6
Elliptic Curves

We introduce elliptic curves and describe how to put a group structure on the set of points on an elliptic curve. We then apply elliptic curves to two cryptographic problems—factoring integers and constructing public-key cryptosystems. Elliptic curves are believed to provide good security with smaller key sizes, something that is very useful in many applications, e.g., if we are going to print an encryption key on a postage stamp, it is helpful if the key is short! Finally, we consider elliptic curves over the rational numbers, and briefly survey some of the key ways in which they arise in number theory.

6.1 The Definition

Definition 6.1.1 (Elliptic Curve). An *elliptic curve* over a field K is a curve defined by an equation of the form

$$y^2 = x^3 + ax + b,$$

where $a, b \in K$ and $-16(4a^3 + 27b^2) \neq 0$.

The condition that $-16(4a^3 + 27b^2) \neq 0$ implies that the curve has no "singular points", which will be essential for the applications we have in mind (see Exercise 6.1).

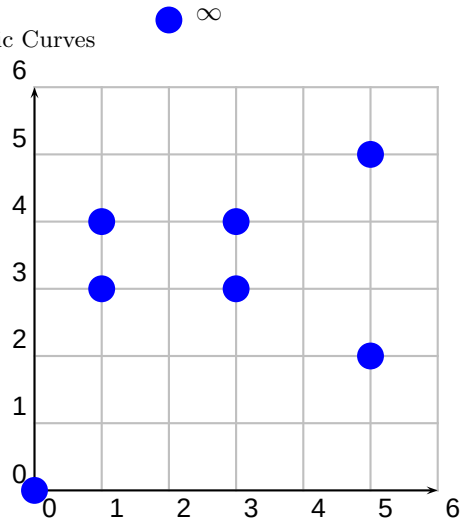

FIGURE 6.1. The Elliptic Curve $y^2 = x^3 + x$ over $\mathbf{Z}/7\mathbf{Z}$

In Section 6.2 we will put a natural abelian group structure on the set

$$E(K) = \{(x, y) \in K \times K : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$$

of K-rational points on an elliptic curve E over K. Here $\mathcal{O}$ may be thought of as a point on E "at infinity". In Figure 6.1 we graph $y^2 = x^3 + x$ over the finite field $\mathbf{Z}/7\mathbf{Z}$, and in Figure 6.2 we graph $y^2 = x^3 + x$ over the field $K = \mathbf{R}$ of real numbers.

Remark 6.1.2. If K has characteristic 2 (e.g., $K = \mathbf{Z}/2\mathbf{Z}$), then for any choice of a, b, the quantity $-16(4a^3 + 27b^2) \in K$ is 0, so according to Definition 6.1.1 there are no elliptic curves over K. There is a similar problem in characteristic 3. If we instead consider equations of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

we obtain a more general definition of elliptic curves, which correctly allows for elliptic curves in characteristic 2 and 3; these elliptic curves are popular in cryptography because arithmetic on them is often easier to efficiently implement on a computer.

6.2 The Group Structure on an Elliptic Curve

Let E be an elliptic curve over a field K, given by an equation $y^2 = x^3 + ax + b$. We begin by defining a binary operation $+$ on $E(K)$.

Algorithm 6.2.1 (Elliptic Curve Group Law). Given $P_1, P_2 \in E(K)$, this algorithm computes a third point $R = P_1 + P_2 \in E(K)$.

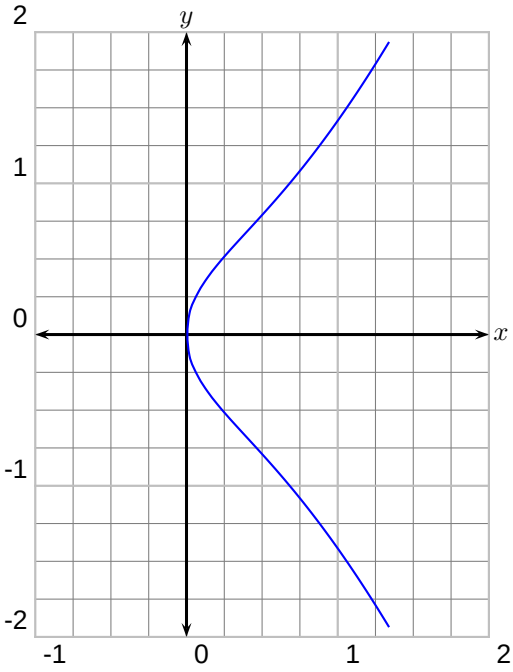

FIGURE 6.2. The Elliptic Curve $y^2 = x^3 + x$ over $\mathbf{R}$

1. [Is $P_i = \mathcal{O}$?] If $P_1 = \mathcal{O}$ set $R = P_2$ or if $P_2 = \mathcal{O}$ set $R = P_1$ and terminate. Otherwise write $(x_i, y_i) = P_i$.
2. [Negatives] If $x_1 = x_2$ and $y_1 = -y_2$, set $R = \mathcal{O}$ and terminate.
3. [Compute λ] Set $\lambda = \begin{cases} (3x_1^2 + a)/(2y_1) & \text{if } P_1 = P_2, \\ (y_1 - y_2)/(x_1 - x_2) & \text{otherwise.} \end{cases}$
4. [Compute Sum] Then $R = \left(\lambda^2 - x_1 - x_2, -\lambda x_3 - \nu\right)$, where $\nu = y_1 - \lambda x_1$ and $x_3 = \lambda^2 - x_1 - x_2$ is the x-coordinate of R.

Note that in Step 3 if $P_1 = P_2$, then $y_1 \neq 0$; otherwise, we would have terminated in the previous step.

We implement this algorithm in Section 7.6.1.

Theorem 6.2.2. *The binary operation + defined above endows the set $E(K)$ with an abelian group structure, in which $\mathcal{O}$ is the identity element.*

Before discussing why the theorem is true, we reinterpret + geometrically, so that it will be easier for us to visualize. We obtain the sum $P_1 + P_2$ by finding the third point P_3 of intersection between E and the line L determined by P_1 and P_2, then reflecting P_3 about the x-axis. (This description requires suitable interpretation in cases 1 and 2, and when $P_1 = P_2$.) This is illustrated in Figure 6.3, in which $(0, 2) + (1, 0) = (3, 4)$

on $y^2 = x^3 - 5x + 4$. To further clarify this geometric interpretation, we prove the following proposition.

Proposition 6.2.3 (Geometric group law). *Suppose $P_i = (x_i, y_i)$, $i = 1, 2$ are distinct point on an elliptic curve $y^2 = x^3+ax+b$, and that $x_1 \neq x_2$. Let L be the unique line through P_1 and P_2. Then L intersects the graph of E at exactly one other point*

$$Q = \left(\lambda^2 - x_1 - x_2, \quad \lambda x_3 + \nu\right),$$

where $\lambda = (y_1 - y_2)/(x_1 - x_2)$ and $\nu = y_1 - \lambda x_1$.

Proof. The line L through P_1, P_2 is $y = y_1 + (x - x_1)\lambda$. Substituting this into $y^2 = x^3 + ax + b$ we get

$$(y_1 + (x - x_1)\lambda)^2 = x^3 + ax + b.$$

Simplifying we get $f(x) = x^3-\lambda^2x^2+\cdots = 0$, where we omit the coefficients of x and the constant term since they will not be needed. Since P_1 and P_2 are in $L\cap E$, the polynomial f has x_1 and x_2 as roots. By Proposition 2.5.2, the polynomial f can have at most three roots. Writing $f = \prod(x - x_i)$ and equating terms, we see that $x_1 + x_2 + x_3 = \lambda^2$. Thus $x_3 = \lambda^2 - x_1 - x_2$, as claimed. Also, from the equation for L we see that $y_3 = y_1 + (x_3 - x_1)\lambda = \lambda x_3 + \nu$, which completes the proof. □

To prove Theorem 6.2.2 means to show that + satisfies the three axioms of an abelian group with $\mathcal{O}$ as identity element: existence of inverses, commutativity, and associativity. The existence of inverses follows immediately from the definition, since $(x, y) + (x, -y) = \mathcal{O}$. Commutativity is also clear from the definition of group law, since in parts 1–3, the recipe is unchanged if we swap P_1 and P_2; in part 4 swapping P_1 and P_2 does not change the line determined by P_1 and P_2, so by Proposition 6.2.3 it does not change the sum $P_1 + P_2$.

It is more difficult to prove that + satisfies the associative axiom, i.e., that $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$. This fact can be understood from at least three points of view. One is to reinterpret the group law geometrically (extending Proposition 6.2.3 to all cases), and thus transfer the problem to a question in plane geometry. This approach is beautifully explained with exactly the right level of detail in [ST92, §I.2]. Another approach is to use the formulas that define + to reduce associativity to checking specific algebraic identities; this is something that would be extremely tedious to do by hand, but can be done using a computer (also tedious). A third approach (see e.g. [Sil86] or [Har77]) is to develop a general theory of "divisors on algebraic curves", from which associativity of the group law falls out as a natural corollary. The third approach is the best, because it opens up many new vistas; however we will not pursue it further because it is beyond the scope of this book.

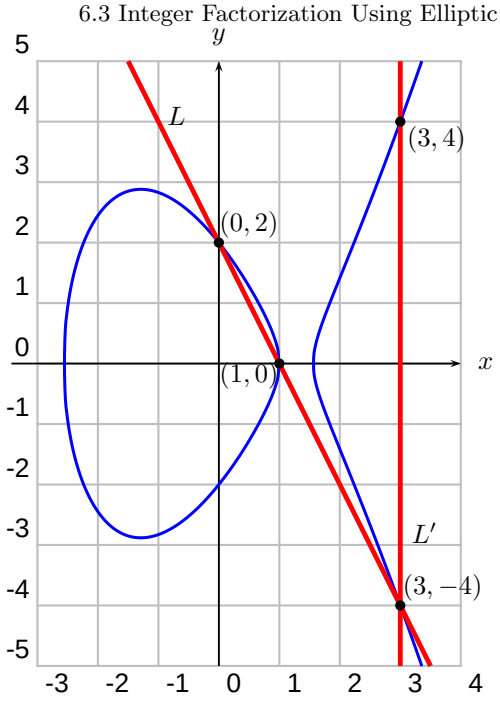

FIGURE 6.3. The Group Law: $(1,0)+(0,2)=(3,4)$ on $y^2=x^3-5x+4$

6.3 Integer Factorization Using Elliptic Curves

In 1987, Hendrik Lenstra published the landmark paper [Len87] that introduces and analyzes the Elliptic Curve Method (ECM), which is a powerful algorithm for factoring integers using elliptic curves. Lenstra's method is also described in [ST92, §IV.4], [Dav99, §VIII.5], and [Coh93, §10.3].

Lenstra

Lenstra's algorithm is well suited for finding "medium sized" factors of an integer N, which today means 10 to 20 decimal digits. The ECM method is not *directly* used for factoring RSA challenge numbers (see Section 1.1.3), but it is used on auxiliary numbers as a crucial step in the "number field sieve", which is the best known algorithm for hunting for such factorizations. Also, implementation of ECM typically requires little memory.

6.3.1 Pollard's $(p-1)$-Method

Lenstra's discovery of ECM was inspired by Pollard's $(p-1)$-method, which we describe in this section.

Definition 6.3.1 (Power smooth). Let B be a positive integer. If n is a positive integer with prime factorization $n = \prod p_i^{e_i}$, then n is *B-power smooth* if $p_i^{e_i} \leq B$ for all i.

Thus $30 = 2 \cdot 3 \cdot 5$ is B power smooth for $B = 5, 7$, but $150 = 2 \cdot 3 \cdot 5^2$ is not 5-power smooth (it is $B = 25$-power smooth).

We will use the following algorithm in both the Pollard $p-1$ and elliptic curve factorization methods.

Algorithm 6.3.2 (Least Common Multiple of First B Integers). Given a positive integer B, this algorithm computes the least common multiple of the positive integers up to B.

1. [Sieve] Using, e.g., the Sieve of Eratosthenes (Algorithm 1.2.3), compute a list P of all primes $p \leq B$.
2. [Multiply] Compute and output the product $\prod_{p \in P} p^{\lfloor \log_p(B) \rfloor}$.

Proof. Let $m = \operatorname{lcm}(1, 2, \ldots, B)$. Then

$$\operatorname{ord}_p(m) = \max(\{\operatorname{ord}_p(n) : 1 \leq n \leq B\}) = \operatorname{ord}_p(p^r),$$

where p^r is the largest power of p that satisfies $p^r \leq B$. Since $p^r \leq B < p^{r+1}$, we have $r = \lfloor \log_p(B) \rfloor$. □

We implement Algorithm 6.3.2 in Section 7.6.2.

Let N be a positive integer that we wish to factor. We use the Pollard $(p-1)$-method to look for a nontrivial factor of N as follows. First we choose a positive integer B, usually with at most six digits. Suppose that there is a prime divisor p of N such that $p-1$ is B-power smooth. We try to find p using the following strategy. If $a > 1$ is an integer not divisible by p then by Theorem 2.1.12,

$$a^{p-1} \equiv 1 \pmod{p}.$$

Let $m = \operatorname{lcm}(1, 2, 3, \ldots, B)$, and observe that our assumption that $p-1$ is B-power smooth implies that $p - 1 \mid m$, so

$$a^m \equiv 1 \pmod{p}.$$

Thus

$$p \mid \gcd(a^m - 1, N) > 1.$$

If $\gcd(a^m - 1, N) < N$ also then $\gcd(a^m - 1, N)$ is a nontrivial factor of N. If $\gcd(a^m - 1, N) = N$, then $a^m \equiv 1 \pmod{q^r}$ for every prime power divisor q^r of N. In this case, repeat the above steps but with a smaller choice of B or possibly a different choice of a. Also, it is a good idea to check from the start whether or not N is not a perfect power M^r, and if so replace N by M. We formalize the algorithm as follows:

Algorithm 6.3.3 (Pollard $p-1$ Method). Given a positive integer N and a bound B, this algorithm attempts to find a nontrivial factor m of N. (Each prime $p \mid m$ is likely to have the property that $p-1$ is B-power smooth.)

1. [Compute lcm] Use Algorithm 6.3.2 to compute $m = \operatorname{lcm}(1, 2, \ldots, B)$.
2. [Initialize] Set $a = 2$.
3. [Power and gcd] Compute $x = a^m - 1 \pmod{N}$ and $g = \gcd(x, N)$.
4. [Finished?] If $g \neq 1$ or N, output g and terminate.
5. [Try Again?] If $a < 10$ (say), replace a by $a + 1$ and go to step 3. Otherwise terminate.

We implement Algorithm 6.3.3 in Section 7.6.2.

For fixed B, Algorithm 6.3.3 often splits N when N is divisible by a prime p such that $p-1$ is B-power smooth. Approximately 15% of primes p in the interval from 10^{15} and $10^{15}+10000$ are such that $p-1$ is 10^6 power-smooth, so the Pollard method with $B = 10^6$ already fails nearly 85% of the time at finding 15-digit primes in this range (see also Exercise 7.14). We will not analyze Pollard's method further, since it was mentioned here only to set the stage for the elliptic curve factorization method.

The following examples illustrate the Pollard $(p-1)$-method.

Example 6.3.4. In this example, Pollard works perfectly. Let $N = 5917$. We try to use the Pollard $p-1$ method with $B = 5$ to split N. We have $m = \operatorname{lcm}(1, 2, 3, 4, 5) = 60$; taking $a = 2$ we have

$$2^{60} - 1 \equiv 3416 \pmod{5917}$$

and

$$\gcd(2^{60} - 1, 5917) = \gcd(3416, 5917) = 61,$$

so 61 is a factor of 5917.

Example 6.3.5. In this example, we replace B by larger integer. Let $N = 779167$. With $B = 5$ and $a = 2$ we have

$$2^{60} - 1 \equiv 710980 \pmod{779167},$$

and $\gcd(2^{60} - 1, 779167) = 1$. With $B = 15$, we have

$$m = \operatorname{lcm}(1, 2, \ldots, 15) = 360360,$$

$$2^{360360} - 1 \equiv 584876 \pmod{779167},$$

and

$$\gcd(2^{360360} - 1, N) = 2003,$$

so 2003 is a nontrivial factor of 779167.

Example 6.3.6. In this example, we replace B by a smaller integer. Let $N = 4331$. Suppose $B = 7$, so $m = \text{lcm}(1, 2, \ldots, 7) = 420$,

$$2^{420} - 1 \equiv 0 \pmod{4331},$$

and $\gcd(2^{420} - 1, 4331) = 4331$, so we do not obtain a factor of 4331. If we replace B by 5, Pollard's method works:

$$2^{60} - 1 \equiv 1464 \pmod{4331},$$

and $\gcd(2^{60} - 1, 4331) = 61$, so we split 4331.

Example 6.3.7. In this example, $a = 2$ does not work, but $a = 3$ does. Let $N = 187$. Suppose $B = 15$, so $m = \text{lcm}(1, 2, \ldots, 15) = 360360$,

$$2^{360360} - 1 \equiv 0 \pmod{187},$$

and $\gcd(2^{360360} - 1, 187) = 187$, so we do not obtain a factor of 187. If we replace $a = 2$ by $a = 3$, then Pollard's method works:

$$3^{360360} - 1 \equiv 66 \pmod{187},$$

and $\gcd(3^{360360} - 1, 187) = 11$. Thus $187 = 11 \cdot 17$.

6.3.2 Motivation for the Elliptic Curve Method

Fix a positive integer B. If $N = pq$ with p and q prime and $p-1$ and $q-1$ are not B-power smooth, then the Pollard $(p-1)$-method is unlikely to work. For example, let $B = 20$ and suppose that $N = 59 \cdot 101 = 5959$. Note that neither $59 - 1 = 2 \cdot 29$ nor $101 - 1 = 4 \cdot 25$ is B-power smooth. With $m = \text{lcm}(1, 2, 3, \ldots, 20) = 232792560$, we have

$$2^m - 1 \equiv 5944 \pmod{N},$$

and $\gcd(2^m - 1, N) = 1$, so we do not find a factor of N.

As remarked above, the problem is that $p-1$ is not 20-power smooth for either $p = 59$ or $p = 101$. However, notice that $p - 2 = 3 \cdot 19$ is 20-power smooth. Lenstra's ECM replaces $(\mathbf{Z}/p\mathbf{Z})^*$, which has order $p - 1$, by the group of points on an elliptic curve E over $\mathbf{Z}/p\mathbf{Z}$. It is a theorem that

$$\#E(\mathbf{Z}/p\mathbf{Z}) = p + 1 \pm s$$

for some nonnegative integer $s < 2\sqrt{p}$ (see e.g., [Sil86, §V.1] for a proof). (Also every value of s subject to this bound occurs, as one can see using "complex multiplication theory".) For example, if E is the elliptic curve

$$y^2 = x^3 + x + 54$$

over $\mathbf{Z}/59\mathbf{Z}$ then by enumerating points one sees that $E(\mathbf{Z}/59\mathbf{Z})$ is cyclic of order 57. The set of numbers $59 + 1 \pm s$ for $s \leq 15$ contains 14 numbers that are B-power smooth for $B = 20$ (see Exercise 7.14). Thus working with an elliptic curve gives us more flexibility. For example, $60 = 59 + 1 + 0$ is 5-power smooth and $70 = 59 + 1 + 10$ is 7-power smooth.

FIGURE 6.4. Hendrik Lenstra

6.3.3 Lenstra's Elliptic Curve Factorization Method

Algorithm 6.3.8 (Elliptic Curve Factorization Method). Given a positive integer N and a bound B, this algorithm attempts to find a nontrivial factor m of N. Carry out the following steps:

1. [Compute lcm] Use Algorithm 6.3.2 to compute $m = \operatorname{lcm}(1, 2, \ldots, B)$.
2. [Choose Random Elliptic Curve] Choose a random $a \in \mathbf{Z}/N\mathbf{Z}$ such that $4a^3 + 27 \in (\mathbf{Z}/N\mathbf{Z})^*$. Then $P = (0, 1)$ is a point on the elliptic curve $y^2 = x^3 + ax + 1$ over $\mathbf{Z}/N\mathbf{Z}$.
3. [Compute Multiple] Attempt to compute mP using an elliptic curve analogue of Algorithm 2.3.7. If at some point we cannot compute a sum of points because some denominator in step 3 of Algorithm 6.2.1 is not coprime to N, we compute the $\gcd$ of this denominator with N. If this $\gcd$ is a nontrivial divisor, output it. If every denominator is coprime to N, output "Fail".

We implement Algorithm 6.3.8 in Section 7.6.2.

If Algorithm 6.3.8 fails for one random elliptic curve, there is an option that is unavailable with Pollard's $(p-1)$-method—we may repeat the above algorithm with a different elliptic curve. With Pollard's method we always work with the group $(\mathbf{Z}/N\mathbf{Z})^*$, but here we can try many groups $E(\mathbf{Z}/N\mathbf{Z})$ for many curves E. As mentioned above, the number of points on E over $\mathbf{Z}/p\mathbf{Z}$ is of the form $p + 1 - t$ for some t with $|t| < 2\sqrt{p}$; Algorithm 6.3.8 thus has a chance if $p+1-t$ is B-power-smooth for some t with $|t| < 2\sqrt{p}$.

6.3.4 Examples

For simplicity, we use an elliptic curve of the form

$$y^2 = x^3 + ax + 1,$$

which has the point $P = (0, 1)$ already on it.

We factor $N = 5959$ using the elliptic curve method. Let

$$m = \operatorname{lcm}(1, 2, \ldots, 20) = 232792560 = 11011110000000100001111110000_2,$$

where x_2 means x is written in binary. First we choose $a = 1201$ at random and consider $y^2 = x^3 + 1201x + 1$ over $\mathbf{Z}/5959\mathbf{Z}$. Using the formula for $P+P$ from Algorithm 6.2.1 implemented on a computer (see Section 7.6) we compute $2^i \cdot P = 2^i \cdot (0,1)$ for $i \in B = \{4,5,6,7,8,13,21,22,23,24,26,27\}$. Then $\sum_{i \in B} 2^i P = mP$. It turns out that during no step of this computation does a number not coprime to 5959 appear in any denominator, so we do not split N using $a = 1201$. Next we try $a = 389$ and at some stage in the computation we add $P = (2051, 5273)$ and $Q = (637, 1292)$. When computing the group law explicitly we try to compute $\lambda = (y_1 - y_2)/(x_1 - x_2)$ in $(\mathbf{Z}/5959\mathbf{Z})^*$, but fail since $x_1 - x_2 = 1414$ and $\gcd(1414, 5959) = 101$. We thus find a nontrivial factor 101 of 5959.

For bigger examples and an implementation of the algorithm, see Section 7.6.2.

6.3.5 A Heuristic Explanation

Let N be a positive integer and for simplicity of exposition assume that $N = p_1 \cdots p_r$ with the p_i distinct primes. It follows from Lemma 2.2.5 that there is a natural isomorphism

$$f : (\mathbf{Z}/N\mathbf{Z})^* \longrightarrow (\mathbf{Z}/p_1\mathbf{Z})^* \times \cdots \times (\mathbf{Z}/p_r\mathbf{Z})^*.$$

When using Pollard's method, we choose an $a \in (\mathbf{Z}/N\mathbf{Z})^*$, compute a^m, then compute $\gcd(a^m - 1, N)$. This gcd is divisible exactly by the primes p_i such that $a^m \equiv 1 \pmod{p_i}$. To reinterpret Pollard's method using the above isomorphism, let $(a_1, \ldots, a_r) = f(a)$. Then $(a_1^m, \ldots, a_r^m) = f(a^m)$, and the p_i that divide $\gcd(a^m - 1, N)$ are exactly the p_i such that $a_i^m = 1$. By Theorem 2.1.12, these p_i include the primes p_j such that $p_j - 1$ is B-power smooth, where $m = \operatorname{lcm}(1, \ldots, m)$.

We will not define $E(\mathbf{Z}/N\mathbf{Z})$ when N is composite, since this is not needed for the algorithm (where we assume that N is prime and hope for a contradiction). However, for the remainder of this paragraph, we pretend that $E(\mathbf{Z}/N\mathbf{Z})$ is meaningful and describe a heuristic connection between Lenstra and Pollard's methods. The significant difference between Pollard's method and the elliptic curve method is that the isomorphism f is replaced by an isomorphism (in quotes)

$$\text{“}g : E(\mathbf{Z}/N\mathbf{Z}) \to E(\mathbf{Z}/p_1\mathbf{Z}) \times \cdots \times E(\mathbf{Z}/p_r\mathbf{Z})\text{”}$$

where E is $y^2 = x^3 + ax + 1$, and the a of Pollard's method is replaced by $P = (0,1)$. We put the isomorphism in quotes to emphasize that we have not defined $E(\mathbf{Z}/N\mathbf{Z})$. When carrying out the elliptic curve factorization algorithm, we attempt to compute mP and if some components of $f(Q)$ are $\mathcal{O}$, for some point Q that appears during the computation, but others are nonzero, we find a nontrivial factor of N.

6.4 Elliptic Curve Cryptography

In this section we discuss an analogue of Diffie-Hellman that uses an elliptic curve instead of $(\mathbf{Z}/p\mathbf{Z})^*$. The idea to use elliptic curves in cryptography was independently proposed by Neil Koblitz and Victor Miller in the mid 1980s. We then discuss the ElGamal elliptic curve cryptosystem.

6.4.1 Elliptic Curve Analogues of Diffie-Hellman

The Diffie-Hellman key exchange from Section 3.1 works well on an elliptic curve with no serious modification. Michael and Nikita agree on a secret key as follows:

1. Michael and Nikita agree on a prime p, an elliptic curve E over $\mathbf{Z}/p\mathbf{Z}$, and a point $P \in E(\mathbf{Z}/p\mathbf{Z})$.
2. Michael secretly chooses a random m and sends mP.
3. Nikita secretly chooses a random n and sends nP.
4. The secret key is nmP, which both Michael and Nikita can compute.

Presumably, an adversary can not compute nmP without solving the discrete logarithm problem (see Problem 3.1.2 and Section 6.4.3 below) in $E(\mathbf{Z}/p\mathbf{Z})$. For well-chosen E, P, and p experience suggests that the discrete logarithm problem in $E(\mathbf{Z}/p\mathbf{Z})$ is much more difficult than the discrete logarithm problem in $(\mathbf{Z}/p\mathbf{Z})^*$ (see Section 6.4.3 for more on the elliptic curve discrete log problem).

6.4.2 The ElGamal Cryptosystem and Digital Rights Management

This section is about the ElGamal cryptosystem, which works well on an elliptic curves. This section draws on a paper by a computer hacker named Beale Screamer who cracked a "Digital Rights Management" (DRM) system.

The elliptic curve used in the DRM is an elliptic curve over the finite field $k = \mathbf{Z}/p\mathbf{Z}$, where

$$p = 7859631023794288223766947894468973962074985689 51.$$

In base 16 the number p is

$$89ABCDEF012345672718281831415926141424F7,$$

which includes counting in hexadecimal, and digits of e, π, and $\sqrt{2}$. The elliptic curve E is

$$y^2 = x^3 + 3176890812513255034763174764138276932727469559 27x + 7905289660787875871812057202571853543210065193 4.$$

We have

$$\#E(k) = 7859631023794288223766930248817149576126861574 29,$$

and the group $E(k)$ is cyclic with generator

$$B = (771507216262649826170648268565579889907769254176,$$
$$390157510246556628525279459266514995562533196655).$$

Our heroes Nikita and Michael share digital music when they are not out fighting terrorists. When Nikita installed the DRM software on her computer, it generated a private key

$$n = 67080503113991051351752720769306045630021705447 3,$$

which it hides in bits and pieces of files. In order for Nikita to play Juno Reactor's latest hit `juno.wma`, her web browser contacts a web site that sells music. After Nikita sends her credit card number, that web site allows Nikita to download a license file that allows her audio player to unlock and play `juno.wma`.

As we will see below, the license file was created using the ElGamal public-key cryptosystem in the group $E(k)$. Nikita can now use her license file to unlock `juno.wma`. However, when she shares both `juno.wma` and the license file with Michael, he is frustrated because even with the license his computer still does not play `juno.wma`. This is because Michael's computer does not know Nikita's computer's private key (the integer n above), so Michael's computer can not decrypt the license file.

We now describe the ElGamal cryptosystem, which lends itself well to implementation in the group $E(\mathbf{Z}/p\mathbf{Z})$. To illustrate ElGamal, we describe how Nikita would set up an ElGamal cryptosystem that anyone could use to encrypt messages for her. Nikita chooses a prime p, an elliptic curve E over $\mathbf{Z}/p\mathbf{Z}$, and a point $B \in E(\mathbf{Z}/p\mathbf{Z})$, and publishes p, E, and B. She also chooses a random integer n, which she keeps secret, and publishes nB. Her public key is the four-tuple (p, E, B, nB).

Suppose Michael wishes to encrypt a message for Nikita. If the message is encoded as an element $P \in E(\mathbf{Z}/p\mathbf{Z})$, Michael computes a random integer r

and the points rB and $P+r(nB)$ on $E(\mathbf{Z}/p\mathbf{Z})$. Then P is encrypted as the pair $(rB, P+r(nB))$. To decrypt the encrypted message, Nikita multiplies rB by her secret key n to find $n(rB) = r(nB)$, then subtracts this from $P + r(nB)$ to obtain

$$P = P + r(nB) - r(nB).$$

We implement this cryptosystem in Section 7.6.3.

Remark 6.4.1. It also make sense to construct an ElGamal cryptosystem in the group $(\mathbf{Z}/p\mathbf{Z})^*$.

Returning out our story, Nikita's license file is an encrypted message to her. It contains the pair of points $(rB, P + r(nB))$, where

$$rB = (179671003218315746385026655733086044982194424660,$$
$$697834385359686368249301282675141830935176314718)$$

and

$$P + r(nB) = (137851038548264467372645158093004000343639118915,$$
$$110848589228676224057229230223580815024224875699).$$

When Nikita's computer plays `juno.wma`, it loads the secret key

$$n = 67080503113991051351752720769306045630021705447 3$$

into memory and computes

$$n(rB) = (328901393518732637577115650601768681044040715701,$$
$$586947838087815993601350565488788846203887988162).$$

It then subtracts this from $P + r(nB)$ to obtain

$$P = (14489646124220757767,$$
$$669337780373284096274895136618194604469696830074).$$

The x-coordinate 14489646124220757767 is the key that unlocks `juno.wma`.

If Nikita knew the private key n that her computer generated, she could compute P herself and unlock `juno.wma` and share her music with Michael. Beale Screamer found a weakness in the implementation of this system that allows Nikita to detetermine n, which is not a huge surprise since n is stored on her computer after all.

6.4.3 The Elliptic Curve Discrete Logarithm Problem

Problem 6.4.2 (Elliptic Curve Discrete Log Problem). Suppose E is an elliptic curve over $\mathbf{Z}/p\mathbf{Z}$ and $P \in E(\mathbf{Z}/p\mathbf{Z})$. Given a multiple Q of P, the *elliptic curve discrete log problem* is to find $n \in \mathbf{Z}$ such that $nP = Q$.

For example, let E be the elliptic curve given by $y^2 = x^3 + x + 1$ over the field $\mathbf{Z}/7\mathbf{Z}$. We have

$$E(\mathbf{Z}/7\mathbf{Z}) = \{\mathcal{O}, (2,2), (0,1), (0,6), (2,5)\}.$$

If $P = (2,2)$ and $Q = (0,6)$, then $3P = Q$, so $n = 3$ is a solution to the discrete logarithm problem.

If $E(\mathbf{Z}/p\mathbf{Z})$ has order p or $p \pm 1$ or is a product of reasonably small primes, then there are some methods for attacking the discrete log problem on E, which are beyond the scope of this book. It is thus important to be able to compute $\#E(\mathbf{Z}/p\mathbf{Z})$ efficiently, in order to verify that the elliptic curve one wishes to use for a cryptosystem doesn't have any obvious vulnerabilities. The naive algorithm to compute $\#E(\mathbf{Z}/p\mathbf{Z})$ is to try each value of $x \in \mathbf{Z}/p\mathbf{Z}$ and count how often $x^3 + ax + b$ is a perfect square mod p, but this is of no use when p is large enough to be useful for cryptography. Fortunately, there is an algorithm due to Schoof, Elkies, and Atkin for computing $\#E(\mathbf{Z}/p\mathbf{Z})$ efficiently (polynomial time in the number of digits of p), but this algorithm is beyond the scope of this book.

In Section 3.1.1 we discussed the discrete log problem in $(\mathbf{Z}/p\mathbf{Z})^*$. There are general attacks called "index calculus attacks" on the discrete log problem in $(\mathbf{Z}/p\mathbf{Z})^*$ that are slow, but still faster than the known algorithms for solving the discrete log in a "general" group (one with no extra structure). For most elliptic curves, there is no known analogue of index calculus attacks on the discrete log problem. At present it appears that given p the discrete log problem in $E(\mathbf{Z}/p\mathbf{Z})$ is much harder than the discrete log problem in the multiplicative group $(\mathbf{Z}/p\mathbf{Z})^*$. This suggests that by using an elliptic curve-based cryptosystem instead of one based on $(\mathbf{Z}/p\mathbf{Z})^*$ one gets equivalent security with much smaller numbers, which is one reason why building cryptosystems using elliptic curves is attractive to some cryptographers. For example, Certicom, a company that strongly supports elliptic curve cryptography, claims:

> "[Elliptic curve crypto] devices require less storage, less power, less memory, and less bandwidth than other systems. This allows you to implement cryptography in platforms that are constrained, such as wireless devices, handheld computers, smart cards, and thin-clients. It also provides a big win in situations where efficiency is important."

For an up-to-date list of elliptic curve discrete log challenge problems that Certicom sponsors, see [Cer]. For example, in April 2004 a specific cryptosystem was cracked that was based on an elliptic curve over $\mathbf{Z}/p\mathbf{Z}$, where p has 109 bits. The first unsolved challenge problem involves an elliptic curve over $\mathbf{Z}/p\mathbf{Z}$, where p has 131 bits, and the next challenge after that is one in which p has 163 bits. Certicom claims at [Cer] that the 163-bit challenge problem is computationally infeasible.

FIGURE 6.5. Louis J. Mordell

6.5 Elliptic Curves Over the Rational Numbers

Let E be an elliptic curve defined over $\mathbf{Q}$. The following is a deep theorem about the group $E(\mathbf{Q})$.

Theorem 6.5.1 (Mordell). *The group $E(\mathbf{Q})$ is finitely generated. That is, there are points $P_1, \ldots, P_s \in E(\mathbf{Q})$ such that every element of $E(\mathbf{Q})$ is of the form $n_1P_1 + \cdots + n_sP_s$ for integers $n_1, \ldots n_s \in \mathbf{Z}$.*

Mordell's theorem implies that it makes sense to ask whether or not we can compute $E(\mathbf{Q})$, where by "compute" we mean find a finite set $P_1, \ldots, P_s$ of points on E that generate $E(\mathbf{Q})$ as an abelian group. There is a systematic approach to computing $E(\mathbf{Q})$ called "descent" (see e.g., [Cre97, Cre, Sil86]). It is widely believed that descent will always succeeds, but nobody has yet proved that it does. Proving that descent works for all curves is one of the central open problem in number theory, and is closely related to the Birch and Swinnerton-Dyer conjecture (one of the Clay Math Institute's million dollar prize problems). The crucial difficulty amounts to deciding whether or not certain explicitly given curves have any rational points on them or not (these are curves that have points over $\mathbf{R}$ and modulo n for all n).

The details of using descent to computing $E(\mathbf{Q})$ are beyond the scope of this book. In several places below we will simply assert that $E(\mathbf{Q})$ has a certain structure or is generated by certain elements. In each case, we computed $E(\mathbf{Q})$ using a computer implementation of this method.

6.5.1 The Torsion Subgroup of $E(\mathbf{Q})$ and the Rank

For any abelian group G, let G_{tor} be the subgroup of elements of finite order. If E is an elliptic curve over $\mathbf{Q}$, then $E(\mathbf{Q})_{\text{tor}}$ is a subgroup of $E(\mathbf{Q})$, which must be finite because of Theorem 6.5.1 (see Exercise 6.6).

One can also prove that $E(\mathbf{Q})_{\text{tor}}$ is finite by showing that there is a prime p and an injective reduction homomorphism $E(\mathbf{Q})_{\text{tor}} \hookrightarrow E(\mathbf{Z}/p\mathbf{Z})$, then noting that $E(\mathbf{Z}/p\mathbf{Z})$ is finite. For example, if E is $y^2 = x^3 - 5x + 4$, then $E(\mathbf{Q})_{\text{tor}} = \{\mathcal{O}, (1,0)\} \cong \mathbf{Z}/2\mathbf{Z}$.

The possibilities for $E(\mathbf{Q})_{\text{tor}}$ are known.

Theorem 6.5.2 (Mazur, 1976). *Let E be an elliptic curve over $\mathbf{Q}$. Then $E(\mathbf{Q})_{\text{tor}}$ is isomorphic to one of the following 15 groups:*

$$\begin{aligned} \mathbf{Z}/n\mathbf{Z} \qquad & \text{for } n \leq 10 \text{ or } n = 12, \\ \mathbf{Z}/2 \times \mathbf{Z}/2n \qquad & \text{for } n \leq 4. \end{aligned}$$

The quotient $E(\mathbf{Q})/E(\mathbf{Q})_{\text{tor}}$ is a finitely generated free abelian group, so it is isomorphism to $\mathbf{Z}^r$ for some integer r, called the *rank* of $E(\mathbf{Q})$. For example, using descent one finds that if E is $y^2 = x^3 - 5x + 4$, then $E(\mathbf{Q})/E(\mathbf{Q})_{\text{tor}}$ is generated by the point $(0, 2)$. Thus $E(\mathbf{Q}) \cong \mathbf{Z} \times (\mathbf{Z}/2\mathbf{Z})$.

The following is a folklore conjecture, not associated to any particular mathematician:

Conjecture 6.5.3. *There are elliptic curves over $\mathbf{Q}$ of arbitrarily large rank.*

The "world record" is the following curve, whose rank is at least 24:

$$\begin{aligned} y^2 + xy + y = x^3 &- 120039822036992245303534619191166796374x \\ &+ 5042249924849106700108017991680827267594437562229114151 16 \end{aligned}$$

It was discovered in January 2000 by Roland Martin and William McMillen of the National Security Agency.

6.5.2 The Congruent Number Problem

Definition 6.5.4 (Congruent Number). We call a nonzero rational number n a *congruent number* if $\pm n$ is the area of a right triangle with rational side lengths. Equivalently, n is a *congruent number* if the system of two equations

$$\begin{aligned} a^2 + b^2 &= c^2 \\ \frac{1}{2}ab &= n \end{aligned}$$

has a solution with $a, b, c \in \mathbf{Q}$.

For example, 6 is the area of the right triangle with side lengths 3, 4, and 5, so 6 is a congruent number. Less obvious is that 5 is also a congruent number; it is the area of the right triangle with side lengths 3/2, 20/3, and 41/6. It is nontrivial to prove that 1, 2, 3, and 4 are not congruent numbers. Here is a list of the integer congruent numbers up to 50:

$$5, 6, 7, 13, 14, 15, 20, 21, 22, 23, 24, 28, 29, 30, 31, 34, 37, 38, 39, 41, 45, 46, 47.$$

Every congruence class modulo 8 except 3 is represented in this list, which incorrectly suggests that if $n \equiv 3 \pmod 8$ then n is not a congruent number. Though no $n \leq 218$ with $n \equiv 3 \pmod 8$ is a congruent number, $n = 219$ is a congruent number congruent and $219 \equiv 3 \pmod 8$.

Deciding whether an integer n is a congruent number can be subtle since the simplest triangle with area n can be very complicated. For example, as Zagier pointed out, the number 157 is a congruent number, and the "simplest" rational right triangle with area 157 has side lengths

$$a = \frac{6803298487826435051217540}{411340519227716149383203} \text{ and } b = \frac{411340519227716149383203}{21666555693714761309610}.$$

This solution would be difficult to find by a brute force search.

We call congruent numbers "congruent" because of the following proposition, which asserts that any congruent number is the common "congruence" between three perfect squares.

Proposition 6.5.5. *Suppose n is the area of a right triangle with rational side lengths a, b, c, with $a \leq b < c$. Let $A = (c/2)^2$. Then*

$$A - n, \quad A, \text{ and } A + n$$

are all perfect squares of rational numbers.

Proof. We have

$$\begin{aligned} a^2 + b^2 &= c^2 \\ \frac{1}{2}ab &= n \end{aligned}$$

Add or subtract 4 times the second equation to the first to get

$$\begin{aligned} a^2 \pm 2ab + b^2 &= c^2 \pm 4n \\ (a \pm b)^2 &= c^2 \pm 4n \\ \left(\frac{a \pm b}{2}\right)^2 &= \left(\frac{c}{2}\right)^2 \pm n \\ &= A \pm n \end{aligned}$$

□

The main motivating open problem related to congruent numbers, is to give a systematic way to recognize them.

Open Problem 6.5.6. *Give an algorithm which, given n, outputs whether or not n is a congruent number.*

Fortunately, the vast theory developed about elliptic curves has something to say about the above problem. In order to understand this connection, we begin with an elementary algebraic proposition that establishes a link between elliptic curves and the congruent number problem.

Proposition 6.5.7 (Congruent numbers and elliptic curves). *Let n be a rational number. There is a bijection between*

$$A = \left\{(a,b,c) \in \mathbf{Q}^3 \,:\, \frac{ab}{2} = n,\, a^2+b^2=c^2\right\}$$

and

$$B = \left\{(x,y) \in \mathbf{Q}^2 \,:\, y^2 = x^3 - n^2x, \text{ with } y \neq 0\right\}$$

given explicitly by the maps

$$f(a,b,c) = \left(-\frac{nb}{a+c},\ \frac{2n^2}{a+c}\right)$$

and

$$g(x,y) = \left(\frac{n^2-x^2}{y},\ -\frac{2xn}{y},\ \frac{n^2+x^2}{y}\right).$$

The proof of this proposition is not deep, but involves substantial (elementary) algebra and we will not prove it in this book.

For $n \neq 0$, let E_n be the elliptic curve $y^2 = x^3 - n^2x$.

Proposition 6.5.8 (Congruent number criterion). *The rational number n is a congruent number if and only if there is a point $P = (x,y) \in E_n(\mathbf{Q})$ with $y \neq 0$.*

Proof. The number n is a congruent number if and only if the set A from Proposition 6.5.7 is nonempty. By the proposition A is nonempty if and only if B is nonempty. □

Example 6.5.9. Let $n = 5$. Then E_n is $y^2 = x^3 - 25x$, and we notice that $(-4,-6) \in E_n(\mathbf{Q})$. We next use the bijection of Proposition 6.5.7 to find the corresponding right traingle:

$$g(-4,-6) = \left(\frac{25-16}{-6}, -\frac{-40}{-6}, \frac{25+16}{-6}\right) = \left(-\frac{3}{2}, -\frac{20}{3}, -\frac{41}{6}\right).$$

Multiplying through by -1 yields the side lengths of a rational right triangle with area 5. *Are there any others?*

Observe that we can apply g to any point in $E_n(\mathbf{Q})$ with $y \neq 0$. Using the group law we find that $2(-4,-6) = (1681/144, 62279/1728)$, and

$$g(2(-4,-6)) = \left(-\frac{1519}{492}, -\frac{4920}{1519}, \frac{3344161}{747348}\right).$$

Example 6.5.10. Let $n = 1$, so E_1 is defined by $y^2 = x^3 - x$. Since 1 is not a congruent number, the elliptic curve E_1 has no point with $y \neq 0$. See Exercise 6.10.

Example 6.5.9 foreshadows the following theorem.

Theorem 6.5.11 (Infinitely Many Triangles). *If n is a congruent number, then there are infinitely many distinct right triangles with rational side lengths and area n.*

We will not prove this theorem, except to note that one proves it by showing that $E_n(\mathbf{Q})_{\text{tor}} = \{\mathcal{O}, (0,0), (n,0), (-n,0)\}$, so the elements of the set B in Proposition 6.5.7 all have infinite order, hence B is infinite so A is infinite.

Tunnell has proved that the Birch and Swinnerton-Dyer (alluded to above), implies the existence of an elementary way to decide whether or not an integer n is a congruent number. We state Tunnell's elementary way in the form of a conjecture.

Conjecture 6.5.12. *Let a, b, c denote integers. If n is an even square-free integer then n is a congruent number if and only if*

$$\#\left\{(a,b,c) \in \mathbf{Z}^3 : 4a^2 + b^2 + 8c^2 = \frac{n}{2} : c \text{ is even}\right\}$$

$$= \#\left\{(a,b,c) : 4a^2 + b^2 + 8c^2 = \frac{n}{2} : c \text{ is odd}\right\}.$$

If n is odd and square free then n is a congruent number if and only if

$$\#\left\{(a,b,c) : 2a^2 + b^2 + 8c^2 = n : c \text{ is even}\right\}$$

$$= \#\left\{(a,b,c) : 2a^2 + b^2 + 8c^2 = n : c \text{ is odd}\right\}.$$

Enough of the Birch and Swinnerton-Dyer conjecture is known to prove one direction of Conjecture 6.5.12. In particular, it is a very deep theorem that if we do not have equality of the displayed cardinalities, then n is not a congruent number. For example, when $n = 1$,

The even more difficult (and still open!) part of Conjecture 6.5.12 is the converse: If one has equality of the displayed cardinalities, prove that n is a congruent number. The difficulty in this direction, which appears to be very deep, is that we must somehow construct (or prove the existence of) elements of $E_n(\mathbf{Q})$. This has been accomplished in some cases do to groundbreaking work of Gross and Zagier ([GZ86]) but much work remains to be done.

The excellent book [Kob84] is about congruent numbers and Conjecture 6.5.12, and we encourage the reader to consult it. The Birch and Swinnerton-Dyer conjecture is a Clay Math Institute million dollar millennium prize problem (see [Cla, Wil00]).

6.6 Exercises

6.1 Write down an equation $y^2 = x^3 + ax + b$ over a field K such that $-16(4a^3+27b^2) = 0$. Precisely what goes wrong when trying to endow the set $E(K) = \{(x, y) \in K \times K : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$ with a group structure?

6.2 One rational solution to the equation $y^2 = x^3 - 2$ is $(3, 5)$. Find a rational solution with $x \neq 3$ by drawing the tangent line to $(3, 5)$ and computing the second point of intersection.

6.3 Let E be the elliptic curve over the finite field $K = \mathbf{Z}/5\mathbf{Z}$ defined by the equation

$$y^2 = x^3 + x + 1.$$

(a) List all 9 elements of $E(K)$.

(b) What is the structure of $E(K)$, as a product of cyclic groups?

6.4 Let E be the elliptic curve defined by the equation $y^2 = x^3 + 1$. For each prime $p \geq 5$, let N_p be the cardinality of the group $E(\mathbf{Z}/p\mathbf{Z})$ of points on this curve having coordinates in $\mathbf{Z}/p\mathbf{Z}$. For example, we have that $N_5 = 6, N_7 = 12, N_{11} = 12, N_{13} = 12, N_{17} = 18, N_{19} = 12, , N_{23} = 24,$ and $N_{29} = 30$ (you do not have to prove this).

(a) For the set of primes satisfying $p \equiv 2 \pmod 3$, can you see a pattern for the values of N_p? Make a general conjecture for the value of N_p when $p \equiv 2 \pmod 3$.

(b) (*) Prove your conjecture.

6.5 Let E be an elliptic curve over the real numbers $\mathbf{R}$. Prove that $E(\mathbf{R})$ is not a finitely generated abelian group.

6.6 (*) Suppose G is a finitely generated abelian group. Prove that the subgroup G_{tor} of elements of finite order in G is finite.

6.7 Suppose $y^2 = x^3+ax+b$ with $a, b \in \mathbf{Q}$ defines an elliptic curve. Show that there is another equation $Y^2 = X^3 + AX + B$ with $A, B \in \mathbf{Z}$ whose solutions are in bijection with the solutions to $y^2 = x^3+ax+b$.

6.8 Suppose a, b, c are relatively prime integers with $a^2 + b^2 = c^2$. Then there exist integers x and y with $x > y$ such that $c = x^2 + y^2$ and either $a = x^2 - y^2$, $b = 2xy$ or $a = 2xy$, $b = x^2 - y^2$.

6.9 (*) Fermat's Last Theorem for exponent 4 asserts that any solution to the equation $x^4 + y^4 = z^4$ with $x, y, z \in \mathbf{Z}$ satisfies $xyz = 0$. Prove of Fermat's Last Theorem for exponent 4, as follows.

(a) Show that if the equation $x^2 + y^4 = z^4$ has no integer solutions with $xyz \neq 0$, then Fermat's Last Theorem for exponent 4 is true.

(b) Prove that $x^2 + y^4 = z^4$ has no integer solutions with $xyz \neq 0$ as follows. Suppose $n^2 + k^4 = m^4$ is a solution with $m > 0$ minimal amongst all solutions. Show that there exists a solution with m smaller using Exercise 6.8 (consider two cases).

6.10 (*) Prove that 1 is not a congruent number by showing that the elliptic curve $y^2 = x^3 - x$ has no rational solutions except $(0, 1)$ and $(0, 0)$, as follows:

(a) Write $y = \frac{p}{q}$ and $x = \frac{r}{s}$, where p, q, r, s are all positive integers and $\gcd(p, q) = \gcd(r, s) = 1$. Prove that $s \mid q$, so $q = sk$ for some $k \in \mathbf{Z}$.

(b) Prove that $s = k^2$, and substitute to see that $p^2 = r^3 - rk^4$.

(c) Prove that r is a perfect square by supposing there is a prime ℓ such that $\mathrm{ord}_\ell(r)$ is odd and analyzing ord_ℓ of both sides of $p^2 = r^3 - rk^4$.

(d) Write $r = m^2$, and substitute to see that $p^2 = m^6 - m^2k^4$. Prove that $m \mid p$.

(e) Divide through by m^2 and deduce a contradiction to Exercise 6.9.