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).

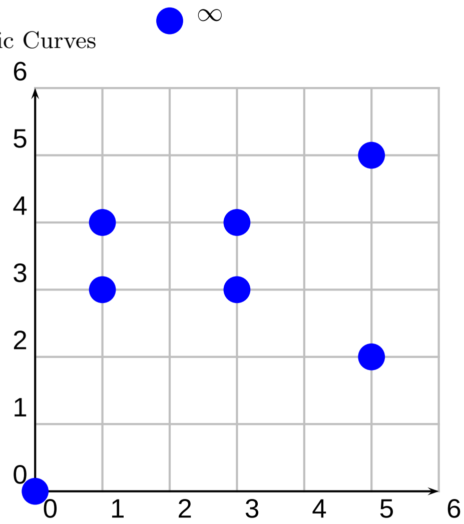

FIGURE 6.1. The Elliptic Curve $y^2 = x^3 + x$ over $\mathbf{Z}/7\mathbf{Z}$

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 $R = P_1 + P_2 \in E(K)$.

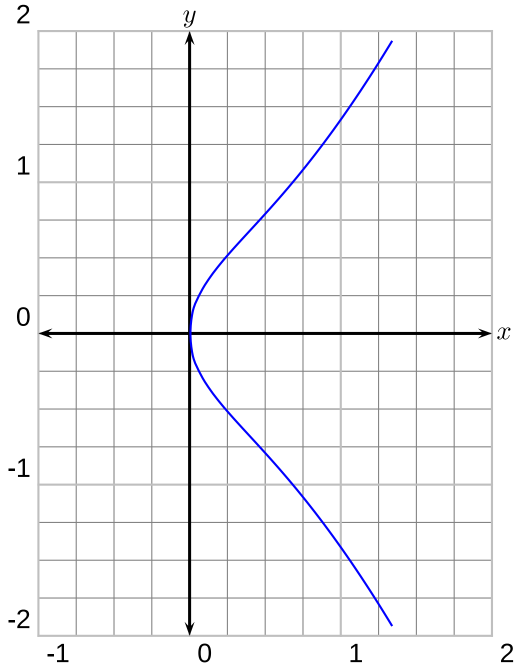

FIGURE 6.2. The Elliptic Curve $y^2 = x^3 + x$ over $\mathbf{R}$

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 $f(x) = x^3 - \lambda^2 x^2 + \cdots = 0$, 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. $\square$

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.

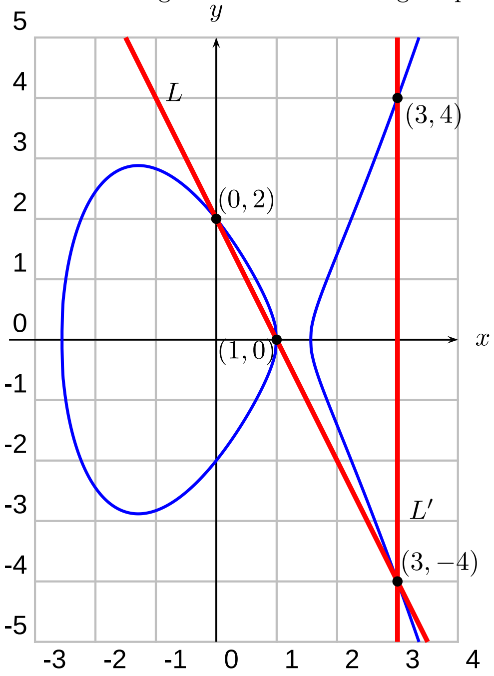

FIGURE 6.3. The Group Law: $(1, 0) + (0, 2) = (3, 4)$ on $y^2 = x^3 - 5x + 4$

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'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.

Lenstra

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 $\prod_{p \in P} \lfloor \log_p(B) \rfloor$.

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

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

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 $r = \lfloor \log_p(B) \rfloor$. $\square$

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 $m = \mathrm{lcm}(1, 2, 3, \ldots, B)$, 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 $m = \mathrm{lcm}(1, 2, \ldots, B)$.
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 $m = \mathrm{lcm}(1, 2, 3, 4, 5) = 60$; 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

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

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

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 $m = \mathrm{lcm}(1, 2, \ldots, B)$.
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

$$m = \mathrm{lcm}(1, 2, \ldots, 20) = 232792560 = 1101111000000010000111110000_2,$$

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.