

# Mathematics 191: Finding Rational Points on Elliptic Curves

Gagan Tara Nanda

05<sup>th</sup> November, 2003

## 1 Introduction

In this article, we shall use the machinery provided in §III.6 of the text to find rational points on specific elliptic curves. We assume the reader is familiar with most of the material in this section. Before proceeding with the examples, we shall provide some of the relevant and important results that we shall need.

## 2 Some Preliminaries

We denote the equation of an elliptic curve by

$$C : y^2 = x^3 + ax^2 + bx.$$

By Mordell's Theorem, we know that the group of rational points on  $C$  is a finitely generated abelian group. The fundamental theorem on abelian groups then tells us that

$$\Gamma \cong \underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{r \text{ times}} \oplus \mathbb{Z}_{p_1^{e_1}} \oplus \mathbb{Z}_{p_2^{e_2}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{e_s}}.$$

The integer  $r$  is called the rank of  $\Gamma$ . The group  $\Gamma$  will be finite if and only if it has rank  $r = 0$ . There is another way of expressing the rank of  $\Gamma$ :

$$2^r = \frac{\#\alpha(\Gamma) \cdot \#\bar{\alpha}(\bar{\Gamma})}{4},$$

where  $\alpha$  is a homomorphism

$$\alpha : \Gamma \rightarrow \mathbb{Q}^*/\mathbb{Q}^{*2} \text{ defined by } \begin{cases} \alpha(x, y) = x \pmod{\mathbb{Q}^{*2}} \\ \alpha(T) = b \pmod{\mathbb{Q}^{*2}} \end{cases}.$$

Note that  $T = (0, 0)$ . We now give a general procedure for finding the order of  $\alpha(\Gamma)$ . We take the integer  $b$  and factor it as a product  $b = b_1 b_2$  in all possible ways. For each way of factoring, we consider the equation

$$N^2 = b_1 M^4 + a M^2 e^2 + b_2 e^4. \tag{1}$$

Here,  $a, b_1, b_2$  are fixed, and  $M, e, N$  are variables. Then  $\alpha(\Gamma)$  consists of  $b \pmod{\mathbb{Q}^{*2}}$ , together with those  $b_1 \pmod{\mathbb{Q}^{*2}}$  such that (1) has a solution  $(M, e, N)$  with  $M \neq 0$ . The new point obtained on the curve is given by

$$x = \frac{b_1 M^2}{e^2} \text{ and } y = \frac{b_1 M N}{e^3}.$$

It is important to note that any admissible solution  $(M, e, N)$  must also satisfy

$$\gcd(M, e) = \gcd(N, e) = \gcd(b_1, e) = \gcd(b_2, M) = \gcd(M, N) = 1.$$

### 3 Example 1

In our first example, we consider the two curves

$$\begin{aligned} C & : y^2 = x^3 - x, \\ \overline{C} & : y^2 = x^3 + 4x. \end{aligned} \tag{2}$$

Recall that our general elliptic curve is represented by the equation  $y^2 = x^3 + ax^2 + bx$ , so in (2), we have  $a = 0$  and  $b = -1$ . We first factor  $b$  into all possible factors  $b_1$ . Since

$$-1 = -1 \times 1 \text{ and } -1 = 1 \times -1,$$

we see that  $b_1 = \pm 1$ . Recall that the homomorphism  $\alpha : \Gamma \rightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$  has the properties  $\alpha(\mathcal{O}) = 1$  and  $\alpha(T) = b = -1$ . Let  $\Gamma$  be the group of rational points on  $C$ . Observe that

$$a^2 - 4b = 0 + 4 = (\pm 2)^2,$$

so  $\alpha(\Gamma)$  contains

$$\frac{-a \pm 2}{2} = \pm 1.$$

If we let  $b_1 = 1$  and  $b_2 = -1$ , then the equations

$$\begin{aligned} N^2 & = b_1 M^4 + a M^2 e^2 + b_2 e^4, \\ N^2 & = b_2 M^4 + a M^2 e^2 + b_1 e^4, \end{aligned}$$

are equivalent to the equations

$$N^2 = \left( \frac{-a \pm d}{2} \right) M^4 + a M^2 e^2 + \left( \frac{-a \mp d}{2} \right) e^4.$$

Thus  $\alpha(\Gamma) = \{\pm 1 \pmod{\mathbb{Q}^{*2}}\}$ , which is a group with two elements. Next we need to find  $\overline{\alpha}(\overline{\Gamma})$ , so we shall have to find all possible factors of  $\overline{b} = 4$ . We can choose

$$\overline{b}_1 = \pm 1, \pm 2, \pm 4.$$

Since  $\mathbb{Q}^{*2}$  is the subgroup of squares of elements of  $\mathbb{Q}^*$ , we have

$$\begin{aligned} 4 & \equiv 1 \pmod{\mathbb{Q}^{*2}}, \\ -4 & \equiv -1 \pmod{\mathbb{Q}^{*2}}. \end{aligned}$$

So  $\overline{\alpha}(\overline{\Gamma})$  consists of at most four elements — the elements of  $\{1, -1, 2, -2\}$ . Recall that  $\overline{b} \in \overline{\alpha}(\overline{\Gamma})$ , but since  $\overline{b} = 4$  is a square, we don't get any new information from here. We thus consider the following four equations:

$$N^2 = M^4 + 4e^4, \tag{3}$$

$$N^2 = -M^4 - 4e^4, \tag{4}$$

$$N^2 = 2M^4 - 2e^4, \tag{5}$$

$$N^2 = -2M^4 + 2e^4. \tag{6}$$

With the restriction  $M \neq 0$  and since  $N^2 \geq 0$ , we see that (4) and (6) have no solutions in real numbers, since their right-hand sides are strictly negative. In particular, (4) and (6) have no solutions in integers. Observe that

(3) has the solution  $(M, e, N) = (1, 0, 1)$ , which corresponds to the fact that  $\bar{b}_1 = 1 \in \bar{\alpha}(\bar{\Gamma})$ . Next we see that  $\#\alpha(\Gamma) \cdot \#\bar{\alpha}(\bar{\Gamma})$  is at least four. Since  $\#\alpha(\Gamma) = 2$ , we have  $\#\bar{\alpha}(\bar{\Gamma}) \geq 2$ , so  $\bar{\alpha}(\bar{\Gamma})$  must have order at least two. This implies that (5) has a solution. In fact, it isn't too hard to see that (5) has the solution  $(M, e, N) = (1, 1, 2)$ . We thus conclude that  $\bar{\alpha}(\bar{\Gamma})$  has order exactly two. Then

$$2^r = \frac{\#\alpha(\Gamma) \cdot \#\bar{\alpha}(\bar{\Gamma})}{4} = \frac{2 \cdot 2}{4} = 1 \Rightarrow r = 0,$$

so the rank of  $\Gamma$  is 0, as is the rank of  $\bar{\Gamma}$ . This shows that the group of rational points on  $C$  and  $\bar{C}$  are each finite, and so all the rational points have finite order. We now use the Nagell-Lutz Theorem to find these points. If  $P = (x, y)$  is a point of finite order in  $\Gamma$ , then either  $y = 0$  or  $y$  divides  $b^2(a^2 - 4b) = 4$ . Note that

$$x^3 - x = x(x^2 - 1) = 0 \Rightarrow x = 0, \pm 1,$$

so the points with  $y = 0$  are  $(0, 0)$  and  $(\pm 1, 0)$ . It can be checked that there are no points with  $y = \pm 1, \pm 2, \pm 4$ . So the group of rational points on  $C$  is precisely

$$\Gamma = \{\mathcal{O}, (0, 0), (1, 0), (-1, 0)\} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z},$$

since each point has order 1 or 2. Similarly, the points of finite order in  $\bar{\Gamma}$  satisfy either  $y = 0$  or  $y$  divides  $\bar{b}^2(\bar{a}^2 - 4\bar{b}) = -256$ . We have

$$x^3 + 4x = x(x^2 + 4) = 0 \Rightarrow x = 0,$$

so one point is  $(0, 0)$ . It can be checked that the only values of  $y$  dividing  $-256$  that yield integer points on  $\bar{C}$  are  $y = \pm 4$ , in which case  $x = 2$ . Thus the group of rational points on  $\bar{C}$  is

$$\bar{\Gamma} = \{\mathcal{O}, (0, 0), (2, 4), (2, -4)\} \cong \mathbb{Z}/4\mathbb{Z},$$

which is a cyclic group of order four. Note that we could have also obtained the third point as follows:

$$(b_1, M, e, N) = (2, 1, 1, 2) \Rightarrow x = \frac{b_1 M^2}{e^2} = 2 \text{ and } y = \frac{b_1 M N}{e^3} = 4.$$

## 4 Example 2

Now we consider the elliptic curves

$$\begin{aligned} C &: y^2 = x^3 - 5x, \\ \bar{C} &: y^2 = x^3 + 20x. \end{aligned} \tag{7}$$

In (7), we have  $a = 0$  and  $b = -5$ , so the possibilities for  $b_1$  are  $\pm 1, \pm 5$ . The equations to consider are

$$N^2 = M^4 - 5e^4, \tag{8}$$

$$N^2 = -M^4 + 5e^4, \tag{9}$$

$$N^2 = 5M^4 - e^4, \tag{10}$$

$$N^2 = -5M^4 + e^4. \tag{11}$$

Note that (8) and (9) are the same as (11) and (10), respectively, with the variables  $M$  and  $e$  interchanged, so we need only consider solutions to (8) and (9). After some trial-and-error, we see that  $(M, e, N) = (3, 2, 1)$  is a solution to (8), since

$$1^2 = 3^4 - 5 \cdot 2^4.$$

Also,  $(M, e, N) = (1, 1, 2)$  is a solution to (9), since

$$2^2 = -1^4 + 5 \cdot 1^4.$$

So all four equations (8) – (11) have solutions, and so

$$\alpha(\Gamma) = \{\pm 1, \pm 5 \pmod{\mathbb{Q}^{*2}}\},$$

which is the Klein Four Group. We thus get the rational points on  $C$ :

$$\begin{aligned} (b_1, M, e, N) &= (1, 3, 2, 1) \Rightarrow x = \frac{9}{4} \text{ and } y = \pm \frac{3}{8}; \\ (b_1, M, e, N) &= (-1, 1, 1, 2) \Rightarrow x = -1 \text{ and } y = \pm 2; \\ (b_1, M, e, N) &= (5, 1, 1, 2) \Rightarrow x = 5 \text{ and } y = \pm 10; \\ (b_1, M, e, N) &= (-5, 2, 3, 1) \Rightarrow x = -\frac{20}{9} \text{ and } y = \pm \frac{10}{27}. \end{aligned}$$

Now we wish to find  $\bar{\alpha}(\bar{\Gamma})$ . Here,  $\bar{b} = 20$ , so the possibilities for  $\bar{b}_1$  are

$$\bar{b}_1 = \pm 1, \pm 2, \pm 4, \pm 5, \pm 10, \pm 20.$$

However,  $\pm 4 = \pm 2^2$ , and  $\pm 20 = \pm (5 \cdot 2^2)$ , so the only possibilities for  $\bar{b}_1$  modulo squares are  $\pm 1, \pm 2, \pm 5, \pm 10$ . Next we observe that since  $\bar{b} = \bar{b}_1 \bar{b}_2 = 20 > 0$ , both  $\bar{b}_1$  and  $\bar{b}_2$  will have the same sign. If they are negative, then the equation

$$N^2 = \bar{b}_1 M^4 + \bar{b}_2 e^4$$

will have a strictly negative right-hand side, and hence no non-zero rational solutions. So we have simplified our guess to

$$\bar{\alpha}(\bar{\Gamma}) \subseteq \{1, 2, 5, 10 \pmod{\mathbb{Q}^{*2}}\}.$$

We know that  $\bar{\alpha}(\bar{\mathcal{O}}) = 1$  and  $\bar{\alpha}(\bar{\Gamma}) = \bar{b} = 20 \equiv 5 \pmod{\mathbb{Q}^{*2}}$  are both in  $\bar{\alpha}(\bar{\Gamma})$ . We shall next show that we can eliminate  $\bar{b}_1 = 2$  and  $\bar{b}_1 = 10$ . We need to check if the equation

$$N^2 = 2M^4 + 10e^4 \tag{12}$$

has a solution in integers. It is enough to show that there are no solutions with

$$\gcd(b_2, M) = \gcd(10, M) = 1.$$

Suppose that there is a solution to (12). Since  $(M, 5) = 1$ , we know from Fermat's Little Theorem that  $M^4 \equiv 1 \pmod{5}$ . So reducing (12) modulo 5, we get

$$N^2 \equiv 2 \pmod{5}. \tag{13}$$

However, (13) has no solutions, from which we conclude that (12) has no solutions with  $\gcd(M, 10) = 1$ . So  $2 \notin \bar{\alpha}(\bar{\Gamma})$ . We can similarly show that  $10 \notin \bar{\alpha}(\bar{\Gamma})$ . There is an alternate, and easier, way of showing this. Since  $\bar{\alpha}(\bar{\Gamma})$  is a subgroup of  $\mathbb{Q}^*/\mathbb{Q}^{*2}$  and we know that 5 is in this subgroup but 2 is not, then we immediately see that 10 is not in this subgroup. So we conclude that

$$\bar{\alpha}(\bar{\Gamma}) = \{1, 5 \pmod{\mathbb{Q}^{*2}}\}.$$

Then we see that

$$2^r = \frac{\#\alpha(\Gamma) \cdot \#\bar{\alpha}(\bar{\Gamma})}{4} = \frac{4 \cdot 2}{4} = 2 \Rightarrow r = 1,$$

which means the rank of  $\Gamma$  is 1. Hence  $C$  has an infinite number of rational points.