Topics: Reduction of elliptic curves modulo primes, zeta functions.

10.1. Let a and b be integers such that $a \equiv 16 \pmod{35}$ and $b \equiv 29 \pmod{35}$, and consider the elliptic curve over $\mathbf{Q}$ given by the Weierstrass equation

$$E : \ y^2 = x^3 + ax + b.$$

(a) Prove that the discriminant of E is not divisible by 5 nor by 7.

(b) Show that the torsion subgroup of E is trivial.

Solution.

(a) From the given conditions we have $a \equiv 1 \pmod{5}$ and $b \equiv -1 \pmod{5}$, so

$$4a^3 + 27b^2 \equiv 31 \equiv 1 \pmod{5},$$

hence $5 \nmid \Delta$.

Similarly, $a \equiv 2 \pmod{7}$ and $b \equiv 1 \pmod{7}$, so

$$4a^3 + 27b^2 \equiv 31 \equiv 3 \pmod{7},$$

hence $7 \nmid \Delta$.

(b) Reduce E modulo 5 and count points: for $\tilde{E} : \ y^2 = x^3 + x + 4$ we have

x	$x^3 + x + 4$	y
0	4	2, 3
1	1	1, 4
2	4	2, 3
3	4	2, 3
4	2	—

Therefore $\#\tilde{E}(\mathbf{F}_5) = 9$.

Now reduce E modulo 7: for $\tilde{E} : \ y^2 = x^3 + 2x + 1$ we have

x	$x^3 + 2x + 1$	y
0	1	1, 6
1	4	2, 5
2	6	—
3	6	—
4	3	—
5	3	—
6	5	—

Therefore $\#\tilde{E}(\mathbf{F}_7) = 5$.

Since $\#E(\mathbf{Q})$ must divide both 9 and 5, it is 1. □

10.2. Let E be an elliptic curve over $\mathbf{F}_p$, where p is a prime.

Let $N_1 = \#E(\mathbf{F}_p)$ and $a = p + 1 - N_1$. Let α, β be the (possibly complex) roots of the quadratic polynomial

$$x^2 - ax + p = (x - \alpha)(x - \beta),$$

so that $\alpha\beta = p$ and $\alpha + \beta = a$.

For every $m \in \mathbf{Z}_{\geqslant 1}$, let

$$N_m = p^m + 1 - \alpha^m - \beta^m.$$

(Note that this is consistent with the above definition of N_1.)

Finally, define formally (don't worry about convergence issues)

$$Z_E(T) = \exp\left(\sum_{m=1}^{\infty} N_m \frac{T^m}{m}\right).$$

Use the definition of N_m and the expansion $-\log(1-x) = \displaystyle\sum_{m=1}^{\infty} \frac{x^m}{m}$ to prove that

$$Z_E(T) = \frac{pT^2 - aT + 1}{(1-T)(1-pT)}.$$

Solution. We have

$$\begin{aligned} Z_E(T) &= \exp\left(\sum_{m=1}^{\infty} (p^m + 1 - \alpha^m - \beta^m)\frac{T^m}{m}\right) \\ &= \exp\left(\sum_{m=1}^{\infty} \frac{(pT)^m}{m}\right) \exp\left(\sum_{m=1}^{\infty} \frac{T^m}{m}\right) \exp\left(-\sum_{m=1}^{\infty} \frac{(\alpha T)^m}{m}\right) \exp\left(-\sum_{m=1}^{\infty} \frac{(\beta T)^m}{m}\right) \\ &= \exp\big(-\log(1-pT)\big) \exp\big(-\log(1-T)\big) \exp\big(\log(1-\alpha T)\big) \exp\big(\log(1-\beta T)\big) \\ &= \frac{(1-\alpha T)(1-\beta T)}{(1-pT)(1-T)} = \frac{1 - aT + pT^2}{(1-pT)(1-T)}. \end{aligned}$$

□

10.3. Let E be an elliptic curve over $\mathbf{F}_p$, where p is a prime.

We pick up where Tutorial Question 10.2 left off.

For a complex variable s, define the zeta function of E by

$$\zeta_E(s) = Z_E(p^{-s}).$$

(a) Find the values $s \in \mathbf{C}$ where the function ζ_E is not defined.

(b) Prove the functional equation $\zeta_E(s) = \zeta_E(1-s)$.

(c) Let α, β denote the (complex) roots of the quadratic polynomial $x^2 - ax + p$. Prove that if $|a| \leqslant 2\sqrt{p}$ then $\beta = \overline{\alpha}$ and $|\alpha| = |\beta| = \sqrt{p}$.

(d) Prove the Riemann Hypothesis for ζ_E: if $\zeta_E(s) = 0$ then $\mathsf{Re}\,(s) = 1/2$.

[**Hint**: Use the Hasse bound and part (c).]

Solution.

(a) Looking at the denominator of

$$\zeta_E(s) = \frac{p(p^{-s})^2 - ap^{-s} + 1}{(1-p^{-s})(1-p(p^{-s}))} = \frac{p^{1-2s} - ap^{-s} + 1}{(1-p^{-s})(1-p^{1-s})},$$

we see that the function is undefined at $s = 0$ and $s = 1$.

(b) We have

$$\zeta_E(1-s) = \frac{p^{1-2(1-s)} - ap^{-(1-s)} + 1}{(1-p^{-(1-s)})(1-p^{1-(1-s)})} = \frac{p^{2s-1} - ap^{s-1} + 1}{(1-p^{s-1})(1-p^s)}$$
$$= \frac{1 - ap^{-s} + p^{1-2s}}{(1-p^{-s})(1-p^{1-s})} = \zeta_E(s).$$

(c) The quadratic formula gives

$$\alpha, \beta = \frac{a \pm \sqrt{a^2 - 4p}}{2}$$

and by assumption we have $|a| \leqslant 2\sqrt{p}$, so that $a^2 - 4p \leqslant 0$. This implies that $\beta = \overline{\alpha}$, so

$$|\alpha| = |\beta| = |\alpha\beta|^{1/2} = p^{1/2} = \sqrt{p}.$$

(d) If $\zeta_E(s) = 0$ then the numerator is zero:

$$p^{1-2s} - ap^{-s} + 1 = 0 \quad \Rightarrow \quad p - ap^s + p^{2s} = 0,$$

so p^s is a root of the quadratic polynomial $x^2 - ax + p = 0$.

The Hasse bound gives $|a| \leqslant 2\sqrt{p}$, so by part (c) we have $|p^s| = \sqrt{p}$. Therefore

$$p^{\mathsf{Re}\,(s)} = |p^s| = \sqrt{p} = p^{1/2},$$

so that $\mathsf{Re}\,(s) = 1/2$. □

10.4. Let $f : G \longrightarrow H$ be a function between abelian groups.

Prove that f is a group homomorphism if and only if the following two conditions are satisfied:

(a) for all $g \in G$ we have $f(-g) = -f(g)$;

(b) for all $g_1, g_2, g_3 \in G$, if $g_1 + g_2 + g_3 = 0_G$, then $f(g_1) + f(g_2) + f(g_3) = 0_H$.

Solution. If f is a group homomorphism then the two properties follow from Exercise 1.15. Conversely, if $x, y \in G$, then

$$x + y - (x + y) = 0_G.$$

Using property (b) we get

$$f(x) + f(y) + f(-(x+y)) = 0_H.$$

Property (a) says that $f(-(x+y)) = -f(x+y)$, and so we get

$$f(x) + f(y) - f(x+y) = 0_H,$$

showing that f is a homomorphism. □

10.5. (*) Let E be an elliptic curve over $\mathbf{Q}$, p a prime not dividing the discriminant of E, and $\tilde{E}$ the reduction of E modulo p.

Recall the function $\varphi : E_{\text{tors}}(\mathbf{Q}) \longrightarrow \tilde{E}(\mathbf{F}_p)$ by $\varphi(\mathcal{O}) = \tilde{\mathcal{O}}$ and $\varphi(x, y) = (\tilde{x}, \tilde{y})$.

Use Tutorial Question 10.4 to prove that φ is a group homomorphism.

(For condition (b), there are a few special cases to consider; feel free to restrict to the generic case where P_1, P_2, P_3 are distinct points that are not the point at infinity. To prove that the condition holds, review how the formulas for the group law were obtained in the lectures.)

Solution. We first check the condition about the negatives. Since $-\mathcal{O} = \mathcal{O}$ and $-\tilde{\mathcal{O}} = \tilde{\mathcal{O}}$, we have

$$\varphi(-\mathcal{O}) = \varphi(\mathcal{O}) = \tilde{\mathcal{O}} = -\tilde{\mathcal{O}} = -\varphi(\mathcal{O}).$$

If $P = (x, y)$ then $-P = (x, -y)$ and $-\tilde{P} = (\tilde{x}, -\tilde{y})$ so

$$\varphi(-P) = \varphi(x, -y) = (\tilde{x}, -\tilde{y}) = -(\tilde{x}, \tilde{y}) = -\varphi(x, y) = -\varphi(P).$$

Now for the second condition. We look at the generic case: let P_1, P_2, P_3 be distinct points, neither of which is the point at infinity. The equation $P_1 + P_2 + P_3 = \mathcal{O}$ says that the points lie on the same line, say of equation $y = mx + n$. We know from the formulas for the group law that

$$m^2 = x_1 + x_2 + x_3 \in \mathbf{Z} \qquad \text{and} \qquad n = y_3 - mx_3.$$

We also have $m = (y_2 - y_1)/(x_2 - x_1) \in \mathbf{Q}$, so both m and n must be integers.

Substituting $y = mx + n$ in the equation $y^2 = x^3 + ax + b$ we have

$$x^3 + ax + b - (mx + n)^2 = (x - x_1)(x - x_2)(x - x_3),$$

which is equivalent to $P_1 + P_2 + P_3 = \mathcal{O}$.

Since all the coefficients are integers, we can reduce this equation mod p to get

$$x^3 + \tilde{a}x + \tilde{b} - (\tilde{m}x + \tilde{n})^2 = (x - \tilde{x}_1)(x - \tilde{x}_2)(x - \tilde{x}_3).$$

But we also have $\tilde{y}_1 = \tilde{m}\tilde{x}_1 + \tilde{n}$, etc. We conclude that the line $y = \tilde{m}x + \tilde{n}$ intersects the curve $\tilde{E}$ in the three points $\varphi(P_1), \varphi(P_2), \varphi(P_3)$, so that $\varphi(P_1) + \varphi(P_2) + \varphi(P_3) = \tilde{\mathcal{O}}$. □