_4^3 - j\Delta$, known as the icosahedral equation. The map $\lambda \rightarrow j(E_\lambda)$ is 60-to-one because $X(5)$ is a 60-fold cover of $X(1)$. The Galois action on this cover has group $PSL_2(\mathbb{F}_5) \simeq A_5$.

Chapter 9

Homework Assignment #3

Due Monday, October 21 at the start of lecture.

Problem 1. Let $c_4, c_6 \in \mathbb{Q}$ such that $c_4 c_6 (c_4^3 - c_6^2) \neq 0$.

1. Show that, after a rational change of variables, the elliptic curve

$$y^2 = x^3 - \frac{3}{12^2} c_4 x - \frac{2}{12^3} c_6$$

may also be expressed in the Weierstrass form

$$y^2 = x^3 - \frac{3j}{j-1728} D^2 x - \frac{2j}{j-1728} D^3;$$

for some $D \in \mathbb{Q}^\times$ and $j = 1728 c_4^3 / (c_4^3 - c_6^2)$.

2. Show that any elliptic curve in the form

$$E : y^2 + a_1 x y + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

with $j(E) \neq 0, 1728$; may also be expressed in the form above for some $D \in \mathbb{Q}^\times$ and $j = j(E)$.

Problem 2. Show that the following are equivalent for a rational elliptic curve E :

1. E has a rational 2-isogeny.
2. E is of the form $y^2 = x^3 + a x^2 + b x$ for some $a, b \in \mathbb{Q}$.

3. There exists $a, b \in \mathbb{Q}$ such that j -invariant of E is of the form

$$j(E) = \frac{256 (a^2 - 3b)^3}{b^2 (a^2 - 4b)}.$$

Problem 3. Let $k \in \mathbb{Q}$ such that $k \neq 0, 1$. Show that the elliptic curve

$$C : y^2 = (1 - x^2) (1 - k^2 x^2)$$

has a rational 2-isogeny.

Problem 4. Show that the following are equivalent for a rational elliptic curve E :

1. E has a rational 3-isogeny.
2. A twist of E is of the form $y^2 + axy + by = x^3$ for some $a, b \in \mathbb{Q}$.
3. There exists $a, b \in \mathbb{Q}$ such that j -invariant of E is of the form

$$j(E) = \frac{a^3 (a^3 - 24b)^3}{b^3 (a^3 - 27b)}.$$

Chapter 10

Lecture 7: Monday, October 21

10.1 My Favorite Elliptic Curve

10.1.1 Basic Properties

For this lecture, we consider the elliptic curve

$$E : y^2 = x^3 - 4x + 4. \quad (10.1)$$

The constants associated to this curve are

$$c_4 = 192, \quad c_6 = -3456, \quad \Delta(E) = \frac{c_4^3 - c_6^2}{1728} = -2816, \quad j(E) = \frac{c_4^3}{\Delta(E)} = -\frac{27658}{11}. \quad (10.2)$$

10.1.2 Rational Points

Some rational points on this curve are

$$P = (2, 2), \quad [2]P = (0, 2), \quad [3]P = (-2, -2), \quad [7]P = \left(\frac{10}{9}, \frac{26}{27}\right). \quad (10.3)$$

In fact, the only integral points on E are $[m]P$ for $1 \leq m \leq 6$ and $m = 11$:

$$[11]P = (310, -5458). \quad (10.4)$$

We think of $[11]P$ as being “near” the point at infinity \mathcal{O} because it is such a large integral point. That is, P is “near” $[12]P$:

$$[12]P = \left(\frac{273}{11^2}, \frac{3383}{11^3}\right) = (2.2562, 2.5417). \quad (10.5)$$

10.1.3 Mordell-Weil Group

First I claim that this curve has no torsion points. The cubic polynomial $x^3 - 4x + 4$ is irreducible i.e. has no rational roots, so E has no 2-torsion points. By Mazur's Theorem, the only possibilities for $\text{Tor}(E)$ are $\mathbb{Z}/N\mathbb{Z}$ for $N = 1, 3, 5, 7, 9$. In fact, the division polynomials are $\psi_N(x)$ are irreducible so E does not have any N -isogenies for $N > 1$.

It is more difficult to prove, but E has rank 1, and is generated by $P = (2, 2)$. That is, $E(\mathbb{Q}) = \langle (2, 2) \rangle \simeq \mathbb{Z}$. Hence, since $[11]P \approx \mathcal{O}$, we actually think of $E(\mathbb{Q}) \approx \mathbb{Z}/11\mathbb{Z}$.

10.2 Triangles with Concurrent Cevians

10.2.1 Triangles to Elliptic Curves

Let's consider an integer triangle ABC such that 1) the median from A i.e. the line AX through A which bisects side BC , 2) the bisector of angle B i.e. the line BY through B which divides this angle equally, and 3) the altitude from C i.e. the line CZ through C which meets AB at a right angle; are all concurrent i.e. meet at a common point. Any equilateral triangle with integral sides satisfies these properties. We wish to describe all such triangles.

Let's make this more explicit. Ceva's Theorem states that these lines are related by the product

$$\frac{BX}{XC} \cdot \frac{CY}{YA} \cdot \frac{AZ}{ZB} = 1. \quad (10.6)$$

We substitute

$$\begin{aligned} a &= \text{length of side } BC \text{ opposite } A, \\ b &= \text{length of side } AC \text{ opposite } B, \\ c &= \text{length of side } AB \text{ opposite } C. \end{aligned} \quad (10.7)$$

Then we have

$$\frac{BX}{XC} = 1, \quad \frac{CY}{YA} = \frac{CB}{BA} = \frac{a}{c} \text{ (similar triangles),} \quad \frac{AZ}{ZB} = \frac{b \cos A}{a \cos B}. \quad (10.8)$$

Ceva's Theorem may be restated as

$$\frac{b \cos A}{c \cos B} = 1 \implies a(b^2 + c^2 - a^2) = 2abc \cos A = 2ac^2 \cos B = c(c^2 + a^2 - b^2). \quad (10.9)$$

That is,

$$x = \frac{2c}{a+c}, \quad y = \frac{2b}{a+c} \implies y^2 = x^3 - 4x + 4. \quad (10.10)$$

Hence given an integral triangle with concurrent cevians, we find a rational point on the elliptic curve E .

10.2.2 Elliptic Curves to Triangles

Conversely, when given a point (x, y) on E , we find a integral triangle ABC with concurrent cevians if we can choose $\lambda \in \mathbb{Q}^\times$ so that

$$a = \frac{2-x}{\lambda}, \quad b = \frac{y}{\lambda}, \quad c = \frac{x}{\lambda} \quad \text{are positive integers.} \quad (10.11)$$

For example, when $(x, y) = [-4]P = (1, 1)$ we find an equilateral triangle: $a = b = c$. We only consider points (x, y) such that $0 < x < 2$ and $0 < y < 2$, so we can always find $\lambda > 0$. (If $-2 < x < 0$ and $2 < y$, we actually find an common point to the cevians that is external to the triangle. This divides the problem into two cases: those with an internal common point, and those with an external common point.)

Here are some examples:

Point (x, y)	Multiple of P	Triangle ABC
$(1, 1)$	$[-4]P$	$(1, 1, 1)$
$(10/3^2, 26/3^3)$	$[7]P$	$(12, 13, 15)$
$(88/7^2, 554/7^3)$	$[-10]P$	$(35, 277, 308)$
$(206/31^2, 52894/31^3)$	$[13]P$	$(26598, 26447, 3193)$
$(9362/103^2, 1175566/103^3)$	$[-15]P$	$(610584, 587783, 4832143)$

Recall that $E(\mathbb{Q}) \approx \mathbb{Z}/11\mathbb{Z}$, so we expect that 4/11 of the multiples $[m]P$ will yield good triangles.

10.3 Period Maps and Elliptic Logarithms

10.3.1 The Real Lattice

Let e_1, e_2 , and e_3 be the roots of the cubic $x^3 - 4x + 4$, and define

$$\omega_1 = 2 \int_{e_1}^{\infty} \frac{dt}{\sqrt{t^3 - 4t + 4}}, \quad \omega_2 = 2 \int_{e_2}^{e_3} \frac{dt}{\sqrt{t^3 - 4t + 4}}. \quad (10.12)$$

The cubic $x^3 - 4x + 4$ has exactly one real root $e_1 = -2.38298$, so $\omega_1 = 8.50506 \in \mathbb{R}$ and $\omega_2 = 3.31085i \in \mathbb{C}$.

We have a group isomorphism

$$\phi: E(\mathbb{C}) \rightarrow \mathbb{C} / \mathbb{Z}\langle \omega_1, \omega_2 \rangle, \quad (x, y) \mapsto \int_x^{\infty} \frac{dt}{\sqrt{t^3 - 4t + 4}}. \quad (10.13)$$

We now consider $E(\mathbb{R})$ as a subgroup of $E(\mathbb{C})$. This means that we consider the lattice

$$\mathbb{Z}\langle \omega_1, \omega_2 \rangle \cap \mathbb{R} = 2\Omega(E)\mathbb{Z} \quad \text{where} \quad \Omega(E) = \frac{\omega_1}{2} = \int_{e_1}^{\infty} \frac{dt}{\sqrt{t^3 - 4t + 4}} \in \mathbb{R}. \quad (10.14)$$

Then using the Lattice Isomorphism Theorems $E(\mathbb{R}) \simeq \mathbb{R} / 2\Omega\mathbb{Z}$.

10.3.2 Approximations at Infinity

Define $g(E)$ as the ratio

$$g(E) = \frac{1}{2\Omega(E)} \cdot \phi(P) = \frac{1}{\omega_1} \int_2^\infty \frac{dt}{\sqrt{t^3 - 4t + 4}} = 0.180604\dots \quad (10.15)$$

(Guy's "My Favorite Elliptic Curve" considers $1 - g(E)$ instead.) A continued fraction for $g(E)$ is

$$g(E) = \frac{1}{5 + \frac{1}{1 + \frac{1}{1 + \frac{1}{6 + \dots}}}} \approx \frac{0}{1}, \frac{1}{5}, \frac{1}{6}, \frac{2}{11}, \frac{13}{72}, \frac{41}{227}, \dots \quad (10.16)$$

Hence we have

$$\phi(P) \approx \frac{2}{11} \cdot 2\Omega \implies \phi([11]P) \approx 2 \cdot 2\Omega\mathbb{Z}. \quad (10.17)$$

This explains why we consider $[11]P \approx \mathcal{O}$. Note that an even better approximation is $[72]P \approx \mathcal{O}$ because

$$[72]P = (4543.72\dots, 306279.98\dots). \quad (10.18)$$

We can consider $\{m \cdot g(E)\} = m \cdot g(E) - \lfloor m \cdot g(E) \rfloor$ for various integers m . The best (i.e. closest to an integer) candidates are

Integer m	Fractional Part $\{m \cdot g(E)\}$
1	0.180604
5	0.90302
6	0.083624
11	0.986644
72	0.00348858
227	0.99711

Chapter 11

Lecture 8: Wednesday, October 23

11.1 Period Maps and Elliptic Logarithms (continued)

11.1.1 Elliptic Curves Over \mathbb{R}

Consider an elliptic curve $y^2 = x^3 + Ax + B$ with A and B real numbers, and let e_1, e_2 , and e_3 be the roots of the cubic $x^3 + Ax + B$. We focus on the case where these roots are all real i.e. $\Delta(E) > 0$, and label them so that $e_1 < e_2 < e_3$. (The discriminant is

$$\Delta(E) = 16(e_1 - e_2)^2(e_1 - e_3)^2(e_2 - e_3)^2 \quad (11.1)$$

so $\Delta(E) > 0$ if and only if all three roots are real.)

First, I claim that the integrals

$$\Omega(E) = 2 \int_{e_1}^{e_2} \frac{dt}{\sqrt{t^3 + At + B}} = 2 \int_{e_3}^{\infty} \frac{dt}{\sqrt{t^3 + At + B}} \in \mathbb{R}. \quad (11.2)$$

Consider the following substitution:

$$u = (e_2 - e_3) \frac{x - e_1}{x - e_2} + e_3 \implies \frac{du}{dx} = \frac{(e_3 - e_2)(e_2 - e_1)}{(x - e_2)^2} > 0. \quad (11.3)$$

This is a transposition map defined over \mathbb{R} that takes $e_1 \mapsto e_3$ and $e_2 \mapsto \infty$. Hence we find

$$\begin{aligned} \int_{e_1}^{e_2} \frac{dx}{\sqrt{x^3 + Ax + B}} &= \int_{e_1}^{e_2} \frac{dx}{\sqrt{(x - e_1)(x - e_2)(x - e_3)}} \\ &= \int_{e_3}^{\infty} \frac{du}{\sqrt{(u - e_1)(u - e_2)(u - e_3)}} = \int_{e_3}^{\infty} \frac{du}{\sqrt{u^3 + Au + B}}. \end{aligned} \quad (11.4)$$

Also, the cubic $x^3 + Ax + B$ is positive on the regions $e_1 \leq x \leq e_2$ and $e_3 \leq x$ so its square root is a real number. Hence, $\Omega(E)$ is a real number as claimed.

We have the isomorphism $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$ where $\Lambda = \mathbb{Z}\langle\omega_1, \omega_2\rangle$ in terms of

$$\omega_1 = 2 \int_{e_1}^{\infty} \frac{dt}{\sqrt{t^3 + At + B}} \quad \text{and} \quad \omega_2 = 2 \int_{e_2}^{e_3} \frac{dt}{\sqrt{t^3 + At + B}}. \quad (11.5)$$

Note that ω_2 must be purely imaginary since $x^3 + Ax + B$ is negative in the region $e_2 < x < e_3$; and $\omega_1 - \omega_2 = 2\Omega(E)$ is a real number. Hence $\Lambda \cap \mathbb{R} = 2\Omega(E)\mathbb{Z}$ and $\Lambda \cap i\mathbb{R} = \omega_2\mathbb{Z}$. As before, we consider $E(\mathbb{R})$ as a subgroup of $E(\mathbb{C})$, and look at the map

$$\phi : E(\mathbb{R}) \rightarrow \mathbb{C}/\Lambda, \quad (x, y) \mapsto \int_x^{\infty} \frac{dt}{\sqrt{t^3 + At + B}}. \quad (11.6)$$

This map is injective, but certainly not surjective. When $e_3 \leq x$ then $\phi(x, y)$ is a real number, but when $e_1 \leq x \leq e_2$ the integral is complex. Explicitly,

$$\operatorname{Re} \int_x^{\infty} \frac{dt}{\sqrt{t^3 + At + B}} = \begin{cases} \int_x^{e_2} \frac{dt}{\sqrt{t^3 + At + B}} + \int_{e_3}^{\infty} \frac{dt}{\sqrt{t^3 + At + B}} & \text{if } e_1 \leq x \leq e_2; \\ \int_x^{\infty} \frac{dt}{\sqrt{t^3 + At + B}} & \text{if } e_3 \leq x. \end{cases} \quad (11.7)$$

We must be careful about the image because the 2-torsion points map to

$$(e_1, 0) \mapsto \Omega + \frac{\omega_2}{2}, \quad (e_2, 0) \mapsto \frac{\Omega}{2} + \frac{\omega_2}{2}, \quad (e_3, 0) \mapsto \frac{\Omega}{2}; \quad (11.8)$$

so we actually map

$$(x, y) \mapsto (\operatorname{Re} \phi(x, y) \bmod \Omega(E)\mathbb{Z}, \operatorname{Im} \phi(x, y) \bmod \omega_2\mathbb{Z}). \quad (11.9)$$

Note that the imaginary part of the integral $\operatorname{Im} \phi(x, y)$ is either $\frac{1}{2}\omega_2$ or zero. Hence we may think of the second coordinate in the map above as taking values in $\mathbb{Z}/2\mathbb{Z}$, where the value is 1 if $e_1 \leq x \leq e_3$ and the value is 0 if $e_3 \leq x$.

This gives an isomorphism

$$E(\mathbb{R}) \simeq \begin{cases} \mathbb{R}/2\Omega(E)\mathbb{Z} & \text{if } \Delta(E) > 0, \\ \mathbb{R}/\Omega(E)\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{if } \Delta(E) < 0. \end{cases} \quad (11.10)$$

11.1.2 Relation with the Circle

We remark that there is a similarity in the construction with the unit circle. Given a real point (x, y) on the circle $C : x^2 + y^2 = 1$, we have an isomorphism

$$C(\mathbb{R}) \simeq \mathbb{R}/2\Omega(C)\mathbb{Z}, \quad (x, y) \mapsto \int_x^1 \frac{dt}{\sqrt{1-t^2}} \quad \text{where} \quad \Omega(C) = \int_{-1}^1 \frac{dt}{\sqrt{1-t^2}} = \pi. \quad (11.11)$$

The group operation on C is just multiplication:

$$(x, y) \oplus (u, v) = (xu - yv, xv + yu), \quad \mathcal{O} = (1, 0). \quad (11.12)$$

Note that the circle has just one connected component. The expressions for $E(\mathbb{R})$ depend on whether $E(\mathbb{R})$ has one or two connected components, which means it depends on whether we have one or two copies of the circle.

11.1.3 Approximations at Infinity

Now consider the elliptic curve $E : y^2 + y = x^3 - x$. It turns out that $E(\mathbb{Q}) \simeq \mathbb{Z}$ is generated by $P = (0, 0)$, so making the substitution

$$\begin{aligned} X &= 4x \\ Y &= 8y + 4 \end{aligned} \implies E : Y^2 = X^3 - 16x + 16 \quad \text{with generator } (0, 4). \quad (11.13)$$

The cubic $X^3 - 16x + 16$ has all real roots, so we compute

$$E(\mathbb{R}) \simeq \mathbb{R} / \Omega(E)\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \quad \text{where } \Omega(E) = 2.99346\dots \quad (11.14)$$

The parameter $g(E)$ is now

$$g(E) = \frac{1}{\Omega(E)} \operatorname{Re} \int_0^\infty \frac{dt}{\sqrt{t^3 - 16t + 16}} = 0.689459\dots \quad (11.15)$$

which has continued fraction expansion

$$g(E) = \frac{1}{1 + \frac{1}{2 + \frac{1}{4 + \frac{1}{1 + \frac{1}{1 + \frac{1}{5 + \frac{1}{2 + \dots}}}}}}}} \approx \frac{1}{1}, \frac{2}{3}, \frac{9}{13}, \frac{11}{16}, \frac{20}{29}, \frac{111}{161}, \dots \quad (11.16)$$

(Again, Richard Guy uses $g = 1 - g(E)$ in his paper “My Favorite Elliptic Curve.”) Say that we can approximate $g(E) \approx \frac{n}{m}$. Then

$$P \mapsto \operatorname{Re} \int_0^\infty \frac{dt}{\sqrt{t^3 - 16t + 16}} \approx \frac{n}{m} \cdot \Omega(E) \implies [m]P \mapsto 0 \pmod{\Omega(E)\mathbb{Z}}. \quad (11.17)$$

However, we can't say that $[m]P \approx \mathcal{O}$ unless m is even because we have to take in account the $\mathbb{Z}/2\mathbb{Z}$ portion of the isomorphism above. Hence, either $[m]P \approx \mathcal{O}$ or $[2m]P \approx \mathcal{O}$ depending on whether m is even or odd.

The following table lists some examples.

m	$[m]P$	$[2m]P$
1	(0, 0)	(1, 0)
3	(-1, -1)	(6, 14)
13	(-1.07469, -0.211098)	(20.3477, -92.1754)
16	(113.635, 1210.79)	-
29	(-1.10638, -0.45435)	(858.885, -25171.6)

The approximation $E(\mathbb{Q}) \approx \mathbb{Z}/16\mathbb{Z}$ works particularly well.

11.2 Heron Triangles

11.2.1 Basic Formulas

We call a triangle with integral sides and rational area a Heron Triangle. One type of Heron Triangle are those formed from Pythagorean Triplets. For example, if the sides are a , b , and c , then there are integers m and n such that

$$\begin{aligned} a &= m^2 - n^2 \\ b &= 2mn \implies a^2 + b^2 = c^2, \quad \text{Area} = \frac{1}{2} ab = mn(m^2 - n^2). \\ c &= m^2 + n^2 \end{aligned} \quad (11.18)$$

These are the so-called Right Heron Triangles. Next week we will consider Heron Triangles in more generality, but during this lecture we will only focus on those that are Isosceles. That is we just double the length of the base and set

$$\begin{aligned} a &= 2(m^2 - n^2) \\ b &= m^2 + n^2 \implies \text{Area} = 2mn(m^2 - n^2). \\ c &= m^2 + n^2 \end{aligned} \quad (11.19)$$

Note that any triangle with rational sides a , b , and c has area given by Heron's Formula:

$$\text{Area} = \sqrt{s(s-a)(s-b)(s-c)} \quad \text{where} \quad s = \frac{a+b+c}{2}. \quad (11.20)$$

11.2.2 Relation with Rectangles

Say that we have a rectangle with integer sides p and q . We would like to find Isosceles Heron Triangles such that they have the same perimeter and area. That is, we're seeking solutions to the Diophantine System

$$\begin{aligned} 2(p+q) &= a+b+c = 4m^2 \\ pq &= 2mn(m^2 - n^2). \end{aligned} \quad (11.21)$$

Note that p and q must be roots of a quadratic equation, namely $(x-p)(x-q) = x^2 - (p+q)x + pq$, so we want the discriminant to be a square:

$$(p-q)^2 = (p+q)^2 - 4pq = 4m^4 - 8mn(m^2 - n^2). \quad (11.22)$$

Another way to say this is

$$x = \frac{2n}{m}, \quad y = \frac{p-q}{m^2} \implies y^2 = x^3 - 4x + 4. \quad (11.23)$$

This time rational points (x, y) give rise to rectangles. Some examples are given in the table below. Recall that for the elliptic curve $E: y^2 = x^3 - 4x + 4$, the group of rational points $E(\mathbb{Q}) \simeq \mathbb{Z}$ has generator $P = (2, 2)$.

Point (x, y)	$[m]P$	Triangle (a, b, c)	Rectangle (p, q)
$(1, 1)$	$[-4]P$	$(6, 5, 5)$	$(6, 2)$
$(10/3^2, 26/3^3)$	$[7]P$	$(56, 53, 53)$	$(60, 21)$
$(88/7^2, 554/7^3)$	$[-10]P$	$(930, 4337, 4337)$	$(462, 4340)$
$(206/31^2, 52894/31^3)$	$[13]P$	$(912912, 467065, 467065)$	$(871689, 51832)$

Note that the $6 - 5 - 5$ triangle is just a doubling of the $3 - 4 - 5$ triangle.

Chapter 12

Homework Assignment #4

Due Monday, October 28 at the start of lecture.

Problem 1. Let $x^3 + Ax + B$ be a cubic polynomial over \mathbb{R} with exactly one real root e_1 . Denote the complex roots by e_2 and e_3 , and consider the periods

$$\omega_1 = 2 \int_{e_1}^{\infty} \frac{dx}{\sqrt{x^3 + Ax + B}} \quad \text{and} \quad \omega_2 = 2 \int_{e_2}^{e_3} \frac{dx}{\sqrt{x^3 + Ax + B}}.$$

1. Show that $\omega_1 \in \mathbb{R}$.
2. Show that the real part of ω_2 is zero i.e. ω_2 is purely imaginary.
3. Prove that $E(\mathbb{R}) \simeq \mathbb{R} / 2\Omega\mathbb{Z}$ in terms of the real period $\Omega = \omega_1/2$.

Problem 2. Consider the elliptic curve $E : y^2 = x^3 + 3$. You may use the fact that $E(\mathbb{Q}) \simeq \mathbb{Z}$ is generated by the point $P = (1, 2)$.

1. Compute the numerical value of the ratio

$$g(E) = \frac{1}{2\Omega} \int_1^{\infty} \frac{dx}{\sqrt{x^3 + 3}} \quad \text{where} \quad \Omega = \int_{-\sqrt[3]{3}}^{\infty} \frac{dx}{\sqrt{x^3 + 3}}.$$

2. Use the continued fraction expansion of $g(E)$ to find an integer $m > 50$ such that $[m]P$ has large coordinates i.e. $[m]P \approx \mathcal{O}$.

Problem 3. Consider the elliptic curve $E : y^2 = x^3 - 43x + 166$. You may use the fact that $E(\mathbb{Q})$ is generated by the point $P = (3, 8)$.

1. Compute the numerical value of the ratio

$$g(E) = \frac{1}{2\Omega} \int_3^\infty \frac{dx}{\sqrt{x^3 - 43x + 166}} \quad \text{where} \quad \Omega = \int_e^\infty \frac{dx}{\sqrt{x^3 - 43x + 166}}$$

in terms of the real root e of $x^3 - 43x + 166$.

2. Use the continued fraction expansion of $g(E)$ to find a positive integer m such that $[m]P = \mathcal{O}$.

Problem 4. Consider the curve $E_\tau^{(n)} : y^2 = x(x - n\tau)(x + n\tau^{-1})$ for $n, \tau \in \mathbb{Q}^\times$.

1. Show that if $(x, y) \in E_\tau^{(n)}(\mathbb{Q})$ does not have order 2 then

$$(x, \pm y) \oplus (0, 0) = \left(-\frac{n^2}{x}, \pm \frac{n^2 y}{x^2} \right).$$

2. Show that if $E_\tau^{(n)}(\mathbb{Q})$ has a point of infinite order then one may always choose such a point with positive x - and y -coordinates.

Chapter 13

Lecture 9: Monday, October 28

13.1 Congruent Numbers

13.1.1 Right Heron Triangles

In the previous lecture, we found that an integral right triangle has integral area. Specifically, given integers s and t with $s > t$, the right triangle with sides

$$\begin{aligned} a &= s^2 - t^2 \\ b &= 2st \quad \implies \text{area} = \frac{1}{2}ab = st(s^2 - t^2). \\ c &= s^2 + t^2 \end{aligned} \quad (13.1)$$

Such triangles are called Right Heron Triangles. Conversely, we ask the following: given a positive integer n , does there exist a right Heron triangle $a - b - c$ with area n ? For example, when $n = 6$ the triangle $3 - 4 - 5$ would suffice. Such a question is known as the Congruent Number problem.

13.1.2 Congruent Numbers

We generalize slightly. We say that a positive integer n is a congruent number if we can find a rational right triangle $a - b - c$ with area n . I claim the following: n is a congruent number if and only if there is a rational number x such that $x - n$, x , and $x + n$ are each the square of a rational number. First suppose n is a congruent number. That is, we can find a rational triangle $a - b - c$ such that $a^2 + b^2 = c^2$ and $\frac{1}{2}ab = n$. We choose

$$x = \left(\frac{c}{2}\right)^2 \implies x \pm n = \frac{c^2 \pm 4n}{4} = \frac{a^2 \pm 2ab + b^2}{4} = \left(\frac{a \pm b}{2}\right)^2. \quad (13.2)$$

Conversely, say that $x - n$, x , and $x + n$ are all rational squares. We choose

$$\begin{aligned} a &= \sqrt{x+n} - \sqrt{x-n} \\ b &= \sqrt{x+n} + \sqrt{x-n} \implies a^2 + b^2 = c^2, \quad n = \frac{1}{2} ab. \\ c &= 2\sqrt{x} \end{aligned} \tag{13.3}$$

I'd like to make two remarks using this idea. Note that when $n = 6$ we can choose $x = 25/4$. Then $x - n = 1/4$ and $x + n = 49/4$. As an application, I claim that $n = 1$ is not a congruent number. Assume otherwise; then $x = X^2$ for some rational number X , and $(x-1)(x+1) = Y^2$ for some rational number Y . Hence $Y^2 = X^4 - 1$ has a rational solution. However, we discussed this curve in lecture 1; it has no rational solutions! This leads to a contradiction, so $n = 1$ must not be a congruent number.

Note that some integers are congruent numbers while others are not. The difficulty in working with the Congruent Number Problem is that it is not easy to decide when a positive integer is indeed a congruent number.

13.1.3 Tunnell's Theorem

There is a nice result by Jerry Tunnell from 1983. Let n be a square-free positive integer. Consider the following sets:

$$A(n) = \begin{cases} \#\{x_1, x_2, x_3 \in \mathbb{Z} \mid n = 2x_1^2 + x_2^2 + 32x_3^2\} & \text{if } n \text{ is odd;} \\ \#\{x_1, x_2, x_3 \in \mathbb{Z} \mid n/2 = 4x_1^2 + x_2^2 + 32x_3^2\} & \text{if } n \text{ is even.} \end{cases} \tag{13.4}$$

$$B(n) = \begin{cases} \#\{x_1, x_2, x_3 \in \mathbb{Z} \mid n = 2x_1^2 + x_2^2 + 8x_3^2\} & \text{if } n \text{ is odd;} \\ \#\{x_1, x_2, x_3 \in \mathbb{Z} \mid n/2 = 4x_1^2 + x_2^2 + 8x_3^2\} & \text{if } n \text{ is even.} \end{cases}$$

Then if n is congruent, then $B(n) = 2 \cdot A(n)$. It is only conjectured that the converse is always true. However, the contrapositive states that if $B(n) \neq 2 \cdot A(n)$ then n is not congruent. For example, when $n = 1$ we have $A(1) = B(1) = 2$, and so $n = 1$ is not congruent. When $n = 2$ we also have $A(2) = B(2) = 2$ so $n = 2$ is not congruent either.

13.1.4 Elliptic Curves

Using the criterion above, we know that n is a congruent number if and only if this rational number x exists. Make the substitution

$$x = \left(\frac{c}{2}\right)^2, \quad y = \frac{c(a^2 - b^2)}{8} \implies y^2 = x^3 - n^2 x. \tag{13.5}$$

Hence, if n is a congruent number, then $E^{(n)} : y^2 = x^3 - n^2 x$ has a rational point. In particular, this is not a point of order 2 because $y \neq 0$. For example, when $n = 6$ when $E^{(n)}$ has the rational point $(x, y) = (25/4, -35/8)$.

Unfortunately, the converse is not true i.e. each point (x, y) on $E^{(n)}$ does not give a rational triangle $a - b - c$. For example,

$$E^{(6)}(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z} \quad \text{has generators} \quad (\pm n, 0), \quad (-3, 9). \quad (13.6)$$

In fact, $(25/4, -35/8) = [2](-3, 9)$. However, the point $(-3, 9)$ cannot correspond to a right rational triangle since $x = -3$ is not the square of a rational number. This motivates a general trick. If (x, y) is a rational point not of order 2 on $E^{(n)}$ then

$$[2](x, y) = \left(\left(\frac{x^2 + n^2}{2y} \right)^2, \frac{(x^2 + n^2)(x^2 - 2nx - n^2)(x^2 + 2nx - n^2)}{(2y)^3} \right). \quad (13.7)$$

In fact, $(x', y') = [2](x, y)$ gives

$$x' - n = \left(\frac{x^2 - 2nx - n^2}{2y} \right)^2, \quad x' = \left(\frac{x^2 + n^2}{2y} \right)^2, \quad x' + n = \left(\frac{x^2 + 2nx - n^2}{2y} \right)^2. \quad (13.8)$$

Hence, in general (x, y) does not give a rational triangle with area n , but $[2](x, y)$ does:

$$\begin{aligned} a &= \sqrt{x' + n} - \sqrt{x' - n} = \frac{2nx}{y}, \\ b &= \sqrt{x' + n} + \sqrt{x' - n} = \frac{x^2 - n^2}{y}, \\ c &= 2\sqrt{x'} = \frac{x^2 + n^2}{y}. \end{aligned} \quad (13.9)$$

(We have taken positive square roots.)

We've shown that the following are equivalent for a positive integer n :

1. n is a congruent number.
2. There exists a rational number x such that $x - n$, x , and $x + n$ are all consecutive squares.
3. The curve $y^2 = x^3 - n^2x$ has a rational point which is not of order 2.

13.2 The Elliptic Curve $E^{(n)}$

13.2.1 Torsion Points

I claim something stronger than stated above: n is a congruent number if and only if the curve $E^{(n)}$ has a rational point of infinite order. In particular, if n is the area of one right triangle, then it is the area of infinitely many!

Clearly, if $E^{(n)}$ has a point of infinite order then the formulas above show that n is congruent. To prove the converse, it suffices to show that the torsion group of $E^{(n)}(\mathbb{Q})$ is $\text{Tor}(E^{(n)}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. This is because if $(x, y) \in E^{(n)}(\mathbb{Q})$ is a point not of order 2, then $(x, y) \notin \text{Tor}(E^{(n)})$ and so (x, y) must be a rational

point of infinite order. We prove this using the strength of Mazur's Theorem. (For an alternative proof, see Koblitz's "Introduction to Elliptic Curves and Modular Forms," Chapter 1, §9, Proposition 17.) Note that $E^{(n)}[2]$ is rational because

$$E^{(n)}[2] = \{(-n, 0), (0, 0), (n, 0), \mathcal{O}\}. \quad (13.10)$$

Then Mazur's Theorem states that the torsion subgroup of $E^{(n)}(\mathbb{Q})$ is one of four types: $\text{Tor}(E^{(n)}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$ for $N = 1, 2, 3, 4$. We show that $N = 1$ is the only possibility.

I claim that N cannot be even. If it were, then there is some rational point P such that $[2N]P = \mathcal{O}$, so let $(x, y) = [N/2]P$ be a point of order 4. Then the y -coordinate of $[2](x, y)$ must be zero, and hence

$$\begin{aligned} (x^2 + n^2)(x^2 - 2nx - n^2)(x^2 + 2nx - n^2) &= 0 \\ \implies \frac{x}{n} &= \pm i, 1 \pm \sqrt{2}, -1 \pm \sqrt{2}. \end{aligned} \quad (13.11)$$

Since $x \notin \mathbb{Q}$ we see that $P \notin E^{(n)}(\mathbb{Q})$. This is a contradiction, so N must be odd.

Now I claim that $N \neq 3$. If it were, then there is some rational point (x, y) of order 3. Then $[2](x, y) = [-1](x, y)$, so by considering the x -coordinates,

$$\left(\frac{x^2 + n^2}{2y}\right)^2 = x \implies 3x^4 - 6n^2x^2 - n^4 = 0 \implies \frac{x^2}{n^2} = \frac{3 \pm 2\sqrt{3}}{3}. \quad (13.12)$$

Since $x \notin \mathbb{Q}$ we see that $(x, y) \notin E^{(n)}(\mathbb{Q})$. This is a contradiction, so $N \neq 3$. Hence $N = 1$ is the only possibility.

We have shown that the Mordell-Weil Group of the elliptic curve is

$$E^{(n)}(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^r \quad (13.13)$$

for some nonnegative integer r . In fact, n is a congruent number if and only if $r > 0$.

13.2.2 Ranks of Twists of Curves

The elliptic curve $E^{(n)} : y^2 = x^3 - n^2x$ is a twist of the curve $E : y^2 = x^3 - x$. These curves have j -invariant $j(E^{(n)}) = 1728$. Note that E has rank $r = 0$ because $n = 1$ is not a congruent number, however $E^{(6)}$ has rank $r = 1$ because $n = 6$ is a congruent number. The following table shows how the ranks vary as we twist for various values of n .

Twist n	Rank r	Generator of $E^{(n)}$	Triangle $a - b - c$
$1 \leq n \leq 4$	0	—	—
5	1	(-4, 6)	$\frac{9}{6} - \frac{40}{6} - \frac{41}{6}$
6	1	(-3, 9)	3-4-5
7	1	$(\frac{112}{3^2}, \frac{980}{3^3})$	$\frac{175}{60} - \frac{288}{60} - \frac{337}{60}$
$8 \leq n \leq 12$	0	—	—
13	1	$(-\frac{36}{5^2}, \frac{1938}{5^3})$	$\frac{23400}{9690} - \frac{104329}{9690} - \frac{106921}{9690}$

Note that $n = 5$ and $n = 7$ are both congruent numbers. $n = 5$ is the smallest congruent number, and $n = 7$ was first shown to be congruent by Euler.

Chapter 14

Lecture 10: Wednesday, October 30

14.1 Heron Triangles

14.1.1 Motivation

In 1959, Robert Carmichael considered triangles with integral sides and integral area. He showed that if such a triangle has sides of length a , b , and c and has area n , then there are integers p , q , and r

$$\begin{aligned} n = pqr(p+q)(pq-r^2) \implies \begin{aligned} a &= q(p^2+r^2) \\ b &= p(q^2+r^2) \\ c &= (p+q)(pq-r^2) \end{aligned} \quad ; \end{aligned} \quad (14.1)$$

as long as $pq > r^2$. Recall that this may be verified by Heron's formula

$$n = \sqrt{s(s-a)(s-b)(s-c)} \quad \text{where} \quad s = \frac{a+b+c}{2}. \quad (14.2)$$

Richard Guy states that Indian mathematician Brahmagupta (598-668 A.D.) proved this as well, and was probably the first to do so.

We are motivated by the following question: given a positive integer n , does there always exist a rational triangle $a-b-c$ with area n ? This is a generalization of the congruent number problem, where the rational triangle is assumed to be a right triangle. For example, $n = 1$ is not a congruent number, but it is the area of a rational triangle:

$$a = \frac{3}{2}, \quad b = \frac{5}{3}, \quad c = \frac{17}{6} \implies \text{area} = 1. \quad (14.3)$$

(This example doesn't appear to correspond to any p , q , and r from above.)

14.1.2 Elliptic Curves

I will prove that a positive integer n can be expressed as the area of a triangle with rational sides if and only if for some positive rational number τ the elliptic curve

$$E_\tau^{(n)} : y^2 = x(x + n\tau^{-1})(x - n\tau) \quad (14.4)$$

has a rational point which is not of order 2. n is a congruent number if $\tau = 1$.

Say that we have a triangle $\triangle ABC$ with area n . Let a denote the length of side A ; and similarly with b and B ; and similarly with c and C . Finally, denote θ as the angle $\angle AB$ between sides A and B . Then the area of the triangle is $n = \frac{1}{2}ab \sin \theta$. By considering the Law of Cosines and the area, we have the relations

$$\cos \theta = \frac{a^2 + b^2 - c^2}{2ab} \quad \text{and} \quad \sin \theta = \frac{2n}{ab}. \quad (14.5)$$

Denote τ as the rational number

$$\tau = \tan \frac{\theta}{2} = \frac{4n}{(a+b)^2 - c^2}; \quad (14.6)$$

in particular, $\tau = 1$ if we have a right triangle.

Set $u = (a - b \cos \theta)/c$ and $v = (b \sin \theta)/c$ so that

$$u^2 + v^2 = 1 \implies \begin{aligned} u &= \frac{t^2 - 1}{t^2 + 1} & a &= s(t^2 + 2 \cot \theta t - 1) \\ v &= \frac{2t}{t^2 + 1} & b &= 2st \csc \theta \\ & & c &= s(t^2 + 1) \end{aligned} \quad (14.7)$$

for some rational s and t . Then $y^2 = x^3 + \alpha x^2 + \beta x$ in terms of

$$\alpha = \frac{2n}{\tan \theta} = \frac{a^2 + b^2 - c^2}{2}, \quad \text{and} \quad \beta = -n^2; \quad (14.8)$$

and we have a rational point

$$x = nt = \frac{(a+c)^2 - b^2}{4}, \quad y = \frac{n^2}{s} = a \frac{(a+c)^2 - b^2}{4}. \quad (14.9)$$

which does not have order 2. Denote this curve by $E_\tau^{(n)}$. (Note that $E_\tau^{(n)}$ is a twist of $E_\tau : y^2 = x(x - \tau)(x + \tau^{-1})$.) The discriminant of the curve is

$$\Delta [E_\tau^{(n)}] = 16(\alpha^2 - 4\beta)\beta^2 = 16n^6(\tau + \tau^{-1})^2 \neq 0; \quad (14.10)$$

hence $E_\tau^{(n)}$ is indeed an elliptic curve. Conversely, let (x, y) be a rational point on $E_\tau^{(n)}$ which is not of order 2. Of the four points

$$[\pm 1](x, y) = (x, \pm y), \quad \text{and} \quad (0, 0) \oplus [\pm 1](x, y) = \left(-\frac{n^2}{x}, \pm \frac{n^2 y}{x^2}\right) \quad (14.11)$$

we can choose one, say (X, Y) , with $X > 0$ and $Y > 0$. We find a triangle with area n if we choose sides of length

$$a = \frac{Y}{X}, \quad b = \frac{\sqrt{\Delta[E_\tau^{(n)}]}}{4n^2} \frac{X}{Y}, \quad c = \frac{X^2 + n^2}{Y}. \quad (14.12)$$

14.2 The Elliptic Curve $E_\tau^{(n)}$

14.2.1 2-Torsion

The more general elliptic curve $E_\tau^{(n)}$ has all of its 2-torsion rational:

$$E_\tau^{(n)}[2] = \left\{ (0, 0), \left(\frac{c^2 - (a+b)^2}{4}, 0 \right), \left(\frac{c^2 - (a-b)^2}{4}, 0 \right), \mathcal{O} \right\}. \quad (14.13)$$

We will use this to gain more information about the torsion points on $E_\tau^{(n)}$. In the congruent number problem, the elliptic curve $E_1^{(n)}$ only has points of order 2, but there may be points of other orders on $E_\tau^{(n)}$ for $\tau \neq 1$.

14.2.2 3-Torsion

Denote by C_n the hyperelliptic curve

$$C_n : v^2 = (u^4 + n^2)(9u^4 + n^2). \quad (14.14)$$

I claim that $E_\tau^{(n)}(\mathbb{Q})$ has a rational point of order 3 for some $\tau \in \mathbb{Q}^\times$ if and only if there exists a nontrivial rational point on C_n i.e. a point with $u \neq 0$. This is a strong statement, because C_n has genus 4, and so by Falting's Theorem we expect that it has only finitely many rational points. In fact, I will eventually show that it never has rational points!

To see why, say that (x, y) is a rational point of order 3 on $E_{n,\tau}$. Then x is a root of the 3-division polynomial:

$$\psi_3(x) = 3x^4 - 4n(\tau - \tau^{-1})x^3 - 6n^2x^2 - n^4 \quad (14.15)$$

(See page 105 of Silverman's "The Arithmetic of Elliptic Curves" for more properties of the division polynomials.) Now express τ in terms of x :

$$\tau = \frac{3x^4 - 6n^2x^2 - n^4 \pm (x^2 + n^2)\sqrt{(x^2 + n^2)(9x^2 + n^2)}}{8nx^3}. \quad (14.16)$$

Then $(x^2 + n^2)(9x^2 + n^2) = v^2$ for some rational number v . On the other hand, since y is rational we have

$$y^2 = x(x + n\tau^{-1})(x - n\tau) = \frac{(x^2 + n^2)^2}{4x}; \quad (14.17)$$

so that $x = u^2$ for some rational number u . Hence (u, v) is a nontrivial rational point on C_n . Conversely, say that (u, v) is a rational point on C_n with $u \neq 0$. Set

$$\tau = \frac{3u^8 - 6n^2u^4 - n^4 + v(u^4 + n^2)}{8nu^6}, \quad x = u^2, \quad y = \frac{u^4 + n^2}{2u}. \quad (14.18)$$

Then (x, y) is a rational point of order 3 on $E_\tau^{(n)}$.

14.2.3 4-Torsion

Denote by D_n the elliptic curve

$$D_n : \quad v^2 = u^4 + n^2. \quad (14.19)$$

I will show the following are equivalent:

1. $E_\tau^{(n)}$ has a rational point of order 4 for some τ .
2. There exists a nontrivial rational point on D_n i.e. a point with $u \neq 0$.
3. n is the area of a rational isosceles triangle.

(1 \implies 2). Say that (x, y) is a rational point of order 4 on $E_\tau^{(n)}$. Then x is a root of the 4-division polynomial:

$$\psi_4(x) = 2(x^2 + n^2)(x^2 - 2n\tau x - n^2)(x^2 + 2n\tau^{-1}x - n^2) \quad (14.20)$$

Since x is rational, we only have four possibilities for x :

$$x = n\tau \pm n\sqrt{1 + \tau^2} \quad \text{or} \quad x = -n\tau^{-1} \pm n\tau^{-1}\sqrt{1 + \tau^2}. \quad (14.21)$$

In either case this implies $n^2 + (n\tau)^2 = v^2$ for some rational number v . On the other hand, since y is rational we have

$$y^2 = n\tau^{-1} \left(\frac{x^2 + n^2}{2n} \right)^2 \quad \text{or} \quad -n\tau \left(\frac{x^2 + n^2}{2n} \right)^2. \quad (14.22)$$

In either case this implies $(n\tau)^2 = u^4$ for some rational number u . Hence (u, v) is a nontrivial rational point on D_n .

(2 \implies 3). Say that (u, v) is a rational point on D_n with $u \neq 0$. Without loss of generality, assume u and v are positive. We set

$$\tau = \frac{u^2}{n}, \quad x = u^2 + v, \quad y = \frac{u^2v + v^2}{u}; \quad (14.23)$$

then (x, y) is a point of order 4 on $E_\tau^{(n)}$. The discriminant is

$$\Delta [E_\tau^{(n)}] = 16n^4 \frac{v^4}{u^4} \implies a = \frac{v}{u}, \quad b = \frac{v}{u}, \quad c = 2u; \quad (14.24)$$

defines a rational isosceles triangle with area n .

(3 \implies 1) Assume n is the area of some isosceles triangle. One checks that the associated point on the elliptic curve has order 4.

As an application of this, say $n = 3$. Then D_n has the rational point $(u, v) = (2, 5)$, and this corresponds to the rational isosceles triangle

$$a = \frac{5}{2}, \quad b = \frac{5}{2}, \quad c = 4 \implies \text{area} = 3. \quad (14.25)$$

14.2.4 Mazur's Theorem

We now use all of the previous information to classify the torsion subgroup of $E_\tau^{(n)}$. I claim the following:

1. $E_\tau^{(n)}$ does not have a point of order 6 or 8.
2. The torsion subgroup of $E_\tau^{(n)}$ is either $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.
3. If D_n has no nontrivial rational points, then the torsion subgroup of $E_\tau^{(n)}$ is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

The proof we give of the first statement is similar to that of Theorem 3 in Rusin's "Rational Triangles with Equal Area." Assume that $E_\tau^{(n)}$ has a rational point of order 6. Then it also has a point of order 3, so C_n has a nontrivial rational point, say (u, v) . Then $(U, V) = (u^2/n, v/n)$ is a nontrivial rational point on the hyperelliptic curve

$$V^2 = (U^2 + 1)(9U^2 + 1). \quad (14.26)$$

However the only rational points are $(U, V) = (0, \pm 1)$. This is a contradiction, so $E_\tau^{(n)}$ does not have any rational points of order 6. Now say (x, y) is a point on $E_\tau^{(n)}$ of order 8. Consider the point

$$(X, Y) = [2](x, y) = \left(\left(\frac{x^2 + n^2}{2y} \right)^2, \frac{\psi_4(x)}{16y^3} \right) \quad (14.27)$$

in terms of the 4-division polynomial. This is a point of order 4, so say $X^2 - 2n\tau X - n^2 = 0$. (The other roots come from the reflection $\tau \mapsto -\tau^{-1}$.) Recall that $n\tau = u^2$ and $X = u^2 + v$ for some rational u and v on the curve $v^2 = u^4 + n^2$. Choose a rational number z such that $x = (1 + z)v + u^2$. Then the relation $X = ((x^2 + n^2)/(2y))^2$ implies $4(1 + z)^2(u^2 + v)^2 = u^2 v z^4$, so that $v = w^2$ for some rational number w . Then $(U, V) = (w/u, n/u^2)$ is a nontrivial rational point on the hyperelliptic curve

$$V^2 = U^4 - 1. \quad (14.28)$$

Again, the only rational points are $(U, V) = (\pm 1, 0)$. Again, this is a contradiction, so $E_\tau^{(n)}$ does not have any rational points of order 8.

We now focus on the last two statements. The torsion of $E_\tau^{(n)}$ contains $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ hence the torsion subgroup is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$ for $N = 1, 2, 3, 4$. But N cannot be 3 or 4 by the discussion above.

14.3 Main Theorem

14.3.1 Points of Infinite Order

Say that a positive integer n is given. I will show that there are infinitely many rational triangles with area n . In fact, I will show that if n is the area of a rational triangle with an angle θ and if such a triangle is not isosceles, there are infinitely many rational triangles with area n possessing this fixed angle.

The first statement was answered by a paper of N. J. Fine from 1976; our proof will be a simplified version of his. To show that there exists at least one triangle having area n , it suffices to find some $E_\tau^{(n)}$ with a rational point not of order 2. We choose

$$\tau = \frac{2}{2n+1} \quad \text{and} \quad (x, y) = \left(\frac{2n+1}{4}, \frac{4n^2-1}{8} \right). \quad (14.29)$$

This gives the rational triangle

$$a = \frac{2n-1}{2}, \quad b = \frac{n(4n^2+4n+5)}{4n^2-1}, \quad c = \frac{20n^2+4n+1}{2(4n^2-1)}. \quad (14.30)$$

It is easy to verify that $a \neq b$ so it corresponds to a rational point not of order 2. But this point also does not have order 4 so it is not torsion, and hence must be a point of infinite order.

Say that we have a triangle $\triangle ABC$ with area n , with θ as the angle $\angle A$ between sides A and B . Then we have a rational point on the elliptic curve $E_\tau^{(n)}$ where $\tau = \tan \frac{\theta}{2}$. Since $\triangle ABC$ is not isosceles, it corresponds to a point of infinite order on the elliptic curve. But each point corresponds to a rational triangle of area n having fixed angle θ .

14.3.2 Examples

Here are some examples. I've chosen the triangles with the simplest denominators, and I've set $\tau = \frac{4n}{(a+b)^2 - c^2}$.

Area n	Triangle $a - b - c$	Torsion $E_\tau^{(n)}$	Rank $E_\tau^{(n)}$
1	$\frac{9}{6} - \frac{10}{6} - \frac{17}{6}$	$Z_2 \times Z_2$	1
2	$\frac{5}{6} - \frac{29}{6} - \frac{30}{6}$	$Z_2 \times Z_2$	1
3	$\frac{5}{2} - \frac{5}{2} - \frac{8}{2}$	$Z_2 \times Z_4$	1
4	$\frac{9}{3} - \frac{10}{3} - \frac{17}{3}$	$Z_2 \times Z_2$	1
5	$\frac{9}{6} - \frac{40}{6} - \frac{41}{6}$	$Z_2 \times Z_2$	1

Chapter 15

Homework Assignment #5

Due Monday, November 4 at the start of lecture.

Problem 1. Let $n \in \mathbb{Z}_{>0}$, and consider the elliptic curve $E^{(n)} : y^2 = x^3 - n^2 x$. Let $N = d^2 n$ for some $d \in \mathbb{Z}_{>0}$.

1. Show that $E^{(N)}$ is rationally equivalent to $E^{(n)}$.
2. Show that the rank of $E^{(N)}$ is the same as the rank of $E^{(n)}$. (Note: this is stronger than saying N is congruent if and only if n is congruent.)
3. Show that if n is a power of 2 or a power of 3, then n is not a congruent number.

Problem 2. Let $n \in \mathbb{Z}_{>0}$. Show that n is a congruent number if and only if $2n$ is the area of an isosceles rational triangle.

The following problems discuss the concept of resolution of singularities by “blowing up” points.

Problem 3. Consider the (affine) curve

$$E : y^2 = x^4 + a_1 x + a_2 x^2 + a_3 x + a_4.$$

Denote $(x_1 : x_2 : x_0)$ as the equivalence class of points $(x_1, x_2, x_0) \neq (0, 0, 0)$ modulo scalar multiples, and \mathbb{P}^2 as the collection of such classes. Define the (projective) curve

$$C = \{(x_1 : x_2 : x_0) \in \mathbb{P}^2 \mid x_0^2 x_2^2 = x_1^4 + a_1 x_0 x_1^3 + a_2 x_0^2 x_1^2 + a_3 x_0^3 x_1 + a_4 x_0^4\}.$$

1. Show that E is the intersection of C with the line $x_0 = 1$.
2. Show that the point “at infinity” $\mathcal{O} = (0 : 1 : 0) \in C$ is a singular point.
3. Show that any other point $(x_1 : x_2 : x_0) \in C$ is a singular point if and only if the quartic $x^4 + a_1 x + a_2 x^2 + a_3 x + a_4$ has repeated roots.

Problem 4. Similar to above, denote $(x_1 : x_2 : x_3 : x_0)$ as the equivalence class of points $(x_1, x_2, x_3, x_0) \neq (0, 0, 0, 0)$ modulo scalar multiples, and \mathbb{P}^3 as the collection of such classes. Define the (projective) surface \tilde{C} as

$$\left\{ (x_1 : x_2 : x_3 : x_0) \in \mathbb{P}^3 \left| \begin{array}{l} x_1^2 = x_0 x_3 \\ x_2^2 = x_3^2 + a_1 x_1 x_3 + a_2 x_0 x_3 + a_3 x_0 x_1 + a_4 x_0^2 \end{array} \right. \right\}.$$

1. Show that E is the intersection of \tilde{C} with the surface $x_0 = 1$.
2. Show that \tilde{C} has two points “at infinity” arising when $x_0 = 0$.
3. Show that the points “at infinity” \mathcal{O}_1 and \mathcal{O}_2 are not singular.

Chapter 16

Lecture 11: Monday, November 4

16.1 Solvability of the Quintic

16.1.1 History

It had been questioned for a long time whether the roots of an arbitrary quintic polynomial

$$a_5 x^5 + a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0, \quad a_i \in \mathbb{Q}; \quad (16.1)$$

could be expressed in terms of radicals. It was not until work of Norwegian mathematician Niels Henrik Abel (1802 - 1829) in 1824 that a complete proof surfaced. French mathematician Evariste Galois (1811 - 1832) is usually credited with this proof, since he showed in general during his work from 1830 to 1832 that an arbitrary n th degree polynomial cannot be solved in radicals. See the introduction to Part I in Dummit and Foote's "Abstract Algebra" for more history.

16.1.2 Solvable by Radicals?

Instead of wondering whether a quintic *cannot* be solved by radicals, we can ask whether it *can* be solved by radicals. For example, it is known that if the quintic above has roots x_i , then the degree 6 polynomial associated to the resolvent

$$x_1 x_2 + x_2 x_3 + x_3 x_4 + x_4 x_5 + x_5 x_1 \quad (16.2)$$

has a rational root. For example, Dummit and Foote (exercise 21 on page 620 of the second edition) states that the trinomial $x^5 + Bx + C$ is solvable by radicals if and only if the resolvent sextic

$$x^6 + 8Bx^5 + 40B^2x^4 + 160B^3x^3 + 400B^4x^2 + (512B^5 - 3125C^4)x + (256B^6 - 9375BC^4) \quad (16.3)$$

has a rational root. In particular, $x^5 - x - 1$ is not solvable by radicals, whereas $x^5 - 5x + 12$ is indeed solvable by radicals.

16.1.3 Frobenius Group

In general, a quintic is solvable by radicals if and only if its Galois group is a subgroup of the Frobenius group of order 20:

$$F_{20} = \langle \sigma, \tau \mid \sigma^5 = \tau^4 = 1, \tau \sigma \tau^{-1} = \sigma^2 \rangle \simeq \langle (1\ 2\ 3\ 4\ 5), (2\ 3\ 5\ 4) \rangle \quad (16.4)$$

We also have the isomorphism

$$F_{20} \simeq \left\{ \begin{pmatrix} a & b \\ 1 & 1 \end{pmatrix} \in GL_2(\mathbb{F}_5) \mid a \in \mathbb{F}_5^\times, b \in \mathbb{F}_5 \right\}, \quad (16.5)$$

$$\sigma \mapsto \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \quad \tau \mapsto \begin{pmatrix} 2 & \\ & 1 \end{pmatrix}.$$

Note that $[S_5 : F_{20}] = 6$, so this is equivalent to saying that the resolvent sextic has a rational root.

Often in practical computations it is helpful to consider the degree 12 polynomial associated to the resolvent

$$(x_1 x_2 + x_2 x_3 + x_3 x_4 + x_4 x_5 + x_5 x_1) - (x_1 x_3 + x_3 x_5 + x_5 x_2 + x_2 x_4 + x_4 x_1) \quad (16.6)$$

If the discriminant of the quintic is a square, then we find this degree 12 polynomial actually factors into two polynomials of degree 6 – with smaller coefficients than that of the sextic above. In fact, the Galois group will be contained in $A_5 \cap F_{20} = D_{10}$, the dihedral group of order 10. Note that $[A_5 : D_{10}] = 6$. We will focus on those quintics with Galois group A_5 .

16.1.4 Bring-Jerrard Form

In 1786, Swedish mathematician Erland Bring (1736 - 1798) showed (with later generalizations in 1834 by English mathematician George Jerrard (1804 - 1863)) that any quintic can be brought to the form $x^5 + Bx + C$. Bring did not know Abel's work to be discovered 40 years later, and so did not know a quintic could not be solved by radicals. Jerrard was aware of this, and was able to show a quintic is solvable by radicals if and only if the so-called Bring-Jerrard form is solvable by radicals. As an example, the quintic $x^5 + 10x^3 - 10x^2 + 35x - 18$ can be brought into Bring-Jerrard form $5x^5 + 20x + 16$, and it can be shown that this quintic cannot be solved by radicals.

16.1.5 Tschirnhausen Transformations

We sketch a proof: the ideas go back to the German mathematician Ehrenfried Tschirnhaus (1651 - 1708). If the roots of the quintic are x_i , then form a new quintic by considering the resolvent root

$$y_i = z_1 + z_2 x_i + z_3 x_i^2 + z_4 x_i^3 + z_5 x_i^4 \quad (16.7)$$

for some z_i to be found. (This is known as a Tschirnhausen Transformation.) This will create a quintic polynomial, say $b_5 y^5 + b_4 y^4 + b_3 y^3 + b_2 y^2 + b_1 y + b_0$. We want to set $b_4 = b_3 = b_2 = 0$ so that we have the quintic $y^5 + B y + C$ in terms of $B = b_1/b_5$ and $C = b_0/b_5$. This is equivalent to saying $\text{tr } y = \text{tr } y^2 = \text{tr } y^3 = 0$. (We define $\text{tr } y^n = \sum_{i=1}^5 y_i^n$ as the sum of the Galois conjugates.) This in turn is equivalent to choosing $(z_1, z_2, z_3, z_4, z_5)$ to be a nontrivial point on the curve defined by the three equations

$$\sum_{i=1}^5 \sigma^{(i-1)} z_i = \sum_{i=1}^5 \sum_{j=1}^5 \sigma^{(i+j-2)} z_i z_j = \sum_{i=1}^5 \sum_{j=1}^5 \sum_{k=1}^5 \sigma^{(i+j+k-3)} z_i z_j z_k = 0 \quad (16.8)$$

where $\sigma^{(n)} = \text{tr } x^n \in \mathbb{Q}$. This can always be done since we have 3 equations and 5 unknowns (actually 4 since this system is projective). Hence Bring's result follows.

As an example, the quintic $x^5 + 10x^3 - 10x^2 + 35x - 18$ can be transformed into $5x^5 + 20x + 16$ via the point $(568, 91, 152, 9, 8)$ i.e. the substitution

$$x_i \mapsto 568 + 91 x_i + 152 x_i^2 + 9 x_i^3 + 8 x_i^4. \quad (16.9)$$

In general we have the intersection of a linear, quadratic, and cubic polynomial, so the field $L = \mathbb{Q}(\dots, z_i, \dots)$ generated by the z_i will form a degree 6 extension of \mathbb{Q} i.e. $\text{Gal}(L/\mathbb{Q})$ will be a subgroup of S_3 . It may be helpful to keep in mind that if K is the splitting field of the polynomial at hand, then we have the following diagram:

$$\begin{array}{ccc} K & \text{-----} & KL \\ | & & | \\ \mathbb{Q} & \text{-----} & L \end{array} \implies \text{Gal}(K/\mathbb{Q}) \simeq \text{Gal}(KL/L) \quad \text{whenever } K \cap L = \mathbb{Q}. \quad (16.10)$$

16.2 Klein's Work

16.2.1 Motivation

In 1884 in the text "Lectures on the Icosahedron," German mathematician Felix Klein (1849 - 1925) introduced a series of ideas on realizing the icosahedral group A_5 with various geometric objects. Simply put, he realized A_5 is both

1. the group of rotations of the icosahedron; and
2. $\text{Aut}(E[5]) \simeq \text{PSL}_2(\mathbb{F}_5)$ for most elliptic curves E over $\mathbb{Q}(\zeta_5)$.

We will eventually show that even though the roots of a quintic cannot be expressed in terms of radicals, they can be expressed in terms of Weierstrass \wp -functions i.e. elliptic functions.

16.2.2 Sketch of Discussion

We give a sketch of the ideas since the proof will involve two lectures. Say we have a quintic polynomial over \mathbb{Q} , and let K denote its splitting field. If this quintic is not solvable, then $\text{Gal}(K/\mathbb{Q})$ is either S_5 or A_5 . We'll explain another way to generate such nonsolvable extensions. Say that we have an elliptic curve E defined over $\mathbb{Q}(\zeta_5)$. Then the mod 5 representation gives a map

$$\bar{\rho}_{E,5} : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\zeta_5)) \longrightarrow \text{Aut}(E[5]) \subseteq SL_2(\mathbb{F}_5) \quad (16.11)$$

where $\bar{\mathbb{Q}}$ is an algebraic closure of \mathbb{Q} . (In general $E[5] \simeq \mathbb{F}_5 \times \mathbb{F}_5$ so that $\text{Aut}(E[5]) \subseteq GL_2(\mathbb{F}_5)$, but recall that the matrices have determinant 1 because of the Weil pairing.) The kernel of this map yields an extension

$$\text{Gal}(\mathbb{Q}(E[5])/\mathbb{Q}(\zeta_5)) = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\zeta_5))/\ker \varphi \simeq \text{Aut}(E[5]) \subseteq SL_2(\mathbb{F}_5) \quad (16.12)$$

where $\mathbb{Q}(E[5])$ is that extension of $\mathbb{Q}(\zeta_5)$ that is generated by both the x - and y -coordinates of the 5-torsion points on E . The subfield $\mathbb{Q}(E[5]_x)$ generated by just the x -coordinates has Galois group contained in $PSL_2(\mathbb{F}_5) = SL_2(\mathbb{F}_5)/Z(\mathbb{F}_5) \simeq A_5$. It may be helpful to place these fields in a diagram:

$$\mathbb{Q} \text{ --- } \mathbb{Q}(\zeta_5) \text{ --- } \mathbb{Q}(E[5]_x) \text{ --- } \mathbb{Q}(E[5]) \quad (16.13)$$

Ultimately we will show that there is an elliptic curve E defined over $L(\zeta_5)$ such that $K L(\zeta_5) = L(E[5]_x)$. In particular, if K is the splitting field of a quintic in Bring-Jerrard form (i.e. $L = \mathbb{Q}$) then there is an elliptic curve E defined over $\mathbb{Q}(\zeta_5)$ such that $K(\zeta_5) = \mathbb{Q}(E[5]_x)$. It may help to keep the following diagram in mind:

$$\begin{array}{ccccc} K & \text{---} & K L & \text{---} & K L(\zeta_5) = L(E[5]_x) \\ | & & | & & | \\ \mathbb{Q} & \text{---} & L & \text{---} & L(\zeta_5) \end{array} \quad (16.14)$$

where all of the columns have the same Galois group whenever $K \cap L(\zeta_5) = \mathbb{Q}$. Note that if $\text{Gal}(K/\mathbb{Q}) \simeq A_5$, then K has no subfields of degree dividing 6 since A_5 has no subgroups of index dividing 6, so $K \cap L(\zeta_5) = \mathbb{Q}$ is indeed satisfied.

16.2.3 Geometry of the Icosahedron

We begin with a discussion of how A_5 can be realized as the rotations of the icosahedron.

There are five Platonic Solids: the tetrahedron, cube, octahedron, dodecahedron, and icosahedron. They have 4, 6, 8, 12, and 20 faces respectively. More specifically, the icosahedron is that Platonic Solid which consists of 12 vertices, 30 edges (where 5 surround each vertex), and 20 faces. The so-called Euler Characteristic states

$$\text{No. of Vertices} - \text{No. of Edges} + \text{No. of Faces} = 2 \quad (V - E + F = 2) \quad (16.15)$$

The Platonic Solids are the only regular polyhedra in 3-dimensions (i.e. having the same number of edges surrounding each vertex) that satisfy the Euler Characteristic.

We'll explicitly express these 12 vertices as points on the unit sphere:

$$\begin{aligned}
P_\infty^{(+)} &= (1, 0, 0) \\
P_\nu^{(+)} &= \left(\frac{1}{\sqrt{5}}, \frac{2}{\sqrt{5}} \cos \frac{2\pi\nu}{5}, \frac{2}{\sqrt{5}} \sin \frac{2\pi\nu}{5} \right) \\
P_\nu^{(-)} &= \left(-\frac{1}{\sqrt{5}}, -\frac{2}{\sqrt{5}} \cos \frac{2\pi\nu}{5}, \frac{2}{\sqrt{5}} \sin \frac{2\pi\nu}{5} \right) \quad \text{for } \nu = 1, 2, \dots, 5; \\
P_\infty^{(-)} &= (-1, 0, 0).
\end{aligned} \tag{16.16}$$

There are 60 rotations which bring the icosahedron into itself, with three being

$$\begin{aligned}
S &= \begin{pmatrix} 1 & & \\ & \cos \frac{2\pi}{5} & -\sin \frac{2\pi}{5} \\ & \sin \frac{2\pi}{5} & \cos \frac{2\pi}{5} \end{pmatrix} & \text{maps } & P_\nu^{(\pm)} \mapsto P_{\nu\pm 1}^{(\pm)} \\
T &= \begin{pmatrix} \frac{1}{\sqrt{5}} & \frac{2}{\sqrt{5}} & \\ \frac{2}{\sqrt{5}} & -\frac{1}{\sqrt{5}} & \\ & & -1 \end{pmatrix} & \text{maps } & \begin{aligned} P_\infty^{(\pm)} &\mapsto P_0^{(\pm)} \\ P_1^{(\pm)} &\mapsto P_4^{(\pm)} \\ P_2^{(\pm)} &\mapsto P_3^{(\mp)} \end{aligned} \\
U &= \begin{pmatrix} -1 & & \\ & -1 & \\ & & 1 \end{pmatrix} & \text{maps } & P_\nu^{(\pm)} \mapsto P_\nu^{(\mp)}
\end{aligned} \tag{16.17}$$

One can actually show that $A_5 \simeq \langle S, T, U \rangle$ is the desired group of rotations.

Chapter 17

Lecture 12: Wednesday, November 6

17.1 Klein's Work (continued)

17.1.1 Stereographic Projection

Consider the canonical map from $\pi : S^2(\mathbb{R}) \rightarrow \mathbb{C}$ which takes 3-dimensional points on the unit sphere into complex numbers:

$$\begin{aligned} (x_0, x_1, x_2) &\mapsto \frac{x_1 + i x_2}{1 - x_0}, \\ x + i y &\mapsto \left(\frac{x^2 + y^2 - 1}{x^2 + y^2 + 1}, \frac{2x}{x^2 + y^2 + 1}, \frac{2y}{x^2 + y^2 + 1} \right). \end{aligned} \quad (17.1)$$

This is known as stereographic projection. Then the vertices of the icosahedron transform as

$$P_\infty^{(+)} \mapsto \infty, \quad P_\nu^{(\pm)} \mapsto \frac{1 \pm \sqrt{5}}{2} \zeta_5^{\pm \nu}, \quad P_\infty^{(-)} \mapsto 0; \quad (17.2)$$

We have a dual map $\pi^* : O_3(\mathbb{R}) \mapsto PGL_2(\mathbb{C})$ that takes $M \mapsto \pi \circ M \circ \pi^{-1}$. The 3×3 orthogonal matrices are simply rotations of the unit sphere, and the projective general linear group $PGL_2(\mathbb{C})$ acts on the complex plane via fractional linear transformations:

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \implies \gamma z = \frac{az + b}{cz + d}. \quad (17.3)$$

Abusing notation, the matrices introduced in the previous lecture transform as

$$S z = \zeta_5 z, \quad T z = \frac{z + \varepsilon}{\varepsilon z - 1}, \quad U z = -\frac{1}{z}; \quad \text{in terms of } \varepsilon = \frac{-1 + \sqrt{5}}{2}. \quad (17.4)$$

One verifies that

$$S^5 = T^2 = U^2 = 1, \quad UT = TU, \quad USU^{-1} = S^{-1} \quad (17.5)$$

$$V_4 = \langle T, U \rangle, \quad D_5 = \langle S, U \rangle, \quad A_4 = \langle S^4 T S^2, T, U \rangle, \quad A_5 = \langle S, T, U \rangle. \quad (17.6)$$

17.1.2 Invariant Polynomials

Consider the homogeneous polynomials

$$\begin{aligned} \Delta(z_1, z_2) &= \left(-z_1 z_2 \prod_{\nu=0}^4 [z_1 - P_\nu^{(+)} z_2] [z_1 - P_\nu^{(-)} z_2] \right)^5 \\ c_4(z_1, z_2) &= (z_1^{20} + z_2^{20}) - 228 (z_1^{15} z_2^5 - z_1^5 z_2^{15}) + 494 z_1^{10} z_2^{10} \\ c_6(z_1, z_2) &= (z_1^{30} + z_2^{30}) + 522 (z_1^{25} z_2^5 - z_1^5 z_2^{25}) - 10005 (z_1^{20} z_2^{10} + z_1^{10} z_2^{20}) \end{aligned} \quad (17.7)$$

They are invariant under $A_5 = \langle S, T, U \rangle$, and they satisfy the relation $c_4^3 - c_6^2 = 1728 \Delta$. The action of $A_5 \subseteq PGL_2(\mathbb{C})$ is given by

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \implies \begin{aligned} \gamma z_1 &= a z_1 + b z_2 \\ \gamma z_2 &= c z_1 + d z_2. \end{aligned} \quad (17.8)$$

We remark in passing that Δ vanishes on the 12 vertices, c_4 vanishes on the midpoints of the 20 faces, and c_6 vanishes on the midpoints of the 30 edges.

Actually, A_5 doesn't really act on polynomials because in general we have rational linear transformations. Hence, we should really work with rational functions. To this end, define the two homogeneous rational functions

$$\begin{aligned} \lambda(z_1, z_2) &= \frac{[z_1^2 + z_2^2]^2 [z_1^2 - 2 \cdot P_0^{(+)} z_1 z_2 - z_2^2]^2 [z_1^2 - 2 \cdot P_0^{(-)} z_1 z_2 - z_2^2]^2}{\Delta(z_1, z_2)^{1/5}} \\ \mu(z_1, z_2) &= \frac{125 z_1^6 z_2^6}{\Delta(z_1, z_2)^{1/5}} \end{aligned} \quad (17.9)$$

Note that λ is invariant under $V_4 = \langle T, U \rangle$ while μ is invariant under $D_5 = \langle S, U \rangle$. This will give polynomials of degree 5 and degree 6, respectively (since $[A_5 : V_4] = 15$ and $[A_5 : D_5] = 6$). Note that if either $\lambda = \infty$ or $\mu = \infty$ then $\Delta = 0$; if either $\lambda + 3 = 0$ or $\mu^2 + 10\mu + 5 = 0$ then $c_4 = 0$; and if either $\lambda^2 + 10\lambda + 45 = 0$ or $\mu^2 + 4\mu - 1 = 0$ then $c_6 = 0$. That is, the zeroes correspond to the geometry of the icosahedron.

Finally, we define the j -invariant

$$j = \frac{c_4^3}{\Delta} = (\lambda + 3)^3 (\lambda^2 + 11\lambda + 64) = \frac{(\mu^2 + 10\mu + 5)^3}{\mu}. \quad (17.10)$$

Here, when we say *invariant* we actually mean invariant under action by A_5 .

17.1.3 Klein's Results

We wish to define a family of quintics using the rational functions above. To this end, let m and n be constants, and define

$$x_\nu = \frac{m}{\lambda_\nu + 3} + \frac{n}{(\lambda_\nu + 3)(\lambda_\nu^2 + 10\lambda_\nu + 45)} \quad \text{where } \lambda_\nu = \lambda \circ S^\nu. \quad (17.11)$$

These are roots of a principal quintic $x^5 + Ax^2 + Bx + C$ with coefficients

$$\begin{aligned} A &= -\frac{20}{j} \left[(2m^3 + 3m^2n) + 432 \frac{6mn^2 + n^3}{1728 - j} \right] \\ B &= -\frac{5}{j} \left[m^4 - 864 \frac{3m^2n^2 + 2mn^3}{1728 - j} + 559872 \frac{n^4}{(1728 - j)^2} \right] \\ C &= -\frac{1}{j} \left[m^5 - 1440 \frac{m^3n^2}{1728 - j} + 62208 \frac{15mn^4 + 4n^5}{(1728 - j)^2} \right] \end{aligned} \quad (17.12)$$

One verifies this using a symbolic calculator. Note that Klein worked out these formulas in 1884, without the aid of a computer!

Conversely, given a principal quintic $x^5 + A_0x^2 + B_0x + C_0$ with discriminant D_0 , there exist m_0 , n_0 , and j_0 in $\mathbb{Q}(\sqrt{5D_0})$ to invert this system. Klein also inverted this system in 1884 without the aid of a computer! As an example, say we have the quintic $5x^5 + 20x + 16$. Then $j_0 = 86048 - 38496\sqrt{5}$, so $m_0, n_0, j_0 \in \mathbb{Q}(\sqrt{5})$ in this case.

Now in general, say we have a quintic $a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$. Then we work over a quadratic extension $\mathbb{Q}(\sqrt{\alpha})$ to find a principal quintic $x^5 + A_0x^2 + B_0x + C_0$, so that the j -invariant really lies in the biquadratic extension $\mathbb{Q}(\sqrt{\alpha}, \sqrt{5D_0})$. In particular, if we have a quintic in Bring-Jerrard form such that the discriminant is a square, then $j_0 \in \mathbb{Q}(\sqrt{5})$.

17.1.4 Modular Functions

Given a complex number τ with positive imaginary part, define

$$j(\tau) = \frac{1}{q} + 744 + 196884q + \cdots, \quad \eta(\tau) = q^{1/24} \prod_{n \geq 1} (1 - q^n); \quad q = e^{2\pi i \tau}. \quad (17.13)$$

as the usual j -invariant and the Dedekind η -function. These are modular functions:

$$j\left(\frac{a\tau + b}{c\tau + d}\right) = j(\tau), \quad \eta\left(\frac{a\tau + b}{c\tau + d}\right) = \chi(\gamma)\eta(\tau); \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}). \quad (17.14)$$

We when we discussed modular curves, define the modular function

$$\begin{aligned} \mu(\tau) &= 125 \left(\frac{\eta(5\tau)}{\eta(\tau)} \right)^6 \\ &= 125 q \prod_{n \geq 1} (1 + q^n + q^{2n} + q^{3n} + q^{4n})^6 \implies j = \frac{(\mu^2 + 10\mu + 5)^3}{\mu}. \end{aligned} \tag{17.15}$$

(This is not the same as the function $r = j_{5,0}(\tau)$ we defined in a previous lecture, but actually it is the function $5^3/r$ we find after acting by the Atkin-Lehner involution.) Recall that this parameter parametrizes elliptic curves E_r with a subgroup C_r of order 5; that is, we have the commutative diagram

$$\begin{array}{ccc} \mathcal{H}^*/\Gamma_0(5) & \longrightarrow & \mathcal{H}^*/\Gamma(1) \\ \mu \downarrow & & j \downarrow \\ \mathbb{C} \cup \{\infty\} & \longrightarrow & \mathbb{C} \cup \{\infty\} \end{array} \tag{17.16}$$

where the map on the bottom explains the degree 6 rational function that relates μ and j .

17.1.5 Klein's Results Revisited

Assume $x^5 + A_0 x^2 + B_0 x + C_0$ has Galois group A_5 , and let K be its splitting field. I'll explain why there is an elliptic curve E defined over $\mathbb{Q}(\sqrt{5})$ such that $K \subseteq \mathbb{Q}(E[5])$.

Using Klein's formulas, find j_0 and then τ_0 such that $j(\tau_0) = j_0$, and substitute

$$\mu(\tau_0) = \frac{125 z_1^6 z_2^6}{\Delta(z_1, z_2)^{1/5}} = -\frac{125 t}{t^2 + 11t - 1} \quad \text{where} \quad t = \frac{z_1^5}{z_2^5}. \tag{17.17}$$

Note that $t = j_{5,1}(\tau_0)$ is a modular function that parametrizes elliptic curves E_t along with a point P_t of order 5:

$$E_t : \quad y^2 + (1+t)xy + ty = x^3 + tx^2, \quad P_t = (0, 0); \tag{17.18}$$

where $j(E_t) = j_0$. As a diagram, we have maps

$$\begin{array}{ccccccc} \mathcal{H}^*/\Gamma(5) & \longrightarrow & \mathcal{H}^*/\Gamma_1(5) & \longrightarrow & \mathcal{H}^*/\Gamma_0(5) & \longrightarrow & \mathcal{H}^*/\Gamma(1) \\ \downarrow & & t \downarrow & & \mu \downarrow & & j \downarrow \\ \mathbb{C} \cup \{\infty\} & \longrightarrow & \mathbb{C} \cup \{\infty\} & \longrightarrow & \mathbb{C} \cup \{\infty\} & \longrightarrow & \mathbb{C} \cup \{\infty\} \end{array} \tag{17.19}$$

Hence the roots τ_0 are associated to the 5-torsion of an elliptic curve. The elliptic curve can be defined over $\mathbb{Q}(\sqrt{5})$ because a model we can choose is a twist of

$$y^2 = x^3 - \frac{3j_0}{j_0 - 1728} x - \frac{2j_0}{j_0 - 1728}. \tag{17.20}$$

In general, we must work over a quadratic extension $\mathbb{Q}(\sqrt{\alpha})$ to place a quintic in principal form. As a diagram,

$$\begin{array}{ccccc}
 K & \xrightarrow{4} & K(\sqrt{\alpha}, \sqrt{5}) & \xrightarrow{2} & K(\sqrt{\alpha}, \zeta_5) = \mathbb{Q}(E[5]_x) \\
 60 \downarrow & & 60 \downarrow & & 60 \downarrow \\
 \mathbb{Q} & \xrightarrow{4} & \mathbb{Q}(\sqrt{\alpha}, \sqrt{5}) & \xrightarrow{2} & \mathbb{Q}(\sqrt{\alpha}, \zeta_5)
 \end{array} \tag{17.21}$$

17.1.6 Applications

The polynomial $x^5 + 10x^3 - 10x^2 + 35x - 18$ has the same splitting field as $5x^5 + 20x + 16$, and its Galois group is A_5 . We find the elliptic curve

$$y^2 = x^3 + (5 - \sqrt{5})x^2 + \sqrt{5}x \tag{17.22}$$

That is, the splitting field is contained in the field generated by the 5-torsion.

Assume a quintic in Bring-Jerrard form $x^5 + B_0x + C_0$ has Galois group A_5 . The splitting field is contained in the field generated by the 5-torsion of the elliptic curve

$$y^2 = x^3 + 2x^2 + \frac{1 + \sqrt{5}d}{2}x \quad \text{where} \quad d = \frac{\sqrt{256B_0^5 + 3125C_0^4}}{125C_0^2}. \tag{17.23}$$

Chapter 18

Homework Assignment #6

Due Monday, November 11 at the start of lecture.

Problem 1. Let x_i be roots of the quintic

$$a_5 x^5 + a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0 = a_5 \prod_{i=1}^5 (x - x_i);$$

where $a_5 \neq 0$, and each $a_i \in \mathbb{Q}$.

1. Express the sums

$$\sigma^{(1)} = \sum_{i=1}^5 x_i, \quad \sigma^{(2)} = \sum_{i=1}^5 x_i^2, \quad \sigma^{(3)} = \sum_{i=1}^5 x_i^3$$

in terms of the coefficients a_i .

2. Show that $\sigma^{(1)} = \sigma^{(2)} = \sigma^{(3)} = 0$ if and only if $a_4 = a_3 = a_2 = 0$.

Problem 2. Continue the notation from above, and define $y_i = z_1 + z_2 x_i + z_3 x_i^2$ for some z_j to be determined. Show that there is a quadratic extension $\mathbb{Q}(\sqrt{\alpha})$ containing the z_j such that $\text{tr } y = \text{tr } y^2 = 0$. Conclude that every quintic can be brought into principal form (i.e. the x^4 and x^3 terms missing) over a quadratic extension of the base field.

Problem 3. Choose $d \in \mathbb{Q}^\times$ that is not a square, and consider the elliptic curve

$$E : y^2 = x^3 + 2 \frac{r+64}{r^2} x^2 + \frac{r+64}{r^3} x \quad \text{where} \quad r = 64 \frac{1+\sqrt{d}}{1-\sqrt{d}}.$$

Note that E is defined over the quadratic field $\mathbb{Q}(\sqrt{d})$.

1. Show that E is a quadratic \mathbb{Q} -curve i.e. E is an elliptic curve defined over $\mathbb{Q}(\sqrt{d})$ that is 2-isogeneous (up to twisting) to each of its Galois conjugates.
2. Show that a twist of E is of the form $y^2 = x^3 + 2x^2 + \frac{1+\sqrt{d}}{2}x$ i.e. there exists $D \in \mathbb{Q}(\sqrt{d})^\times$ such that

$$2 \cdot D = 2 \frac{r+64}{r^2} \quad \text{and} \quad \frac{1+\sqrt{d}}{2} \cdot D^2 = \frac{r+64}{r^3}.$$

Problem 4. Continue the notation from above. Show the converse i.e. if E is a quadratic \mathbb{Q} -curve, then for some $d \in \mathbb{Q}^\times$ a twist of E has Weierstrass equation $y^2 = x^3 + 2x^2 + \frac{1+\sqrt{d}}{2}x$. (Hint: If E is 2-isogeneous, then choose $r = 64(1+t)/(1-t)$ for some t .)

Chapter 19

Lecture 13: Monday, November 11

19.1 Factoring Integers

19.1.1 Motivation

An integer $n > 1$ is called composite if there are integers $d_1, d_2 > 1$ such that $n = d_1 \cdot d_2$. We say that n is a prime if it is not composite. We ask two questions given an integer $n > 1$: (1) determine whether it is prime, and (2) determine the complete factorization of n . The first will involve the Elliptic Curve Primality Proving (ECPP) while the second will involve the Elliptic Curve Factorization Method (ECM).

We give a motivating example. Let $n = 341$; we wish to determine if n is prime or composite. Say that n is prime. Then for any $a \in \mathbb{Z}$ that is not a multiple of n , we know that $a^{n-1} \equiv 1 \pmod{n}$; this follows from the structure of $\mathbb{Z}/n\mathbb{Z}$, which is assumed to be a finite field in this case. However, when $a = 3$ we have $a^{n-1} - 1 \equiv 55 \pmod{n}$, so n must not be a prime. Hence n is composite.

Now say that we wish to find the factors of n . Using the ideas above, let's consider the sequence of integers $d(a) = \text{GCD}(a^{n-1} - 1, n)$. If $d \neq n$ then d is a proper divisor of n . (Finding the GCD is easy; it's just the Euclidean Algorithm.) Here is a brief table:

$$d(1) = 341, \quad d(2) = 341, \quad d(3) = 11. \quad (19.1)$$

Hence one factor of 341 is 11, so $n = 341 = 11 \cdot 31$. (I trust you believe that both 11 and 31 are prime, so that this is the complete factorization of n .)

19.1.2 Pollard's $p - 1$ Algorithm

We explain the general concept. Choose an integer n , and consider the ring $\mathbb{Z}/n\mathbb{Z}$ of residue classes modulo n . We have

$$a^{\varphi(n)} \equiv 1 \pmod{n} \quad \text{if } GCD(a, n) = 1, \text{ where } \varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right). \quad (19.2)$$

This is known as the Fermat Little Theorem. We'll use this to devise an algorithm that will determine whether n is composite by producing a prime factor of n . The idea is to find integers a and k such that $d = GCD(a^k - 1, n)$ is less than n .

Note that if $p - 1$ divides k for a prime p then $a^k - 1 \equiv 0 \pmod{p}$ whenever p does not divide a . Hence, if we can choose k so that k has a lot of divisors, then we'll have a better shot at finding divisors of n .

Let's perform the following steps:

- Step 1. Choose an integer k that is the product of primes to small powers.
- Step 2. Choose an integer a such that $1 < a < n$.
- Step 3. Calculate $GCD(a, n)$. If this is nontrivial, then we have a divisor d of n , so terminate.
- Step 4. Calculate $d = GCD(a^k - 1, n)$. If $d = 1$ then go back to (1) and choose a different k . If $d = n$ then go back to (2) and choose a different a . Otherwise we have a divisor of n , so terminate.

This is known as Pollard's $p - 1$ Algorithm. This was outlined by J. M. Pollard in 1978 in a paper on Monte Carlo methods.

Here is an example. Say that we wish to find a factor of $n = 246\,082\,373$. We know this is not prime because

$$2^{n-1} - 1 \equiv 180\,137\,692 \not\equiv 0 \pmod{n} \quad (19.3)$$

In fact, we'll use Pollard's Algorithm for $a = 2$; the trick is to choose k carefully. It seems to be the most useful to fix an upperbound B , and let $k = LCM(2, 3, \dots, B)$. Note that k is divisible by all of the primes less than B . If we choose

$$B = 10 \implies k = 2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520 \implies 2^k - 1 \equiv 130\,940\,740 \pmod{n}. \quad (19.4)$$

Then we find

$$GCD(2^k - 1, n) = GCD(130\,940\,740, 246\,082\,373) = 2521. \quad (19.5)$$

Hence, one divisor of n is $d = 2521$, so that $246\,082\,373 = 2521 \cdot 97\,613$.

You'll note that this algorithm terminates if n is composite, but it may not terminate if n is prime. For this reason, we'll focus on the problem of

factoring a number rather than the problem of determining whether a number is prime. Usually, one has a set of primes – called the factor base – which one has determined before hand are prime, then one factors numbers according to primes in the factor base. Of course, in principle the factor base should be larger than the integer n one wishes to factor!

The idea with Pollard's $p - 1$ Algorithm is to consider the group $x^k = 1$ modulo n . We will generalize this to elliptic curves by considering the curves modulo n .

Chapter 20

Lecture 14: Wednesday, November 13

20.1 Elliptic Curves Over Finite Fields

20.1.1 Reduction Modulo Primes

Say that we have the elliptic curve $E : y^2 = x^3 + Ax + B$ with A and B integers. (If A and B are rational numbers, then we can always make the substitution $(x, y) \mapsto (x/d^2, y/d^3)$ which will map $A \mapsto d^4 A$ and $B \mapsto d^6 B$, hence clearing denominators if needed.) The discriminant and j -invariant of this curve are

$$\Delta[E] = -16(4A^3 + 27B^2) \quad \text{and} \quad j(E) = 1728 \cdot \frac{4A^3}{4A^3 + 27B^2}. \quad (20.1)$$

If p is a prime that does not divide $\Delta[E]$, then $\Delta[E] \not\equiv 0 \pmod{p}$ and so we find an elliptic curve over the finite field \mathbb{F}_p . The group law stays the same for this curve. The map

$$E(\mathbb{Q}) \rightarrow E(\mathbb{F}_p), \quad P = (x, y) \mapsto \bar{P} = (x \pmod{p}, y \pmod{p}) \quad (20.2)$$

is known as the reduction modulo p map. If either x or y has p in the denominator, we write $\bar{P} = \bar{\mathcal{O}}$ as the point at infinity.

As an example, consider the curve $E : y^2 = x^3 + x + 1$. This curve has discriminant $\Delta[E] = -496 = -2^4 \cdot 31$, so we consider reductions at primes $p \neq 2, 31$. It also turns out that this curve has no torsion, and has rank 1. That is,

$$E(\mathbb{Q}) \simeq \mathbb{Z} \quad \text{with generator} \quad P = (0, 1). \quad (20.3)$$

In fact, the first few points are

$$\begin{aligned}
P &= (0, 1), \\
[2]P &= \left(\frac{1}{4}, -\frac{9}{8}\right), \\
[3]P &= (72, 611), \\
[4]P &= \left(-\frac{287}{36^2}, \frac{40879}{36^3}\right);
\end{aligned} \tag{20.4}$$

Hence the reduction modulo $p = 3$ sends $[4]P \mapsto \overline{\mathcal{O}}$ to the point at infinity. In fact, we have

$$[2]\overline{P} = (1, 0), \quad [3]\overline{P} = [-1]\overline{P} \implies E(\mathbb{F}_3) = \{\overline{\mathcal{O}}, (0, \pm 1), (1, 0)\} \simeq \mathbb{Z}/4\mathbb{Z}. \tag{20.5}$$

More generally, we eventually find

$$[9]P = \left(\frac{51865013741670864}{80653535^2}, \frac{11915777535633550432194263}{80653535^3}\right). \tag{20.6}$$

so the reduction modulo $p = 5$ sends $[9]P \mapsto \overline{\mathcal{O}}$. This gives the reductions

$$[2]\overline{P} = (4, 2), \quad [3]\overline{P} = (2, 1), \quad [4]\overline{P} = (3, -1), \dots \tag{20.7}$$

and also

$$E(\mathbb{F}_5) = \{\overline{\mathcal{O}}, (0, \pm 1), (2, \pm 1), (3, \pm 1), (4, \pm 2)\} \simeq \mathbb{Z}/9\mathbb{Z}. \tag{20.8}$$

20.1.2 Gauss's Theorem

As an example, consider the curve

$$u^3 + v^3 + w^3 = 0 \quad \text{over} \quad \mathbb{P}^2(\mathbb{F}_p) = \{(u, v, w) \in \mathbb{F}_p \times \mathbb{F}_p \times \mathbb{F}_p\} / \sim \tag{20.9}$$

(where \simeq means modulo scalar multiplication.) We can translate this into Weierstrass form via the substitution

$$x = -\frac{12u}{v+w}, \quad y = 36\frac{v-w}{v+w} \implies y^2 = x^3 - 432. \tag{20.10}$$

This is an elliptic curve if $p > 3$, and in fact has invariant $j(E) = 0$. We consider the number of points on this curve:

$$\#E(\mathbb{F}_p) = \#\{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p \mid y^2 = x^3 - 432\} + 1. \tag{20.11}$$

(The “+1” comes from the point at infinity.) When $p \equiv 2 \pmod{3}$ it turns out that $\#E(\mathbb{F}_p) = p + 1$. (This is an exercise on this week's homework.) On the other hand, when $p \equiv 1 \pmod{3}$ it turns out that $\#E(\mathbb{F}_p) = p + 1 - a_p$, where

$$4p = a_p^2 + 27b_p^2 \quad \text{where} \quad a_p \equiv 2 \pmod{3}. \tag{20.12}$$

This is a result proved by Gauss. As an example, take $p = 7$; then the points on $E(\mathbb{F}_p)$ are

$$E(\mathbb{F}_7) = \{\overline{\mathcal{O}}, (0, \pm 3), (3, \pm 1), (5, \pm 1), (6, \pm 1)\} \implies \#E(\mathbb{F}_7) = 9. \quad (20.13)$$

But we also have

$$4 \cdot 7 = 1^2 + 27 \cdot 1^2 \implies a_7 = b_7 = -1 \implies p + 1 - a_p = 9. \quad (20.14)$$

20.1.3 Hasse-Weil Inequality

Note that $|a_p| < 2\sqrt{p}$ for the curve $y^2 = x^3 - 432$ whenever $p \neq 2, 3$. In fact, this is part of a more general theorem:

Let E be an elliptic curve over a finite field \mathbb{F}_p , and denote $a_p = p + 1 - \#E(\mathbb{F}_p)$. Then $|a_p| < 2\sqrt{p}$. This was first conjectured by Emil Artin in the 1910's in his thesis, then proved by Helmut Hasse in 1933 (and generalized to curves of higher genus by Andre Weil in 1949). This can also be stated as

$$(\sqrt{p} - 1)^2 < \#E(\mathbb{F}_p) < (\sqrt{p} + 1)^2. \quad (20.15)$$

Whenever $a_p = 0$, we say that p is a supersingular prime for E . Note that for the curve $y^2 = x^3 - 432$ a prime $p \neq 2, 3$ is a supersingular prime if and only if $p \equiv 2 \pmod{3}$.

Chapter 21

Homework Assignment #7

Due Monday, November 18 at the start of lecture.

Problem 1: Supersingular Primes for Curves with $j(E) = 0$. Let $p \equiv 3 \pmod{4}$ be a prime, and let $f(x) = x^3 + Ax$ where $A \in \mathbb{F}_p^\times$.

1. Show that for $x \in \mathbb{F}_p^\times$ exactly one of x or $-x$ is a square in \mathbb{F}_p . (Hint: $\mathbb{F}_p[\sqrt{-1}]$ is the unique quadratic extension of \mathbb{F}_p .)
2. Show that for $x \in \mathbb{F}_p$, one of the points $(x, \sqrt{f(x)})$ or $(-x, \sqrt{f(-x)})$ is in $\mathbb{F}_p \times \mathbb{F}_p$. (Hint: Consider the cases $f(x) = 0$ separately.)
3. Show that, counting the point at infinity, the elliptic curve $y^2 = x^3 + Ax$ has $p + 1$ points over \mathbb{F}_p .

Problem 2: Supersingular Primes for Curves with $j(E) = 1728$. Let $p \equiv 2 \pmod{3}$ be an odd prime, and let $f(x) = x^3 + B$ where $B \in \mathbb{F}_p^\times$.

1. Show that $x^3 + B = 0$ has at most one solution over \mathbb{F}_p . (Hint: $\mathbb{F}_p[\sqrt{-3}]$ is the unique quadratic extension of \mathbb{F}_p .)
2. Show that, counting the point at infinity, the elliptic curve $y^2 = x^3 + B$ has $p + 1$ points over \mathbb{F}_p . (Hint: Consider $(y^2 - B)^{(2-p)/3}$.)

Problem 3: Zeta Function of a Curve. Let \mathbb{F}_{p^n} be the finite field of p^n elements, and say that E is an elliptic curve over \mathbb{F}_p that has $1 - \alpha^n - \beta^n + p^n$ elements when viewed over \mathbb{F}_{p^n} , where $\alpha\beta = p$. Show that, as a function of $s \in \mathbb{C}$,

$$Z(E/\mathbb{F}_p, s) = \exp \left[\sum_{n=1}^{\infty} \#E(\mathbb{F}_{p^n}) \frac{1}{n p^{sn}} \right] = \frac{1 - a_p p^{-s} + p^{1-2s}}{(1 - p^{-s})(1 - p^{1-s})}.$$

where $a_p = \alpha + \beta = p + 1 - \#E(\mathbb{F}_p)$. (Hint: Consider the series expansion for $\log(1 - \alpha T)$ with $T = p^{-s}$, but don't worry about regions of convergence.)

Problem 4: Riemann Hypothesis for Curves. Continue notation as above, but assume that α and β are not real numbers.

1. Show that $Z(E/\mathbb{F}_p, s)$ has no poles when $\operatorname{Re} s > \frac{3}{2}$.
2. Show that $|a_p| < 2\sqrt{p}$ and $|\alpha| = |\beta| = \sqrt{p}$.
3. Show that if $Z(E/\mathbb{F}_p, s) = 0$ then $\operatorname{Re} s = \frac{1}{2}$.

Chapter 22

Lecture 15: Monday, November 18

22.1 Elliptic Curves Over Finite Fields (continued)

22.1.1 Reduction Modulo p Theorem

Also, the elliptic curve over the rational numbers has order 3:

$$E(\mathbb{Q}) = \{\mathcal{O}, (12, 36), (12, -36)\} \simeq \mathbb{Z}/3\mathbb{Z} \quad (22.1)$$

which correspond to the trivial points $w = 0$. (This explains why $x^3 + y^3 = 1$ has no nontrivial solutions over \mathbb{Q} .) But is there a way to see this with $E(\mathbb{F}_p)$? Note that

$$\#E(\mathbb{F}_p) = \begin{cases} p+1 & \text{if } p \equiv 2 \pmod{3}; \\ p+1-a_p & \text{if } p \equiv 1 \pmod{3}. \end{cases} \implies \#E(\mathbb{F}_p) \equiv 0 \pmod{3}. \quad (22.2)$$

So we could have predicted that $E(\mathbb{Q})$ has a rational point of order 3 by considering the various reductions of the elliptic curves modulo primes p .

In general, let $\text{Tor}(E)$ be the torsion group of some elliptic curve over \mathbb{Q} , and assume that the mod p reduction gives an elliptic curve over \mathbb{F}_p . Then $\text{Tor}(E)$ injects to subgroup of E over \mathbb{F}_p . That is, under the reduction map $E(\mathbb{Q}) \rightarrow E(\mathbb{F}_p)$ the torsion subgroup is never contained in the kernel.

As an example, the Mordell-Weil group of the elliptic curve $E : y^2 = x^3 - 432$ is just torsion, so the reduction map $E(\mathbb{Q}) \rightarrow E(\mathbb{F}_p)$ is always injective. However, this map is not surjective in general: when $p = 7$, we saw above that $\#E(\mathbb{F}_7) = 9 > 3 = \#E(\mathbb{Q})$.

Here is another example of this theorem. Say we are given the elliptic curve $y^2 = x^3 + x$. The discriminant is $\Delta[E] = -64$, so we will reduce modulo primes

$p \neq 2$. We quickly compute

$$\begin{aligned} E(\mathbb{F}_3) &= \{\overline{O}, (0, 0), (2, 1), (2, 2)\} \simeq \mathbb{Z}/4\mathbb{Z} & \#E(\mathbb{F}_3) &= 4 \\ E(\mathbb{F}_5) &= \{\overline{O}, (0, 0), (2, 0), (3, 0)\} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & \#E(\mathbb{F}_5) &= 4. \end{aligned} \quad (22.3)$$

Hence the torsion subgroup must inject into both $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, so it cannot be more than $\mathbb{Z}/2\mathbb{Z}$. But $(0, 0)$ is a rational point of order 2, so the torsion subgroup must be cyclic of order 2. In fact, $E(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$, but of course this is more difficult to show.

22.1.2 Elliptic Curves over $\mathbb{Z}/n\mathbb{Z}$

We've seen how to compute on an elliptic curve over a finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, so we explain how to generalize to compute on an elliptic curve over a ring $\mathbb{Z}/n\mathbb{Z}$.

The affine equation $y^2 = x^3 + Ax + B$ actually defines a projective variety:

$$E(\mathbb{Q}) = \{(x_1 : x_2 : x_0) \in \mathbb{P}^2(\mathbb{Q}) \mid x_0 x_2^2 = x_1^3 + A x_0^2 x_1 + B x_0^3\} \quad (22.4)$$

where we define

$$\mathbb{P}^2(\mathbb{Q}) = \{(x_1, x_2, x_0) \in \mathbb{Q}^3 \mid (x_1, x_2, x_0) \neq (0, 0, 0)\} / \sim \quad (22.5)$$

in terms of the equivalence relation $(x_1 : x_2 : x_0) \sim (y_1 : y_2 : y_0)$ if and only if $(x_1, x_2, x_0) = \lambda(y_1, y_2, y_0)$ for some $\lambda \in \mathbb{Q}^\times$. Note that every equivalence class $(x_1 : x_2 : x_0)$ has a representative with $x_1, x_2, x_0 \in \mathbb{Z}$ and $GCD(x_1, x_2, x_0) = 1$.

We mimic this definition for an elliptic curve over the ring $\mathbb{Z}/n\mathbb{Z}$:

$$E(\mathbb{Z}/n\mathbb{Z}) = \{(x_1 : x_2 : x_0) \in \mathbb{P}^2(\mathbb{Z}/n\mathbb{Z}) \mid x_0 x_2^2 = x_1^3 + A x_0^2 x_1 + B x_0^3\} \quad (22.6)$$

where we define

$$\mathbb{P}^2(\mathbb{Z}/n\mathbb{Z}) = \{(x_1, x_2, x_0) \in (\mathbb{Z}/n\mathbb{Z})^3 \mid GCD(x_1, x_2, x_0) = 1\} / \sim \quad (22.7)$$

in terms of the equivalence relation $(x_1 : x_2 : x_0) \sim (y_1 : y_2 : y_0)$ if and only if $(x_1, x_2, x_0) = \lambda(y_1, y_2, y_0)$ for some $\lambda \in (\mathbb{Z}/n\mathbb{Z})^\times$.

We now define the reduction modulo n map to be

$$\begin{aligned} E(\mathbb{Q}) &\rightarrow E(\mathbb{Z}/n\mathbb{Z}), \\ (x_1 : x_2 : x_0) &\mapsto (x_1 \pmod n : x_2 \pmod n : x_0 \pmod n). \end{aligned} \quad (22.8)$$

Recall that we may choose a class $(x_1 : x_2 : x_0) \in \mathbb{P}^2(\mathbb{Q})$ to satisfy $x_1, x_2, x_0 \in \mathbb{Z}$ so the reduction modulo n makes sense. In general, this is not a group homomorphism! Indeed, say we have two points $P = (x, y)$ and $Q = (u, v)$ on $E(\mathbb{Q})$. Then

$$P \oplus Q = (-x - u + m^2, mx + mu - m^3 - b) \quad \text{in terms of} \quad \begin{aligned} m &= \frac{y - v}{x - u}, \\ b &= \frac{vx - yu}{x - u}. \end{aligned} \quad (22.9)$$

If $GCD(x - u, n) > 1$ then $P_1 \oplus P_2$ may not be defined in $E(\mathbb{Z}/n\mathbb{Z})$. Of course, this motivates an algorithm for elliptic curves over $\mathbb{Z}/n\mathbb{Z}$: if we find two points that cannot be added, then we have a nontrivial divisor of n .

22.2 Elliptic Curve Factoring Method

22.2.1 Motivation

Say that we start with a positive integer n that we know is composite. We saw before that Pollard's algorithm gives returns a factor of n . That is, we perform the following steps:

- Step 1. Choose a random integer k .
- Step 2. Choose a random integer a such that $1 < a < n$.
- Step 3. Calculate $GCD(a, n)$. If this is nontrivial, then terminate.
- Step 4. Calculate $d = GCD(a^k - 1, n)$. If $d = 1$ then go back to (1). If $d = n$ then go back to (2). Otherwise terminate.

Note that this is a probabilistic method i.e. the time it takes to find a factor depends on the initial choices of k and a . Of course, we often choose either $k = LCM(1, 2, \dots, K)$ or $k = K!$ in terms of some bound K so that we can find many prime factors of k .

We can use elliptic curves to devise another method. Pollard's Algorithm uses the assumption that the congruence $a^k \equiv 1 \pmod{n}$ will fail at some point because not every $a \in \mathbb{Z}$ is invertible modulo n . For elliptic curves, say that we have a point \bar{P} on some curve $y^2 = x^3 + \bar{A}x + \bar{B}$ modulo n . Then we can write

$$[k]P = \left(\frac{a}{d^2}, \frac{b}{d^3} \right). \quad (22.10)$$

When $GCD(d, n) > 1$ we may have a nontrivial divisor of n .

Chapter 23

Lecture 16: Wednesday, November 20

23.1 Elliptic Curve Factoring Method (continued)

23.1.1 Lenstra's Elliptic Curve Algorithm

We explain the algorithm for elliptic curve factorization. Say that we start with a positive integer n that we know is composite. Perform the following steps:

Step 1. Compute $n^{1/r}$ for $r = 1, 2, \dots, \lceil \log_2 n \rceil$. If any are integers, then terminate.

Step 2. Choose a random integer k .

Step 3. Choose random integers A , x_1 , and y_1 , set $B = y_1^2 - x_1^3 - Ax_1$, and denote

$$E : y^2 = x^3 + Ax + B, \quad P = (x_1, y_1), \quad \Delta(E) = -16(4A^3 + 27B^2). \quad (23.1)$$

Step 4. Compute $GCD(\Delta(E), n)$. If it equals n , go back to (3) and choose a different A . If this is nontrivial, then terminate.

Step 5. Compute

$$d = GCD(d_k, n) \quad \text{in terms of} \quad [k]P = \left(\frac{a_k}{d_k^2}, \frac{b_k}{d_k^3} \right). \quad (23.2)$$

If $d = 1$ then go back to (2) and increase k , or go back to (3) and choose a different A . If $d = n$ then go back to (2) and decrease k . Otherwise, terminate.

Step 1 checks that we do not have a trivial factorization like $n = m^r$ for some integer m . Step 3 chooses a random point $P = (x_1, y_1)$ and a random curve E that has P as a rational point. Note that it's not the other way around: it's more difficult to find a rational point given an elliptic curve! Step 4 verifies that E is really an elliptic curve.

For step 2, note that we can choose either $k = LCM(1, 2, \dots, K)$ or $k = K!$ in terms of some bound K . To compute $[k]P$, we actually express k in base 2 notation:

$$\begin{aligned} k &= k_0 + 2 \cdot k_1 + 2^2 \cdot k_2 + \dots + 2^r k_r \\ \implies [k]P &= [k_0]P_0 \oplus [k_1]P_1 \oplus [k_2]P_2 \oplus \dots \oplus [k_r]P_r \end{aligned} \tag{23.3}$$

That is, we add r points when double r points $P_0 = P$, $P_1 = [2]P_0, \dots, P_r = [2]P_{r-1}$ recursively. Clearly $r = \lceil \log_2 n \rceil$, so we can compute $[k]P$ in at most $2 \cdot \lceil \log_2 n \rceil$ steps. We perform these steps modulo n .

If n is composite, we expect this algorithm to terminate since given two points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ we can add them if and only if $d = GCD(x_2 - x_1, n) = 1$. If not, then either $d = n$ in which case $P_1 = -P_2$ or $d < n$ so that we have a nontrivial factor. In the latter case, we are done, but in the former case P_1 has order 2, so we've doubled one too many times. This is why we decrease k .

This algorithm was introduced by UC Berkeley math professor Hendrik W. Lenstra, Jr. in 1987 in a paper entitled "Factoring Integers Using Elliptic Curves." Many of the actual implementations come from Peter Montgomery's paper published the same year but in a different journal. Often this algorithm is called the Elliptic Curve Factorization Method (ECM).

23.1.2 Worked Example

As an example, say that we want to factor the integer $n = 1\,715\,761\,513$. First, we check that n is not prime and that n is not of the form m^r :

$$\begin{aligned} 2^{n-1} - 1 &\equiv 93\,082\,890 \pmod{n}, \\ n^{1/2} &= 41\,421.751\dots \\ n^{1/3} &= 1\,197.160\dots \\ &\vdots \\ n^{1/31} &= 1.986\dots \end{aligned} \tag{23.4}$$

Now we pick a point P and an integer k . We will pick

$$P = (2, 1), \quad k = LCM(1, 2, \dots, 17) = 12252240. \tag{23.5}$$

We note that we express k base 2 as

$$k = 2^4 + 2^6 + 2^{10} + 2^{12} + 2^{13} + 2^{14} + 2^{15} + 2^{17} + 2^{19} + 2^{20} + 2^{21} + 2^{23} \tag{23.6}$$

so we can compute $[k]P$ in at most 46 steps.

Note that we have not chosen the elliptic curve yet! We choose $A = 1$ so that $B = y_1^2 - x_1^3 - Ax_1 = -9$. Hence we consider the elliptic curve

$$E : y^2 = x^3 + x - 9 \implies \Delta(E) = -35056 \implies GCD(\Delta(E), n) = 1. \quad (23.7)$$

We finally compute $[k]P$:

$$[k]P \equiv (421\,401\,044, 664\,333\,727) \pmod{n}. \quad (23.8)$$

Since this is a well-defined rational point on E , we must do one of two steps: (1) choose a different k , or (2) choose a different A . We opt for the latter. We only need to perform 46 more steps to compute $[k]P$.

Now choose $A = 2$ so that $B = y_1^2 - x_1^3 - Ax_1 = -11$. Then

$$E' : y^2 = x^3 + 2x - 11 \implies \Delta(E') = -52784 \implies GCD(\Delta(E'), n) = 1. \quad (23.9)$$

Now when we try and compute $[k]P$ we run into problems! In fact,

$$\begin{aligned} [k - 2^{23}]P &\equiv (1\,115\,004\,543, 1\,676\,196\,055), \\ [2^{23}]P &\equiv (1\,267\,572\,925, 848\,156\,341) \end{aligned} \quad (23.10)$$

so that

$$GCD(1\,115\,004\,543 - 1\,267\,572\,925, n) = 26\,927. \quad (23.11)$$

In fact, $n = 26\,927 \cdot 63\,719$. It turns out that both factors are prime, so this is the complete factorization of n .

23.1.3 Actual Implementations

Mathematica has a standard built-in package `FactorInteger[]` which uses Pollard's algorithm. Mathematica also uses an add-on package entitled

`<<NumberTheory`FactorIntegerECM``

to call Lenstra's algorithm. Specifically, it uses the command

`FactorIntegerECM[]`

assuming the integer n is at least 10^{12} but at most 10^{40} . Mathematica's program is optimized to find factors around 10^{17} .

We give some numerical tests of the program. For example, to do

$$n = 1\,715\,761\,513 \quad (23.12)$$

(which is of the order 10^9) takes 0.06 seconds, and returns the answer 63 719. (Curiously, it finds the larger prime factor of n .) By comparison, the command `FactorInteger[]` takes 0.0 seconds, so it's clear that `FactorIntegerECM[]` should be used for larger integers n . As another test of Mathematica, say we want to factor

$$n = 2^{2^6} + 1 = 18\,446\,744\,073\,709\,551\,617. \quad (23.13)$$

This is on the order 10^{20} . Mathematica returns the factor 274 177 in 0.44 seconds. By comparison, the command `FactorInteger[]` takes less than 1/20th the time, at only 0.02 seconds. As yet another test, say we want to factor

$$n = 2^{2^7} + 1 = 340\,282\,366\,920\,938\,463\,463\,374\,607\,431\,768\,211\,457. \quad (23.14)$$

This is on the order 10^{39} . Mathematica returns the factor 59 649 589 127 497 217 in 638.35 seconds; this factor is on the order 10^{17} . (The Mathematica book quotes a run time of 3 hours.) By comparison, the command `FactorInteger[]` takes 126.06 seconds, about a factor of 5 less.

23.2 Elliptic Curve Primality Proving

23.2.1 Motivation

Recall that for each positive integer, we ask two questions: (1) determine whether it is prime, and (2) determine the complete factorization of n . We've explained how to do the latter with Lenstra's algorithm; it's simply the Elliptic Curve Factorization Method (ECM). The problem is, how do we know the factors of n really are prime? This will involve Elliptic Curve Primality Proving (ECP).

The idea is simple: ECM is a probabilistic test, so one can run the algorithm more than once to get factors. One would like to issue a *certificate* so that it will be easier to check the primality of the factors than the first time around. It should take a shorter period of time to verify the certificate than to verify the actual found factor.

23.2.2 Primality Proving for Pollard's Algorithm

First, we explain how one can use information about the ring $\mathbb{Z}/n\mathbb{Z}$ to show n is prime. We ignore the cases when (1) n is even, and (2) $n = m^r$.

If n is prime, then $(\mathbb{Z}/n\mathbb{Z})^\times$ is a cyclic group. One conclusion we can draw is $a^{n-1} \equiv 1 \pmod n$ for any $a \in \mathbb{Z}$ with $GCD(a, n) = 1$. Unfortunately, the converse is not true: take for example $n = 561 = 11 \cdot 51$.

If n is composite, then we consider the structure of $(\mathbb{Z}/n\mathbb{Z})^\times$ in more detail. Explicitly, if $n = n_1 n_2$ with $GCD(n_1, n_2) = 1$, then the Chinese Remainder Theorem states

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq (\mathbb{Z}/n_1\mathbb{Z})^\times \times (\mathbb{Z}/n_2\mathbb{Z})^\times \quad (23.15)$$

We conclude that n is prime if and only if $(\mathbb{Z}/n\mathbb{Z})^\times$ is a cyclic group. (Recall that n is not even and n is not of the form m^r .)

Chapter 24

Homework Assignment #8

Due Monday, November 25 at the start of lecture.

Problem 1. Consider the elliptic curve $E : y^2 = x^3 + 4x$.

1. Show that this curve has good reduction at all odd primes.
2. Compute the order of $E(\mathbb{F}_3)$ and $E(\mathbb{F}_5)$.
3. Given that $P = (2, 4) \in E(\mathbb{Q})$ is a torsion point, compute its order.

Problem 2. Consider the elliptic curve $E : y^2 - y = x^3 - x^2$.

1. Show that its discriminant $\Delta(E)$ is a prime.
2. Find four rational points on this curve.
3. Assuming that the Mordell-Weil group $E(\mathbb{Q})$ is finite, compute its order.

Problem 3. Consider the elliptic curve $E : y^2 = x^3 - 43x + 166$. Given that the point $P = (3, 8)$ has finite order, compute the torsion subgroup of E .

Problem 4. Consider the elliptic curve $E : y^2 = x^3 - 432$, and let $p \equiv 1 \pmod{3}$ be a prime. Show that

$$\#E(\mathbb{F}_p) \equiv 0 \pmod{9}.$$

(Hint: Show that $(p-1)^2 \equiv 2a_p \cdot \#E(\mathbb{F}_p) \pmod{9}$ where $4p = a_p^2 + 27b_p^2$.)

Chapter 25

Lecture 17: Monday, November 25

25.1 Elliptic Curve Primality Proving (continued)

25.1.1 Primality Proving for Pollard's Algorithm

First, we explain how one can use information about the ring $\mathbb{Z}/n\mathbb{Z}$ to show n is prime. We ignore the cases when (1) n is even, and (2) $n = m^r$.

If n is prime, then $(\mathbb{Z}/n\mathbb{Z})^\times$ is a cyclic group. One conclusion we can draw is $a^{n-1} \equiv 1 \pmod n$ for any $a \in \mathbb{Z}$ with $\text{GCD}(a, n) = 1$. Unfortunately, the converse is not true: take for example $n = 561 = 11 \cdot 51$.

If n is composite, then we consider the structure of $(\mathbb{Z}/n\mathbb{Z})^\times$ in more detail. Explicitly, if $n = n_1 n_2$ with $\text{GCD}(n_1, n_2) = 1$, then the Chinese Remainder Theorem states

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq (\mathbb{Z}/n_1\mathbb{Z})^\times \times (\mathbb{Z}/n_2\mathbb{Z})^\times \quad (25.1)$$

We conclude that n is prime if and only if $(\mathbb{Z}/n\mathbb{Z})^\times$ is a cyclic group. (Recall that n is not even and n is not of the form m^r .)

25.1.2 Lucas's Test

Now say that we can find an integer a such that for every proper divisor k of $n - 1$ we know that $a^k \not\equiv 1 \pmod n$. Then $(\mathbb{Z}/n\mathbb{Z})^\times$ is a cyclic group. This can be modified slightly: if for every prime divisor p of $n - 1$ there is an integer a such that (1) $a^{n-1} \equiv 1 \pmod n$ and (2) $a^{(n-1)/p} \not\equiv 1 \pmod n$ then n is prime. This test was devised by French mathematician Edouard Lucas in 1891.

For example, if $n = 2^{2^m} + 1$ we can use this test. Primes in this form $F_m = 2^{2^m} + 1$ are called Fermat primes. $m = 4$ is the largest known Fermat prime.

25.1.3 Primality Proving for Elliptic Curves

In 1986, MIT professors Shafi Goldwasser and James R. Kilian, Jr. used this to devise a test for elliptic curves. This appeared in a paper entitled “Almost all primes can be quickly certified.” They proved the following: Say that P is a point on E over $\mathbb{Z}/n\mathbb{Z}$, where P has order m . If

1. For every divisor k of m we have $[k]P \neq \overline{O}$, and
2. $m > (\sqrt[n]{n} + 1)^2$;

then n is prime. Note that $m < (\sqrt[n]{n} + 1)^2$ by the Hasse-Weil inequality.

25.2 Fermat’s Last Theorem

25.2.1 Fermat’s Conjecture

Given a positive integer n , say that we wish to find integer solutions $a - b - c$ to the equation

$$a^n + b^n = c^n \quad \text{such that} \quad abc \neq 0. \quad (25.2)$$

When $n = 1, 2$, the equation has infinitely many solutions: given positive integers p, q, r we have nontrivial parametrizations

$$\begin{array}{ll} a = p & a = p(q^2 - r^2) \\ n = 1 : \quad b = q & n = 2 : \quad b = 2pqr \\ c = p + q; & c = p(q^2 + r^2); \end{array} \quad (25.3)$$

whenever $q > r$. A conjecture of French mathematician Pierre de Fermat from around 1630 states that this equation has no nontrivial solutions when $n \geq 3$.

25.2.2 Case-by-Case Analysis

We discuss this for the first few cases.

When $n = 3$, make the substitution

$$x = \frac{3a}{c-b}, \quad y = \frac{5b+4c}{c-b} \implies y^2 + y = x^3 - 7. \quad (25.4)$$

The elliptic curve $y^2 + y = x^3 - 7$ has only three rational points, namely $[m](3, 4)$ for $m \in \mathbb{Z}/3\mathbb{Z}$, which correspond to trivial points having $x = 3$ i.e. $abc = 0$. (Note that this elliptic curve has j -invariant 0 and discriminant -3^9 . It also has a 3-isogeny.) Hence, the equation $a^3 + b^3 = c^3$ has no nontrivial solutions as conjectured. German mathematician Leonhard Euler gave a similar proof of this case in 1753.

When $n = 4$, we make the substitution

$$x = 2\frac{c+b}{c-b}, \quad y = \left(\frac{2a}{c-b}\right)^2 \implies y^2 = x^3 + 4x. \quad (25.5)$$

The elliptic curve $y^2 = x^3 + 4x$ has only four rational points, namely $[m](2, 4)$ for $m \in \mathbb{Z}/4\mathbb{Z}$, which correspond to the trivial points having $x = 0$ or 2 i.e. $abc = 0$. (Note that this elliptic curve has j -invariant 1728 and discriminant -2^{12} . It also has a 4-isogeny.) Hence, the equation $a^4 + b^4 = c^4$ has no nontrivial solutions also as conjectured. Fermat gave a similar proof of this case around 1630, right when he made his more general conjecture.

When $n = 5$, we make the substitution

$$x = \frac{a}{c-b}, \quad y = \frac{2b^2 + bc + 2c^2}{(c-b)^2} \implies y^2 + y = 5x^5 + 1. \quad (25.6)$$

This hyperelliptic curve has three rational points, namely \mathcal{O} , $(1, 2)$, and $(1, -3)$. Again, they correspond to the trivial points i.e. $abc = 0$. (This hyperelliptic curve has discriminant 5^{15} . Perhaps it has a 5-isogeny? If we are willing to work over $\mathbb{Q}(\sqrt{5})$ we find two extra points: $\left(0, \frac{-1 \pm \sqrt{5}}{2}\right)$ so the hyperelliptic curve actually has 5 points.) Hence, the equation $a^5 + b^5 = c^5$ has no nontrivial solutions. Both French mathematicians Peter Gustav Lejeune Dirichlet and Adrien Marie Legendre gave similar proofs of this case in 1825.

When $n = 7$, we make the substitution

$$\begin{aligned} \frac{x+12}{7^2} &= \frac{(a^2 + b^2 + c^2 + ab - ac - bc)^2 - abc(a+b-c)}{(a+b-c)^4} \\ \frac{x+2y}{7^3} &= \frac{\left((a^2 + b^2 + c^2 + ab - ac - bc)^2 - abc(a+b-c)\right)(a^2 + b^2 + c^2)}{(a+b-c)^6} \end{aligned} \quad (25.7)$$

which gives the relation

$$y^2 + xy = x^3 - x^2 - 107x + 552. \quad (25.8)$$

The elliptic curve $y^2 + xy = x^3 - x^2 - 107x + 552$ has only two rational points, namely $[m](-12, 6)$ for $m \in \mathbb{Z}/2\mathbb{Z}$. (Note that this elliptic curve has j -invariant -3375 and discriminant -7^9 . It also has a 7-isogeny.) French mathematician Gabriel Lamé gave a similar proof of this case in 1839.

25.2.3 General Remarks

In general let's consider two cases for $n \geq 3$: either n has an odd prime factor ℓ or not. In the first case, we write

$$\begin{aligned} u &= a^{n/\ell} \\ v &= b^{n/\ell} \implies u^\ell + v^\ell + w^\ell = a^n + b^n - c^n = 0, \quad uvw = (-abc)^{n/\ell}. \\ w &= -c^{n/\ell} \end{aligned} \quad (25.9)$$

Hence, if Fermat's conjecture is true for ℓ then it is true for n . In the second case, we write

$$\begin{aligned} u &= a^{n/4} \\ v &= b^{n/4} \implies u^4 + v^4 - w^4 = a^n + b^n - c^n = 0, \quad uvw = (abc)^{n/4}. \quad (25.10) \\ w &= c^{n/4} \end{aligned}$$

so that Fermat's conjecture is always true. So to prove Fermat's conjecture we assume $n = \ell$ is a prime with $\ell > 7$.

25.2.4 The Frey Curve

In 1986, German mathematician Gerhard Frey noticed a general relationship with elliptic curves. Say that Fermat's conjecture is true for some exponent n . Let $a - b - c$ be a solution, and consider the curve

$$E : y^2 = x(x - a^n)(x + b^n) \implies \Delta[E] = 16 a^{2n} b^{2n} (a^n + b^n)^2 = 16 (abc)^{2n}. \quad (25.11)$$

Hence, $a - b - c$ is a nontrivial solution if and only if E is an elliptic curve. Frey's hope was that information about this curve would give a contradiction about a nontrivial solution to Fermat's equation.

Chapter 26

Lecture 18: Wednesday, November 27

26.1 Modular Forms

26.1.1 Cusp Forms of Weight 2

Recall that we have an action of the extended upper-half plane $\mathcal{H}^* = \mathcal{H} \cup \{i\infty\}$ by $\Gamma(1) = SL_2(\mathbb{Z})$:

$$\gamma\tau = \frac{a\tau + b}{c\tau + d} \quad \text{where} \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \quad (26.1)$$

For a positive integer N , recall the subgroup

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid c \equiv 0 \pmod{N} \right\}. \quad (26.2)$$

We consider functions $f : \mathcal{H}^* \rightarrow \mathbb{C}$ that satisfy

1. f is holomorphic on \mathcal{H} i.e. f analytic on the upper-half plane;
2. $\lim_{\tau \rightarrow i\infty} f(\tau) = 0$; and
3. $f(\gamma\tau) = (c\tau + d)^2 f(\tau)$ for $\gamma \in \Gamma_0(N)$.

Denote such functions by $S_2(\Gamma_0(N))$. These are the cusp forms of weight 2 and level N . (Ribet denotes these by $S(N)$ in his article “Galois Representations and Modular Forms.”)

Recall that the Dedekind eta function

$$\begin{aligned} \eta(\tau) &= q^{1/24} \prod_{n \geq 1} (1 - q^n) \\ \implies \eta\left(-\frac{1}{\tau}\right) &= \sqrt{-i\tau} \eta(\tau), \quad \eta(\tau + 1) = e^{2\pi i/24} \eta(\tau) \end{aligned} \quad (26.3)$$

is a modular form of weight 1/2. We will use this function again later.

26.1.2 q -Expansions

In particular, when

$$\gamma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_0(N) \implies f(\tau + 1) = f(\tau) \quad (26.4)$$

so that each cusp form has a Fourier series expansion:

$$f(\tau) = \sum_{n \in \mathbb{Z}} a_n \exp[2\pi i n \tau] = \sum_{n \in \mathbb{Z}} a_n q^n \quad \text{where } q = e^{2\pi i \tau}. \quad (26.5)$$

This is usually called the q -expansion of $f(\tau)$. The condition $f(i\infty) = 0$ forces $a_n = 0$ when $n \leq 0$, so we actually have $f(\tau) = \sum_{n \geq 1} a_n q^n$ for all $f(\tau) \in S_2(\Gamma_0(N))$.

26.1.3 Relation with Modular Curves

Recall that we may identify $X_0(N) = \mathcal{H}^*/\Gamma_0(N)$ as a compact Riemann surface. (That is, it is the upper-half plane where we identify points via this action by $\Gamma_0(N)$.) If instead we choose $Y_0(N) = \mathcal{H}/\Gamma_0(N)$ then we ignore the points at infinity, namely $\mathbb{Q} \cup \{i\infty\}$. These are known as the cusps. This Riemann surface is not compact.

Consider the differential $d\tau$. Note that if

$$w = \frac{a\tau + b}{c\tau + d} \implies \frac{dw}{d\tau} = \frac{ad - bc}{(c\tau + d)^2} \implies dw = \frac{d\tau}{(c\tau + d)^2} \quad (26.6)$$

when we an action by $SL_2(\mathbb{Z})$. Hence consider the differential form $\omega(\tau) = f(\tau) d\tau$ since it has the property

$$\omega(w) = f(w) dw = f(\tau) d\tau = \omega(\tau) \quad \text{for } w = \gamma\tau, \gamma \in \Gamma_0(N). \quad (26.7)$$

for any weight 2 cusp form $f(\tau)$. That is, ω is an differential invariant under action by $\Gamma_0(N)$, so it is a differential on the compact Riemann surface $X_0(N)$.

In fact, we have an isomorphism: The space of weight 2 cusp forms on \mathcal{H} is in bijection with the space of holomorphic (analytic) differentials on $X_0(N)$. The bijection is the map $f(\tau) \mapsto \omega(\tau) = f(\tau) d\tau$. Hence, by the Riemann-Roch theorem,

$$\dim_{\mathbb{C}} S_2(\Gamma_0(N)) = \text{dimension of holomorphic differentials} = \text{genus of } X_0(N). \quad (26.8)$$

26.1.4 Dimension of Space of Cusp Forms

The genus may be computed by considering the ramification of the points in the covering map $X_0(N) \rightarrow X(1)$ coming from the inclusion $\Gamma_0(N) \rightarrow \Gamma(1)$. Here is a table of some values:

$\dim_{\mathbb{C}} S_2(\Gamma_0(N))$	N
0	1, ..., 10, 12, 13, 16, 18, 25
1	11, 14, 15, 17, 19, 20, 21, 24, 27, 32, 36, 49
2	22, 23, 26, 28, 29, 31, 37, 50
3	30, 33, 34, 35, 39, 40, 41, 43, 45, 48
4	38, 44, 47
5	42, 46

These are the integers N up to 50.

26.1.5 Examples of Cusp Forms

Note that the trivial form $f(\tau) := 0$ is always a cusp form. To find nontrivial examples, we consider the first case when the genus of $X_0(N)$ is nontrivial, say $N = 11$. It turns out that a nontrivial cusp form is given by

$$f(\tau) = \eta(\tau)^2 \eta(11\tau)^2 = q \prod_{n \geq 1} (1 - q^n)^2 (1 - q^{11n})^2 = \sum_{n \geq 1} a_n q^n \quad (26.9)$$

That is, this is a holomorphic function on \mathcal{H} of weight 2 and level 11. This follows directly from the properties of the Dedekind eta function.

When $N = 22$, the genus is 2 so we expect two cusp forms, namely

$$f(\tau) = \eta(\tau)^2 \eta(11\tau)^2 \quad \text{and} \quad f(2\tau) = \eta(2\tau)^2 \eta(22\tau)^2. \quad (26.10)$$

This follows because $\Gamma_0(22) \subset \Gamma_0(11)$. In a sense, these examples are actually coming from $S_2(\Gamma_0(11))$.

26.1.6 Hecke Operators

We can define an action of certain operators on $S(N) = S_2(\Gamma_0(N))$. For each $n \in \mathbb{Z}_{>0}$, define

$$(f|T_n)(\tau) = \sum_{a \equiv n \pmod{d}} \sum_{0 \leq b < d} \langle a \rangle \frac{a}{d} \cdot f\left(\frac{a\tau + b}{d}\right) \quad (26.11)$$

where $\langle a \rangle = 1$ if $\text{GCD}(d, N) = 1$ and $\langle a \rangle = 0$ otherwise. (The $\langle \cdot \rangle$ are known as the diamond operators, although they are trivial since we have trivial nebentype.) Note that there are

$$[\Gamma(1) : \Gamma_0(N)] = N \prod_{p|N} \left(1 + \frac{1}{p}\right). \quad (26.12)$$

terms in this sum.

In particular, when $n = p$ is a prime, this formula simplifies to

$$\begin{aligned} (f|T_p)(\tau) &= \sum_{b=0}^{p-1} \frac{1}{p} f\left(\frac{\tau + b}{p}\right) + \langle p \rangle p \cdot f(p\tau) \\ &= \begin{cases} \sum_{n \geq 1} a_n p q^n + p \sum_{n \geq 1} q_n q^{np} & \text{if } p \nmid N \\ \sum_{n \geq 1} a_n p q^n & \text{if } p \mid N \end{cases} \end{aligned} \quad (26.13)$$

Sometimes people define $U_p = T_p$ whenever $p \mid N$. In either case, we formally write the T_n using the generating function

$$\prod_{p \nmid N} (1 - T_p p^{-s} + p^{1-2s})^{-1} \cdot \prod_{p \mid N} (1 - U_p p^{-s})^{-1} = \sum_{n \geq 1} \frac{T_n}{n^s} \quad (26.14)$$

(This relation is inspired by German mathematician Erich Hecke's results from 1917.) We denote $\mathbb{T}(N)$ as the \mathbb{C} -algebra generated by the Hecke operators T_n . Note that

$$\mathbb{T}(N) \subseteq \text{End}_{\mathbb{C}} S_2(\Gamma_0(N)). \quad (26.15)$$

26.1.7 Petersson Pairing

Given two functions $f(\tau)$ and $g(\tau)$ in $S(N) = S_2(\Gamma_0(N))$, we define a pairing $\langle \cdot, \cdot \rangle : S(N) \times S(N) \rightarrow \mathbb{C}$ by the integral

$$\langle f, g \rangle = \frac{1}{[\Gamma(1) : \Gamma_0(N)]} \int_{X_0(N)} f(\tau) \overline{g(\tau)} dx dy \quad (26.16)$$

Then each T_n for $GCD(n, N) = 1$ is self-adjoint with respect to this pairing:

$$\langle f|T_n, g \rangle = \langle f, g|T_n \rangle \quad (26.17)$$

This was proved by German mathematician Hans Petersson in the 1940's.

Chapter 27

Homework Assignment #9

Due Monday, December 2 at the start of lecture.

For the following problems, let $f(\tau) = \sum_{n \geq 1} a_n q^n$ be a cusp form of weight 2 and level N , with q -expansion in terms of $q = e^{2\pi i \tau}$.

Problem 1: The Mellin Transform. For $s \in \mathbb{C}$, show that the integral

$$\Lambda(f, s) = \sqrt{N}^s \int_0^\infty f(iy) y^{s-1} dy = \left(\frac{\sqrt{N}}{2\pi} \right)^s \Gamma(s) L(f, s)$$

where

$$\Gamma(s) = \int_0^\infty e^{-t} t^{s-1} dt = (s-1)! \quad \text{and} \quad L(f, s) = \sum_{n \geq 1} \frac{a_n}{n^s}.$$

Problem 2: Right Action on Cusp Forms. Define the action

$$(f|\gamma)(\tau) = \frac{ad - bc}{(c\tau + d)^2} f\left(\frac{a\tau + b}{c\tau + d}\right) \quad \text{for} \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Q}).$$

1. Show that $f|\gamma = f$ for $\gamma \in \Gamma_0(N)$.
2. Show that for $\gamma_1, \gamma_2 \in GL_2(\mathbb{Q})$ we have $(f|\gamma_1)|\gamma_2 = f|(\gamma_1\gamma_2)$.

Problem 3: The Atkin-Lehner Involution. Denote

$$w_N = \begin{pmatrix} & -1 \\ N & \end{pmatrix} \quad \text{and} \quad \hat{f}(\tau) = -(f|w_N)(\tau) = -\frac{1}{N\tau^2} f\left(-\frac{1}{N\tau}\right).$$

Show that \widehat{f} is also a cusp form of weight 2 and level N i.e.

1. \widehat{f} is holomorphic on the upper-half plane;
2. $\lim_{\tau \rightarrow i\infty} \widehat{f}(\tau) = 0$; and
3. $\widehat{f}(\gamma\tau) = (c\tau + d)^2 \widehat{f}(\tau)$ for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$.

(Hint: Assume that $f(\tau)$ is bounded as $\tau \rightarrow 0$. If $\gamma \in \Gamma_0(N)$ show that $\gamma' = w_N \gamma w_N^{-1} \in \Gamma_0(N)$ as well.)

Problem 4: Functional Equation. Show that $\Lambda(\widehat{f}, 2 - s) = \Lambda(f, s)$.

Chapter 28

Lecture 19: Monday, December 2

28.1 Modular Forms (continued)

28.1.1 Normalized Eigenform

Recall that for n with $GCD(n, N) = 1$, we define the Hecke operator as

$$(f|T_n)(\tau) = \sum_{a \equiv n} \sum_{0 \leq b < d} \frac{a}{d} \cdot f\left(\frac{a\tau + b}{d}\right) \quad (28.1)$$

We denote $\mathbb{T}(N)$ as the \mathbb{C} -algebra generated by the Hecke operators T_n . The Petersson pairing makes $S(N) = S_2(\Gamma_0(N))$ into a finite-dimensional Hilbert space. Recall that we have the generating function

$$\prod_{p \nmid N} \frac{1}{1 - T_p p^{-s} + p^{1-2s}} \cdot \prod_{p|N} \frac{1}{1 - U_p p^{-s}} = \sum_{n \geq 1} \frac{T_n}{n^s} \quad (28.2)$$

We say a cusp form $f(\tau) = \sum_{n \geq 1} a_n q^n$ is an eigenform if $f|T_n = \lambda_n f$ for all n with $GCD(n, N) = 1$. This implies

$$a_n = \lambda_n a_1 \implies f(\tau) = \sum_{n \geq 1} a_n q^n = a_1 \cdot \sum_{n \geq 1} \lambda_n q^n. \quad (28.3)$$

We say that $f(\tau)$ is a normalized eigenform if $a_1 = 1$. In this case,

$$L(f, s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_{p \nmid N} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \cdot \prod_{p|N} \frac{1}{1 - a_p p^{-s}} \quad (28.4)$$

This is known as the Euler product of the L -series associated to $f(\tau)$. This result was proved by Hecke. In general, the coefficients a_n lie in an extension of degree $d \leq g!$, where $g = \dim_{\mathbb{C}} S_2(\Gamma_0(N)) = \text{genus}(X_0(N))$.

28.1.2 Functional Equation

We consider the complete L -function

$$\Lambda(f, s) = \sqrt{N}^s \int_0^\infty f(iy) y^{s-1} dy = \left(\frac{\sqrt{N}}{2\pi} \right)^s \Gamma(s) L(f, s) \quad (28.5)$$

We know that this function is analytic when $\operatorname{Re}(s) > 1$, and in fact, it is analytic when $\operatorname{Re}(s) = 1$. The functional equation

$$\Lambda(\widehat{f}, 2-s) = \Lambda(f, s) \quad \text{where} \quad \widehat{f}(\tau) = (f|w_N)(\tau) = -\frac{1}{N\tau^2} f\left(-\frac{1}{N\tau}\right) \quad (28.6)$$

shows that $L(f, s)$ can be analytically continued to the entire complex plane whenever $\widehat{f} = \pm f$. This “ \pm ” sign is known as the sign of the functional equation.

28.2 Modular Elliptic Curves

28.2.1 Jacobians of Modular Curves

Fix a positive integer N , and consider the modular curve $X_0(N) = \mathcal{H}^*/\Gamma_0(N)$. If E is an elliptic curve with j -invariant $X = j(\tau)$, then an N -isogenous curve E' has j -invariant $Y = j(N\tau)$. By considering the q -expansions of X and Y , we find a polynomial of degree

$$[\Gamma(1) : \Gamma_0(N)] = N \prod_{p|N} \left(1 + \frac{1}{p} \right) \quad (28.7)$$

such that $\phi_N(X, Y) = 0$. This is called the modular polynomial.

For example, when $N = 2$ we found before that

$$\phi_2(X, Y) = -(XY)^2 + 1485(X+Y+27675)XY + (X+Y-54000)^3. \quad (28.8)$$

The modular curve $X_0(2)$ has genus 0. Explicitly, a parametrization of the curve $\phi_2(X, Y) = 0$ is given by

$$X = \frac{(r+256)^3}{r^2} \quad \text{and} \quad Y = \frac{(r+16)^3}{r} \quad (28.9)$$

for some parameter r .

Let $J_0(N)$ be the Jacobian of $X_0(N)$ i.e. the projective variety defined by the curve $\phi_N(X, Y) = 0$. We imbed $X_0(N) \hookrightarrow J_0(N)$ by $\tau \mapsto (j(\tau), j(N\tau))$, but this might not be a surjection since we have to be careful about points at infinity. When $N = 11$, we know that $X_0(11)$ has genus 1, so $J_0(11)$ is an elliptic curve.

28.2.2 Action by the Hecke Algebra

The Hecke algebra $\mathbb{T}(N)$ acts on the Jacobian in a canonical way. For example, we map $X_0(N) \rightarrow X_0(N)$ by sending

$$\tau \mapsto \frac{a\tau + b}{c\tau + d}, \quad \text{where} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{Mat}_2(\mathbb{Z}), \quad GCD(n, N) = 1. \quad (28.10)$$

Each γ is an isogeny of degree $n = ad - bc$. This induces an action on $J_0(N)$. The Hecke operator T_n is a sum

$$T_n = \bigoplus_{a|n} \bigoplus_{0 \leq b < d} \begin{bmatrix} d \\ a \end{bmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{End}(J_0(N)) \quad (28.11)$$

with addition being the group law of the projective variety $J_0(N)$. For example, if $\omega = f(\tau) d\tau$ is a differential on $X_0(N)$, then

$$\begin{aligned} d\left(\frac{a\tau + b}{c\tau + d}\right) &= \frac{a}{d} \cdot d\tau \\ \implies \omega|T_n &= (f|T_n) d\tau = \left[\sum_{a|n} \sum_{0 \leq b < d} \frac{a}{d} \cdot f\left(\frac{a\tau + b}{d}\right) \right] d\tau. \end{aligned} \quad (28.12)$$

28.2.3 Shimura's Construction

We explain a construction due to German mathematician Martin Eichler in the 1954, later generalized by Princeton professor Goro Shimura in 1971. Fix a positive integer N , and choose a cusp form $f \in S_2(\Gamma_0(N))$. Recall that we can write

$$f(\tau) = \sum_{n=1}^{\infty} a_n q^n, \quad a_n = a_n(f). \quad (28.13)$$

We define a bilinear pairing

$$\mathbb{T}(N) \times S_2(\Gamma_0(N)) \rightarrow \mathbb{C}, \quad (T, f) \mapsto a_1(f|T). \quad (28.14)$$

Hence, the Hecke algebra $\mathbb{T}(N) \simeq S_2(\Gamma_0(N))^\vee$ is the dual of the space of weight 2 cusp forms. This induces a linear map $\lambda_f = (\cdot, f)$ that sends $\mathbb{T}(N) \rightarrow \mathbb{C}$. Instead of working with the \mathbb{C} -linear combinations $\mathbb{T}(N)$, just work with the \mathbb{Z} -linear combinations $\mathbb{T}_{\mathbb{Z}}$. Then we have a map $\lambda_f : \mathbb{T}_{\mathbb{Z}} \rightarrow \mathbb{C}$. The kernel is a subalgebra of $\mathbb{T}_{\mathbb{Z}}$ that acts on the projective variety $J_0(N)$. Define A_f as that projective variety that fits into the short exact sequence

$$0 \longrightarrow \ker \lambda_f \cap \mathbb{T}_{\mathbb{Z}} \cdot J_0(N) \longrightarrow J_0(N) \longrightarrow A_f \longrightarrow 0 \quad (28.15)$$

As an example, when $N = 11$, the modular form $f(\tau) = \eta(\tau)^2 \eta(11\tau)^2$ discussed in the previous lecture gives $A_f \simeq J_0(11)$, which is just the elliptic

curve $y^2 + y = x^3 - x^2 = 10x - 20$. In general, if $f(\tau)$ is a newform of level N with rational coefficients, then A_f will be an elliptic curve, called the strong modular curve, or the Weil curve. In this case, Shimura showed that

$$a_p = p + 1 - \#A_f(\mathbb{F}_p) \quad \text{when} \quad f(\tau) = \sum_{n=1}^{\infty} a_n q^n. \quad (28.16)$$

28.3 Elliptic Curves

28.3.1 Isogenies

Consider the elliptic curve $E : y^2 + y = x^3 - x^2$. We know that this curve has discriminant $\Delta(E) = -11$, and the Mordell-Weil Group is

$$E(\mathbb{Q}) = \langle (0, 0) \mid [5](0, 0) = \mathcal{O} \rangle \simeq \mathbb{Z}/5\mathbb{Z}. \quad (28.17)$$

Hence for any $p \neq 11$ we know that 5 divides $\#E(\mathbb{F}_p)$. In fact, set $a_p = p + 1 - \#E(\mathbb{F}_p)$ so that we have the following table:

p	2	3	5	7	11	13	17	19	(28.18)
$\#E(\mathbb{F}_p)$	5	5	5	10	11	10	20	20	
a_p	-2	-1	1	-2	1	4	-2	0	

This elliptic curve has a point of order 5, so it has a 5-isogeny. Explicitly, every elliptic curve with a 5-isogeny is in the form

$$E : y^2 = x^3 - \frac{3j}{j-1728} D^2 x - \frac{2j}{j-1728} D^3, \quad j = \frac{(r^2 + 10r + 5)^3}{r}; \quad (28.19)$$

for some $D, r \in \mathbb{Q}^\times$. Explicitly in our case $D = -19/24$ and $r = -11$. The 5-isogenous curve can be found by mapping $r \mapsto 125/r$ i.e. $r \mapsto -125/11$. This curve is birationally equivalent to the elliptic curve

$$A : y^2 + y = x^3 - x^2 = 10x - 20 \quad (28.20)$$

(where $D \mapsto 2501/744$.) It turns out that $\Delta(A) = -11^5$ and the Mordell-Weil Group is

$$A(\mathbb{Q}) = \langle (5, 5) \mid [5](5, 5) = \mathcal{O} \rangle \simeq \mathbb{Z}/5\mathbb{Z}. \quad (28.21)$$

Actually, this elliptic curve has two different 5-isogenies: the 5-division polynomial has a linear factor $x - 5$ and a quadratic factor $5x^2 + 5x - 29$, so the roots generate cyclic subgroups C_1 and C_2 and hence isogenies $A \rightarrow A/C_1$ and $A \rightarrow A/C_2$. Explicitly, A corresponds to either $r = -125/11$ or $r = -1/11$, so we can map either $r \mapsto -11$ or $r \mapsto -125 \cdot 11$. The second gives the elliptic curve

$$A' : y^2 + y = x^3 - x^2 - 7820x - 263580. \quad (28.22)$$

Now $\Delta(A') = 11$ with trivial Mordell-Weil Group: $A'(\mathbb{Q}) = \{\mathcal{O}\}$. Hence,

$$A/C_1 \simeq A' \quad \text{yet} \quad A/C_2 \simeq E. \quad (28.23)$$

28.3.2 Conductor

Note that in all of these examples, the discriminant is a power of ± 11 . So it appears that $p = 11$ is the one common factor to all of these. This motivates a quantity that is invariant under isogeny or twisting, such as the j -invariant is.

Say that we have the elliptic curve $E : y^2 = x^3 + Ax + B$, and a twist $E^{(D)} : y^2 = x^3 + AD^2x + BD^3$. These curves have the associated quantities

$$\frac{c_4(E^{(D)})}{c_4(E)} = D^2, \quad \frac{c_6(E^{(D)})}{c_6(E)} = D^3, \quad \frac{\Delta(E^{(D)})}{\Delta(E)} = D^6, \quad \text{and} \quad \frac{j(E^{(D)})}{j(E)} = 1. \quad (28.24)$$

Hence we can always twist the curve E such that $c_4, c_6, \Delta \in \mathbb{Z}$. We say $E^{(D)}$ is minimal if we can twist so that c_4, c_6, Δ are as small as possible. For any prime p , we say that

1. p is a prime of good reduction if $p \nmid \Delta$.
2. p is a prime of multiplicative reduction if $p \mid \Delta$ yet $p \nmid c_6$.
3. p is a prime of additive reduction if $p \mid \Delta$ and $p \mid c_6$.

In these various cases, (1) $E(\mathbb{F}_p)$ is an elliptic curve; (2) $E(\mathbb{F}_p)$ has a node; and (3) $E(\mathbb{F}_p)$ has a cusp. We define the conductor of E as the positive integer

$$N_E = \prod_p p^{f_p} \quad \text{where} \quad f_p = \begin{cases} 0 & \text{if } p \nmid \Delta; \\ 1 & \text{if } p \mid \Delta \text{ yet } p \nmid c_6; \\ 2 & \text{if } p \mid \Delta, p \mid c_6, \text{ and } p \geq 5. \end{cases} \quad (28.25)$$

As an example, the three elliptic curves above have conductor $N_E = 11$ because $y^2 + y = x^3 - x^2$ has discriminant $\Delta(E) = -11$.

We say an elliptic curve E is semistable if its conductor is square-free. That is, either $f_p = 0, 1$. Another way to say this is the elliptic curve has either good or multiplicative reduction. Karl Rubin and Alice Silverberg have remarked that any elliptic curve in the form $y^2 = x(x - a^\ell)(x + b^\ell)$ must necessarily be semistable.

28.3.3 L -Series

If two elliptic curves E and E' are isogenous, then $\#E(\mathbb{F}_p) = \#E'(\mathbb{F}_p)$. However, it is not true that $E(\mathbb{F}_p) \simeq E'(\mathbb{F}_p)$! The L -series is independent of the choice of isogeny class:

$$L(E, s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_{p \nmid N_E} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \cdot \prod_{p \mid N_E} \frac{1}{1 - a_p p^{-s}} \quad (28.26)$$

where $a_p = p + 1 - \#E(\mathbb{F}_p)$ when $p \nmid N_E$, and $a_p = 0, \pm 1$ otherwise. An elliptic curve is semistable if and only if $a_p = \pm 1$ for $p \mid N$; in fact, a twist of E can be chosen so that $a_p = 1$ in these cases.

28.3.4 Taniyama-Shimura Conjecture

Recall that we considered the modular form

$$\begin{aligned}
 f(\tau) &= \eta(\tau)^2 \eta(11\tau)^2 = q \prod_{n \geq 1} (1 - q^n)^2 (1 - q^{11n})^2 \\
 &= q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} \\
 &\quad + q^{11} - 2q^{12} + 4q^{13} + 4q^{14} - q^{15} - 4q^{16} - 2q^{17} + 4q^{18} + O(q^{20})
 \end{aligned} \tag{28.27}$$

We showed above that the elliptic curve associated to this modular form is $A_f : y^2 + y = x^3 - x^2 = 10x - 20$. Hence, we see that

$$L(f, s) = L(A_f, s) = L(E, s) \tag{28.28}$$

We wish to generalize this idea.

Japanese mathematicians Yukata Taniyama and Goro Shimura conjectured in 1955 (when Taniyama was just 27) that this should always happen: that is, given an elliptic curve E , one should be able to find a modular form f such that $L(f, s) = L(E, s)$. Another way to say this is given E there is an isogeny such that $E \simeq A_f$.

We found this above when $N_E = 11$. The three curves

$$\begin{aligned}
 E : \quad & y^2 + y = x^3 - x^2 \\
 A_f : \quad & y^2 + y = x^3 - x^2 = 10x - 20 \\
 A' : \quad & y^2 + y = x^3 - x^2 - 7820x - 263580
 \end{aligned} \tag{28.29}$$

are modular. Note that all three are isogenous to the Weil curve A_f .

Chapter 29

Lecture 20: Wednesday, December 4

29.1 Proof of Fermat's Conjecture

29.1.1 Relation with Frey's Curve

Let $\ell > 7$ be a prime, and consider an integer solution to the equation

$$u^\ell + v^\ell + w^\ell = 0 \quad \text{where } u v w \neq 0. \quad (29.1)$$

Gerhard Frey thought to consider the curve

$$E: y^2 = x(x - u^\ell)(x + v^\ell) \implies \begin{aligned} c_6 &= 32(u^\ell - v^\ell)(u^\ell - w^\ell)(v^\ell - w^\ell), \\ \Delta(E) &= 16(u v w)^{2\ell}. \end{aligned} \quad (29.2)$$

which is an elliptic curve over \mathbb{Q} . The Taniyama-Shimura-Weil conjecture states E is modular for some $f \in S_2(\Gamma_0(N_E))$. However, what is the conductor of E ?

If we assume that

$$\begin{aligned} u^\ell &\equiv -1 \quad (4) \\ v^\ell &\equiv 0 \quad (16) \implies y^2 + x y = x^3 + \frac{v^\ell - u^\ell - 1}{4} x^2 - \frac{u^\ell v^\ell}{16} x \\ w^\ell &\equiv 1 \quad (4) \end{aligned} \quad (29.3)$$

is a minimal Weierstrass equation for E . It has discriminant $(u v w)^{2\ell}/2^8$. One can use this to show E is semistable. For example, when $p \neq 2$, if $p \mid \Delta(E)$ and $p \mid c_6$ then $p \mid GCD(u, v, w)$; and we can always assume $GCD(u, v, w) = 1$. The conditions above on u and v force E to be semistable even at $p = 2$. (Note that these conditions fail if $\ell = 2$.)

29.1.2 Conductor of the Frey Curve

We know that E has a mod ℓ representation

$$\bar{\rho}_{E,\ell} : \text{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q}) \longrightarrow GL_2(\mathbb{F}_\ell) \quad (29.4)$$

found by acting on the ℓ -division points of E . This representation is surjective because $\ell > 7$; this is a theorem of Barry Mazur from the 1970's. Moreover, we say that $\bar{\rho}_{E,\ell}$ is ramified at p if p ramifies in the algebraic extension $\mathbb{Q}(E[\ell])/\mathbb{Q}$. (A necessary condition for this to happen is p divide $\ell \cdot \Delta(E)$, but this is not sufficient.) There is a theorem that states $\bar{\rho}_{E,\ell}$ is unramified at $p \neq \ell$ if and only if ℓ divides the p -adic valuation of the minimal discriminant. In particular, for our specific choice E , $p \neq 2$, ℓ is always unramified. Hence, N_E divides 2ℓ .

French mathematician Jean-Pierre Serre conjectured in 1985 and UC Berkeley professor Ken Ribet proved in 1990 that ℓ does not divide N_E i.e. $N_E = 2$ through a series of arguments called “level-lowering.” Hence

$$\text{Taniyama-Shimura-Weil} \implies f \in S_2(\Gamma_0(2)) \quad (29.5)$$

However, the space $S_2(\Gamma_0(2))$ has dimension 0, so no such modular form exists. Hence, if the Taniyama-Shimura-Weil conjecture is true, then Fermat's conjecture is true. In fact, it suffices to prove the Taniyama-Shimura-Weil conjecture for semistable elliptic curves.

29.1.3 Galois Representations

Given a positive integer n , we have

$$E[\ell^n] \simeq \mathbb{Z}/\ell^n \mathbb{Z} \times \mathbb{Z}/\ell^n \mathbb{Z} \implies T_\ell(E) = \text{proj} \lim_n E[\ell^n] \simeq \mathbb{Z}_\ell \times \mathbb{Z}_\ell \quad (29.6)$$

This inverse limit is known as the Tate module. Similarly, the Galois groups have an inverse limit:

$$G_\mathbb{Q} = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) = \text{proj} \lim_n \text{Gal}(\mathbb{Q}(E[\ell^n])/\mathbb{Q}). \quad (29.7)$$

Hence, we have an ℓ -adic Galois representation

$$\rho_{E,\ell} : G_\mathbb{Q} \longrightarrow GL_2(\mathbb{Z}_\ell) \quad \text{where} \quad \rho_{E,\ell} \pmod{\ell} = \bar{\rho}_{E,\ell}. \quad (29.8)$$

American mathematician John Tate showed in the 1950's that

$$\begin{aligned} \text{tr} \rho_{E,\ell}(\text{Frob}_p) &= p + 1 - \#E(\mathbb{F}_p); \\ \det \rho_{E,\ell}(\text{Frob}_p) &= p \end{aligned} \quad \text{whenever} \quad p \nmid N_E. \quad (29.9)$$

Digression: Algebraic Number Theory. The element Frob_p is known as the Frobenius element. Let me digress to explain where it comes from. Fix a prime p , and consider the p -adic numbers \mathbb{Q}_p . We can talk about its algebraic closure $\bar{\mathbb{Q}}_p$, and hence the absolute Galois group $G_p = \text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$; this is

usually called the decomposition group at p . Given a polynomial $\sum_n \alpha_n x^n$ with coefficients in \mathbb{Z}_p , we can consider the mod p reduction $\bar{\alpha}_n \in \mathbb{F}_p$. The roots of the polynomial $r_k \in \overline{\mathbb{Q}}_p$ reduce to roots $\bar{r}_k \in \overline{\mathbb{F}}_p$, and so we have a surjective map of the Galois groups

$$\text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \rightarrow \text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p). \quad (29.10)$$

Denote I_p as the kernel of this map; this is usually called the inertia group at p . Recall that every finite extension $\mathbb{F}_{p^f}/\mathbb{F}_p$ is cyclic of order f – usually called the residue degree – and is generated the Frobenius element $x \mapsto x^p$. Hence, the quotient $G_p/I_p \simeq \text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ is an infinite cyclic group with the Frobenius element Frob_p as the generator.

One can use this to given an approach to proving that the Taniyama-Shimura-Weil conjecture is true. For example, given a normalized eigenform $f \in S_2(\Gamma_0(N))$ with rational coefficients a_p , we can use Shimura's construction to find an elliptic curve A_f . We then construct the Tate module for A_f , and use this to construct an ℓ -adic representation for the modular form:

$$\rho_f = \rho_{A_f, \ell} : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{Z}_{\ell}). \quad (29.11)$$

where we have

$$\begin{aligned} \text{tr } \rho_f(\text{Frob}_p) &= a_p; \\ \det \rho_f(\text{Frob}_p) &= p \end{aligned} \quad \text{whenever } p \nmid N. \quad (29.12)$$

Using this construction, we have

$$E \text{ is modular} \iff \rho_{E, \ell} \simeq \rho_f. \quad (29.13)$$

(We say $\rho_1 \simeq \rho_2$ whenever $\rho_1(\sigma) = M \rho_2(\sigma) M^{-1}$ for some $M \in GL_2(\overline{\mathbb{Q}}_{\ell})$ that is independent of $\sigma \in G_{\mathbb{Q}}$.) Note that

$$a_p = \text{tr } \rho_f(\text{Frob}_p) = \text{tr } \rho_{E, \ell}(\text{Frob}_p) = p + 1 - \#E(\mathbb{F}_p) \quad (29.14)$$

for all $p \nmid N_E$.

29.1.4 Wiles' Approach

Princeton University professor Sir Andrew Wiles outlined an approach to proving the weak form of the Taniyama-Shimura-Weil conjecture by performing the following two steps: Given a semistable elliptic curve E defined over \mathbb{Q} ,

1. Understand the mod ℓ representation $\bar{\rho}_{E, \ell}$.
2. Understand the ℓ -adic representation $\rho_{E, \ell}$.

In his 1994 proof, he proved the following:

$$\bar{\rho}_{E, \ell} \simeq \bar{\rho}_f \quad \text{for some } f \in S_2(\Gamma_0(N_E)). \quad (29.15)$$

(The latter is the mod ℓ reduction of the ℓ -adic Galois representation associated to the modular form. Wiles actually shows this for $\ell = 3$, but the result holds for all primes ℓ .) Hence, Wiles could show that every semistable elliptic curve E is residually modular. He then asked the following question: Given two ℓ -adic representations

$$\rho_1, \rho_2 : G_{\mathbb{Q}} \rightarrow GL(\mathbb{Z}_{\ell}) \quad \text{such that} \quad \bar{\rho}_1 \simeq \bar{\rho}_2 \implies \rho_1 \simeq \rho_2? \quad (29.16)$$

Such questions fall under the guise of Deformation Theory. Andrew Wiles and Harvard University professor Barry Mazur had been studying such questions since the 1970's.

29.1.5 Universal Deformation Ring

Barry Mazur showed that for each residual representation $\bar{\rho} : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{F}_{\ell})$ there is a ring $R = R(\bar{\rho})$ of finite dimension over \mathbb{Q}_{ℓ} and a Galois representation $\rho^{(univ)} : G_{\mathbb{Q}} \rightarrow GL(R)$ such that if $\rho : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{Z}_{\ell})$ is any ℓ -adic Galois representation with $\rho \bmod \ell \simeq \bar{\rho}$, then there is a surjective map φ such that $\rho = \varphi \circ \rho^{(univ)}$ i.e. ρ factors through $\rho^{(univ)}$. The ring R is called the Universal Deformation Ring, and the map $\rho^{(univ)}$ is called the Universal Deformation of $\bar{\rho}$. (Actually, Mazur needs a few conditions such as $\bar{\rho}$ must be absolutely irreducible, but this is satisfied in our case when $\ell > 7$.)

On the other hand, Wiles constructed a universal ring out of the Hecke algebra $\mathbb{T}(N_E)$. Fix an eigenform $f \in S_2(\Gamma_0(N_E))$ with rational coefficients, and consider the composite map

$$\mathbb{T}(N_E) \rightarrow \mathbb{Z}_{\ell} \rightarrow \mathbb{F}_{\ell}, \quad T_p \mapsto a_p \mapsto \bar{a}_p = a_p \bmod \ell \quad \text{for all } p \nmid N_E. \quad (29.17)$$

The kernel of this map is contained in some maximal ideal \mathfrak{m} , so consider the localization $\mathbb{T} = \mathbb{T}(N_E)_{\mathfrak{m}}$. We define a Galois representation $\rho^{(mod)} : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{T})$ by sending

$$\begin{aligned} \text{tr } \rho^{(mod)}(\text{Frob}_p) &= T_p; \\ \det \rho^{(mod)}(\text{Frob}_p) &= p \end{aligned} \quad \text{whenever } p \nmid N_E. \quad (29.18)$$

Note that by construction $\rho^{(mod)} \bmod \mathfrak{m} \simeq \bar{\rho}_f$ since $T_p \equiv a_p \bmod \mathfrak{m}$. Hence, if $\bar{\rho}_{E,\ell} \simeq \bar{\rho}_f$, then there is a surjective map $\phi : R \rightarrow \mathbb{T}$ such that $\rho^{(mod)} = \phi \circ \rho^{(univ)}$.

29.1.6 The “ $R = \mathbb{T}$ ” Argument

Wiles made the following key observation: if ϕ is an isomorphism, then $\rho_{E,\ell} \simeq \rho_f$ for some modular form f . Consider the following diagram:

$$\begin{array}{ccccc} G_{\mathbb{Q}} & \xrightarrow{\rho^{(mod)}} & GL_2(R) & \xrightarrow{\varphi} & GL_2(\mathbb{Z}_{\ell}) \\ & & \downarrow \phi & & \\ G_{\mathbb{Q}} & \xrightarrow{\rho^{(mod)}} & GL_2(\mathbb{T}) & \xrightarrow{\pi_f} & GL_2(\mathbb{Z}_{\ell}) \end{array} \quad (29.19)$$

The vertical maps are all isomorphisms while $\rho_{E,\ell} = \varphi \circ \rho^{(univ)}$. Since ϕ is an isomorphism, define $\pi_f = \varphi \circ \phi^{-1}$. Although this is a map from $GL_2(\mathbb{T}) \rightarrow GL_2(\mathbb{Z}_\ell)$, we actually identify this with a map $\mathbb{T} \rightarrow \mathbb{Z}_\ell$. In fact, this is just the map sending $T_p \mapsto a_p$, so the composition $\rho_f = \pi_f \circ \rho^{(mod)}$ sends $\text{Frob}_p \mapsto T_p \mapsto a_p$. Hence,

$$\rho_{E,\ell} = \varphi \circ \rho^{(univ)} = \varphi \circ (\phi^{-1} \circ \rho^{(mod)}) = \pi_f \circ \rho^{(mod)} = \rho_f \quad (29.20)$$

as desired!

So to prove the Taniyama-Shimura-Weil conjecture for semistable elliptic curves over \mathbb{Q} (and hence to prove Fermat's conjecture) it suffices to show $\phi : R \rightarrow \mathbb{T}$ is an isomorphism. Mazur showed in his general construction that ϕ is surjective, so it suffices to show ϕ is injective. This is the bulk of Wiles' work.

Chapter 30

Homework Assignment #10

Due Monday, December 9 at 5:00 PM in the Instructor's Mailbox

Problem 1. Consider the elliptic curve

$$E : y^2 + y = x^3 + x^2 - 9x - 15.$$

1. Compute c_4 , c_6 , $\Delta(E)$, and $j(E)$.
2. Compute the conductor of this curve. (Hint: Determine the primes that divide c_6 and $\Delta(E)$.)
3. Compute the Mordell-Weil Group of this curve. (Hint: You may assume the rank of this curve is 0.)

Problem 2. The elliptic curve E above has two rational subgroups of order 3, say C_1 generated by $x = 5$ and C_2 generated by $x = -4/3$. Hence E has two 3-isogenies.

1. Show that C_1 is generated by a rational point while C_2 is not.
2. Show that the polynomial $(r + 3)^3 (r + 27) - j(E)r$ has two rational roots.
3. Show that there exist $D, r \in \mathbb{Q}^\times$ such that E is also of the form

$$y^2 = x^3 - \frac{3j}{j-1728} D^2 x - \frac{2j}{j-1728} D^3 \quad \text{where} \quad j = \frac{(r+3)^3 (r+27)}{r}.$$

Problem 3. Consider the elliptic curve

$$E_1 : y^2 + y = x^3 + x^2 - 769x - 8470.$$

1. Compute the conductor of this curve.
2. Compute the torsion subgroup of $E_1(\mathbb{Q})$.
3. Show that $E/C_1 = E_1$. (Hint: Compute $j(E_1)$ then compute r as above.)

Problem 4. Consider the elliptic curve

$$E_2 : y^2 + y = x^3 + x^2 + x.$$

1. Compute the conductor of this curve.
2. Compute the torsion subgroup of $E_2(\mathbb{Q})$.
3. Show that $E/C_2 = E_2$.