11
Algorithmic Applications of Elliptic Curves

We assume the reader has read Chapter 10 about elliptic curves.

11.1 Elliptic Curves Over $\mathbb{Z}/p$

The applications of elliptic curves that we discuss in this chapter involve elliptic curves over finite fields or rings.

Let p be a prime and let $\mathbb{F}_p = \mathbb{Z}/p$ denote the field with p elements. There is an analogue $\mathbb{P}^2_{\mathbb{F}_p}$ of the projective plane from Section 10.1.2 over the field $\mathbb{F}_p$. The set of points $\mathbb{P}^2(\mathbb{F}_p)$ of $\mathbb{P}^2_{\mathbb{F}_p}$ rational over $\mathbb{F}_p$ is the set of triples $(a : b : c)$ with $a, b, c \in \mathbb{F}_p$ not all zero modulo the equivalence relation in which $(\lambda a : \lambda b : \lambda c) = (a : b : c)$ for any nonzero $\lambda \in \mathbb{F}_p$.

Definition 11.1.1 (Elliptic Curve Over $\mathbb{F}_p$). An elliptic curve over $\mathbb{F}_p$ is a (closed) curve in $\mathbb{P}^2_{\mathbb{F}_p}$ that can be defined by an equation of the form $y^2 = x^3 + ax + b$ such that $a, b \in \mathbb{F}_p$ and $4a^3 + 27b^2 \neq 0$.

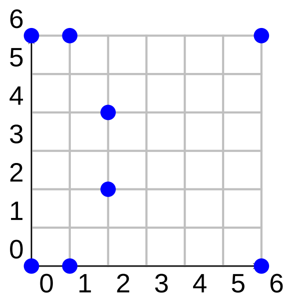

FIGURE 11.1. $y^2 + y = x^3 - x$ over $\mathbb{F}_7$

Remark 11.1.2. It is more natural to define an elliptic curve to be a "nonsingular" plane cubic curve in $\mathbb{P}^2_{\mathbb{F}_p}$ equipped with a distinguished $\mathbb{F}_p$-rational point. When $p \geq 5$, every such curve can be transformed by a change of variables (completing the square, etc.) into a curve of the form $y^2 = x^3 + ax + b$. When $p = 2, 3$, this is not the case. For the applications in this chapter, we may assume that $p \geq 5$.

The set of points on an elliptic curve over $\mathbb{F}_p$ is

$$E(\mathbb{F}_p) = \{(x, y) : y^2 = x^3 + ax + b\} \cup \{(0 : 1 : 0)\},$$

where, as usual, we write (a, b) for $(a : b : 1) \in \mathbb{P}^2(\mathbb{F}_p)$. Just as was the case for $E(\mathbb{C})$, the set $E(\mathbb{F}_p)$ is equipped with a natural group structure.

11.1.1 The Possibilities for $E(\mathbb{F}_p)$

In contrast to the situation with $E(\mathbb{Q})$ (see Section 10.3), the possibilities for the group $E(\mathbb{F}_p)$ are well understood.

Theorem 11.1.3. *The finite abelian group $E(\mathbb{F}_p)$ is either cyclic or a product of two cyclic groups.*

Proof. We only sketch the proof. Since $E(\mathbb{F}_p)$ is finite, there is an integer m such that

$$E(\mathbb{F}_p) \subset E(\mathbb{F}_p)[m] = \{x \in E(\mathbb{F}_p) : mx = 0\}.$$

It is a nontrivial fact (see ??) that for any elliptic curve over any field K, the m-torsion subgroup $E(K)[m]$ is a subgroup of $\mathbb{Z}/m \times \mathbb{Z}/m$. For example, when $K \subset \mathbb{C}$ this follows from the fact that

$$\begin{aligned} E(K)[m] \subset E(\mathbb{C})[m] &= (\mathbb{R}/\mathbb{Z} \oplus \mathbb{R}/\mathbb{Z})[m] \\ &= \left(\frac{1}{m}\mathbb{Z}\right)/\mathbb{Z} \oplus \left(\frac{1}{m}\mathbb{Z}\right)/\mathbb{Z} = \mathbb{Z}/m \times \mathbb{Z}/m. \end{aligned}$$

To finish the proof, use elementary group theory to see that any subgroup of $\mathbb{Z}/m \times \mathbb{Z}/m$ can be generated by two elements (See Exercise 2.11). $\square$

Theorem 11.1.4 (Hasse). *The cardinality of $E(\mathbb{F}_p)$ is bounded as follows:*

$$|\#E(\mathbb{F}_p) - (p + 1)| < 2\sqrt{p},$$

and every possibility for $\#E(\mathbb{F}_p)$ occurs.

Elliptic curves over finite fields are useful for much more than just computational applications. As we will see in Chapter **??**, a key step in the proof of Fermat's Last Theorem involves considering an elliptic curve $y^2 = x^3 + ax + b$ over $\mathbb{Q}$, and showing that a certain generating function whose coefficients encode $\#E(\mathbb{F}_p)$ (and other related information), for all but finitely many p, has good transformation properties.

11.2 Factorization

In 1987, Hendrik Lenstra published the landmark paper [Len87] that describes 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 useful for factoring RSA challenge numbers (see Section 3.1.3), but surprisingly it is used in intermediate steps of some the algorithms that are used for hunting for such factorizations. Implementation of ECM typically requires little memory. Lenstra's discovery of ECM was inspired by Pollard's $(p-1)$-method, which we will describe in Section 11.2.1 below.

Lenstra

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

Definition 11.2.1 (Power-smooth). Let B be a positive integer. A positive integer n is *B-power smooth* if all prime powers dividing n are less than or equal to B.

Thus 30 is 7-power smooth and 5-power smooth, but 4 is not 2-power smooth.

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 $\leq 10^6$ in practice. Suppose that there is a prime divisor p of N such that $p-1$ is B-power smooth. We try to find p computationally using the following strategy. If $a > 1$ is an integer not divisible by p then by Theorem 3.3.14,

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

Letting $m = \mathrm{lcm}(1, 2, 3, \ldots, B)$, 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, check from the start whether or not N is not a perfect power M^r, and if so replace N by M.

For fixed B, this algorithm usually splits N when N is divisible by a prime p such that $p-1$ is B-power smooth. Only 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. We will not analyze Pollard's method further, since it was mentioned here only to set the stage for the ECM.

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

Example 11.2.2. 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 11.2.3. 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 11.2.4. In this example, we replace B by a smaller integer. Let $N = 4331$. Suppose $B = 7$, so $m = \mathrm{lcm}(1,2,\ldots,7) = 420$,

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

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

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

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 $187 = 11 \cdot 17$.

11.2.2 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 $107 - 1 = 2 \cdot 53$ is B-power smooth. With $m = \mathrm{lcm}(1, 2, 3, \ldots, 20) = 232792560$, 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 $\mathbb{F}_p^\times$, which has order $p-1$, by the group of points on an elliptic curve E over $\mathbb{F}_p$. By Theorem 11.1.4,

$$\#E(\mathbb{F}_p) = p + 1 \pm s$$

for some nonnegative integer $s < 2\sqrt{p}$ and any s can occur. For example, if E is the elliptic curve

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

over $\mathbb{F}_{59}$ then by enumerating points one sees that $E(\mathbb{F}_{59})$ is cyclic of order 57 (every abelian group of order 57 is cyclic). The set of numbers $59 + 1 \pm s$ for $s \leq 15$ contains 14 numbers that are B-power smooth for $B \leq 20$. For example, $60 = 59 + 1 + 0$ is 5-power smooth and $70 = 59 + 1 + 10$ is 7-power smooth.

11.2.3 The Elliptic Curve Method

The following description of the ECM algorithm is taken from [Len87], with slight changes to the notation and wording.

> The new method is obtained from Pollard's $(p-1)$-method by replacing the multiplicative group $\mathbb{F}_p^\times$ by the group of points on a random elliptic curve. To find a non-trivial divisor of an integer $N > 1$, one begins by selecting an elliptic curve E over $\mathbb{Z}/N$, a point P on E with coordinates in $\mathbb{Z}/N$, and an integer $m = \mathrm{lcm}(2, 3, \ldots, B)$. Using the addition law of the curve, one next calculates the multiple $m \cdot P$ of P. One now hopes that there is a prime divisor p of N for which $m \cdot P$ and the neutral element $\mathcal{O}$ of the curve become the same modulo p; if E is given by a Weierstrass equation $y^2 = x^3 + ax + b$, with $\mathcal{O} = (0 : 1 : 0)$, then this is equivalent to the third coordinate of $m \cdot P$ being divisible by p. Hence one hopes to find a non-trivial factor of N by calculating the greatest common divisor of this third coordinate with m.

If the above algorithm fails with a specific elliptic curve E, there is an option that is unavailable with Pollard's $(p-1)$-method. We may repeat the above algorithm with a different choice of E. The number of points on E over $\mathbb{Z}/p$ is of the form $p+1-t$ for some t with $|t|<2\sqrt{p}$, and the algorithm is likely to succeed if $p+1-t$ is B-power-smoth.

Suppose that $P=(x_1,y_1)$ and $Q=(x_2,y_2)$ are nonzero points on an elliptic curve $y^2=x^3+ax+b$ and that $P\neq\pm Q$. Let $\lambda=(y_1-y_2)/(x_1-x_2)$ and $\nu=y_1-\lambda x_1$. Recall from Section 10.2.9 the explicit formula for computing $P+P$ and also that $P+Q=(x_3,y_3)$ where

$$x_3=\lambda^2-x_1-x_2 \qquad \text{and} \qquad y_3=-\lambda x_3-\nu.$$

We try to compute mP using the powering algorithm from Section 3.5.2. If at some step we can not compute 2^iP+2^jP because we can not compute the inverse modulo N of x_1-x_2, or we can not compute 2^iP because we can not compute the inverse of y_1 modulo N, then we compute the gcd of N and x_1-x_2 or y_1. With luck, this gcd is a nontrivial divisor of N.

11.2.4 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 ECM, then we factor a much larger integer. Let

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

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 $\mathbb{Z}/5959$. Using the formula for $P+P$ from Section 10.2.9 (implemented on a computer) 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 $\sum_{i\in B}2^iP=mP$. 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 have to 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 $(\mathbb{Z}/5959)^\times$, but fail since $x_1-x_2=1414$ and $\gcd(1414,5959)=101$. We thus find a nontrivial factor 5959 of 101.

11.2.5 A Conceptual Connection

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. Recall from Section 3.4.1 that there is an isomorphism

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

When using Pollard's method, we choose an $a\in(\mathbb{Z}/N)^\times$, 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 $a_i^m = 1$. These are, in turn, the primes p_i such that $p_i - 1$ is B-power smooth, where $m = \mathrm{lcm}(1, \ldots, m)$.

From this point of view, the only significant difference between Pollard's method and ECM is that the isomorphism f is replaced by an isomorphism

$$g_a : E_a(\mathbb{Z}/N)^\times \to E_a(\mathbb{Z}/p_1) \times \cdots \times E_a(\mathbb{Z}/p_r)$$

where E_a is defined by $y^2 = x^3 + ax + 1$, and the a of Pollard's method is replaced by the point $P = (0 : 1 : 1)$. Here $E_a(\mathbb{Z}/N)^\times$ is the *group* of elements in

$$\mathbb{P}^2(\mathbb{Z}/N) = \frac{\{(x : y : z) : x, y, z \in \mathbb{Z}/N \text{ and } \gcd(x, y, z) = 1\}}{(\text{scalar multiplication by } (\mathbb{Z}/N)^\times)}$$

that satisfy $y^2 z = x^3 + axz^2 + z^3$. The map g_a is defined by reducing $(x : y : z)$ modulo p_i for each i. When carrying out the ECM we compute mP and if some of the component of $g_a(mP)$ are zero, but others are nonzero, we find a nontrivial factor of N by taking the gcd of N and the third component of mP. The advantage of ECM is that for a fixed m we can carry out this process for many different choices of a, each time increasing the chances that we will split off "medium sized" factors of N.

11.3 Cryptography

In this section we discuss analogues of Diffie-Hellman and RSA for elliptic curves. We then discuss how the elliptic curve cryptosystem used in version 2 of the Microsoft Digital Rights Management (MS-DRM) system was cracked.

11.3.1 Elliptic Curve Analogues of RSA and Diffie-Hellman

The Diffie-Hellman key exchange from Section 4.1 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 $\mathbb{Z}/p$, and a point $P \in E(\mathbb{Z}/p)$.

2. Michael secretely chooses a random m and sends mP.

3. Nikita secretely chooses a random n and sends nP.

4. The secrete 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 4.1.2 and Section 11.3.3 below) in $E(\mathbb{Z}/p)$. For well-chosen E, P, and p experience suggests that the discrete logarithm problem in $E(\mathbb{Z}/p)$ is much more difficult than the discrete logarithm problem in $(\mathbb{Z}/p)^\times$.

There is an analogue for elliptic curves of the RSA cryptosystem of Section 4.2, but the author has never heard of anyone actually using it. Nikita sets up an RSA-elliptic curve public key, as follows:

1. Nikita secretely chooses primes p and q, and lets $N = pq$.

2. Nikita chooses an elliptic curve E over $\mathbb{Z}/N$ and considers the group $E(\mathbb{Z}/N)$ (see Section 11.2.5 for the meaning of $E(\mathbb{Z}/N)$).

3. Since Nikita knows p and q, she can use a sophisticated polynomial time algorithm of Schoof, Elkies, and Atkin (see) to compute
$$m = \#E(\mathbb{Z}/N) = \#E(\mathbb{Z}/p) \cdot \#E(\mathbb{Z}/q).$$

4. Nikita chooses a random integer e between 1 and $m-1$ that is coprime to m. She lets d be the inverse of e modulo m.

5. To encrypt a message to Nikita, Michael encodes the message as a point $P \in E(\mathbb{Z}/N)$, then sends eP. To decrypt, Nikita computes $d(eP) = (de)P = P$.

This is at best no more secure than RSA, since factoring N breaks the cryptosystem, which probably explains why it is so unpopular.

11.3.2 The ElGamal Cryptosystem and Microsoft Digital Rights Management

This section is about the ElGamal cryptosystem, which works well on an elliptic curves. It is used in version 2 of the Microsoft Digital Rights Management (MS-DRM) system.

This section draws on a paper by a hacker named Beale Screamer who cracked version 2 of MS-DRM.

The elliptic curve used in MS-DRM is an elliptic curve over the finite field $k = \mathbb{F}_p$, where
$$p = 785963102379428822376694789446897396207498568951.$$

As Beale Screamer remarks, this modulus has high nerd appeal because in hexadecimal it is
$$\text{89ABCDEF012345672718281831415926141424F7},$$
which includes counting in hexadecimal, and digits of e, π, and $\sqrt{2}$. The Microsoft elliptic curve E is
$$\begin{aligned} y^2 = x^3 &+ 317689081251325503476317476413827693272746955927x \\ &+ 79052896607878758718120572025718535432100651934. \end{aligned}$$

We have

$$\#E(k) = 785963102379428822376693024881714957612686157429,$$

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

$$\begin{aligned}B = (&771507216262649826170648268565579889907769254176, \\ &390157510246556628525279459266514995562533196655).\end{aligned}$$

Our heros Nikita and Michael love to share digital music when they are not out thwarting terrorists. When Nikita installed Microsoft's content rights management software on her laptop, it generated a private key

$$n = 670805031139910513517527207693060456300217054473,$$

which it hid in bits and pieces of files (e.g., `blackbox.dll`, `v2ks.bla`, and `IndivBox.key`). In order for Nikita to play Juno Reactor's latest hit `juno.wma`, her web browser contacts a Microsoft rights management partner. After Nikita sends her credit card number, the rights management partner sends her a license to 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 laptop still does not play `juno.wma`. This is because Michael's laptop does not know Nikita's laptop's private key (the integer n above), so Michael's laptop can not decrypt the license file.

`juno.wma`

11.3.3 The Elliptic Curve Discrete Logarithm Problem

Definition 11.3.1. If E is an elliptic curve over $\mathbb{F}_p$ and B is a point on E, then the *discrete log problem* on E to the base B is the following problem: given a point $P \in E$ such that $P = mB$ for some m, find an integer n such that $P = nB$.

For example, let E be the elliptic curve given by $y^2 = x^3 + x + 1$ over the field $\mathbb{F}_7$. We have

$$E(\mathbb{F}_7) = \{\mathcal{O}, (2,2), (0,1), (0,6), (2,5)\}.$$

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

When p is large, the discrete logarithm problem on an elliptic curve E over $\mathbb{F}_p$ is conjectured to be "very difficult", except in two special cases: if $\#E(\mathbb{F}_p)$ is "smooth" (i.e., a product of small primes) or E is "supersingular" (i.e., $\#E(\mathbb{F}_p) = p + 1$). The Microsoft curve has neither of these deficiencies, so we expect that the discrete logarithm on that curve is difficult. Beale Screamer does not solve the discrete logarithm on E; this is not how he circumvents MS-DRM.

11.3.4 ElGamal

The ElGamal public-key cryptosystem lends itself well to implementation in the group $E(\mathbb{F}_p)$. 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 $\mathbb{F}_p$, and a point $B \in E(\mathbb{F}_p)$, 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 $P \in E(\mathbb{F}_p)$, Michael computes a random integer r and the points rB and $P + r(nB)$ on $E(\mathbb{F}_p)$. 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

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

Example 11.3.2. Nikita's license files contains the pair of points $(rB, P + r(nB))$, where

$$\begin{aligned} rB = (&1796710032183157463850266557330860449821944246 60,\\ &697834385359686368249301282675141830935176314718) \end{aligned}$$

and

$$\begin{aligned} P + r(nB) = (&1378510385482644673726451580930040003436391189 15,\\ &1108485892286762240572292302235808150242248756 99). \end{aligned}$$

Nikita's laptop loads the secret key

$$n = 670805031139910513517527207693060456300217054473$$

into memory and computes

$$\begin{aligned} n(rB) = r(nB) = (&328901393518732637577115650601768681044040715701,\\ &586947838087815993601350565488788846203887988162). \end{aligned}$$

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

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

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

If Nikita knew the private key n that her laptop generated, she could compute P herself and unlock `juno.wma` and share her music with Michael. Beale Screamer found a weakness in Microsoft's system that let him find n:

> "These secret keys are stored in linked lists ... interspersed with the code in the library. The idea is that they can be read by that library, used internally by that library, and never communicated outside the library. Since the `IndivBox.key` file is shuffled in a random way for each client, these keys would be extremely difficult to extract from the file itself. Fortunately, we don't have to: these keys are part of the object state that is maintained by this library, and since the offset within this object of these secret keys is known, we can let the library itself extract the secret keys! The code for this simply loads up the 'black box' library, has it initialize an instance of the object, and then reads the keys right out of that object. This is clearly a weakness in the code which can be corrected by the DRM software fairly easily, but for now it is the basis of our exploit."

11.3.5 Why Use Elliptic Curves?

There are several advantages to using elliptic curves in cryptography.

Elliptic curve based cryptosystems with relatively small key sizes are, under certain assumptions, provably as secure as "classical" cryptosystems like RSA with much larger key sizes. And size does matter. According to Dan Boneh of Stanford University, Microsoft may soon use an elliptic curve based cryptosystem during the installation of some of their products. It is unreasonable to ask a user to type in a license key with hundreds of digits; using an elliptic curve system, they can ask the user to type in a much smaller key instead.

EXERCISES

11.1 Let $N = pq$ be a product of distinct odd primes and let $a, b \in \mathbb{Z}/N$ be such that $4a^3 + 27b^2 \neq 0$. Let E be the elliptic curve defined by $y^2 = x^3 + ax + b$. Prove that reduction modulo p and modulo q induces an isomorphism

$$E(\mathbb{Z}/N) \to E(\mathbb{Z}/p) \times E(\mathbb{Z}/q).$$

(See Section 11.2.5 for a discussion of the meaning of $E(\mathbb{Z}/N)$.)

11.2 Let m be a positive integer. Prove that any subgroup of $\mathbb{Z}/m \times \mathbb{Z}/m$ can be generated by two elements. (Hint: Count ℓ-torsion for each prime ℓ.)