Problem Set Solutions for

Advanced Number Theory

Nandana Madhukara
nandana.madhukara@gmail.com

Contents

1 Week 1

(1)

n	$\mathbb{Z}[i]$	$\mathbb{Z}[\omega]$
2	$(1+i)(1-i)$	2
3	3	$(1+\omega)(1-\omega)^2$

(3) Let $a = a_1^2 + a_2^2$ and $b = b_1^2 + b_2^2$. Notice that

$$\begin{aligned} ab &= (a_1^2 + a_2^2)(b_1^2 + b_2^2 \\ &= (a_1b_1)^2 + (a_2b_2)^2 + (a_1b_2)^2 + (a_2b_1)^2 \\ &= (a_1b_1 + a_2b_2)^2 + (a_1b_2 - a_2b_1)^2. \end{aligned}$$

(4) Elements in $\mathbb{Z}[\sqrt{-2}]$ are of the form $a + b\sqrt{2}i$ so for $z \in \mathbb{Z}[\sqrt{-2}]$ is $N(z) = a^2 + 2b^2$. Setting this equal to 1, we find that $b = 0$ and $a = \pm 1$ meaning that the units are $\boxed{\pm 1}$.

(5) The norm for $z = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ is $N(z) = (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$. Setting this equal to 1 means that $a^2 - 2b^2 = 1$ which is just Pell's equation for $n = 2$. It has been proven that if n is not a perfect square, then there are an infinite number of integer solutions to the equation. More explicitly, if (a, b) is a solution then $(4b^2 + 1, 2ab)$ is also a solution:

$$\begin{aligned} (4b^2+1)^2 - 2(2ab)^2 &= (4b^2+1)^2 - 8b^2(2b^2+1) \\ &= 16b^4 + 8b^2 + 1 - 16b^4 - 8b^2 = 1 \end{aligned}$$

Finally, we see that a solution indeed exists, namely $(3, 2)$, so this finishes the proof.

Now for $\mathbb{Z}[\sqrt{3}]$ our equation is $a^2 - 3b^2 = 1$. Just like before, we can notice that if (a, b) is a solution, then $(2a + 3b, a + 2b)$ is also a solution. Additionally, we have that $(2, 1)$ is a solution which proves that there are an infinite number of integer solutions. Therefore, there are an infinite number of units in $\mathbb{Z}[\sqrt{2}]$ and $\mathbb{Z}[\sqrt{3}]$.

(6) Suppose π is not prime. Then it can be written as $\pi = ab$ where neither a nor b is a unit. Taking the norm of both sides gives us $N(\pi) = N(ab) = N(a)N(b)$, using the multiplicative property of norms. Since neither a nor b is a unit, we know that $N(a), N(b) \neq 1$. Therefore we have factorized $N(\pi)$ which is supposedly prime into two integers that are neither 1 or $N(\pi)$, so this results in a contradiction.

(7) If $R = \mathbb{Z}$, then $N(\alpha) = \alpha$ and $N(\beta) = \beta$ so the claim holds. Now if $R = \mathbb{Z}[i]$, then we can have $N(\alpha) = N(\beta)$ and α and β differ by a phase $\phi \neq 0$. However, there is no guarantee $e^{i\phi} \in \mathbb{Z}[i]$.

2 Week 2

(1)

(a) From Corollary 1.4, we know that -1 is a quadratic residue of an odd prime p iff $p \equiv 1 \pmod 4$. Since this is not the case for 71, which is an odd prime, we have $\left(\frac{-1}{71}\right) = \boxed{-1}$.

(b) By Proposition 1.8, we see that $\left(\frac{2}{67}\right) = \boxed{-1}$ since $67 \equiv 3 \pmod 8$.

(c) Using Quadratic Reciprocity, we have

$$\left(\frac{61}{127}\right) = \left(\frac{127}{61}\right) = \left(\frac{5}{61}\right) = \left(\frac{61}{5}\right) = \left(\frac{1}{5}\right) = \boxed{1}.$$

(d) Using Quadratic Reciprocity, we have

$$\begin{aligned}\left(\frac{53}{79}\right) &= \left(\frac{79}{53}\right)\\ &= \left(\frac{26}{53}\right)\\ &= \left(\frac{2}{53}\right)\cdot\left(\frac{13}{53}\right)\\ &= -\left(\frac{53}{13}\right)\\ &= -\left(\frac{1}{13}\right)\\ &= \boxed{-1}.\end{aligned}$$

(e) Using multiplicativity of Legendre symbols and factoring, we have

$$\left(\frac{12}{59}\right) = \left(\frac{2}{59}\right)^2\cdot\left(\frac{3}{59}\right).$$

Now Quadratic Reciprocity gives us

$$\left(\frac{3}{59}\right) = -\left(\frac{59}{3}\right) = -\left(\frac{2}{3}\right) = 1.$$

Now the square of a Legendre symbol is always 1 so $\left(\frac{12}{59}\right) = \boxed{1}$.

(2) Clearly p and q are odd primes so by Quadratic Reciprocity, we have

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$$

meaning that q is a QR of p since p is a NQR of q. Therefore, there exists an $x \in \mathbb{F}_p$ such that $x^2 \equiv q \pmod{p}$. The other solution is $p - x$.

(3) We must find the primes p such that 13 is a QR of p. Trivially, we see that $p = 2$ works. For odd primes, we must find p such that $\left(\frac{13}{p}\right) = 1$. By Quadratic Reciprocity, we have

$$\left(\frac{13}{p}\right) = \left(\frac{p}{13}\right) = 1$$

since 13 is not 3 modulo 4.

First, assume $p < 13$ so $p = 3, 5, 7, 11$. Using the first form, we see that $p = 3, 7$ works. Now we consider the case where $p > 13$ so we use the second form. The quadratic residues modulo 13 are $1, 3, 4, 9, 10$, and 12 so p must equal one of these modulo 13.

(4) Since $p \neq 2$, we have

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv 1, 3 \pmod 8 \\ -1 & p \equiv -1, -3 \pmod 8 \end{cases}$$

from casework.

(5) We have

$$\begin{aligned}\sum_{a=1}^{p-1} g_a &= \sum_{a=1}^{p-1}\sum_{t=0}^{p-1}\left(\frac{t}{p}\right)\zeta^{at} \\ &= \sum_{t=0}^{p-1}\left(\frac{t}{p}\right)\sum_{a=1}^{p-1}\zeta^{at} \\ &= 0\end{aligned}$$

where the last step is because of Lemma 2.1 since $t < p$ so $t \not\equiv 0 \pmod{p}$.

3 Week 3

(1) Since $11 \equiv -6 \pmod{17}$, we have

$$\left(\frac{11+3\omega}{17}\right)_3 = \left(\frac{-6+3\omega}{17}\right) = \left(\frac{3}{17}\right)_3 \left(\frac{\omega-2}{17}\right)_3.$$

From Corollary 1.9, we get

$$\left(\frac{11+3\omega}{17}\right)_3 = \left(\frac{\omega-2}{17}\right)_3.$$

Now $\omega - 2 = \omega^2(\omega^2 - 2\omega) = \omega^2(-1-3\omega)$ so

$$\left(\frac{\omega-2}{17}\right)_3 = \left(\frac{\omega^2}{17}\right)_3 \left(\frac{-1-3\omega}{17}\right)_3.$$

(2) Let us first compute $\left(\frac{\omega}{\pi}\right)_3 = \left(\frac{\omega}{a+b\omega}\right)_3$. We know that $a = 3m-1$ but since π primary, we have $b \equiv 0 \pmod{3}$ so $b = 3n$. Now we have

$$\begin{aligned}\frac{N(\pi)-1}{3} &= \frac{(3m-1)^2 - (3m-1)(3n) + (3n)^2 - 1}{3} \\ &= 3m^2 - 2m - 3mn + n + 3n^2 \\ &= 3(m^2 - mn + n^2) - 2m + n.\end{aligned}$$

This gives us

$$\left(\frac{\omega}{a+b\omega}\right) = \omega^{-2m+n}.$$

(3) Let g be a primitive root of p i.e. every $a \in \mathbb{F}_p$ can be written as $a = g^k$ for some k. Therefore, we have

$$\sum_{a\in\mathbb{F}_p} a^n = \sum_{k=0}^{p-2} g^{kn}.$$

Next we multiply both sides by $1 - g^k$ to get

$$(1-g^k)\sum_{a\in\mathbb{F}_p} a^n \equiv (1-g^n)\sum_{k=0}^{p-2} g^{kn} \equiv 1 - g^{(p-1)k} \equiv 0 \pmod{p}$$

by Fermat's Little Theorem. Now since $1 \leq n \leq p-2$, we know that $1 - g^k \not\equiv 0 \pmod{p}$ so the result follows. (How do I do this with cubic reciprocity?)

Now a polynomial with coefficients in $\mathbb{F}_p$ of degree at most $p-2$ with $f(0) = 0$ is of the form $a_{p-2}x^{p-2} + a_{p-3}x^{p-3} + \cdots + x$ so

$$\sum_{a \in \mathbb{F}_p} f(a) = a_{p-2} \sum_{a \in \mathbb{F}_p} a^{p-2} + a_{p-3} \sum_{a \in \mathbb{F}_p} a^{p-3} + \cdots \sum_{a \in \mathbb{F}_p} a = 0.$$

4 Week 4

(1) First, we see that $x^2 + y^2$ is always non-negative. Additionally, if the quadratic form is 0, the only way for this to happen is if $x = y = 0$ so it's positive definite. Similarly, we see that $-x^2 - y^2$ is always negative and equals 0 only if $x = y = 0$ so this quadratic form is negative definite. Next we move on to $x^2 - 2y^2$ which can represent both positive and negative numbers so it's indefinite.

(2) We can factor the quadratic form into $x^2 - 4xy + 4y^2 = (x - 2y)^2$. Now notice that any integer can be written in the form $x - 2y$ which means that any perfect square can be represented by $x^2 - 4xy + 4y^2$.

(4)

(a) We use the bound $a \leq \sqrt{-D/3}$ to get that $a \leq 1$. Clearly $a \neq 0$ since this implies $b = 0$ and the discriminant would be 0. If $a = 1$, we know that either $b = 0$ or $b = 1$. The former case implies $-4c = -11$ so c is not an integer which is a contradiction. Now when $a = b = 1$, we have $1 - 4c = -11 \implies c = 3$. This means that $h(-11) = 1$.

(b) Using the same bound from before gives us $a \leq 2$. Now the cases we must consider are $(a, b) = (1, 0), (1, 1), (2, 0), (2, -1), (2, 1), (2, 2)$. For each of these cases we get the equations

$$-4c = -17$$

$$1 - 4c = -17$$

$$-8c = -17$$

$$1 - 8c = -17$$

$$4 - 8c = -17$$

which all produce non-integer solutions for c. Therefore, we find that $h(-17) = 0$.

(5) Let $f(x, y) = ax^2 + bxy + cy^2$ and $g(x, y) = a'x^2 + b'xy + c'y^2$ be equivalent quadratic forms. This means that for $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ such that $\alpha\delta - \beta\gamma = \pm 1$,

$$\begin{aligned} g(x, y) &= f(\alpha x + \beta y, \gamma x + \delta y) \\ &= a(\alpha x + \beta y)^2 + b(\alpha x + \beta y)(\gamma x + \delta y) + c(\gamma x + \delta y)^2 \\ &= (a\alpha^2 + b\alpha\gamma + c\gamma^2)x^2 + (2a\alpha\beta + b\alpha\delta + b\beta\gamma + 2c\gamma\delta)xy + (a\beta^2 + b\beta\delta + c\delta^2)y^2. \end{aligned}$$

Therefore,

$$a' = \alpha^2 + b\alpha\gamma + c\gamma^2$$

$$b' = 2a\alpha\beta + b\alpha\delta + b\beta\gamma + 2c\gamma\delta$$

$$c' = a\beta^2 + b\beta\delta + c\delta^2.$$

Now one way to write the discriminant of a quadratic form is

$$\text{Disc}(f) = -4 \det \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}.$$

Now notice that

$$\text{Disc}(g) = -4 \det \begin{pmatrix} a' & b'/2 \\ b'/2 & c' \end{pmatrix} = -4 \det \left(\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \right) = \text{Disc}(f)$$

so we are done.

(7) A simple example is that 3 and 21 can be written as a sum of three perfect square: $3 = 1^2 + 1^2 + 1^2$ and $21 = 1^2 + 2^2 + 4^2$. However, notice that 63 cannot be written as a sum of three squares. (I don't know how to mathematically prove this but with a computer we can list out all numbers of the form $a^2 + b^2 + c^2$ where $a, b, c \leq 8$ and 63 is not in this list).

5 Week 5

(1)

(a) First we see that both quadratic forms have discriminant -47 the hypothesis in Lemma 1 is satisfied. Therefore, we must now find a $B \pmod{12}$ such that

$$B \equiv 1 \pmod 4$$

$$B \equiv -1 \pmod 6$$

$$B^2 = -47 \pmod{24}.$$

We can see that $B \equiv 5 \pmod{12}$ so $h'(x, y) = 6x^2 + 5xy + 3y^2$ which properly equivalent to $h(x, y) = 3x^2 + xy + 4y^2$.

(b) For this case, notice that the hypothesis of Lemma 1 does not hold so we write $2x^2 - xy + 9y^2$ as the properly equivalent form $9x^2 + xy + 2y^2$ and write $4x^2 - 3xy + 5y^2$ as the properly equivalent form $5x^2 + 3xy + 4y^2$. This means that we must find a $B \pmod{90}$ such that

$$B \equiv 1 \pmod{18}$$

$$B \equiv 3 \pmod{10}$$

$$B^2 = -71 \pmod{180}.$$

We can see that $B \equiv 73 \pmod{90}$ works so $h'(x, y) = 45x^2 + 73xy + 30y^2$ which is properly equivalent to $h(x, y) = 2x^2 + xy + 9y^2$.

(2) We know that the first two congruences have a unique solution $B \pmod{2aa'}$ by the Chinese Remainder Theorem since $\gcd(a, a') = 1$ so we must now show that this solution satisfies $B^2 \equiv D \pmod{4aa'}$. In other words, we must show that $B^2 - D$ is a multiple of $4aa'$, which we can do by showing that $B^2 - D$ is a multiple of $2a$ and $2a'$. Now notice that

$$B^2 - D \equiv B^2 - b^2 + 4ac \equiv b^2 - b^2 \equiv 0 \pmod{2a}.$$

Similarly, we have

$$B^2 - D \equiv B^2 - b'^2 + 4a'c' \equiv b'^2 - b'^2 \equiv 0 \pmod{2a'}$$

so we are done.

(3) Notice that if $f = ax^2 + bxy + cy^2$, then

$$\text{Disc}(f) = -4 \det \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}.$$

Now let $g(x,y) = f(\alpha x + \beta y, \gamma x + \delta y) = a'x^2 + b'xy + c'y^2$. Expanding $f(\alpha x + \beta y, \gamma x + \delta y)$ out gives us

$$\begin{aligned} a' &= \alpha^2 + b\alpha\gamma + c\gamma^2 \\ b' &= 2a\alpha\beta + b\alpha\delta + b\beta\gamma + 2c\gamma\delta \\ c' &= a\beta^2 + b\beta\delta + c\delta^2. \end{aligned}$$

Therefore

$$\begin{pmatrix} a' & b'/2 \\ b'/2 & c' \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

meaning that

$$\text{Disc}(f) = \det \left(\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \right) = (\alpha\delta - \beta\gamma)^2 \text{Disc}(f).$$

(5)

(a) Notice that 12 can be written as 12, 4×3, 2×6, and $2 \times 2 \times 3$. This corresponds to the abelian groups C_{12}, $C_4 \times C_3$, $C_2 \times C_6$, and $C_2 \times C_2 \times C_3$. However, by the Chinese Remainder Theorem, the first two groups and the last two groups are each isomorphic so the abelian groups of order 12 are C_{12} and $C_2 \times C_2 \times C_3$.

(b) Like before we write 24 as 24, 2×12, 3×8, 4×6, $2 \times 2 \times 6$, $2 \times 3 \times 4$, $2 \times 2 \times 2 \times 3$. Accounting for isomorphisms by the Chinese Remainder Theorem gives us the groups C_{24}, $C_2 \times C_{12}$, $C_2 \times C_2 \times C_6$, $C_2 \times C_2 \times C_2 \times C_3$.

(14) We know that $x^2 + 27y^2$ represents a prime p if and only if $\left(\frac{-108}{p}\right) = 1$. This means that $p \equiv 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97, 103 \pmod{108}$. Notice that all of these are $1 \pmod 3$ and 2 is a cubic residue modulo p.

6 Week 6

(1) For $r_2(n)$ we use the fact $r_2(n) = 4(d_1(n) - d_3(n))$ and for $r_4(n)$ we use Jacobi's theorem to get

n	$r_2(n)$	$r_4(n)$
1	4	8
2	4	16
3	0	16
4	4	16
5	8	16
6	0	32
25	12	24
100	12	48

(2) Let $8n+3$ be an integer 3 modulo 8 so we can write it as a sum of three odd squares:

$$\begin{aligned} 8n+3 &= (2a+1)^2 + (2b+1)^2 + (2c+1)^2 \\ &= 4(a^2+a+b^2+b+c^2+c)+3 \\ &= 8\left(\frac{a(a+1)}{2} + \frac{b(b+1)}{2} + \frac{c(c+1)}{2}\right) + 3. \end{aligned}$$

Therefore, we see that n can be written as a sum of three triangular numbers. Now the other direction (proving that if all numbers can be written as a sum of three triangular numbers, then all numbers 3 modulo 8 can be written as a sum of three squares) is trivial since all steps we have done are reversible.

(3) Using the notation from before, we have $a = 115$, $b = 682$, $c = 557$, and $d = 410$. Now $e = \frac{a+c}{2} = 336$ and $f = \frac{b+d}{2} = 546$. Then, we have $g = \gcd(e, f) = 42$, $s = \frac{e}{g} = 8$, and $t = \frac{f}{g} = 13$. Finally, we have $h = \gcd(e-a, b-f) = 17$. This gives us the factorization $478349 = (42^2+17^2)(8^2+13^2) = \boxed{2053 \times 233}$.

(4) We can use a modified Euclidean algorithm for $\mathbb{Z}[\sqrt{-2}]$ where the norm is defined as $N(x+\sqrt{2}iy) = x^2+2y^2$. Let $j = \sqrt{2}i$. Now let us compute $\gcd(619+684j, 745+618j)$. We let $a_0 = 619+684j$ and $a_1 = 745+618j$. To find a_2, we must find some $k \in \mathbb{Z}[\sqrt{2}i]$ such that $N(a_0 - ka_1) \leq N(a_1)$ so we pick $k = 1$ which gives us $a_2 = a_0 - a_1 = -126+66j$. Next, we have $a_3 = a_1 - (-1-5j)a_2 = -41+54j$. Continuing this gives us $a_4 = a_2 - (2+j)a_3 = 64-j$, $a_5 = a_3 - (-1+j)a_4 = 21-11j$, and $a_6 = 0$. Now since $N(21-11j) = 683$, we get the factorization $1318873 = \boxed{683 \times 1931}$.

7 Week 7

(1) A root r is a double or triple root iff the derivative at r is 0. This means that $3r^2 + a = 0 \implies r = \sqrt{-a/3}$ so we have

$$\left(-\frac{a}{3}\right)^{3/2} + a\sqrt{-\frac{a}{3}} + b = 0.$$

This means that

$$b^2 = \left(\left(-\frac{a}{3}\right)^{3/2} + a\sqrt{-\frac{a}{3}}\right)^2 = -\frac{a^3}{27} - \frac{a^3}{3} + \frac{2a^3}{9} = \frac{-4a^3}{27}$$

so $4a^3 + 27b^2 = 0$.

(2) We know that if $Q = (x, y)$, then the x coordinate of P is

$$\frac{x^4 - 2ax^2 - 8bx + a^2}{4\left(x^3 + ax + b\right)}.$$

Notice that multiple values of x can result in the same value of this result so there may be multiple Q's such that $2Q = P$.

Geometrically, to find Q from P, we must first reflect P across the x-axis, which we can call P', and find tangent lines that pass through P'. The points at which these lines are tangent to E are the possible values of Q. Notice that E can be disjoint or one continuous curve. When it is disjoint we can find at most two tangent lines because of the symmetry about the x-axis. When it is continuous, we can find at most one tangent line.

(4) Consider a elliptic curve E with positive rank. This means that the size of $E(\mathbb{Q})$ is infinite. Now we can pick n of these rational points and find the least common multiple of the denominators of the x coordinates and y coordinates for these points. Let these number be l_x and l_y. If E is of the form $y^2 = x^3 + ax + b$, then $(y/l_y)^2 = (x/l_x)^3 + ax/l_x + b$ must have n integer solutions, namely multiples of the numerators of the x and y coordinates of the n rational points. Therefore the elliptic curve E' of the form

$$y^2 = \frac{l_y^2}{l_x^3} \cdot x^3 + \frac{al_y^2}{l_x} \cdot x + bl_y^2$$

has n integral points.

(5) Recall, that we can parameterize the rational points on $y^2 = x^2(x+1)$ as $(t^2 - 1, t(t^2 - 1))$ for $t \in \mathbb{Q}$. Now if $t \in \mathbb{Z}$, it is easy to see that we get an infinite number of integral points.

(8) We must find the rational points on the elliptic curve $y^2 = x^3 - 36x$. One rational point is $(-3, 9)$ so adding it to itself must give another rational point:

$$2 \cdot (-3, 9) = \left(\frac{25}{4}, -\frac{35}{8}\right)$$

which corresponds to the triangles with sides $\boxed{\left(\frac{7}{10}, \frac{120}{7}, \frac{1201}{70}\right)}$. (My calculator doesn't display enough digits to repeat this since the fractions' numerators and denominators become too large.)

8 Week 8

(1) The points in $E(\mathbb{F}_5)$ are $(0, \pm 2)$, $(2, \pm 1)$, $(4, \pm 1)$, and ∞. Similarly, the points in $E(\mathbb{F}_7)$ are $(0, \pm 2), (1, 0), (2, \pm 3), (3, \pm 3)$, $(6, \pm 1)$, and ∞ and the points in $E(\mathbb{F}_{11})$ are $(0, \pm 2)$, $(1, \pm 7)$, $(2, \pm 4)$, $(3, \pm 2)$, $(6, \pm 1)$, $(7, \pm 3)$, $(8, \pm 2)$, $(10, \pm 1)$, and ∞.

(2)

(a) We can just list the points in $E(\mathbb{F}_5)$. They are $(0, \pm 1), (2, \pm 1), (3, \pm 1), (4, \pm 2)$ and ∞ which are 9 points.

(b) As we saw in the previous part $(0, 1)$ and $(2, 1)$ are in $E(\mathbb{F}_5)$. Next we see

$$2(0, 1) = \left(\frac{1}{4}, -\frac{9}{8}\right).$$

Adding $(0, 1)$ one more time gives us

$$(0, 1) + \left(\frac{1}{4}, -\frac{9}{8}\right) = (72, 611) = (2, 1).$$

(3)

(a) Since $d \in \mathbb{F}_p^\times$, it must be a generator of $\mathbb{F}_p$ so there exist d', a', and b' such that

$$d'd \equiv 1 \pmod{p}$$

$$a'd \equiv a \pmod{p}$$

and

$$b'd \equiv b \pmod{p}.$$

Therefore, we have $\boxed{E' : y^2 = d'x^3 + a'x + b'}$

(b) Notice that the d', a', and b' are essentially just $1/d$, a/d, and b/d modulo p, respectively. Therefore if $f(x) = x^3 + ax + b$ and $f'(x) = d'x^3 + a'x + b'$, we have

$$f(x) \equiv d'f'(x) \pmod{p}.$$

This means that if $f(x) = dy^2$, then

$$dy^2 \equiv d'f'(x) \pmod{p} \implies f'(x) \equiv dy \pmod{p}$$

so $\#E'(\mathbb{F}_p) = \#E(\mathbb{F}_p)$

(4)

(a) Assume k is not a quadratic residue modulo p. Let $f(x) = x^3 - kx$ and for each $x \in \mathbb{F}_p$, let $N(x)$ be the set of points $(x, y) \in E(\mathbb{F}_p)$. Notice that $N(x) = 1 + \left(\frac{f(x)}{p}\right)$. Now $f(x)f(-x) = (x^3 - kx)(-x^3 + kx) = -(x^3 - kx)^2$ so we have

$$\left(\frac{f(x)}{p}\right)\left(\frac{f(-x)}{p}\right) = \left(\frac{f(x)f(-x)}{p}\right) = \left(\frac{-1}{p}\right).$$

When $p \equiv 3 \pmod 4$, we see that $\left(\frac{-1}{p}\right) = -1$ so only one of $f(x)$ and $f(-x)$ is a quadratic residue modulo p. This means that one of $N(x)$ and $N(-x)$ is 2 and other is 0. On average this is 1 so $N_p = p + 1$, including ∞.

9 Week 9

(1) Expanding the elliptic curve gives us

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

Now we use the substitution $(x, y) \mapsto \left(x + \frac{1+\lambda}{3}, y\right)$ to get

$$\begin{aligned} y^2 &= \left(x + \frac{1+\lambda}{3}\right)^3 - (1+\lambda)\left(x + \frac{1+\lambda}{3}\right)^2 + \lambda\left(x + \frac{1+\lambda}{3}\right) \\ &= x^3 + \left(\lambda - \frac{(1+\lambda)^2}{3}\right)x + \frac{\lambda(1+\lambda)}{3} - \frac{2(1+\lambda)^3}{27}. \end{aligned}$$

This means that

$$\begin{aligned} 4a^3 &= 4\left(\lambda - \frac{(1+\lambda)^2}{3}\right)^3 \\ &= 4\lambda^3 - 4\lambda^2(1+\lambda)^2 + \frac{4\lambda(1+\lambda)^4}{3} - \frac{4(1+\lambda)^6}{27} \end{aligned}$$

and

$$\begin{aligned} 27b^2 &= 27\left(\frac{\lambda(1+\lambda)}{3} - \frac{2(1+\lambda)^3}{27}\right)^2 \\ &= 27\left(\frac{\lambda^2(1+\lambda)^2}{9} - \frac{4\lambda(1+\lambda)^4}{81} + \frac{4(1+\lambda)^6}{27^2}\right) \\ &= 3\lambda^2(1+\lambda)^2 - \frac{4\lambda(1+\lambda)^4}{3} + \frac{4(1+\lambda)^6}{27}. \end{aligned}$$

Therefore, the j-invariant is

$$\begin{aligned} j(E) &= 1728\frac{4\lambda^3 - 4\lambda^2(1+\lambda)^2 + \frac{4\lambda(1+\lambda)^4}{3} - \frac{4(1+\lambda)^6}{27}}{4\lambda^3 - \lambda^2(1+\lambda)^2} \\ &= 256\frac{\lambda^6 - 3\lambda^5 + 6\lambda^4 - 7\lambda^3 + 6\lambda^2 - 3\lambda + 1}{\lambda^2(1-\lambda)^2} \\ &= 256\frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(1-\lambda)^2} \\ &= 256\frac{(1-\mu)^3}{\mu^2}. \end{aligned}$$

(2) We must find the short Weierstrass form of $y^2 + y = x^3 - x$. First we do the substitution $(x, y) \mapsto \left(x, y - \frac{1}{2}\right)$ to get

$$\left(y - \frac{1}{2}\right)^2 + \left(y - \frac{1}{2}\right) = x^3 - x^2 \implies y^2 - \frac{1}{2} = x^3 - x^2$$

This eventually turns into $y^2 = x^3 - 432x + 8208$.