8 Elliptic Curve Cryptography

8.1 Elliptic Curves over a Finite Field

For the purposes of cryptography, we want to consider an elliptic curve defined over a finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ for p a prime. Given a specific curve, we can find all of the points on it by exhaustive search.

Example 8.1. Let $E : y^2 = x^3 + 3x + 8$ be an elliptic curve over $\mathbb{F}_{13}$. (We check that $4 \cdot 3^3 + 27 \cdot 8^2 = 1836 \equiv 3 \not\equiv 0 \mod 13$ so this is an elliptic curve.

If we want to find all the points on this elliptic curve, we can plug in the values $0, 1, 2, \ldots, 12$ for x and then see if the equation $y^2 \equiv a \mod 13$ has solutions (for each number, it will have either zero or two).

We start by making a list of all the squares mod 13. We see that

$$\begin{array}{llllll} 1^2 \equiv 1 & 2^2 \equiv 4 & 3^3 \equiv 9 & 4^3 \equiv 3 & 5^2 \equiv 12 & 6^2 \equiv 10 \\ 7^2 \equiv 10 & 8^2 \equiv 12 & 9^2 \equiv 3 & 10^2 \equiv 9 & 11^2 \equiv 4 & 12^2 \equiv 1 \end{array}$$

(You might notice that the second row is just the first row backwards. This is because $(-a)^2 \equiv a^2 \mod p$. Thus $y^2 \equiv a \mod 13$ has a solution if and only if $a \in \{1, 3, 4, 9, 10, 12\}$.

So now we check values for x. If $x = 0$ then we have $y^2 \equiv 8$, which has no solutions. If $x = 1$ then we have $y^2 \equiv 12$, which has the solutions $y \equiv 5$ and $y \equiv 8$. Continuing we get the list:

$$E(\mathbb{F}_{13}) = \{\mathcal{O}, (1,5), (1,8), (2,3), (2,10), (9,6), (9,7), (12,2), (12,11)\}.$$

Thus we see $E(\mathbb{F}_{13})$ has nine points.

How do we do our point addition on these curves? It's really hard to draw pictures of these things that look reasonable, since it's just a scatter of points (see figure 8.3 for an example of a picture here). But we can still write down the same *equations* we always would.

Example 8.2. Let's use the same elliptic curve as above, and let's calculate $(1,5) \oplus (9,6)$. Our line has the equation

$$y = \frac{6-5}{9-1}(x-1) + 5.$$

We need to figure out what $1/8$ is—that is, the inverse of 8 modulo 13. A little experimentation gives us the $8 \cdot 5 = 40 \equiv 1 \mod 13$ so our equation becomes

$$y = 5(x-1) + 5 = 5x.$$

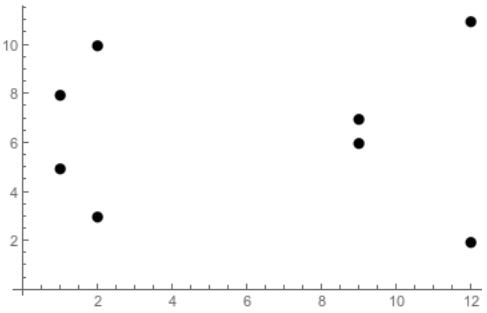

Figure 8.1: The curve $E : y^2 = x^3 + 3x + 8$ over $\mathbb{F}_{13}$

(We check that both our points are on this line; we see that $5 \cdot 1 = 5 \equiv 5$, and $9 \cdot 5 = 45 \equiv 6$).

Plugging this into our original equation gives

$$\begin{aligned}(5x)^2 &= x^3 + 3x + 8\\ 25x^2 &= x^3 + 3x + 8\\ 0 &= x^3 - 25x^2 + 3x + 8\\ &\equiv x^3 + x^2 + 3x + 8.\end{aligned}$$

This seems like it might be painful to solve, but we have effectively three approaches. The first is simply trial and error; there are only thirteen possibilities, so we can just try them all. (This works well as long as p is small).

The second is polynomial long division. We already know two roots of this polynomial: 1 and 9. (We can check that both of these are roots to make sure we haven't screwed anything up). So we can long divide by $(x - 1)$ and then by $(x - 9)$; we see that

$$x^3 + x^2 + 3x + 8 = (x - 1)(x^2 + 2x + 5) = (x - 1)(x - 9)(x - 2).$$

But the third approach extends this to be easier still. We know that our polynomial will be $(x - 1)(x - 9)(x - x_3)$ for some x_3. Thus in particular, we can see that $-1 - 9 - x_3$ will be the coefficient of x^2. Thus we have $-1 - 9 - x_3 \equiv 1 \mod 13$ and so $-x_3 \equiv 11$, so $x_3 \equiv 2$.

Plugging $x = 2$ back intou our line equation gives $y = 10$, so the third point on the line through $(1, 5)$ and $(9, 6)$ is $(2, 10)$. (We check that this point is actually on the curve; indeed, it is).

Our last step is to reflect this point vertically, to get $(2, -10) \equiv (2, 3)$. Thus $(1, 5) \oplus (9, 6) = (2, 3)$.

We can attempt to draw a picture here, but it's not super helpful. here's a picture of the line through P and Q, and then a picture of that line overlaid over E:

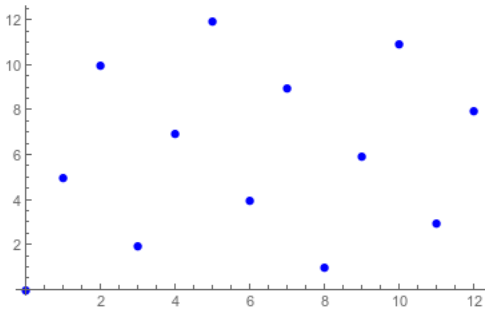

Figure 8.2: The $y = 5x$ through $(1, 5)$ and $(9, 6)$ over $\mathbb{F}_{13}$

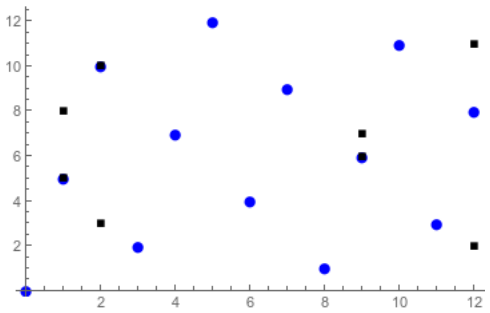

Figure 8.3: The curve $E : y^2 = x^3 + 3x + 8$ (black squares) and the line $y = 5x$ (blue circles)

As you can see, it's somewhat challenging to figure out what's going on here even already knowing the answer! This is why we turn our questions of geometry over finite fields into questions of algebra.

Example 8.3. Let's do another example. This time we'll calculate $(12, 2) \oplus (12, 2)$.

Since we're adding a point to itself, we can't just find the equation of the line going through both points. Instead we need to find the tangent line. It's not necessarily clear exactly what this should mean in modular arithmetic—there certainly isn't a curve in the picture—so we'll just fall back on what the answer "should" be from regular calculus. (I could make this rigorous. I won't). So we calculate

$$\begin{aligned} y^2 &\equiv x^3 + 3x + 8 \\ 2yy' &\equiv 3x^2 + 3 \\ 2 \cdot 2 \cdot y' &\equiv 3(-1)^2 + 3 \\ 4y' &\equiv 6 \\ 2y' &\equiv 3 \\ y' &\equiv 8. \end{aligned}$$

Thus our line is $y \equiv 8(x - 12) + 2$ or $y \equiv 8x + 10$. Again we can plug this into our elliptic

curve:

$$\begin{aligned}(8x+10)^2 &\equiv x^3+3x+8\\ 64x^2+160x+100 &\equiv x^3+3x+8\\ -x^2+4x+9 &\equiv x^3+3x+8\\ 0 &\equiv x^3+x^2-x-1.\end{aligned}$$

As before we know that $x^3+x^2-x-1 \equiv (x-12)(x-12)(x-x_3)$ so we have $-12-12-x_3 \equiv 1$, or $x_3 \equiv 1$. Plugging this into the line equation gives $y \equiv 8+10 \equiv 5$, so the third point on this line is $(1,5)$ (which is in fact on $E(\mathbb{F}_{13})$). We invert the y-coordinate, so we get $(12,2) \oplus (12,2) = (1,8)$.

8.2 The group law by formula

Notice that while we could—and did—work though every step of ellpitic curve addition in detail, most of the work we did is brute algebra, and can be automated into formulas.

Proposition 8.4. *Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve over a field K, and let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be points on $E(K)$. Then:*

1. *If $y_1 = -y_2$ (in K), then $P \oplus Q = \mathcal{O}$.*
2. *If $P_1 = P_2$, then define $\lambda = \frac{3x_1^2+A}{2y_1}$. Set*

   $$x_3 = \lambda^2 - x_1 - x_2 \qquad y_3 = \lambda(x_1 - x_3) - y_1.$$

   Then $P \oplus Q = (x_3, y_3)$.
3. *If $P_1 \neq P_2$, then define $\lambda = \frac{y_2-y_1}{x_2-x_1}$. Then as before, set*

   $$x_3 = \lambda^2 - x_1 - x_2 \qquad y_3 = \lambda(x_1 - x_3) - y_1.$$

   Then $P \oplus Q = (x_3, y_3)$.

Proof. This all follows from the sort of algebraic arguments we just made. We take λ to be the slope of the line through P and Q—the formula if $P = Q$ comes from setting $2yy' = 3x^2 + A$ so that $y' = \frac{3x^2+A}{2y}$.

The formula from x_3 comes from the observation that the coefficient of x^2 in the cubic we're solving is always $-\lambda^2$, so we have $-x_1 - x_2 - x_3 = -\lambda^2$ or $x_3 = \lambda^2 - x_1 - x_2$. The formula for y_3 comes from plugging x_3 into the equation of the line and then multiplying by -1. □

Example 8.5. Let's do one more addition on our elliptic curve $E : y^2 = x^3 + 3x + 8$ over $\mathbb{F}_{13}$. Let's compute $(2,3) \oplus (2,3)$. We observe that this is a repeated point, so we have

$$\lambda = \frac{3x_1^2 + A}{2y_1} = \frac{3 \cdot 2^2 + 3}{2 \cdot 3} = \frac{15}{6} = \frac{5}{2} = 9.$$

Then we have

$$x_3 = \lambda^2 - x_1 - x_2 = 9^2 - 2 - 2 = 60 = 12$$
$$y_3 = \lambda(x_1 - x_3) - y_1 = 9(2 - 12) - 3 = -93 = 11$$

so $(2,3) \oplus (2,3) = (12, 11)$. (This is in fact a point on the curve E, which is good).

Example 8.6. In section 7.3 we worked with the elliptic curve $E : y^2 = x^3 - 15x + 18$ over the field $\mathbb{Q}$, with $Q = (1,2), Q \oplus Q = P = (7,16)$, and $Q \oplus P = 3\mathbb{Q} = S = (-23/9, 170/27)$. Now let's compute $Q \oplus S$.

Our two points are distinct, so we have

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{170/27 - 2}{-23/9 - 1} = \frac{-29}{24}.$$

Then we have

$$x_3 = \lambda^2 - x_1 - x_2 = \frac{29^2}{24^2} - 1 - \frac{-23}{9} = \frac{193}{64}$$
$$y_3 = \lambda(x_1 - x_3) - y_1 = \frac{-29}{24}\left(1 - \frac{193}{64}\right) - 2 = \frac{223}{512}.$$

Thus $Q \oplus S = (193/64, 223/512)$.

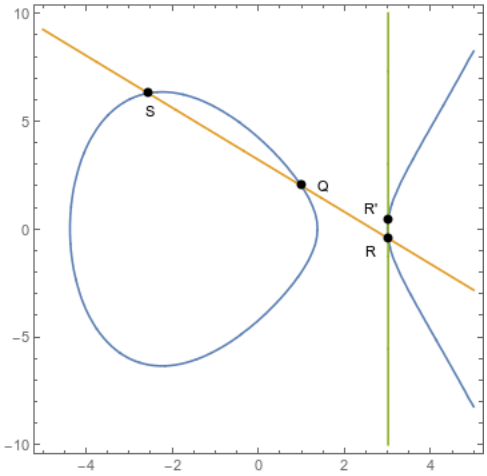

Figure 8.4: Calculating $2Q$

Theorem 8.7 (Hasse)**.** *Let E be an elliptic curve over $\mathbb{F}_p$. Then $|\#E(\mathbb{F}_p) - (p+1)| < 2\sqrt{p}$. Thus an elliptic curve over $\mathbb{F}_p$ has about $p+1$ points on it.*

Remark 8.8. The error term $p + 1 - \#E(\mathbb{F}_p) = t_p$ is called the *trace of Frobenius*, and is the trace of a 2×2 matrix acting on a vector space associated to $E/\mathbb{F}_p$. The details of this are technical, and completely irrelevant to our purposes, but are very important to my PhD research on special values of L-functions (and the Birch and Swinnerton-Dyer Conjecture).

8.3 Elliptic Curve Discrete Logarithms

In order to use elliptic curves in cryptography, we need a problem that is difficult in one direction, and easy in the other—an analogue of the discrete logarithm problem. Fortunately, exactly such a problem exists.

Definition 8.9. Let E be an elliptic curve over the finite field $\mathbb{F}_p$ and let $P, Q \in E(\mathbb{F}_p)$ be points on the curve. The *elliptic curve discrete logarithm problem* is the problem of finding an integer n such that $Q = nP$ (where the operation is the group law on the elliptic curve).

By analogy, we denote this integer by $n = \log_P(Q)$ and call n the elliptic discrete logarithm of Q with respect to P (on the curve $E/\mathbb{F}_p$) .

Example 8.10. For $E : y^2 = x^3 + 3x + 8$, what is $log_{(2,3)}(1, 8)$? That is, for what n do we have $n(2, 3) = (1, 8)$?

We already saw that $2(2, 3) = (12, 11)$. We can then compute that

$$3(2,3) = (12,11) \oplus (2,3) = (9,7)$$
$$4(2,3) = (9,7) \oplus (2,3) = (1,5)$$
$$5(2,3) = (1,5) + (2,3) = (1,8)$$

so $5(2, 3) = (1, 8)$ and we have $\log_{(2,3)}(1, 8) = 5$.

Like the regular discrete logarithm problem, it's somewhat time-consuming and expensive to compute an elliptic curve discrete logarithm. But also like the regular discrete logarithm problem, it's fairly efficient to do the opposite.

Algorithm 8.1 (Double and Add)**.** Suppose we want to compute nP for some point $P \in E(\mathbb{F}_p)$. Let $k = \log_2(n)$. Then we can:

1. Compute $2^k P$ for $2^k \leq a$. That is, compute $g, g^2, g^4, g^8, \ldots, g^{2^k}$. We can do this by repeated squaring, without computing intermediate powers.

2. Now express n in binary. That is, write $n = c_0 + c_1 \cdot 2 + c_2 \cdot 2^2 + \cdots + c_k 2^k$, where $c_i \in \{0, 1\}$.

3. Now we can compute

$$nP = (c_0 + c_1 \cdot 2 + c_2 \cdot 2^2 + \cdots + c_k 2^k)P = c_0 P \oplus c_1 2P \oplus c_2 4P \oplus \cdots \oplus c_k 2^k P$$

   But we already know $2^i P$ for each i, and the c_i are all either 0 or 1 so don't involve any computation. So we only have to do about $2k$ elliptic curve additions.

This should look familiar, since it's exactly the fast exponentiation algorithm we've already seen.

Remark 8.11. We could actually get an additional (minor) speedup by exploiting the fact that elliptic curve subtraction is just as easy as addition—this is *not* analogous to the mod-p multiplication case.

Example 8.12. For $E : y^2 = x^3 + 3x + 8$, let's compute $9(2, 3)$. We already know that $2(2, 3) = (12, 11)$ and $4(2, 3) = (1, 5)$. Then we have $8(2, 3) = (1, 5) \oplus (1, 5) = (2, 10)$. Thus $9(2, 3) = (2, 3) \oplus (2, 10) = \mathcal{O}$.

Remark 8.13. Could we have known that $9(2, 3) = \mathcal{O}$ without doing any calculations? Yes!

We know that E had eight "normal" points on it, plus the identity, for a total of nine elements in the additive group. Thus $9P = \mathcal{O}$ for any $P \in E(\mathbb{F}_{13})$.

We can adapt the baby step-giant step algorithm to attack the elliptic curve discrete logarithm problem, as we did for the regular discrete logarithm problem.

Fact 8.14. *Optimal (known) fast elliptic curve multiplication takes about* $3k/2+1$ *operations in the worst case, and* $4k/3 + 1$ *steps on the average, where* $k = \log_2(n)$*. (Algorithm 8.1 takes about* $2k$ *and* $3k/2$ *respectively, instead).*

Optimal (known) discrete logarithm solving takes about $\sqrt{p}$ *steps, where* p *is the order of the field that* E *is defined over.*

8.4 Cryptographic Algorithms

We can, effectively, implement all of our discrete logarithm-based cryptographic algorithms with elliptic curve discrete logarithms instead.

Algorithm 8.2 (Elliptic Curve Diffie-Hellman)**.** Alice and Bob wish to exchange a key. They follow the following steps:

1. A public party chooses a large prime p, and an elliptic curve E over $\mathbb{F}_p$, and a point $P \in E(\mathbb{F}_p)$.
2. Alice chooses a secret integer n_A, and Bob chooses a secret integer n_B. Neither party reveals this integer to anyone.
3. Alice computes $Q_A = n_A P$ and Bob computes $Q_B = n_B P$. They (publicly) exchange these values with each other.
4. Now Alice computes $n_A Q_B$ and Bob computes $n_B Q_A$.
5. $n_A Q_B = n_A n_B P = n_B n_A P = n_B Q_a$, so they now have a shared key.

Algorithm 8.3 (Elliptic Curve ElGamal)**.** First Alice generates a private key and a public key.

1. Choose a large prime number p, an elliptic curve E over $\mathbb{F}_p$, and a point $P \in E(\mathbb{F}_p)$ of large order. This is generally done by a large trusted party.
2. Alice chooses a private key n_A.
3. Alice computes and publishes a public key $Q_A = n_A P \in E(\mathbb{F}_p)$.

Now suppose Bob wishes to send Alice a a message encoded as a point $M \in E(\mathbb{F}_p)$.

1. Bob generates a random ephemeral key k.
2. Bob computes $C_1 = kP \in E(\mathbb{F}_p), C_2 = M + kQ_A \in E(\mathbb{F}_p)$. Bob transmits the pair of points (C_1, C_2) to Alice.

Alice decrypts the message using her private key n_A. She computes $C_2 - n_A C_1 \in E(\mathbb{F}_p)$. We see that this is

$$C_2 - n_a C_1 = M + kQ_A - n_A kP = M + kn_A P - n_A kP = M.$$

Remark 8.15. Elliptic curve cryptography introduces one layer of added inefficiency: a single point contains about $\log_2(p)$ bits of information, since an elliptic curve over $\mathbb{F}_p$ has about p points. But since we need to transmit two numbers mod p to convey one point, we have to send $2\log_2(p)$ bits of information!

There are various hacks to get around this problem. Most of them involve the fact that if we know the x-coordinate of a point on E, then we know the y-coordinate up to a change of sign. So there are schemes involving only caring about the x coordinate, or involving transmitting the x-coordinate and a parity bit to specify which of the two possible y-coordinates you had chosen, rather than transmitting the entire number.

Another issue with elliptic curve cryptography is the choice of curve and point. It is computationally expensive to ensure that a curve does not have any hidden weaknesses, so curves are generally chosen once by a respected standards body. In practice in the USA, they are often chosen by NIST.

In 2013, the New York Times revealed that some of the standard curves chosen by NIST were chosen due to influence by the NSA, which had introduced a secret weakness into the chosen curves, which allowed it to crack encryption based on those curves.

However, elliptic curve cryptography has a major advantage over algorithms based on modular arithmetic: the General Number Field Sieve. This algorithm, which we discussed in 6.3.1, is the most efficient known algorithm for breaking RSA, and can also be adapted to attack vanilla ElGamal and most similar cryptosystems based on modular arithmetic. But nothing similar is known in the case of elliptic curves. Thus elliptic curve cryptography provides substantially greater strength for the same size key.

Under current knowledge and assumptions, we have the following table, explaining what key lengths provide equivalent levels of security for symmetric algorithms, RSA, and ECC.

Symmetric Key Size	RSA Key Size	ECC Key Size
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Thus modern RSA often uses 2048 bits. AES, which is one of the most common symmetric algorithms, uses 128, 192, or 256 bits instead. Modern ECC uses 224 or 256 bits. Thus ECC keys can be much shorter, and in turn computations with them can be much faster.