Chapter 17

Rational points on elliptic curves

Exercise 17.0.1. Let $\Delta = 4a^3 + 27b^2$. Show that if $a > 0$ or if $\Delta > 0$, then $x^3 + ax + b = 0$ has just one real root. Show that if $a, \Delta < 0$, then $x^3 + ax + b = 0$ has three real roots. Sketch the shape of the curve $y^2 = x^3 + ax + b$ in the two cases.

17.1. The group of rational points on an elliptic curve

Exercise 17.1.1. Prove that there cannot be four points of $E(\mathbb{Q})$ on the same line.

Exercise 17.1.2. In Figure 17.3 the polynomial $x^3 + ax + b$ has three real roots, $r_1 < r_2 < r_3$, and so the points of $E(\mathbb{R})$ come in two continuous components, the *egg* and the *infinite part* $E^+(\mathbb{R}) = \{(x, y) \in E(\mathbb{R}) : \ x > r_3\} \cup \{\mathcal{O}\}$.

(a) Prove that a straight line intersects the egg in exactly 0 or 2 points (counted with multiplicity).
(b) Prove that the tangent at any point $P \in E(\mathbb{R})$ hits E again in $E^+(\mathbb{R})$.
(c) Deduce that $E^+(\mathbb{R})$ is a subgroup of $E(\mathbb{R})$.
(d) Deduce that the egg is the coset $(r_2, 0) + E^+(\mathbb{R})$ (that is, a coset of $E^+(\mathbb{R})$ in $E(\mathbb{R})$).

Exercise 17.1.3. Prove that if $2P = \mathcal{O}$, then either $P = \mathcal{O}$ or $P = (x, 0)$ where $x^3 + ax + b = 0$. Deduce that the number of rational points of order 1 or 2 is one plus the number of integer roots of $x^3 + ax + b$ and therefore equals 1, 2, or 4.

Exercise 17.1.4. Prove that the torsion points form a subgroup of $E(\mathbb{C})$.

Exercise 17.1.5. Suppose that $x^3 + ax + b$ has three real roots.

(a) Prove that if $P \in E(\mathbb{R})$ is a torsion point of odd order, then $P \in E^+(\mathbb{R})$.
(b) Prove that if a torsion point P of E lies on the egg, then it is one of the points of order 2 at either end of the egg.

Exercise 17.1.6. Deduce from Mordell's Theorem that $E(\mathbb{Q})$ is finite if and only if its rank $r = 0$.

17.2. Congruent number curves

Exercise 17.2.1. Prove that if $A = ar^2$ for some rational r, then $E_a(\mathbb{Q})$ is isomorphic to $E_A(\mathbb{Q})$. (We may therefore restrict our attention to E_A where A is a squarefree positive integer.)

Exercise 17.2.2. Suppose that $P \in E_A(\mathbb{Q})$ has order > 2. Prove that exactly one of points P and $P + (0, 0)$ belongs to $E_A^+(\mathbb{Q})$. Therefore this point yields a Pythagorean triangle of area A, with parameters $t = x/A, g = A^2/|y|$).

Exercise 17.2.3. Let $x_P = m/n^2 > A$ and $x_{2P} = M/N^2$ with $(m, n) = (M, N) = 1$.
(a) Prove that $M < 4m^4$.
(b) Prove that if $(m, A) = 1$, then $(m^2 + A^2n^4, 2\ell n) = 1$ or 2, and N is even.
(c) Deduce that if $(m, A) = 1$, then $M > m^4/4$, and also $M > m^4$ if n is even.
(d) Deduce that, in general, $(m^2 + A^2n^4, 2\ell n)$ divides $2(m, A)^2$.
(e)† Prove that $(m^2 + A^2n^4, 2\ell n) = (m, A)^2$ or $2(m, A)^2$.

Exercise 17.2.4. Prove that the torsion subgroup of $E_A(\mathbb{Q})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

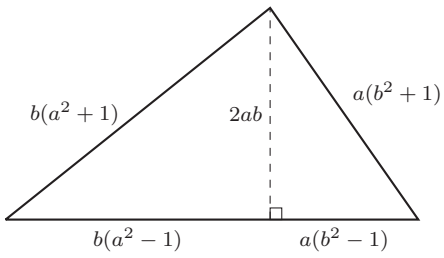
17.3. No non-trivial rational points by descent

17.4. The group of rational points of $y^2 = x^3 - x$

17.5. Mordell's Theorem: $E_A(\mathbb{Q})$ is finitely generated

Exercise 17.5.1. Suppose that $P \in E_A^+(\mathbb{Q})$ and that it corresponds to a Pythagorean triangle of area A, with parameter t. Prove that $Q := P + (A, 0) \in E_A^+(\mathbb{Q})$ and that it corresponds to *the same* Pythagorean triangle of area A, but with parameter T, where $T = \frac{t+1}{t-1}$.

Exercise 17.5.2 (Areas of rational-sided triangles, I)**.** Let T be a triangle with rational side lengths.
(a) Prove that rational-sided isosceles triangles of area $2A$ are in 1-to-1 correspondence with rational-sided right-angled triangles of area A.
(b) Show that if T has rational area A, then it has rational height, no matter which side is the base.
(c) Draw a perpendicular line from the base of the triangle to the top triangle vertex. This splits the triangle into two rational-sided right-angled triangles. Prove that we can parameterize a rational scalar multiple of T as follows, where a and b are rational numbers > 1:



(d) Prove that rational number A is the area of a triangle with rational side lengths if and only if there exist rational numbers a, b, c for which $A = abc^2(a + b)(ab - 1)$.
(e) Verify that for given A and b there is a 1-to-1 correspondence between such triangles and rational points on the elliptic curve $E_{A,b} : y^2 = x(x + Ab)(x - A/b)$ (taking $x = Aa, y = A^2/bc$) with $x > A/b$.
(f) Show that if we are given a point $(Aa, A^2/bc) \in E_{A,b}(\mathbb{Q})$, then we can determine another point $(X, Y) \in E_{A,b}(\mathbb{Q})$ with $X = (\frac{(a^2+1)bc}{2})^2$.

Exercise 17.5.3 (Areas of rational-sided triangles, II)**.** Fix a squarefree positive integer A. Let $t = A^2u^4$ for some $u \in \mathbb{Q}$ and then

$$a = \frac{2(t+1)^2}{9Au^2} \quad \text{and} \quad b = \frac{6A(t+1)u^2}{(2t-1)^2}.$$

Use these parametrizations to prove that there are infinitely many distinct rational-sided triangles of area A. Exhibit several of area 1.

17.6. Some nice examples

Exercise 17.6.1. Prove that if a and b are integers for which $a^3 + b^3 = m$, then $|a|, |b| \leq (4m/3)^{1/2}$.

Appendix 17A. General Mordell's Theorem

17.7. The growth of points

Exercise 17.7.1.‡ Let $P \in E_A^+(\mathbb{Q})$ and $Q = 4P$.

(a) Prove that $(4^{-1/3}H(Q))^{4^r} < H(2^rQ) < (4^{1/3}H(Q))^{4^r}$ for all $r \geq 1$.
(b) Prove that $\lim_{k\to\infty} H(2^kP)^{1/4^k}$ exists, which we denote by $\hat{H}(P)$, the *Néron-Tate height*.
(c) Prove that $\hat{H}(2P) = \hat{H}(P)^4$.
(d) Prove that $4^{-1/3}H(Q) \leq \hat{H}(Q) \leq 4^{1/3}H(Q)$.

Four squares in an arithmetic progression.

Exercise 17.7.2. Use Szemerédi's Theorem (Theorem 15.6 from section 15.6) and Fermat's Theorem to deduce the following: *For any $\delta > 0$ there exists a constant M_δ such that if $N \geq M_\delta$, then any arithmetic progression of length N contains $< \delta N$ squares.* (It is conjectured that the N-term arithmetic progression with the most squares is $1, 1+24, 1+24\cdot 2, \dots, 1+24(N-1)$, which contains about $\sqrt{8N/3}$ squares; the best bound proved to date is at most a little more than $N^{3/5}$ squares.)

Exercise 17.7.3 (Another proof that there are infinitely many primes)**.** Suppose not and that $p_1, \dots, p_k$ is the complete set of primes. We will color the positive integers as follows: By the Fundamental Theorem of Arithmetic one can write every positive integer n in the form $p_1^{e_1}\cdots p_k^{e_k}$ where the e_j are integers ≥ 0. We will color n as $c(n) = p_1^{r_1}\cdots p_k^{r_k}$, where r_j is the least nonnegative residue of $e_j \pmod 2$ for $j = 1, \dots, k$.

(a) Establish that $c(n)$ provides a coloring of the positive integers with 2^k colors.
(b) Use van de Waerden's Theorem (Theorem 15.5 from section 15.6) to establish that there is a four-term arithmetic progression of integers $A, A+D, A+2D, A+3D$ for which $c(A) = c(A+D) = c(A+2D) = c(A+3D)$.
(c) Let $a = A/c(A)$ and $d = D/c(A)$. Prove that each of $a, a+d, a+2d, a+3d$ is a square.
(d) Establish a contradiction using Fermat's Theorem.

Appendix 17B. Pythagorean triangles of area 6

Appendix 17C. 2-parts of abelian groups

17.8. 2-parts of abelian, arithmetic groups

Appendix 17D. Waring's problem

17.9. Waring's problem

Exercise 17.9.1. Let $s_k(n)$ be the smallest number of positive integers $a_1, \dots, a_s$ for which $n = a_1^k + \cdots + a_s^k$.

(a) Prove that $s_k(2^k - 1) = 2^k - 1$.

(b) Prove that if $n = 2^k m - 1$ where $m = [(3/2)^k]$, then $s_k(n) = 2^k + [(3/2)^k] - 2$. Euler's son conjectured that $g(k) = 2^k + [(3/2)^k] - 2$.

(c)‡ Prove that if $2^k\{(3/2)^k\} + [(3/2)^k] \le 2^k$, then Euler Jr's conjecture is true. This inequality follows if $\{(3/2)^k\} < 1 - (3/4)^k$ which is probably true for all integers $k \ge 2$ and is known to hold for $2 \le k < 10^8$.

Exercise 17.9.2. By proving that each of 0, 1, 2, 81, 16, and 17 can be written as the sum of at most 2 fourth powers, deduce that $g(4) \le 50$.