18.704 Fall 2004 Homework 7 Solutions

All references are to the textbook "Rational Points on Elliptic Curves" by Silverman and Tate, Springer Verlag, 1992. Problems marked **(*)** are more challenging exercises that are optional but not required.

1. Do Exercise 3.9(a) from the text.

Solution. We use the method of section III.6. Let C be the curve $y^2 = x^3 + 3x$, and let $\Gamma = C(\mathbb{Q})$. The dual curve is $\overline{C} : y^2 = x^3 - 12x$ with group of rational points $\overline{\Gamma}$. Let $\alpha : \Gamma \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ and $\overline{\alpha} : \overline{\Gamma} \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ be defined as in III.5.

To find $|\alpha(\Gamma)|$, we need to find which divisors b_1 of $b = 3$ are in the image of α. We have $\alpha(\mathcal{O}) = 1$ and $\alpha(T) = b = 3$. Taking $b_1 = -1$, we need to check if the equation $N^2 = -M^4 - 3e^4$ has any solutions in integers (M, N, e) with $M \geq 0$. It doesn't, since the right hand side is always negative. Similarly $b_1 = -3$ leads to no solutions. So $|\alpha(\Gamma)| = 2$.

To find $|\overline{\alpha}(\overline{\Gamma})|$, we check decompositions $-12 = b_1 b_2$ and look for solutions to $n^2 = b_1 M^4 + b_2 e^4$. The possibilities are $b_1 = \pm\{1, 2, 3, 4, 6, 12\}$, but modulo rational squares we only need to consider $b_1 = \pm\{1, 2, 3, 6\}$. So $|\overline{\alpha}(\overline{\Gamma})| \leq 8$.

We know that $\overline{\alpha}(\overline{\mathcal{O}}) = 1$ and $\overline{\alpha}(\overline{T}) = b = -12 \equiv -3$ modulo squares. Considering $b_1 = 6$ and the equation $N^2 = 6M^4 - 2e^4$, we find by inspection the solution $(N, M, e) = (2, 1, 1)$. So we know that $|\overline{\alpha}(\overline{\Gamma})| \geq 3$.

Consider $b_1 = 3$ and the equation $N^2 = 3M^4 - 4e^4$. If some integer solution (N, M, e) with $M \neq 0$ exists, then since any square is congruent to 0 or 1 modulo 4, we see that the only possibility is $4|N$ and $4|M$. Then also $4|e^4$, so $2|e$. Then setting $N = 4N'$, $M = 2M'$, $e = 2e'$, we have a smaller solution (N', M', e') to the equation with $M' \neq 0$. Then we can do the same argument again and get a smaller solution, etc. But this process cannot continue forever, so in fact no solution exists in the first place. So $3 \notin \overline{\alpha}(\overline{\Gamma})$. Thus $\overline{\alpha}(\overline{\Gamma}) \leq 7$.

But finally, from the formula

$$2^r = (1/4)|\alpha(\Gamma)||\overline{\alpha}(\overline{\Gamma})|,$$

where r is the rank of Γ, it is clear that $|\overline{\alpha}(\overline{\Gamma})|$ is a power of 2. So the only possibility is $|\overline{\alpha}(\overline{\Gamma})| = 4$ and thus $r = 1$ as required.

2. This problem is again about the curve $C : y^2 = x^3 + 3x$. Even if we have found the rank of an elliptic curve (as we have for this one in problem 1), it can

be hard to find generators for the group of rational points. In this problem, I ask you to find generators for $\Gamma = C(\mathbb{Q})$. Any way you come up with for doing this is fine. The following steps outline one possible way, which you can ignore if you find a different way.

(a) By inspection, one can easily find the integer point $(1, 2)$ on C. Find all of the points on C with integer coordinates (Hint: Besides $(0, 0)$ and $(1, 2)$, I found two other integer points with positive y-coordinate, and I believe these are all of them. Note that an integer point $(x, y) \in C$ of infinite order need not satisfy the conclusion of the Nagell-Lutz theorem.)

(b)(*) Can you prove these are all of the integer points? (Since we have no theorems so far to help us find all integer points on a cubic, you'll have to invent some ad-hoc argument. I wasn't able to do it.) If you can't or choose not to solve part (b), just assume that you have all of the integer points and go on to (c).

(c) Show that if a rational point $Q = (x, y) \in C(\mathbb{Q})$ does not have integer coordinates, then mQ does not have integer coordinates for all $m \geq 1$ (Hint: review section II.4.)

(d) Prove that the set of points $\{P = (1, 2), T = (0, 0)\}$ generates the group Γ (assuming part (b) is true.) Remember this means that every element of Γ has the form $mP + nT$ for some $m, n \in \mathbb{Z}$.

Solution.

(a),(b). The curve is $y^2 = x(x^2 + 3)$. Suppose that (x, y) is an integer point on the curve such that $3 \nmid x$. Then if p is a prime dividing x, then p does not divide $x^2 + 3$. Thus in this case both x and $x^2 + 3$ must be squares. But if $x^2 + 3 = d^2$ is a square, then $d^2 - x^2 = 3$, and the only two squares differing by 3 are 1 and 4. So in this case, our point must be $(1, \pm 2)$.

Now if (x, y) is an integer point such that $3|x$, then also $3|y$ and we can write $x = 3w$, $y = 3z$. Then $9z^2 = 3w(9w^2 + 3)$ and so $z^2 = w(3w^2 + 1)$ and we are left needing to find integer solutions to this equation. Now if (w, z) is an integer point on this curve, and p is a prime dividing w, then $p \nmid 3w^2 + 1$. So w and $3w^2 + 1$ are squares. Writing $w = v^2$, we have that $3v^4 + 1$ is a square. So we have found that all integer solutions (w, z) to the equation $z^2 = w(3w^2 + 1)$ are given by $(v^2, \pm vu)$ as v ranges over all positive integers such that $3v^4 + 1$ is a square, and where $u = \sqrt{3v^4 + 1}$.

Trying values of v, we quickly see that $3(1)^4 + 1 = 4 = 2^2$ and $3(2)^4 + 1 = 49 = 7^2$. I suspect that for no other positive value of v is $3v^4 + 1$ a square, but that is the part that I don't know how to prove. In any case, we have found the points $(1, \pm 2)$ and $(4, \pm 14)$ on the curve $z^2 = w(3w^2 + 1)$, and thus the points $(3, \pm 6)$, $(12, \pm 42)$ on the original curve. We will assume for the sake of the rest of the problem that we have now found all of the integer points on C:

$$\{\mathcal{O}, (0, 0), (1, \pm 2), (3 \pm 6), (12, \pm 42).\}$$

(c) Let $P = (x, y) \in C$ be a rational point which is not an integer point. Then some prime p divides the denominator of either x or y, and then as is argued on pages 49-50 of the text, there is $\nu \geq 1$ such that $p^{2\nu}$ divides the denominator of x and $p^{3\nu}$ divides the denominator of y. In other words $P \in C(p)$ in the notation of section II.4. But the point of that section is to prove that $C(p)$ is a subgroup of $C(\mathbb{Q})$. Thus $mP \in C(p)$ for all $m \geq 1$. In particular, this means that the points mP do not have integer coordinates for all $m \geq 1$.

(d) First, we figure out how the integer points discovered in part (a) are related in the group $C(\mathbb{Q})$. The point $T = (0, 0)$ is obviously the only point of order 2 on the curve C. Put $P = (1, 2)$; we calculate from the group law that $P + T = (3, -6)$. Also we can calculate that $2P = (1/4, -7/8)$ does not have integer coordinates. But $2P + T = (12, 42)$. These calculations allow us to identify all of the integer points we found as combinations of P and T, since we also have $\mathcal{O} = 0P + 0T$, $(1, -2) = -P$, $(3, 6) = -P - T = -P + T$, and $(12, -42) = -2P - T = -2P + T$.

Now since the group $C(\mathbb{Q})$ is isomorphic to $\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, we can choose a generator Q for the $\mathbb{Z}$ part, and then T, being the only point of order 2, clearly generates the $\mathbb{Z}/2\mathbb{Z}$ part. So we will have generators Q, T for the group. Either $P = mQ$ or else $P = mQ + T$ for some nonzero $m \in \mathbb{Z}$. In the latter case, $(3, -6) = P+T = mQ+2T = mQ$ and so in any case mQ has integer coefficents. If m is negative, then clearly $-mQ$ will still have integer coefficients. Now applying part (c), the only possible conclusion is that Q has integer coefficients.

But then by our earlier calcultions, Q is in the group generated by T and P. Then since by choice of Q we know that T and Q generate $C(\mathbb{Q})$, we must also have that T and P generate $C(\mathbb{Q})$.

3. Consider the curve $C : y^2 = x^3 + px$ for some prime $p \geq 2$ with group of rational points $\Gamma = C(\mathbb{Q})$.

(a) Do Exercise 3.8(a) from the text.

(b) If $p = 73$, show that the rank of Γ is 2.

Solution. (a) This is similar to problem 1. Now we have the curve $\overline{C} : y^2 = x^3 - 4px$ with group of rational points $\overline{\Gamma}$, and again let $\alpha : \Gamma \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ and $\overline{\alpha} : \overline{\Gamma} \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ be defined as in III.5.

Once argues exactly as in the special case $p = 3$ of problem 1 that $|\alpha(\Gamma)| = 2$.

To find $|\overline{\alpha}(\overline{\Gamma})|$, we check decompositions $-4p = b_1 b_2$ and look for solutions to $n^2 = b_1 M^4 + b_2 e^4$ with $M \neq 0$. The possibilities are $b_1 = \pm\{1, 2, 4, p, 2p, 4p\}$, but modulo rational squares we only need to consider $b_1 = \pm\{1, 2, p, 2p\}$. So $|\overline{\alpha}(\overline{\Gamma})| \leq 8$. Then from the formula $2^r = (1/4)|\alpha(\Gamma)||\overline{\alpha}(\overline{\Gamma})|$ it is clear that the rank r is less than or equal to 2 as required.

(b). In case $p = 73$, we have to figure out above for which b_1 in the list $\pm\{1, 2, 73, 146\}$ we get solutions to $N^2 = b_1M^4 + b^2e^4$ with $M \neq 0$. Again, we have $\overline{\alpha}(\mathcal{O}) = 1$ and $\overline{T} = b$ so $1, -4p \equiv -73$ are in the image of $\overline{\alpha}$. Now we find by inspection that $N^2 = 73M^4 - 4e^4$ has the solution $(N, M, e) = (3, 1, 2)$, and so symmetrically $N^2 = -4M^4 + 73e^4$ has the solution $(3, 2, 1)$. Finally, we find that $N^2 = 146M^4 - 2e^4$ has the solution $(12, 1, 1)$. So we have shown that 73, -4 (which is $\equiv -1$ modulo squares), and 146 are also in the image of $\overline{\alpha}$. Altogether we see that $|\overline{\alpha}(\overline{C})|$, which must be a power of 2, is greater than or equal to 5. So $|\overline{\alpha}(\overline{C})| = 8$ and $r = 2$ in this case.

4. Let C be the singular cubic curve $y^2 = x^3$. We have seen that if $\Gamma_{ns} = C(\mathbb{Q}) \setminus \{(0, 0)\}$ is defined to be the set of rational points on C excluding the singular point $(0, 0)$, then Γ_{ns} is a group (with identity point $[0, 1, 0]$ at infinity as usual, and the group law defined in the same way as for nonsingular curves.) In the following steps we will prove part (b) of the Theorem on page 100.

(a) Do Exercise 3.10(a) from the text. The formulas given in this problem do not work for all possible choices of points P, Q; what are the exceptions?

(b) Do Exercise 3.11 from the text. Note that the formula given there needs a minor correction, and that the exceptions to the formula of part (a) need to be dealt with.

(c) So Exercise 3.13(a) from the text. (Hint: it is enough to prove that given any finite set of rational numbers $q_1, q_2, \ldots q_m$, the set

$$\{a_1q_1 + a_2q_2 + \cdots + a_mq_m | a_1, a_2, \ldots, a_m \in \mathbb{Z}\}$$

is not all of $\mathbb{Q}$).

Solution. (a) Since a fair amount of this problem is routine calculation, I will only sketch the proof. We use the same addition formulas as always. So given two nonsingular points $P = (x_1, y_1), Q = (x_2, y_2) \in \Gamma_{ns}$,

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

is the slope of the line through P, Q, and the equation of the line is $y = \lambda x + \nu$ where ν has the formula given in the problem:

$$\nu = \frac{y_1x_2 - x_1y_2}{x_2 - x_1}.$$

Then if $P + Q = (x_3, y_3)$, then $x_3 = \lambda^2 - x_1 - x_2$ and $y_3 = -\lambda x_3 - \nu$. I leave it to you to verify using also the relations $x_1^3 = y_1^2$ and $x_2^3 = y_2^2$ that

$$(x_3, y_3) = \left(\frac{\nu^2}{x_1x_2}, \frac{\nu^3}{y_1y_2}\right).$$

If either P or Q is $\mathcal{O}$ then this formula doesn't work, but we know how to find the sum in that case. Of course neither P nor Q is allowed to be the singular point $(0,0)$, which isn't even in the group. Finally, if $P = Q$ then the formula above is also not correct and one needs a separate formula for that case.

(b) We define $\phi(P) = x/y$ if $P = (x, y)$ is an affine point, but we want to define $\phi(\mathcal{O}) = 0$ (not 1 as stated in the exercise.) Now given distinct points $P = (x_1, y_1)$, $Q = (x_2, y_2)$ not equal to $\mathbb{O}$, one computes $(x_3, y_3) = P + Q$ as in part (a), and from that formula, we get $x_3/y_3 = (y_1y_2)/(x_1x_2\nu)$. Thus to prove ϕ is a homomorphism one needs to show that

$$\frac{y_1y_2}{(x_1x_2\nu)} = \frac{x_1}{y_1} + \frac{x_2}{y_2}.$$

Again this is a straightforward calculation (using $x_1^3 = y_1^2$ and $x_2^3 = y_2^2$) which I leave to you. To finish the proof that ϕ is a homomorphism, one needs to deal with the case $P = Q$, either arguing by continuity, or else by using separate formulas for that case.

Once we know ϕ is a homomorphism, to prove it is bijective it is enough to demonstrate an inverse map. Defining $\psi : \mathbb{Q} \to C_{ns}(\mathbb{Q})$ by $q \mapsto (q^{-2}, q^{-3})$ if $q \neq 0$ and $0 \mapsto \mathcal{O}$, it is easy to check that ϕ and ψ are inverses as maps of sets.

(c) Given any finite set of rational numbers $q_1, q_2, \ldots, q_m$, any integer combination $a_1q_1 + a_2q_2 + \cdots + a_mq_m$ with $a_1, a_2, \ldots, a_m \in \mathbb{Z}$, when written in lowest terms, will have a denominator no bigger than the least common multiple of the denominators of the q_i. Since $\mathbb{Q}$ contains elements with arbitrarily large denominators, there is no way every element of $\mathbb{Q}$ can be expressed this way. So $(\mathbb{Q}, +)$ is not a finitely generated group. Since by part (b) this group is isomorphic to $C_{ns}(\mathbb{Q})$, that group is also not finitely generated.