11

Algorithmic Applications of Elliptic Curves

[1] We assume the reader has read Chapter 10 about elliptic curves. 1

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

All of the applications of elliptic curves that we will discuss in this chapter involve elliptic curves over finite fields (or rings).

Let p be a prime and let $\mathbb{F}_p = \mathbb{Z}/p$ be 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 $\mathbb{P}^2_{\mathbb{F}_p}$ defined by an equation of the form $y^2 = x^3 + ax + b$ such that $a, b \in \mathbb{F}_p$ and $4a^3 + 27b^2 \neq 0$.

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 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 $p \geq 5$.

---

[1] Write introduction to the chapter.

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 Equations for the Group Law

It will be useful later when we factor integers using elliptic curves to have a description of the group law in terms of equations. Suppose that $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ are nonzero points on $y^2 = x^3 + ax + b$. If $P \neq \pm Q$, let $\lambda = (y_1 - y_2)/(x_1 - x_2)$ and $\nu = y_1 - \lambda x_1$. Then $P + Q = (x_3, y_3)$ where

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

If $P = -Q$ (i.e., $x_1 = x_2$ and $y_1 = -y_2$), then $P + Q = 0$. If $P = Q$ (but $P \neq -Q$) then

$$\begin{aligned} x_3 &= \frac{(x_1^2 - a)^2 - 8bx_1}{4y_1^2}, \\ y_3 &= \frac{(3x_1^2 + a)(x_1 - x_3) - 2y_1^2}{2y_1}. \end{aligned}$$

11.1.2 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. Moreover its cardinality is bounded as follows:*

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

We will not prove this theorem in this book.[2] 2

Elliptic curves over finite fields are useful for much more than just computational applications. For example, 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 $E(\mathbb{F}_p)$, for all but finitely many p, has good transformation properties.

[2]Give good references.

11.2 An Elliptic Curve Cryptography Example

This section gives one example of an application of elliptic curves to cryptography. Our example is part of version 2 of the Microsoft Digital Rights Management (MS-DRM) system, as applied to `.wma` audio files. This protocol was made public by a hacker named Beale Screamer.

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 aren't out thwarting terrorists. When Nikita installed Microsoft's content rights management software on her compute, 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 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.

`juno.wma`

11.2.1 The Elliptic Curve Discrete Logarithm Problem

Definition 11.2.1. 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., $\#E(\mathbb{F}_p) = p + 1$).[3] The Microsoft curve has neither of these 3
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.

[3] Find references.

11.2.2 ElGamal

The only public-key cryptosystem that we have studied so far is the RSA cryptosystem (see Section 4.2), which has no natural analogue in the context of elliptic curves. Fortunately the ElGamal public-key cryptosystem lends itself well to implementation in the group $E(\mathbb{F}_p)$.

MS-DRM uses the ElGamal system. 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 of 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

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

The following example is based on an example taken from Beale Screamer's paper.

Example 11.2.2. Nikita's license files contains the pair of points $(rB, P + r(nB))$, where

$$\begin{aligned} rB = (&179671003218315746385026655733086044982194424660,\\ &697834385359686368249301282675141830935176314718) \end{aligned}$$

and

$$\begin{aligned} P + r(nB) = (&137851038548264467372645158093004000343639118915,\\ &110848589228676224057229230223580815024224875699). \end{aligned}$$

Nikita's computer sneakily 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

$$\begin{aligned} P = (&14489646124220757767,\\ &669337780373284096274895136618194604469696830074). \end{aligned}$$

The x coordinate 14489646124220757767 is the content 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 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."

Open Problem 11.2.3. *How can Microsoft store data on Nikita's computer in such a way that Nikita can not access it, but Nikita's computer can?*

11.2.3 Why Use Elliptic Curves?

There are several advantages to using elliptic curves in cryptography.

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