Appendix 17A: General Mordell's Theorem

We need to be a bit more formal about the possible values of p, q, r in (17.5.1). Let $H := \mathbb{Q}^*/(\mathbb{Q}^*)^2$, which means that two non-zero rational numbers whose ratio is a square are considered to be equal in H. We define a map

$$\phi : E_A(\mathbb{Q}) \to \{(a,b,c) \in H : abc = 1 \text{ in } H\} \text{ by } \phi(x,y) = (x - A, x, x + A).$$

if $x - A, x, x + A$ are all non-zero. (So if $x = m/n^2$ then $x - A = m - An^2$ in H, and this $= pq$ in H in (17.5.1).)

If $x + A = 0$ then $x - A, x$ are non-zero, and we let $\phi(P) = (x - A, x, x(x - A))$, and we define $\phi(P)$ analogously if $x = 0$ or $x - A = 0$. The identities in Proposition 17.2.1, and the proof of Proposition 17.5.1, imply that ϕ is a homomorphism. The converse theorem (Theorem 17.2) implies that $\ker \phi = 2E_A(\mathbb{Q})$. The first isomorphism theorem then implies that the image of ϕ,

$$\phi(E_A(\mathbb{Q})) \cong E_A(\mathbb{Q})/2E_A(\mathbb{Q}).$$

We have been working with $E_A^+(\mathbb{Q})$. The condition $x > A$, implies that if $P \in E_A^+(\mathbb{Q})$, each co-ordinate of $\phi(P)$ is positive, and so $\phi(E_A^+(\mathbb{Q}))$ is a subgroup of $\phi(E_A(\mathbb{Q}))$, and the quotient group, $\frac{\phi(E_A(\mathbb{Q}))}{\phi(E_A^+(\mathbb{Q}))}$, is isomorphic to $\{(1,1,1), (-1,-1,1)\}$.

Mordell's Theorem implies that $E(\mathbb{Q})/2E(\mathbb{Q}) = T/2T \oplus (\mathbb{Z}/2\mathbb{Z})^r$. We saw above how to restrict the elements of $\phi(E(\mathbb{Q}))$ to a finite set where each entry is a divisor of $2A$. It was Weil who first fully developed the role of the map ϕ. In honor of their work the group of points $E(\mathbb{Q})$ is known as the *Mordell-Weil group*.

17.7. The growth of points

Another important issue is the growth of the size of the co-ordinates after successive doubling. We define the *height* of a rational number a/b with $(a,b) = 1$ to be $H(a/b) := \max\{|a|, |b|\}$. We extend this to a point $P \in E(\mathbb{Q})$ by letting $H(P) :=$

$H(x(P))$. If $P \in E_A^+(\mathbb{Q})$ then $x(P) = m/n^2 > A$ and so $H(P) = m_P$. By Proposition 17.2.1 and exercise 17.2.3(b,c) we have that if $Q = 2^k P$ with $k \geq 2$ then $H(Q)^4 < H(2Q) < 4H(Q)^4$.

Exercise 17.7.1.‡ Let $P \in E_A^+(\mathbb{Q})$ and $Q = 4P$.
(a) Prove that $H(Q)^{4^r} < H(2^r Q) < (4^{1/3}H(Q))^{4^r}$ for all $r \geq 1$.
(b) Prove that $\lim_{k\to\infty} H(2^k P)^{1/4^k}$ 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 $H(Q) \leq \hat{H}(Q) \leq 4^{1/3}H(Q)$.

One can similarly define the Néron-Tate height for points on an arbitrary elliptic curve. However it is much more challenging to obtain suitable upper and lower bounds on $H(2P)$ in terms of $H(P)$, for the general elliptic curve.

Four squares in an arithmetic progression: If $a-d,\ a,\ a+d$ and $a+2d$ are all squares, say $u_{-1}^2, u_0^2, u_1^2, u_2^2$ then $(-2d/a - 1,\ 2u_{-1}u_0u_1u_2/a^2)$ is a point on the elliptic curve

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

In this case, Image(ϕ) is a subgroup of $\langle(-1,-1,1),(2,1,2),(1,3,3)\rangle$, which is itself a subgroup of $\{(a,b,c) \in H : abc = 1 \text{ in } H\}$. We have the elements $\phi((-1,2)) = (-2,-1,2)$ and $\phi((-3,0)) = (-1,-3,3)$ of Image(ϕ), and we now prove that $(-1,-1,1)$ is not in Image(ϕ). If it were, there would exist integers m,n,u,v,w with $(m,n) = 1$ for which $m - n^2 = -u^2, m = -v^2$ and $m + 3n^2 = w^2$. But then $-v^2 + 3n^2 = w^2$, and so $-v^2 \equiv w^2 \pmod 3$, but as $(\frac{-1}{3}) = -1$ this implies that 3 divides v and w, and so n. Therefore 3 divides $(m,n) = 1$, a contradiction.

We deduce that Image$(\phi) \cong (\mathbb{Z}/2\mathbb{Z})^2$ and so $E(\mathbb{Q})$ is all torsion, since we have four rational points of order dividing 2. One can show that

$$E(\mathbb{Q}) = \{\mathcal{O}, (1,0), (0,0), (-3,0), (3,\pm 6), (-1,\pm 2)\} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}.$$

Translating this back to the original question, yields:

Theorem 17.5 (Fermat's Theorem)**.** *There are no four squares in an arithmetic progression $a-d,\ a,\ a+d, a+2d$.*

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 $1, 1+24, 1+24\cdot 2, \ldots, 1+24(N-1)$, 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 $p_1, \cdots, p_k$ is the complete set of primes. We will colour 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 colour n as $c(n) = p_1^{r_1}\cdots p_k^{r_k}$, where r_j is the least non-negative residue of $e_j \pmod 2$ for $j = 1, \ldots, k$.
(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.