Mordell’s theorem

1 Mordell’s theorem

Theorem 1.1 [Mordell] Let $C$ be a nonsingular cubic curve with rational coefficients. Then the group $\Gamma$ of rational points on $C$ is finitely generated.

That is, there are rational points $P_1, ..., P_t$ on $C$ such that every rational point on $C$ is of the form $n_1P_1 + ... + n_tP_t$ with $n_i \in \mathbb{Z}$.

Viewing $\Gamma$ as direct product of $r$ copies of $\mathbb{Z}$ ($r \geq 0$) and some cyclic groups of prime power order, we can find generators $P_1, ..., P_r$ of infinite order and $Q_1, ..., Q_s$ of finite order, where $Q_i$ has order $p_i^{e_i}$ for some prime $p_i$, such that the representation $P = n_1P_1 + ... + n_rP_r + m_1Q_1 + ... + m_sQ_s$ is unique ($n_i \in \mathbb{Z}$, $m_i \in \mathbb{Z}/p_i^{e_i}\mathbb{Z}$).

The number $r$ is called the rank of $C$.

The group $\Gamma$ is finite if and only if $r = 0$.

It is easy to find the points of finite order.

Theorem 1.2 [Nagell-Lutz] Let $C$ be a nonsingular cubic curve with integral coefficients and equation $y^2 = x^3 + ax^2 + bx + c$, provided with the zero point $O = (0, 1, 0)$. Then the points of finite order on $C$ have integral coordinates. If $(x, y)$ has finite order, then either $y = 0$, or $y|D$, where $D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$ is the discriminant of the curve.

In the general case where $C$ has rational coefficients, one can use a coordinate transformation $x' = d^2x$, $y' = d^3y$ to make the coefficients integral.

Note that there may well be points $(x, y)$ with $y|D$ that do not have finite order. (But the points $(x, y)$ with $y = 0$ have order 2.)

The torsion group (subgroup of $\Gamma$ consisting of the elements of finite order) has restricted shape: there are only 15 possibilities.

Theorem 1.3 [Mazur] The torsion group is one of $\mathbb{Z}/n\mathbb{Z}$ ($1 \leq n \leq 10$ or $n = 12$) or $\mathbb{Z}/2m\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ($1 \leq m \leq 4$).

So it is easy to find the $Q_i$. There is no known algorithm to find the $P_i$, but there are results for very many special cases.

It is unknown whether the rank $r$ is bounded. Examples with larger $r$ are being found every year. The current champion is the curve

$$y^2 + xy + y = x^3 - x^2 - 200677624155755265850332082093338542750930230312178956502x + 348161179503055646703298569039720374855944955319180361266608296291939448732243429$$

with rank 28 found by Elkies (2006). For the record ranks for given torsion, see http://web.math.hr/~duje/tors/tors.html.
\section{Proof of Mordell’s theorem}

After a change of coordinates we may assume the curve has the equation \( y^2 = x^3 + ax^2 + bx + c \) with integral \( a, b, c \).

Define the \textit{height} of a rational number \( r = \frac{m}{n} \) (with \( \gcd(m, n) = 1 \)) by

\[ H(r) = H\left(\frac{m}{n}\right) = \max(|m|, |n|) \]

and the height of a rational point \( P = (x, y) \) on \( C \) by

\[ H(P) = H(x). \]

Also define \( H(O) = 1 \). Let the logarithmic height of \( P \) be \( h(P) := \log H(P) \).

The theorem is an easy consequence of four lemmas, the first three of which use the height function to describe the growth of coordinates under addition.

\textbf{Lemma 2.1} For any constant \( M \), the set \( \{ P \in \Gamma \mid h(P) \leq M \} \) is finite.

\textbf{Lemma 2.2} Let \( P_0 \in \Gamma \) be fixed. There is a constant \( \kappa_0 = \kappa_0(a, b, c, P_0) \) such that \( h(P + P_0) \leq 2h(P) + \kappa_0 \) for all \( P \in \Gamma \).

\textbf{Lemma 2.3} There is a constant \( \kappa = \kappa(a, b, c) \) such that \( h(2P) \geq 4h(P) - \kappa \) for all \( P \in \Gamma \).

The fourth lemma is the difficult part.

\textbf{Lemma 2.4} The subgroup \( 2\Gamma \) has finite index in \( \Gamma \).

Now the proof of Mordell’s theorem is straightforward from these lemmas. Pick representatives \( Q_1, ..., Q_n \) of the cosets of \( 2\Gamma \) in \( \Gamma \). Then for arbitrary \( P \in \Gamma \) we can write

\[ P = 2P_1 + Q_{i_1}, \]

and then

\[ P_1 = 2P_2 + Q_{i_2}, \]

\[ ... \]

\[ P_{m-1} = 2P_m + Q_{i_m}. \]

Let \( \kappa' = \kappa'(a, b, c) \) be the largest of the constants \( \kappa_0(a, b, c, -Q_i) \). Then

\[ h(P - Q_i) \leq 2h(P) + \kappa' \]

for all \( P, Q_i \)

and

\[ 4h(P_j) \leq h(2P_j) + \kappa = h(P_{j-1} - Q_{i_j}) + \kappa \leq 2h(P_{j-1}) + \kappa + \kappa' \]

so that \( h(P_m) \leq \kappa + \kappa' \) for \( m \) sufficiently large. Now

\[ \{Q_1, ..., Q_m\} \cup \{P \mid h(P) \leq \kappa + \kappa'\} \]

is a finite generating set for \( \Gamma \). \hfill \Box
3 Proof of Lemmas 1-3

Lemma 1 is clear.

Lemma 2

For Lemma 2, first observe that the denominator of \( x^3 + ax^2 + bx + c \) is that of \( x^3 \) and equals that of \( y^2 \), so that a point \( P = (x, y) \) of the curve satisfies \( x = \frac{m}{e} \) and \( y = \frac{n}{e} \) where \( m, n, e \) are integers with \( \gcd(m, e) = \gcd(n, e) = 1 \). It follows that

\[
m \leq H(P), \quad e \leq H(P)^{1/2}, \quad n \leq KH(P)^{3/2},
\]

where that last inequality is from substitution of \( x = \frac{m}{e} \) and \( y = \frac{n}{e} \) in \( y^2 = x^3 + ax^2 + bx + c \) to get \( n^2 = m^3 + am^2e^2 + bme^4 + ce^6 \leq (1 + |a| + |b| + |c|)H(P)^3 \).

Now let \( P = (x, y) \) and \( P_0 = (x_0, y_0) \) and \( P + P_0 = (\xi, \eta) \). We want to bound \( h(P + P_0) \) in terms of \( h(P) \). (W.l.o.g. \( P \neq O, P_0, -P_0 \), those finitely many points are handled by increasing \( \kappa_0 \) later. Now all points are finite and distinct.) The line \( y = \lambda x + \mu \) hits the curve \( y^2 = x^3 + ax^2 + bx + c \) in three points with \( x \)-coordinates satisfying \( (\lambda x + \mu)^2 = x^3 + ax^2 + bx + c \) and their sum is minus the coefficient of \( x^2 \). It follows that \( x + x_0 + \xi = \lambda^2 - a \), where \( \lambda = \frac{y - y_0}{x - x_0} \). Now

\[
\xi = \left( \frac{y - y_0}{x - x_0} \right)^2 - a - x_0 - x = \frac{Ag + Bx^2 + Cx + D}{Ex^4 + Fx + G}
\]

for certain integers \( A, B, C, D, E, F, G \) independent of \( x \) (where \( y^2 \) was replaced by \( x^3 + ax^2 + bx + c \), cancelling the \( x^3 \) term). Thus,

\[
H(P + P_0) = H(\xi) \leq \max(|Am + Bn^2 + Cme^2 + De^4|, |Em^2 + Fme^2 + Ge^4|)
\]

\[
\leq \max(|AK| + |B| + |C| + |D|, |E| + |F| + |G|)H(P)^2
\]

and after taking logarithms

\[
h(P + P_0) \leq 2h(P) + \kappa_0.
\]

\[ \square \]

Lemma 3

For Lemma 3, put \( P = (x, y) \) and \( 2P = (\xi, \eta) \). W.l.o.g. \( 2P \neq O \). As before we get \( 2x + \xi = \lambda^2 - a \), where \( \lambda = \frac{dy}{dx}(P) = \frac{3x^2 + 2ax + b}{2y} \), so that

\[
\xi = \lambda^2 - a - 2x = \frac{x^4 + \ldots}{4x^3 + \ldots}
\]

and numerator and denominator here have no common roots since the curve is nonsingular.

It suffices to prove the lower bound in
Lemma 3.1 Let \( f(x), g(x) \in \mathbb{Z}[x] \) be two polynomials without common roots (in \( \mathbb{C} \)). Let \( d \) be the maximum of their degrees. Then, if \( r \in \mathbb{Q}, \ g(r) \neq 0 \) then

\[
dh(r) - \kappa \leq h\left(\frac{f(r)}{g(r)}\right) \leq dh(r) + \kappa
\]

for some constant \( \kappa \) depending on \( f, g \).

Proof Since \( \gcd(f, g) = 1 \) there are \( u, v \in \mathbb{Q}(x) \) with \( u(x)f(x) + v(x)g(x) = 1 \).

For \( r = \frac{m}{n} \) (with \( \gcd(m, n) = 1 \)) let \( F(r) = n^df(r) \) and \( G(r) = n^dg(r) \) so that \( F(r) \) and \( G(r) \) are integers. Now \( u(r)F(r) + v(r)G(r) = n^d \).

Let \( A \) be the l.c.m. of the denominators of the coefficients of \( u, v \) and let \( e \) be the maximum of their degrees. Then \( \gcd(F(r), G(r)) | Aa_0^{d+e} \). On the other hand, if say \( f(x) = a_0x^d + \ldots + a_d \) has degree \( d \), then \( F(r) = a_0m^d + \ldots + a_dn^d \) and \( \gcd(n, F(r)) | a_0 \) and \( \gcd(F(r), G(r)) | Aa_0^{d+e} \).

Put \( R := Aa_0^{d+e} \). Now

\[
H\left(\frac{f(r)}{g(r)}\right) = H\left(\frac{F(r)}{G(r)}\right) \geq \frac{1}{R} \max(|F(r)|, |G(r)|)
\]

gives

\[
\frac{H\left(\frac{f(r)}{g(r)}\right)}{H(r)^e} \geq \frac{\max(|F(r)|, |G(r)|)}{R \max(|m|^d, |n|^d)} = \frac{\max(|f(r)|, |g(r)|)}{R \max(|r|^d, 1)}.
\]

The right hand side is bounded below by a positive constant \( C \) (since there is a finite nonzero limit when \( r \) tends to infinity, and a nonzero minimum on a compact piece since \( f \) and \( g \) do not vanish simultaneously. So

\[
H\left(\frac{f(r)}{g(r)}\right) \geq C.H(r)^d
\]

and

\[
h\left(\frac{f(r)}{g(r)}\right) \geq dh(r) - \kappa
\]

as desired. The other inequality is easier (and not needed). \( \square \)

4 \( 2\Gamma \) has finite index in \( \Gamma \)

Remains to prove Lemma 4. Since that is difficult, we only do a special case, namely that where \( x^3 + ax^2 + bx + c \) has a rational root \( x_0 \), that is, where there is a rational point \((x_0, 0)\) of order 2. Change coordinates so that this point becomes \((0, 0)\). Now the equation is \( y^2 = x^3 + ax^2 + bx \), that is, \( c = 0 \).

The discriminant becomes \( D = b^2(a^2 - 4b) \), and since the curve is nonsingular, this is nonzero.

Play with two curves: \( C \) defined by \( y^2 = x^3 + ax^2 + bx \) and \( \tilde{C} \) defined by \( y^2 = x^3 + \tilde{a}x^2 + bx \), where \( \tilde{a} = -2a \) and \( \tilde{b} = a^2 - 4b \).

Now \( \tilde{a} = 4a \) and \( \tilde{b} = a^2 - 4b = 16b \) so that \( \tilde{C} \) becomes the curve \( y^2 = x^3 + 4ax^2 + 16bx \), and \((x, y) \in \tilde{C} \) iff \((\frac{1}{8}x, \frac{1}{8}y) \in C \).
Define $\phi : C \to \tilde{C}$ by $(x,y) \mapsto (\tilde{x}, \tilde{y})$ with $\tilde{x} = x + \frac{a}{2} = \frac{x}{2}$ and $\tilde{y} = y(1 - \frac{a}{2})$ for $x \neq 0$, and map both $(0,0)$ and $\mathcal{O}$ to $\mathcal{O}$. Then $\phi$ is a group homomorphism with kernel $\{(0,0), \mathcal{O}\}$.

Define $\psi : C \to C$ as the composition of $\phi$ and $(x,y) \mapsto (\frac{1}{4}x, \frac{1}{8}y)$. Then $\psi$ is a group homomorphism with kernel $\{(0,0), \mathcal{O}\}$.

The composition of $\phi$ and $\psi$ is the map $P \mapsto 2P$ on $C$.

All these statements follow by straightforward computation.

The desired result that $2\Gamma$ has finite index in $\Gamma$ will follow from the two facts that $\phi \Gamma$ has finite index in $\Gamma$, and $\psi \Gamma$ has finite index in $\Gamma$. By symmetry it suffices to show one of these, say the latter.

We need a description of $\phi \Gamma$. We have

(i) $\mathcal{O} \in \phi \Gamma$.
(ii) $(0,0) \in \phi \Gamma$ iff $b = a^2 - 4b$ is a square.
(iii) $(\tilde{x}, \tilde{y}) \in \phi \Gamma$ for $\tilde{x} \neq 0$ iff $\tilde{x}$ is a square in $\mathbb{Q}$.

(Indeed, (i) is clear. We have $\tilde{x} = \frac{x^2}{2}$, so $\tilde{x}$ is a square, and $\tilde{x} = 0$ iff $y = 0$, that is, $x(x^2 + ax + b) = 0$ for some rational point $(x,y)$ with $x \neq 0$ on $C$. That is, if $a^2 - 4b$ is a square. Finally, if $\tilde{x} = r^2$, then the point $(x,y)$ with $x = \frac{1}{2}(r^2 - a + \frac{a}{2})$ and $y = xr$ lies on $C$ and maps to $(\tilde{x}, \tilde{y})$.)

Let $\mathbb{Q}^*$ be the multiplicative group of the nonzero rationals, and $\mathbb{Q}^{*2}$ the subgroup of squares. Define a map $\alpha : \Gamma \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ by $P = (x,y) \mapsto x$ for $x \neq 0$, $(0,0) \mapsto b$, $\mathcal{O} \mapsto 1$.

Now $\alpha$ is a group homomorphism: First of all, it maps the unit element $\mathcal{O}$ to the unit element 1. Suppose $P_1 + P_2 + P_3 = \mathcal{O}$. We show that $\alpha(P_1)\alpha(P_2)\alpha(P_3) = 1$. (And that suffices to prove that $\alpha$ is a homomorphism.) The points $P_1, P_2, P_3$ lie on a line $y = \lambda x + \mu$ and $x_1, x_2, x_3$ are roots of $(\lambda x + \mu)^2 = x^3 + ax^2 + bx$. The product of the roots is minus the constant term, that is, is $\mu^2$, so that $\alpha(P_1)\alpha(P_2)\alpha(P_3) = x_1x_2x_3 = \mu^2 = 1$ in $\mathbb{Q}^*/\mathbb{Q}^{*2}$. If $P_1 = (0,0)$ then $\mu = 0$ and $x_2, x_3$ are roots of $\lambda^2 x = x^3 + ax^2 + bx$ and $\alpha(P_1)\alpha(P_2)\alpha(P_3) = bx_2x_3 = b^2 = 1$ in $\mathbb{Q}^*/\mathbb{Q}^{*2}$. If $P_1 = \mathcal{O}$ then $P_2 = -P_3$ and $x_2 = x_3$ and $\alpha(P_1)\alpha(P_2)\alpha(P_3) = 1x_2x_3 = 1$ in $\mathbb{Q}^*/\mathbb{Q}^{*2}$.

Next, the image of $\alpha$ is finite (and is contained in the set of divisors of $b$): Let $P = (x,y) = (\frac{m^2}{n^2}, \frac{m}{n})$ be a point of $C$. Then $\alpha(P) = \frac{m}{n} = m$ in $\mathbb{Q}^*/\mathbb{Q}^{*2}$. From $n^2 = m(m^2 + am^2 + b^2)$ we see that each prime divisor $p$ of $m$ occurs to some even power in $m$, unless it also occurs (to an odd power) in $m^2 + am^2 + b^2$ and hence in $b^2$, and hence in $b$, since $\gcd(m,e) = 1$.

Next, from the description of the image of $\phi$ (applied to $\psi$) it is clear that the kernel of $\alpha$ is precisely the image of $\psi$. Consequently, $\alpha$ induces an isomorphism from $\Gamma/\psi(\Gamma)$ to a subgroup of $\mathbb{Q}^*/\mathbb{Q}^{*2}$ contained in the subgroup of divisors of $b$. In particular, $\Gamma/\psi(\Gamma)$ is finite. 

\qed