1.21 26/07/16 - Finishing the Proof of Mordell's Theorem and the Structure of Finitely Generated Abelian Groups

The first order of business today is to finish the proof of Mordell's Theorem.

1.21.A Wrapping up Descent via Two-Isogeny

The following discussion has been adapted from [2, §3.4].

Recall the set-up we are in: we have $K = \mathbb{Q}$ and $a, b \in \mathbb{Q}$ are such that $b(a^2 - 4b) \neq 0$, and $E/\mathbb{Q}$ is the curve $y^2 = x^3 + ax^2 + bx$, which has the nontrivial rational two-torsion point $T = (0,0) \in E[2](\mathbb{Q}) \smallsetminus \{\mathscr{O}\}$. By definition, $(a', b') := (-2a, a^2 - 4b)$, and $E'/\mathbb{Q}$ is the curve $(y')^2 = (x')^3 + a'(x')^2 + b'x'$, which as its own $T' = (0,0) \in E'[2](\mathbb{Q}) \smallsetminus \{\mathscr{O}'\}$. We have defined maps $\phi : E \to E'$ and $\phi' : E' \to E$ such that $\phi' \circ \phi = [2]_E$ (1.20.13). To prove 1.15.9 (and hence 1.15.8), it only remains to show by 1.20.3 that $E(\mathbb{Q})/\phi'(E'(\mathbb{Q}))$ is finite. This is achieved by

Theorem 1.21.1. In the above setup, let $\alpha : E(\mathbb{Q}) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ be the map given by

$$P \mapsto \begin{cases} [1] & \text{if } P = \mathscr{O}, \\ [b] & \text{if } P = T, \text{ and} \\ [x] & \text{if } P = (x, y) \in E(\mathbb{Q}) \smallsetminus \{\mathscr{O}, T\}. \end{cases}$$

Then:

(a) The map α is a group homomorphism.
(b) We have that $\ker \alpha = \phi'(E'(\mathbb{Q}))$.
(c) The image $\operatorname{Im} \alpha$ is finite.

Note that the definition of α makes sense thanks to 1.20.1(a). As in 1.19.1, we see in the proof below where the right choice of the value of $\alpha(T)$ comes from.

Proof.

(a) As in the proofs of 1.18.1, 1.19.1, and 1.20.13, we invoke 1.15.5 to reduce to showing that if $P_1, P_2, P_3 \in E(\mathbb{Q}) \smallsetminus \{\mathscr{O}\}$ are collinear (with multiplicities as usual), then $\alpha(P_1)\alpha(P_2)\alpha(P_3) = [1]$. First suppose that none of the P_i are T, so that the x-coordinates x_i of the P_i are all nonzero (1.20.1(a)). If $\ell : y = \lambda x + \nu$ is the line containing the P_i for some $\lambda, \nu \in \mathbb{Q}$, then $T \notin \ell(\mathbb{Q})$ implies $\nu \neq 0$. As in previous proofs, x_1, x_2, x_3 are the roots of

$$g(x) = (x^3 + ax^2 + bx) - (\lambda x + \nu)^2,$$

and so Vieta's formulae tell us that $x_1x_2x_3 = \nu^2$, showing that $\alpha(P_1)\alpha(P_2)\alpha(P_3) = [1]$.
Finally, as in the proof of 1.20.13, it remains to deal with the case in which $P_1 = T$ but $P_2, P_3 \neq T$, which means as above that $x_2x_3 \neq 0$. This time, we have using 1.20.10 that

$$\alpha(P_2) = \alpha(-(P_3 + T)) = \alpha(P_3 + T) = \left[\frac{b}{x_3}\right] = \frac{1}{\alpha(T)\alpha(P_3)},$$

where the last equality uses our choice of $\alpha(T)$ (this is where that comes from!). This finishes the proof.

(b) We have to show that if $P \in E(\mathbb{Q})$, then $\alpha(P) = [1]$ iff there is a $P' \in E'(\mathbb{Q})$ such that $\phi'(P') = P$. If $P = \mathscr{O}$, both sides hold and we are done. Next, let's consider the case of $P = T$. We see that $\alpha(T) = [1]$ iff b is a square, in which case $P' \in \{(a \pm 2\sqrt{b}, 0)\} = E'[2](\mathbb{Q}) \smallsetminus \{\mathscr{O}', T'\}$ have the property that $\phi'(P') = T$. Conversely, if there is such a P', then $P' \neq \mathscr{O}', T'$. If we write $P' = (x', y') \in E'(\mathbb{Q}) \smallsetminus \{\mathscr{O}', T'\}$ with $x' \neq 0$, then it follows from the formula (1.20.13) that $(x')^2 + a'x' + b' = 0$. Since x' is rational, the discriminant $a'^2 - 4b' = 16b$ is then a perfect rational square, and hence $\alpha(T) = [b] = [1]$.[10]

[10] The idea behind this proof is that $\alpha(T) = [1]$ iff $b = ((a')^2 - 4b')/16$ is a square. On the one hand, by 1.20.1(b) is

Finally, suppose that $P = (x, y) \in E(\mathbb{Q}) \smallsetminus \{\mathscr{O}, T\}$, which implies $x \neq 0$ (1.20.1(a)). If there is a $P' \in E'(\mathbb{Q})$ with $\phi'(P') = P$, then $P' \neq \mathscr{O}', T'$, and so writing $P' = (x', y')$, we see that

$$x = \frac{1}{4}\left(x' + a' + \frac{b'}{x'}\right) = \left(\frac{y'}{2x'}\right)^2,$$

which shows $\alpha(P) = [x] = [1]$. The converse is more interesting. Suppose that $\alpha(P) = [1]$, which says precisely that x is a square, say $x = u^2$ for $u \in \mathbb{Q}^\times$. The general theory (1.20.C) says there should be two points $P_1, P_2 \in E'(\mathbb{Q})$ with the property that $\phi'(P_i) = P$ for $i = 1, 2$, and a little fiddling around tells us what the coordinates of the P_i should be. Explicitly, let $x_1, x_2, y_1, y_2 \in \mathbb{Q}$ be defined by

$$x_1 := 2x + a + \frac{2y}{u}, \quad y_1 := 2ux_1, \quad x_2 := 2x + a - \frac{2y}{u}, \quad \text{and} \quad y_2 := -2ux_2.$$

We claim that $P_i := (x_i, y_i) \in E'(\mathbb{Q})$ with $\phi'(P_i) = P$ for $i = 1, 2$. Indeed, note that

$$x_1x_2 = (2x + a)^2 - \frac{4y^2}{x} = a^2 + \frac{4}{x}\left(x^3 + ax^2 - y^2\right) = b'.$$

Since $b' \neq 0$, this implies in particular that $x_1x_2 \neq 0$. Therefore, to show that $P_1 \in E'(\mathbb{Q})$, we have to show that

$$\frac{y_1^2}{x_1^2} = x_1 + a' + \frac{b'}{x_1}.$$

The left side of this is clearly $4u^2 = 4x$, and since $b' = x_1x_2$, the right side is $x_1 + a' + x_2 = 4x + 2a + a' = 4x$. Of course, a symmetric argument shows that $P_2 \in E'(\mathbb{Q})$. Finally, we show that $\phi'(P_1) = P$ simply by using the formula in 1.20.13. Indeed, the x-coordinate of $\phi'(P_1)$ is

$$x_1 + a' + \frac{b'}{x_1} = \left(\frac{y_1}{2x_1}\right)^2 = u^2 = x,$$

and the y-cooordinate is

$$\frac{1}{8} \cdot y_1 \cdot \left(1 - \frac{b'}{x_1^2}\right) = \frac{1}{8} \cdot 2ux_1 \cdot \left(1 - \frac{x_2}{x_1}\right) = \frac{u}{4}(x_1 - x_2) = \frac{u}{4} \cdot \frac{4y}{u} = y,$$

finishing the proof (the other case is, of course, symmetric).

(c) Of course, we will find a set S of primes such that $\operatorname{Im}\alpha \subset \mathbb{Q}(S, 2)$. We claim that it suffices to take $S := \{p : p \mid b\}$. Indeed, suppose that $P = (x, y) \in E(\mathbb{Q}) \smallsetminus \{\mathscr{O}, T\}$ and that p is a prime such that $v_p(x) \equiv 1 \pmod 2$; we have to show that $p \mid b$. As in 1.18.1 and 1.19.1, we use 1.14.8 to clear denominators and write P as $(m/e^2, n/e^3)$ for $m, n, e \in \mathbb{Z}$ with $\gcd(m, e) = \gcd(n, e) = 1$; then $P \in E(\mathbb{Q})$ implies after clearing denominators that

$$n^2 = m(m^2 + ame^2 + be^4).$$

Now $v_p(x) \equiv 1 \pmod 2$ implies $v_p(m) \equiv 1 \pmod 2$; since $m \in \mathbb{Z}$, this implies using the above equation that both $p \mid m$ and $p \mid m^2 + ame^2 + be^4$. These together imply that $p \mid be^4$, but again $p \nmid e$ since $\gcd(m, e) = 1$, and hence we conclude that $p \mid b$ as needed.

■

This completes the proof of 1.15.9 and hence of the Mordell Theorem (1.15.8). Let's take a second here to think how magical this is: we put a group structure on the set of points on a cubic curve, and then said something about this group structure, to conclude that (over $\mathbb{Q}$), there are finitely many "seed points" such that every other rational point can be obtained from these by repeated applications of the chord-and-tangent process.

It is clear from the above proof that the size of these "Mordell" or "Mordell-Weil" groups is controlled by the number of prime factors of b. Specifically, in the notation of 1.21.1, we see the the image $\operatorname{Im}\alpha$ of α consists of things that look like $[b_1]$, where $b_1 \in \mathbb{Z}$ is a squarefree divisor of b. Let's give a characterization using the above proof of which such b_1 occur.

equivalent to saying that $E'[2](\mathbb{Q}) \cong_{\mathsf{Ab}} \mathbb{Z}/2 \oplus \mathbb{Z}/2$. On the other hand, it is clear from the geometric picture of §1.20.C that the points P' of E' mapping to T are exactly the nontrivial 2-torsion points other than T', which exist over $\mathbb{Q}$ iff $E'[2](\mathbb{Q})$ is fully split over $\mathbb{Q}$ as above.

Corollary 1.21.2. Continuing the notation of 1.21.1, if we write $b = b_1 b_2$ for some squarefree $b_1 \in \mathbb{Z}$, then $[b_1] \in \operatorname{Im}\alpha$ iff there is a rational solution (u, v, w) to $w^2 = b_1 u^4 + a u^2 v^2 + b_2 v^4$ with not all u, v, w zero.

I learned the following short proof from Fisher.

Proof. If $b_1 = 1$ or b_2 is a square, then both sides of the implication are true (check!). Hence suppose that neither $[b_1]$ nor $[b_2]$ is $[1]$. Then $[b_1] \in \operatorname{Im}\alpha$ iff there is a $P = (x, y) \in E(\mathbb{Q}) \smallsetminus \{\mathscr{O}, T\}$ such that $x = b_1 t^2$ for some $t \in \mathbb{Q}^\times$. If this happens, then we have that

$$y^2 = b_1 t^2 \cdot (b_1^2 t^4 + a b_1 t^2 + b),$$

so that $(u, v, w) = (t, 1, y/(b_1 t))$ is a solution to $w^2 = b_1 u^4 + a u^2 v^2 + b_2 v^4$. Conversely, if (u, v, w) is a solution to $w^2 = b_1 u^4 + a u^2 v^2 + b_2 v^4$ with (u, v, w) not all zero, then in fact $uv \neq 0$, and then we can reverse-engineer what the (x, y) should be; explicitly,

$$\left(b_1 \left(\frac{u}{v}\right)^2, b_1 \left(\frac{u}{v}\right)\left(\frac{w}{v^2}\right) \right) \in E(\mathbb{Q})$$

shows us that $[b_1] \in \operatorname{Im}\alpha$. ∎

Remark 1.21.3. The equations (even curves) of the form $w^2 = b_1 u^4 + a u^2 v^2 + b_2 v^4$ are known as *homogeneous spaces*. The existence of points on these homogeneous spaces determines the rank of the corresponding elliptic curves. This can be done in lots of specific cases, as we shall see next time, but sadly there is no general algorithm known to be able to do this in all cases. This is essentially why there is no algorithmic/constructive proof of the Mordell Theorem (1.15.8).

1.21.B The Structure Theorem for Finitely Generated Abelian Groups

We have proved that if $E/\mathbb{Q}$ is an elliptic curve, then the group $E(\mathbb{Q})$ is finitely generated. Let's spend just a little bit of time reviewing what finitely generated abelian groups look like.

Clearly, a group of the form $A = \mathbb{Z}^{\oplus r} \oplus T$ for $r \in \mathbb{Z}_{\geq 0}$ and T a finite abeian group is a finitely generated abelian group. It is a fact–that needs proof–that these are all.

Theorem 1.21.4. Let A be a finitely generated abelian group. There are unique integers $r, s \in \mathbb{Z}_{\geq 0}$ and unique integers $a_1, \ldots, a_s \in \mathbb{Z}_{\geq 2}$ such that $a_1 \mid a_2 \mid \cdots \mid a_s$ and such that

$$A \cong_{\mathsf{Ab}} \mathbb{Z}^{\oplus r} \oplus \mathbb{Z}/a_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/a_s\mathbb{Z}.$$

The integer r is called the *rank* of A, and the integers a_i are called the *elementary divisors* of A.

As far as I know, the integer s doesn't have a standard name other than the "number of elementary divisors".

Proof. Let's first note the uniqueness of the invariants. If A is expressible in this form, then r can be recovered as the unique integer such that $r = \dim_{\mathbb{F}_p} A/pA$ for all but finitely many primes p. The integer s can be recovered as $\max\{\dim_{\mathbb{F}_q} A/qA\} - r$ (check!). The integer a_s can be recovered as the unique positive annihilator of $\operatorname{Tors}(A)$, i.e., the smallest positive integer a such that $a \cdot \operatorname{Tors}(A) = 0$ (check!). The other a_i's admit a similar description; I will leave this as an exercise on the next Exercise Sheet.

Let's now prove the existence of such r, s, and a_i for a given finitely generated abelian group A. Since A is finitely generated, we can pick finitely many, say $m \in \mathbb{Z}_{\geq 0}$, generators for A; this amounts to giving a surjection $\mathbb{Z}^{\oplus m} \twoheadrightarrow A$. If we let $K \subset \mathbb{Z}^{\oplus m}$ be the kernel of this surjection, then we can express this "presentation" of A via the short exact sequence

$$0 \to K \to \mathbb{Z}^{\oplus m} \to A \to 0.$$

(See 2.5.11 for a reminder on basic properties of exact sequences.) The next step is to prove

Lemma 1.21.5. Let $m \in \mathbb{Z}_{\geq 0}$, and let $K \subset \mathbb{Z}^{\oplus m}$ be a subgroup. Then there is an integer $n \in \mathbb{Z}_{\geq 0}$ with $n \leq m$ such that $K \cong_{\mathsf{Ab}} \mathbb{Z}^{\oplus n}$. In other words, a subgroup of a free abelian group of rank m is free abelian of rank at most n.

Proof. We induct on m, with the case of $m = 0$ being clear. The case $m = 1$ follows from the fact that any subgroup of $\mathbb{Z}$ has the form $c\mathbb{Z}$ for a unique $c \in \mathbb{Z}_{\geq 0}$, with the cases $n = 0$ and $n = 1$ corresponding to $c = 0$ and $c \geq 1$ respectively. Now suppose that $m \geq 2$, and that we have shown the result for $m - 1$, and that $K \subset \mathbb{Z}^{\oplus m}$ is a subgroup. Consider the projection of K to the last factor $\pi_m : K \hookrightarrow \mathbb{Z}^{\oplus m} \twoheadrightarrow \mathbb{Z}$. The image $\pi_m(K) \subset \mathbb{Z}$ is a subgroup, and hence by the above discussion is of the form $c\mathbb{Z}$ for some unique $c \in \mathbb{Z}_{\geq 0}$.

If $c = 0$, then K is actually a subgroup of $\mathbb{Z}^{\oplus(m-1)} \oplus 0 \subset \mathbb{Z}^{\oplus m}$, and hence by induction isomorphic to $\mathbb{Z}^{\oplus n}$ for some $n \leq m - 1$.

If $c \geq 1$, then since $c \in \pi_m(K)$, we can pick an $\alpha \in K$ such that $\pi_m(\alpha) = c$. We claim that α is part of a free basis of K. Explicitly, consider the intersection $K' := K \cap (\mathbb{Z}^{m-1} \oplus 0)$. By induction again, K' is isomorphic to $\mathbb{Z}^{\oplus n}$ for some $n \leq m-1$. Therefore, it suffices to show that the group homomorphism

$$\mathbb{Z} \oplus K' \to K, \quad (r, \beta) \mapsto r\alpha + \beta$$

is an isomorphism. Let's prove injectivity and surjectivity. If $(r, \beta) \in \mathbb{Z} \oplus K'$ are such that $r\alpha + \beta = 0$, then

$$0 = \pi_m(0) = \pi_m(r\alpha + \beta) = r\pi_m(\alpha) + \pi_m(\beta).$$

Since $\beta \in K'$, we have $\pi_m(\beta) = 0$. Since $\pi_m(\alpha) = c \neq 0$, this forces $r = 0$, and then $r\alpha + \beta = 0$ forces $\beta = 0$ as well; this proves injectivity. Conversely, if $\gamma \in K$, then $\pi_m(\gamma) \in \pi_m(K) = c\mathbb{Z}$ tells us that there is an integer $r \in \mathbb{Z}$ such that $\pi_m(\gamma) = rc$. If we let $\beta := \gamma - r\alpha$, then

$$\pi_m(\beta) = \pi_m(\gamma) - r\pi_m(\alpha) = 0,$$

so that $\beta \in K'$. Therefore, $(r, \beta) \in \mathbb{Z} \oplus K'$ has the property that $r\alpha + \beta = \gamma$, proving surjectivity as needed. ∎

At this point, we have a "presentation" of A of the form

$$0 \to \mathbb{Z}^{\oplus n} \xrightarrow{\varphi} \mathbb{Z}^{\oplus m} \to A \to 0,$$

which expresses A as the cokernel of the map φ. The map φ itself is given by an $m \times n$ integer matrix M. If we can perform row and column operations (over the integers, which correspond to choosing different bases of $\mathbb{Z}^{\oplus n}$ and $\mathbb{Z}^{\oplus m}$ respectively) to bring M into a particularly simple form, then we can hope to read off the isomorphism class of A from this simple form. One such simple form is known as the Smith Normal Form.

Lemma 1.21.6 (Smith Normal Form)**.** Let $m, n \in \mathbb{Z}_{\geq 0}$, and let M be an $m \times n$ integer matrix. We can perform row and column operations on M (over the integers!) to bring M into the *Smith Normal Form*, as follows: there is a unique integer $t \in \mathbb{Z}_{\geq 0}$ with $t \leq \min\{m, n\}$ and unique integers $b_1, \ldots, b_t \in \mathbb{Z}_{\geq 1}$ with $b_1 \mid \cdots \mid b_t$ such that upon performing these row and column operations, M transforms into a matrix of the form

$$M \sim \begin{bmatrix} D & 0_{t \times (n-t)} \\ 0_{(m-t) \times t} & 0_{(m-t) \times (n-t)} \end{bmatrix},$$

where $0_{a \times b}$ for $a, b \in \mathbb{Z}_{\geq 0}$ denotes the zero matrix of size $a \times b$, and D is the $t \times t$ diagonal matrix with entries b_i, i.e.,

$$D = \begin{bmatrix} b_1 & & & \\ & b_2 & & \\ & & \ddots & \\ & & & b_t \end{bmatrix}.$$

Proof. Again, let's note uniqueness first: t can be recovered as the rank (say over $\mathbb{Q}$) of the matrix M, and b_1 can be recovered as the unique positive generator (if $t \geq 1$) of the subgroup of $\mathbb{Z}$ generated by the entries of M. Similar descriptions exist also for the b_i for $i \geq 2$; again, I will leave this to you as an exercise on the next sheet.

Existence is best proved by exhibiting the following simple algorithm, which takes input (m, n, M) and returns output $(t; b_1, \ldots, b_t)$ as above.

Algorithm 1.21.7 (Smith Normal Form)**.**

Step 1. Input a triple (m, n, M), where $m, n \in \mathbb{Z}_{\geq 0}$ and M is an $m \times n$ integer matrix. Are all entries of M zero? If yes, return $t = 0$ and the empty list. Else, proceed to Step 2.

Step 2. Pick a nonzero entry c_0 of M with least positive absolute value, and perform row and column switches to bring it to the top left corner. Does the entry c_0 of the top left corner divide every entry of the matrix? If not, proceed to Step 3. If yes, proceed to Step 4.

Step 3. There is some integer c_1 in some row or column that is not divisible by c_0. Is this entry in the first row or column? If yes, proceed to Step 3a; if no, proceed to Step 3b.

Step 3a. Suppose c_1 is in the first *row* (the column case is dual). Subtract a multiple of the first *column* from the column containing c_1 to obtain an entry of smaller positive absolute value than c_0. Return to Step 2, replacing c_0 by this entry.

Step 3b. Every element of the first row and column is divisible by c_0. Subtract a multiple of the first column from each column to make all entries other than c_0 in the topmost row zero. Similarly, subtract a multiple of the first row from each row to make all entries other than c_0 in the leftmost column zero. There is still some entry c_1' not divisible by c_0, but now c_1 is not in the first row or column. By adding the row containing c_1' to the first row, put c_1' in the first row, and now do Step 3a.

Step 4. Every element of M is divisible by c_0. As in Step 3b, clear the entries of the first row and column other than c_0 (i.e., make them zero). If $c_0 < 0$, replace it by $-c_0$ by multiplying the first row by -1 to ensure $c_0 > 0$. Let M' be the matrix obtained from M by deleting the first row and column. Return to Step 1 and input $(m-1, n-1, M')$. If the output is $(t'; b_1', \ldots, b_{t'}')$, then return $(t; b_1, \ldots, b_t) := (t'+1; c_0, b_1', \ldots, b_{t'}')$.

Let's illustrate this with a quick example.

Example 1.21.8. Consider $m = 3, n = 2$, and sequence of moves on the matrix M as follows:

$$M := \begin{bmatrix} 3 & 5 \\ 0 & 2 \\ -3 & 7 \end{bmatrix} \sim \begin{bmatrix} 0 & 2 \\ 3 & 5 \\ -3 & 7 \end{bmatrix} \sim \begin{bmatrix} 2 & 0 \\ 5 & 3 \\ 7 & -3 \end{bmatrix}.$$

At this point, $c_0 = 2$ and we're in Step 3a, where we take $c_1 = 5$. Using this to proceed, we get

$$M \sim \begin{bmatrix} 2 & 0 \\ 1 & 3 \\ 7 & -3 \end{bmatrix} \sim \begin{bmatrix} 1 & 3 \\ 2 & 0 \\ 7 & -3 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 \\ 2 & -6 \\ 7 & -24 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 \\ 0 & -6 \\ 7 & -24 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 \\ 0 & -6 \\ 0 & -24 \end{bmatrix}.$$

At this point, we are in Step 4, and apply the procedure to the submatrix

$$M' := \begin{bmatrix} -6 \\ -24 \end{bmatrix} \sim \begin{bmatrix} 6 \\ -24 \end{bmatrix} \sim \begin{bmatrix} 6 \\ 0 \end{bmatrix}$$

The procedure outputs $t = 2$ and $(b_1, b_2) = (1, 6)$, i.e., the Smith Normal Form of M is

$$M \sim \begin{bmatrix} 1 & 0 \\ 0 & 6 \\ 0 & 0 \end{bmatrix}.$$

■

At this point, we are basically done. We started with a finitely generated abelian group A, and picked a presentation for it of the form

$$0 \to \mathbb{Z}^{\oplus n} \xrightarrow{\varphi} \mathbb{Z}^{\oplus m} \to A \to 0$$

for some $m, n \in \mathbb{Z}_{\geq 0}$ and map φ represented by an $m \times n$ integer matrix M. We use 1.21.6 to put the M into Smith Normal Form up to row and column operations. This expresses A as the cokernel of a matrix map in Smith Normal Form with invariants say $(t; b_1, \ldots, b_t)$. Here, it is not hard to see that we must have $t = n$ (since φ is injective, it has maximal rank), and we therefore see that A is isomorphic to

$$\mathbb{Z}/b_1\mathbb{Z} \oplus \cdots \mathbb{Z}/b_n\mathbb{Z} \oplus \mathbb{Z}^{m-n}.$$

At this point $r = m - n$. It only remains to discard all the b_is which are ones; set $s := \#\{i : b_i \neq 1\}$, and let $a_1, \ldots, a_s$ be the last s of the $b_1, \ldots, b_t$. ■

We now have a good understanding of finitely generated abelian groups. For instance, a finitely generated abelian group is finite iff it is torsion iff it has rank zero. Next time, we will use these ideas to compute the ranks of lots of elliptic curves, and derive several delicious arithmetic consequences.