Chapter 5

The Discrete Logarithm Problem

Let p be a prime and let a, b be integers that are nonzero mod p. Suppose we know that there exists an integer k such that

$$a^k \equiv b \pmod{p}.$$

The classical **discrete logarithm problem** is to find k. Since $k + (p-1)$ is also a solution, the answer k should be regarded as being defined mod $p-1$, or mod a divisor d of $p-1$ if $a^d \equiv 1 \pmod{p}$.

More generally, let G be any group, written multiplicatively for the moment, and let $a, b \in G$. Suppose we know that $a^k = b$ for some integer k. In this context, the discrete logarithm problem is again to find k. For example, G could be the multiplicative group $\mathbf{F}_q^\times$ of a finite field. Also, G could be $E(\mathbf{F}_q)$ for some elliptic curve, in which case a and b are points on E and we are trying to find an integer k with $ka = b$.

In Chapter 6, we'll meet several cryptographic applications of the discrete logarithm problem. The security of the cryptosystems will depend on the difficulty of solving the discrete log problem.

One way of attacking a discrete log problem is simple brute force: try all possible values of k until one works. This is impractical when the answer k can be an integer of several hundred digits, which is a typical size used in cryptography. Therefore, better techniques are needed.

In this chapter, we start by discussing an attack, called the index calculus, that can be used in $\mathbf{F}_p^\times$, and more generally in the multiplicative group of a finite field. However, it does not apply to general groups. Then we discuss the method of Pohlig-Hellman, the baby step, giant step method, and Pollard's ρ and λ methods. These work for general finite groups, in particular for elliptic curves. Finally, we show that for special classes of elliptic curves, namely supersingular and anomalous curves, it is possible to reduce the discrete log problem to easier discrete log problems (in the multiplicative group of a finite field and in the additive group of integers mod a prime, respectively).

5.1 The Index Calculus

Let p be a prime and let g be primitive root (see Appendix A) mod p, which means that g is a generator for the cyclic group $\mathbf{F}_p^\times$. In other words, every $h \not\equiv 0 \pmod{p}$ can be written in the form $h \equiv g^k$ for some integer k that is uniquely determined mod $p-1$. Let $k = L(h)$ denote the **discrete logarithm** of h with respect to g and p, so

$$g^{L(h)} \equiv h \pmod{p}.$$

Suppose we have h_1 and h_2. Then

$$g^{L(h_1h_2)} \equiv h_1h_2 \equiv g^{L(h_1)+L(h_2)} \pmod{p},$$

which implies that

$$L(h_1h_2) \equiv L(h_1) + L(h_2) \pmod{p-1}.$$

Therefore, L changes multiplication into addition, just like the classical logarithm function.

The **index calculus** is a method for computing values of the discrete log function L. The idea is to compute $L(\ell)$ for several small primes ℓ, then use this information to compute $L(h)$ for arbitrary h. It is easiest to describe the method with an example.

Example 5.1

Let $p = 1217$ and $g = 3$. We want to solve $3^k \equiv 37 \pmod{1217}$. Most of our work will be precomputation that will be independent of the number 37. Let's choose a set of small primes, called the **factor base**, to be $B = \{2, 3, 5, 7, 11, 13\}$. First, we find relations of the form

$$3^x \equiv \pm\text{product of some primes in } B \pmod{1217}.$$

Eventually, we find the following:

$$\begin{aligned} 3^1 &\equiv 3 \pmod{1217} \\ 3^{24} &\equiv -2^2 \cdot 7 \cdot 13 \\ 3^{25} &\equiv 5^3 \\ 3^{30} &\equiv -2 \cdot 5^2 \\ 3^{54} &\equiv -5 \cdot 11 \\ 3^{87} &\equiv 13 \end{aligned}$$

These can be changed into equations for discrete logs, where now the congruences are all mod $p-1 = 1216$. Note that we already know that $3^{(p-1)/2} \equiv -1$

(mod p), so $L(-1) = 608$.

$$\begin{aligned} 1 &\equiv L(3) \pmod{1216} \\ 24 &\equiv 608 + 2L(2) + L(7) + L(13) \\ 25 &\equiv 3L(5) \\ 30 &\equiv 608 + L(2) + 2L(5) \\ 54 &\equiv 608 + L(5) + L(11) \\ 87 &\equiv L(13) \end{aligned}$$

The first equation yields $L(3) \equiv 1$. The third yields $L(5) \equiv 819 \pmod{1216}$. The sixth yields $L(13) \equiv 87$. The fourth gives

$$L(2) \equiv 30 - 608 - 2 \cdot 819 \equiv 216 \pmod{1216}.$$

The fifth yields $L(11) \equiv 54 - 608 - L(5) \equiv 1059$. Finally, the second gives

$$L(7) \equiv 24 - 608 - 2L(2) - L(13) \equiv 113 \pmod{1216}.$$

We now know the discrete logs of all the elements of the factor base.

Recall that we want to solve $3^k \equiv 37 \pmod{1216}$. We compute $3^j \cdot 37 \pmod{p}$ for several random values of j until we obtain an integer that can be factored into a product of primes in B. In our case, we find that

$$3^{16} \cdot 37 \equiv 2^3 \cdot 7 \cdot 11 \pmod{1217}.$$

Therefore,

$$L(37) \equiv 3L(2) + L(7) + L(11) - 16 \equiv 588 \pmod{1216},$$

and $3^{588} \equiv 37 \pmod{1217}$. ∎

The choice of the size of the factor base B is important. If B is too small, then it will be very hard to find powers of g that factor with primes in B. If B is too large, it will be easy to find relations, but the linear algebra needed to solve for the logs of the elements of B will be unwieldy. An example that was completed in 2001 by A. Joux and R. Lercier used the first 1 million primes to compute discrete logs mod a 120-digit prime.

There are various methods that produce relations of the form $g^x \equiv$ product of primes in B. A popular one uses the number field sieve. See [58].

The expected running time of the index calculus is approximately a constant times $\exp(\sqrt{2 \ln p \ln \ln p})$ (see [81, p. 129]), which means that it is a subexponential algorithm. The algorithms in Section 5.2, which are exponential algorithms, run in time approximately $\sqrt{p} = \exp(\frac{1}{2} \ln p)$. Since $\sqrt{2 \ln p \ln \ln p}$ is much smaller than $\frac{1}{2} \ln p$ for large p, the index calculus is generally much faster when it can be used.

Note that the index calculus depends heavily on the fact that integers can be written as products of primes. An analogue of this is not available for arbitrary groups.

There is a generalization of the index calculus that works for finite fields, but it requires some algebraic number theory, so we do not discuss it here.

In Section 13.4, we show how an analogue of the index calculus can be applied to groups arising from hyperelliptic curves.

5.2 General Attacks on Discrete Logs

In this section, we discuss attacks that work for arbitrary groups. Since our main focus is elliptic curves, we write our group G additively. Therefore, we are given $P, Q \in G$ and we are trying to solve $kP = Q$ (we always assume that k exists). Let N be the order of G. Usually, we assume N is known. For simplicity, it is usually assumed that P generates G.

5.2.1 Baby Step, Giant Step

This method, developed by D. Shanks [107], requires approximately $\sqrt{N}$ steps and around $\sqrt{N}$ storage. Therefore it only works well for moderate sized N. The procedure is as follows.

1. Fix an integer $m \geq \sqrt{N}$ and compute mP.
2. Make and store a list of iP for $0 \leq i < m$.
3. Compute the points $Q - jmP$ for $j = 0, 1, \cdots m-1$ until one matches an element from the stored list.
4. If $iP = Q - jmP$, we have $Q = kP$ with $k \equiv i + jm \pmod{N}$.

Why does this work? Since $m^2 > N$, we may assume the answer k satisfies $0 \leq k < m^2$. Write $k = k_0 + mk_1$ with $k_0 \equiv k \pmod{m}$ and $0 \leq k_0 < m$ and let $k_1 = (k - k_0)/m$. Then $0 \leq k_1 < m$. When $i = k_0$ and $j = k_1$, we have

$$Q - k_1 mP = kP - k_1 mP = k_0 P,$$

so there is a match.

The point iP is calculated by adding P (a "**baby step**") to $(i-1)P$. The point $Q - jmP$ is computed by adding $-mP$ (a "**giant step**") to $Q - (j-1)mP$. The method was developed by Shanks for computations in algebraic number theory.

Note that we did not need to know the exact order N of G. We only required an upper bound for N. Therefore, for elliptic curves over $\mathbf{F}_q$, we could use this method with $m^2 \geq q + 1 + 2\sqrt{q}$, by Hasse's theorem.

A slight improvement of the method can be made for elliptic curves by computing and storing only the points iP for $0 \leq i \leq m/2$ and checking whether $Q - jmP = \pm iP$ (see Exercise 5.1).

Example 5.2
Let $G = E(\mathbf{F}_{41})$, where E is given by $y^2 = x^3 + 2x + 1$. Let $P = (0, 1)$ and $Q = (30, 40)$. By Hasse's theorem, we know that the order of G is at most 54, so we let $m = 8$. The points iP for $1 \leq i \leq 7$ are

$$(0, 1), (1, 39), (8, 23), (38, 38), (23, 23), (20, 28), (26, 9).$$

We calculate $Q - jmP$ for $j = 0, 1, 2$ and obtain

$$(30, 40),\ (9, 25),\ (26, 9),$$

at which point we stop since this third point matches $7P$. Since $j = 2$ yielded the match, we have

$$(30, 40) = (7 + 2 \cdot 8)P = 23P.$$

Therefore $k = 23$. □

5.2.2 Pollard's ρ and λ Methods

A disadvantage of the Baby Step, Giant Step method is that it requires a lot of storage. Pollard's ρ and λ methods [87] run in approximately the same time as Baby Step, Giant Step, but require very little storage. First, we'll discuss the ρ method, then its generalization to the λ method.

Let G be a finite group of order N. Choose a function $f : G \to G$ that behaves rather randomly. Then start with a random element P_0 and compute the iterations $P_{i+1} = f(P_i)$. Since G is a finite set, there will be some indices $i_0 < j_0$ such that $P_{i_0} = P_{j_0}$. Then

$$P_{i_0+1} = f(P_{i_0}) = f(P_{j_0}) = P_{j_0+1},$$

and, similarly, $P_{i_0+\ell} = P_{j_0+\ell}$ for all $\ell \geq 0$. Therefore, the sequence P_i is periodic with period $j_0 - i_0$ (or possibly a divisor of $j_0 - i_0$). The picture describing this process (see Figure 5.1) looks like the Greek letter ρ, which is why it is called **Pollard's ρ method**. If f is a randomly chosen random function (we'll not make this precise), then we expect to find a match with j_0 at most a constant times $\sqrt{N}$. For an analysis of the running time for various choices of function f, see [119].

A naive implementation of the method stores all the points P_i until a match is found. This takes around $\sqrt{N}$ storage, which is similar to Baby Step, Giant Step. However, as R. W. Floyd has pointed out, it is possible to do much better at the cost of a little more computation. The key idea is that once there is a match for two indices differing by d, all subsequent indices differing by d will yield matches. This is just the periodicity mentioned above. Therefore, we can compute pairs (P_i, P_{2i}) for $i = 1, 2, \ldots$, but only keep the current pair; we don't store the previous pairs. These can be calculated by the rules

$$P_{i+1} = f(P_i), \quad P_{2(i+1)} = f(f(P_{2i})).$$

Suppose $i \geq i_0$ and i is a multiple of d. Then the indices $2i$ and i differ by a multiple of d and hence yield a match: $P_i = P_{2i}$. Since $d \leq j_0$ and $i_0 < j_0$, it follows easily that there is a match for $i \leq j_0$. Therefore, the number of steps to find a match is expected to be at most a constant multiple of $\sqrt{N}$.

Another method of finding a match is to store only those points P_i that satisfy a certain property (call them "distinguished points"). For example, we could require the last k bits of the binary representation of the x-coordinate to be 0. We then store, on the average, one out of every 2^k points P_i. Suppose there is a match $P_i = P_j$ but P_i is not one of these distinguished points. We expect $P_{i+\ell}$ to be a distinguished point for some ℓ with $1 \leq \ell \leq 2^k$, approximately. Then $P_{j+\ell} = P_{i+\ell}$, so we find a match between distinguished points with only a little more computation.

The problem remains of how to choose a suitable function f. Besides having f act randomly, we need to be able to extract useful information from a match. Here is one way of doing this. Divide G into s disjoint subsets $S_1, S_2, \ldots, S_s$ of approximately the same size. A good choice for s seems to be around 20. Choose $2s$ random integers $a_i, b_i \bmod N$. Let

$$M_i = a_i P + b_i Q.$$

Finally, define

$$f(g) = g + M_i \quad \text{if } g \in S_i.$$

The best way to think of f is as giving a random walk in G, with the possible steps being the elements M_i.

Finally, choose random integers a_0, b_0 and let $P_0 = a_0 P + b_0 Q$ be the starting point for the random walk. While computing the points P_j, we also record how these points are expressed in terms of P and Q. If $P_j = u_j P + v_j Q$ and $P_{j+1} = P_j + M_i$, then $P_{j+1} = (u_j + a_i)P + (v_j + b_i)Q$, so $(u_{j+1}, v_{j+1}) = (u_j, v_j) + (a_i, b_i)$. When we find a match $P_{j_0} = P_{i_0}$, then we have

$$u_{j_0} P + v_{j_0} Q = u_{i_0} P + v_{i_0} Q, \text{ hence } (u_{i_0} - u_{j_0})P = (v_{j_0} - v_{i_0})Q.$$

If $\gcd(v_{j_0} - v_{i_0}, N) = d$, we have

$$k \equiv (v_{j_0} - v_{i_0})^{-1}(u_{i_0} - u_{j_0}) \pmod{N/d}.$$

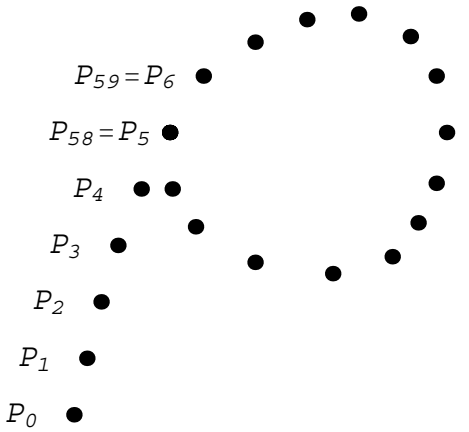

Figure 5.1
Pollard's Rho Method

This gives us d choices for k. Usually, d will be small, so we can try all possibilities until we have $Q = kP$.

In cryptographic applications, N is often prime, in which case, $d = 1$ or N. If $d = N$, we have a trivial relation (the coefficients of both P and Q are multiples of N), so we start over. If $d = 1$, we obtain k.

Example 5.3
Let $G = E(\mathbf{F}_{1093})$, where E is the elliptic curve given by $y^2 = x^3 + x + 1$. We'll use $s = 3$. Let $P = (0, 1)$ and $Q = (413, 959)$. It can be shown that the order of P is 1067. We want to find k such that $kP = Q$. Let

$$P_0 = 3P + 5Q, \quad M_0 = 4P + 3Q, \quad M_1 = 9P + 17Q, \quad M_2 = 19P + 6Q.$$

Let $f : E(\mathbf{F}_{1093}) \to E(\mathbf{F}_{1093})$ be defined by

$$f(x, y) = (x, y) + M_i \quad \text{if } x \equiv i \pmod 3.$$

Here the number x is regarded as an integer $0 \le x < 1093$ and is then reduced mod 3. For example,

$$f(P_0) = P_0 + M_2 = (727, 589),$$

since $P_0 = (326, 69)$ and $326 \equiv 2 \pmod 3$.

We can define $f(\infty) = \infty$ if we want. However, if we encounter $f(\infty)$, we have found a relation of the form $aP + bQ = \infty$ and can find k easily (if the relation isn't something trivial like $1067P + 2134Q = \infty$). Therefore, we don't worry about ∞.

If we compute P_0, $P_1 = f(P_0)$, $P_2 = f(P_1), \ldots$, we obtain

$$P_0 = (326, 69),\ P_1 = (727, 589),\ P_2 = (560, 365),\ P_3 = (1070, 260),$$
$$P_4 = (473, 903),\ P_5 = (1006, 951),\ P_6 = (523, 938),\ \ldots,$$
$$P_{57} = (895, 337),\ P_{58} = (1006, 951),\ P_{59} = (523, 938),\ \ldots.$$

Therefore, the sequence starts repeating at $P_5 = P_{58}$.

If we keep track of the coefficients of P and Q in the calculations, we find that

$$P_5 = 88P + 46Q \quad \text{and} \quad P_{58} = 685P + 620Q.$$

Therefore,

$$\infty = P_{58} - P_5 = 597P + 574Q.$$

Since P has order 1067, we calculate

$$-574^{-1}597 \equiv 499 \pmod{1067}.$$

Therefore, $Q = 499P$, so $k = 499$.

We stored all of the points $P_0, P_1, \ldots, P_{58}$ until we found a match. Instead, let's repeat the computation, but compute the pairs (P_i, P_{2i}) and store nothing except the current pair. We then find that for $i = 53$ there is the match $P_{53} = P_{106}$. This yields

$$620P + 557Q = P_{53} = P_{106} = 1217P + 1131Q.$$

Therefore, $597P + 574Q = \infty$, which yields $k = 499$, as before. ∎

Pollard's λ method uses a function f as in the ρ method, but several random starting points $P_0^{(1)}, \ldots, P_0^{(r)}$ are used. We then get sequences defined by

$$P_{i+1}^{(\ell)} = f(P_i^{(\ell)}), \quad 1 \le \ell \le r, \quad i = 0, 1, 2, \ldots.$$

These can be computed by several computers in parallel. Points satisfying certain conditions are called distinguished and are reported to a central computer. When a match is found among the inputs from the various computers, we have a relation that should allow us to solve the discrete log problem, as in the ρ method. When there is a match between two sequences, these two sequences will always match from that point on. We only need to look at distinguished points because distinguished points should occur soon after a match occurs.

When there are only two random starting points, we have two random walks. Eventually they will have a point in common, and therefore they will coincide thereafter. The picture of this process resembles the Greek letter λ, hence the name.

Sometimes the λ method is described in terms of kangaroos jumping around a field (this is the random walk). A variant of the λ method with two random

walks records every 10th point, for example, in the first sequence and then checks whether the second sequence matches any of these points. In this case, the first sequence is called a tame kangaroo, and the second is called a wild kangaroo. The idea is to use the tame kangaroo to catch the wild kangaroo.

The λ method is expected to find a match in at most a constant times $\sqrt{N}$ steps. If it is run in parallel with many starting points, the running time can be improved significantly.

Finally, we should point out a difference between the baby step, giant step method and the ρ and λ methods. The baby step, giant step method is **deterministic**, which means that it is guaranteed to finish within the predicted time of a constant times $\sqrt{N}$. On the other hand, the ρ and λ methods are **probabilistic**, which means that there is a very high probability that they will finish within the predicted time, but this is not guaranteed.

5.2.3 The Pohlig-Hellman Method

As before, P, Q are elements in a group G and we want to find an integer k with $Q = kP$. We also know the order N of P and we know the prime factorization

$$N = \prod_i q_i^{e_i}$$

of N. The idea of Pohlig-Hellman is to find $k \pmod{q_i^{e_i}}$ for each i, then use the Chinese Remainder theorem to combine these and obtain $k \pmod{N}$.

Let q be a prime, and let q^e be the exact power of q dividing N. Write k in its base q expansion as

$$k = k_0 + k_1 q + k_2 q^2 + \cdots$$

with $0 \leq k_i < q$. We'll evaluate $k \pmod{q^e}$ by successively determining $k_0, k_1, \ldots, k_{e-1}$. The procedure is as follows.

1. Compute $T = \left\{ j \left(\frac{N}{q} P \right) \mid 0 \leq j \leq q-1 \right\}$.
2. Compute $\frac{N}{q} Q$. This will be an element $k_0 \left(\frac{N}{q} P \right)$ of T.
3. If $e = 1$, stop. Otherwise, continue.
4. Let $Q_1 = Q - k_0 P$.
5. Compute $\frac{N}{q^2} Q_1$. This will be an element $k_1 \left(\frac{N}{q} P \right)$ of T.
6. If $e = 2$, stop. Otherwise, continue.
7. Suppose we have computed $k_0, k_1, \ldots, k_{r-1}$, and $Q_1, \ldots, Q_{r-1}$.

8. Let $Q_r = Q_{r-1} - k_{r-1}q^{r-1}P$.

9. Determine k_r such that $\frac{N}{q^{r+1}}Q_r = k_r\left(\frac{N}{q}P\right)$.

10. If $r = e-1$, stop. Otherwise, return to step (7).

Then

$$k \equiv k_0 + k_1 q + \cdot + k_{e-1}q^{e-1} \pmod{q^e}.$$

Why does this work? We have

$$\frac{N}{q}Q = \frac{N}{q}(k_0 + k_1 q + \cdots)P$$
$$= k_0\frac{N}{q}P + (k_1 + k_2 q + \cdots)NP = k_0\frac{N}{q}P,$$

since $NP = \infty$. Therefore, step (2) finds k_0. Then

$$Q_1 = Q - k_0 P = (k_1 q + k_2 q^2 + \cdots)P,$$

so

$$\frac{N}{q^2}Q_1 = (k_1 + k_2 q + \cdots)\frac{N}{q}P$$
$$= k_1\frac{N}{q}P + (k_2 + k_3 q + \cdots)NP = k_1\frac{N}{q}P.$$

Therefore, we find k_1. Similarly, the method produces $k_2, k_3, \ldots$. We have to stop after $r = e-1$ since N/q^{e+1} is no longer an integer, and we cannot multiply Q_e by the noninteger N/q^{e+1}. Besides, we do not need to continue because we now know $k \bmod q^e$.

Example 5.4

Let $G = E(\mathbf{F}_{599})$, where E is the elliptic curve given by $y^2 = x^3 + 1$. Let $P = (60, 19)$ and $Q = (277, 239)$. The methods of Section 4.3.3 can be used to show that P has order $N = 600$. We want to solve $Q = kP$ for k. The prime factorization of N is

$$600 = 2^3 \cdot 3 \cdot 5^2.$$

We'll compute k mod 8, mod 3, and mod 25, then recombine to obtain k mod 600 (the Chinese Remainder Theorem allows us to do this).

k mod 8. We compute $T = \{\infty, (598, 0)\}$. Since

$$(N/2)Q = \infty = 0 \cdot \left(\frac{N}{2}P\right),$$

we have $k_0 = 0$. Therefore,

$$Q_1 = Q - 0P = Q.$$

Since $(N/4)Q_1 = 150Q_1 = (598, 0) = 1 \cdot \frac{N}{2}P$, we have $k_1 = 1$. Therefore,

$$Q_2 = Q_1 - 1 \cdot 2 \cdot P = (35, 243).$$

Since $(N/8)Q_2 = 75Q_2 = \infty = 0 \cdot \frac{N}{2}P$, we have $k_2 = 0$. Therefore,

$$k = 0 + 1 \cdot 2 + 0 \cdot 4 + \cdots \equiv 2 \pmod 8.$$

k mod 3. We have $T = \{\infty, (0, 1), (0, 598)\}$. Since

$$(N/3)Q = (0, 598) = 2 \cdot \frac{N}{3}P,$$

we have $k_0 = 2$. Therefore,

$$k \equiv 2 \pmod 3.$$

k mod 25. We have

$$T = \{\infty,\ (84, 179),\ (491, 134),\ (491, 465),\ (84, 420)\}.$$

Since $(N/5)Q = (84, 179)$, we have $k_0 = 1$. Then

$$Q_1 = Q - 1 \cdot P = (130, 129).$$

Since $(N/25)Q_1 = (491, 465)$, we have $k_1 = 3$. Therefore,

$$k = 1 + 3 \cdot 5 + \cdots \equiv 16 \pmod{25}.$$

We now have the simultaneous congruences

$$\begin{cases} x \equiv 2 \pmod 8 \\ x \equiv 2 \pmod 3 \\ x \equiv 16 \pmod{25} \end{cases}.$$

These combine to yield $k \equiv 266 \pmod{600}$, so $k = 266$. ∎

The Pohlig-Hellman method works well if all of the prime numbers dividing N are small. However, if q is a large prime dividing N, then it is difficult to list the elements of T, which contains q elements. We could try to find the k_i without listing the elements; however, finding k_i is a discrete log problem in the group generated by $(N/q)P$, which has order q. If q is of the same order of magnitude as N (for example, $q = N$ or $q = N/2$), then the Pohlig-Hellman method is of little use. For this reason, if a cryptographic system is based on

discrete logs, the order of the group should be chosen so it contains a large prime factor.

If N contains some small prime factors, then the Pohlig-Hellman method can be used to obtain partial information on the value of k, namely a congruence modulo a product of these small prime factors. In certain cryptographic situations, this could be undesirable. Therefore, the group G is often chosen to be of large prime order. This can be accomplished by starting with a group that has a large prime q in its order. Pick a random point P_1 and compute its order. With high probability (at least $1 - 1/q$; cf. Remark 5.2), the order of P_1 is divisible by q, so in a few tries, we can find such a point P_1. Write the order of P_1 as qm. Then $P = mP_1$ will have order q. As long as q is sufficiently large, discrete log problems in the cyclic group generated by P will resist the Pohlig-Hellman attack.

5.3 Attacks with Pairings

One strategy for attacking a discrete logarithm problem is to reduce it to an easier discrete logarithm problem. This can often be done with pairings such as the Weil pairing or the Tate-Lichtenbaum pairing, which reduce a discrete logarithm problem on an elliptic curve to one in the multiplicative group of a finite field.

5.3.1 The MOV Attack

The MOV attack, named after Menezes, Okamoto, and Vanstone [80], uses the Weil pairing to convert a discrete log problem in $E(\mathbf{F}_q)$ to one in $\mathbf{F}_{q^m}^\times$. Since discrete log problems in finite fields can be attacked by index calculus methods, they can be solved faster than elliptic curve discrete log problems, as long as the field $\mathbf{F}_{q^m}$ is not much larger than $\mathbf{F}_q$. For supersingular curves, we can usually take $m = 2$, so discrete logarithms can be computed more easily for these curves than for arbitrary elliptic curves. This is unfortunate from a cryptographic standpoint since an attractive feature of supersingular curves is that calculations can often be done quickly on them (see Section 4.6).

Recall that for an elliptic curve E defined over $\mathbf{F}_q$, we let $E[N]$ denote the set of points of order dividing N with coordinates in the algebraic closure. If $\gcd(q, N) = 1$ and $S, T \in E[N]$, then the Weil pairing $e_N(S, T)$ is an Nth root of unity and can be computed fairly quickly. The pairing is bilinear, and if $\{S, T\}$ is a basis for $E[N]$, then $e_N(S, T)$ is a primitive Nth root of unity. For any S, $e_N(S, S) = 1$. For more properties of the Weil pairing, see Sections 3.3 and 11.2.

Let E be an elliptic curve over $\mathbf{F}_q$. Let $P, Q \in E(\mathbf{F}_q)$. Let N be the order of P. Assume that

$$\gcd(N, q) = 1.$$

We want to find k such that $Q = kP$. First, it's worthwhile to check that k exists.

LEMMA 5.1

There exists k such that $Q = kP$ if and only if $NQ = \infty$ and the Weil paring $e_N(P, Q) = 1$.

PROOF If $Q = kP$, then $NQ = kNP = \infty$. Also,

$$e_N(P, Q) = e_N(P, P)^k = 1^k = 1.$$

Conversely, if $NQ = \infty$, then $Q \in E[N]$. Since $\gcd(N, q) = 1$, we have $E[N] \simeq \mathbf{Z}_N \oplus \mathbf{Z}_N$, by Theorem 3.2. Choose a point R such that $\{P, R\}$ is a basis of $E[N]$. Then

$$Q = aP + bR$$

for some integers a, b. By Corollary 3.10, $e_N(P, R) = \zeta$ is a primitive Nth root of unity. Therefore, if $e_N(P, Q) = 1$, we have

$$1 = e_N(P, Q) = e_N(P, P)^a e_N(P, R)^b = \zeta^b.$$

This implies that $b \equiv 0 \pmod{N}$, so $bR = \infty$. Therefore, $Q = aP$, as desired. ∎

The idea used to prove the lemma yields the MOV attack on discrete logs for elliptic curves. Choose m so that

$$E[N] \subseteq E(\mathbf{F}_{q^m}).$$

Since all the points of $E[N]$ have coordinates in $\overline{\mathbf{F}}_q = \cup_{j \geq 1} \mathbf{F}_{q^j}$, such an m exists. By Corollary 3.11, the group μ_N of Nth roots of unity is contained in $\mathbf{F}_{q^m}$. All of our calculations will be done in $\mathbf{F}_{q^m}$. The algorithm is as follows.

1. Choose a random point $T \in E(\mathbf{F}_{q^m})$.
2. Compute the order M of T.
3. Let $d = \gcd(M, N)$, and let $T_1 = (M/d)T$. Then T_1 has order d, which divides N, so $T_1 \in E[N]$.
4. Compute $\zeta_1 = e_N(P, T_1)$ and $\zeta_2 = e_N(Q, T_1)$. Then both ζ_1 and ζ_2 are in $\mu_d \subseteq \mathbf{F}_{q^m}^{\times}$.
5. Solve the discrete log problem $\zeta_2 = \zeta_1^k$ in $\mathbf{F}_{q^m}^{\times}$. This will give $k \pmod{d}$.

6. Repeat with random points T until the least common multiple of the various d's obtained is N. This determines $k \pmod N$.

REMARK 5.2 At first, it might seem that $d = 1$ will occur very often. However, the opposite is true because of the structure of $E(\mathbf{F}_{q^m})$. Recall that

$$E(\mathbf{F}_{q^m}) \simeq \mathbf{Z}_{n_1} \oplus \mathbf{Z}_{n_2}$$

for some integers n_1, n_2 with $n_1 | n_2$ (possibly, $n_1 = 1$, in which case the group is cyclic). Then $N | n_2$, since n_2 is the largest possible order of an element of the group. Let B_1, B_2 be points of orders n_1, n_2, respectively, such that B_1, B_2 generate $E(\mathbf{F}_{q^m})$. Then $T = a_1 B_1 + a_2 B_2$. Let ℓ^e be a prime power dividing N. Then $\ell^f | n_2$ with $f \geq e$. If $\ell \nmid a_2$, then ℓ^f divides M, the order of T. Therefore, $\ell^e | d = \gcd(M, N)$. Since the probability that $\ell \nmid a_2$ is $1 - 1/\ell$, the probability is at least this high that the full power ℓ^e is in d. After a few choices of T, this should be the case. (Note that our probability estimates are low, since we never included the possible contribution of the $a_1 B_1$ term.) Therefore, a few iterations of the algorithm should yield k. ∎

Potentially, the integer m could be large, in which case the discrete log problem in the group $\mathbf{F}_{q^m}^\times$, which has order $q^m - 1$, is just as hard as the original discrete log problem in the smaller group $E(\mathbf{F}_q)$, which has order approximately q, by Hasse's theorem. However, for supersingular curves, we can usually take $m = 2$, as the next result shows.

Let E be an elliptic curve over $\mathbf{F}_q$, where q is a power of the prime number p. Then

$$\#E(\mathbf{F}_q) = q + 1 - a$$

for some integer a. The curve E is called **supersingular** if $a \equiv 0 \pmod p$. Corollary 4.32 says that this is equivalent to $a = 0$ when $q = p \geq 5$.

PROPOSITION 5.3

Let E be an elliptic curve over $\mathbf{F}_q$ and suppose $a = q + 1 - \#E(\mathbf{F}_q) = 0$. Let N be a positive integer. If there exists a point $P \in E(\mathbf{F}_q)$ of order N, then $E[N] \subseteq E(\mathbf{F}_{q^2})$.

PROOF The Frobenius endomorphism ϕ_q satisfies $\phi_q^2 - a\phi_q + q = 0$. Since $a = 0$, this reduces to

$$\phi_q^2 = -q.$$

Let $S \in E[N]$. Since $\#E(\mathbf{F}_q) = q + 1$, and since there exists a point of order N, we have $N | q + 1$, or $-q \equiv 1 \pmod N$. Therefore

$$\phi_q^2(S) = -qS = 1 \cdot S.$$

By Lemma 4.5, $S \in E(\mathbf{F}_{q^2})$, as claimed. ∎

Therefore, discrete log problems over $\mathbf{F}_q$ for supersingular curves with $a = 0$ can be reduced to discrete log calculations in $\mathbf{F}_{q^2}^{\times}$. These are much easier.

When E is supersingular but $a \neq 0$, the above ideas work, but possibly $m = 3$, 4, or 6 (see [80] and Exercise 5.12). This is still small enough to speed up discrete log computations.

5.3.2 The Frey-Rück Attack

Frey and Rück showed that in some situations, the Tate-Lichtenbaum pairing τ_n can be used to solve discrete logarithm problems (see [41] and also [40]). First, we need the following.

LEMMA 5.4

Let ℓ be a prime with $\ell | q - 1$, $\ell | \#E(\mathbf{F}_q)$, and $\ell^2 \nmid \#E(\mathbf{F}_q)$. Let P be a generator of $E(\mathbf{F}_q)[\ell]$. Then $\tau_\ell(P, P)$ is a primitive ℓth root of unity.

PROOF If $\tau_\ell(P, P) = 1$, then $\tau_\ell(uP, P) = 1^u = 1$ for all $u \in \mathbf{Z}$. Since τ_ℓ is nondegenerate, $P \in \ell E(\mathbf{F}_q)$. Write $P = \ell P_1$. Then $\ell^2 P_1 = \ell P = \infty$. Since $\ell^2 \nmid \#E(\mathbf{F}_q)$, there are no points of order ℓ^2. Therefore P_1 must have order 1 or ℓ. In particular, $P = \ell P_1 = \infty$, which is a contradiction. Therefore $\tau_\ell(P, P) \neq 1$, so it must be a primitive ℓth root of unity. ∎

Let $E(\mathbf{F}_q)$ and P be as in the lemma, and suppose $Q = kP$. Compute

$$\tau_\ell(P, Q) = \tau_\ell(P, P)^k.$$

Since $\tau_\ell(P, P)$ is a primitive ℓth root of unity, this determines $k \pmod{\ell}$. We have therefore reduced the discrete log problem to one in the multiplicative group of the finite field $\mathbf{F}_q$. Such discrete log problems are usually easier to solve.

Therefore, to choose a situation where the discrete log problem is hard, we should choose a situation where there is a point of order ℓ, where ℓ is a large prime, and such that $\ell \nmid q - 1$. In fact, we should arrange that $q^m \not\equiv 1 \pmod{\ell}$ for small values of m.

Suppose $E(\mathbf{F}_q)$ has a point of order n, but $n \nmid q - 1$. We can extend our field to $\mathbf{F}_{q^m}$ so that $n | q^m - 1$. Then the Tate-Lichtenbaum pairing can be used. However, the following proposition from [9] shows, at least in the case n is prime, that the Weil pairing also can be used.

PROPOSITION 5.5

Let E be an elliptic curve over $\mathbf{F}_q$. Let ℓ be a prime such that $\ell | \#E(\mathbf{F}_q)$,

$E[\ell] \not\subseteq E(\mathbf{F}_q)$, and $\ell \nmid q(q-1)$. Then

$$E[\ell] \subseteq E(\mathbf{F}_{q^m}) \text{ if and only if } q^m \equiv 1 \pmod{\ell}.$$

PROOF If $E[\ell] \subseteq E(\mathbf{F}_{q^m})$, then $\mu_\ell \subseteq \mathbf{F}_{q^m}$ by Corollary 3.11, hence $q^m \equiv 1 \pmod{\ell}$.

Conversely, suppose $q^m \equiv 1 \pmod{\ell}$. Let $P \in E(\mathbf{F}_q)$ have order ℓ and let $Q \in E[\ell]$ with $Q \notin E(\mathbf{F}_q)$. We claim that P and Q are independent points of order ℓ. If not, then $uP = vQ$ for some integers $u, v \not\equiv 0 \pmod{\ell}$. Multiplying by $v^{-1} \pmod{\ell}$, we find that $Q = v^{-1}uP \in E(\mathbf{F}_q)$, which is a contradiction. Therefore $\{P, Q\}$ is a basis for $E[\ell]$.

Let ϕ_q be the Frobenius map. The action of ϕ_q on the basis $\{P, Q\}$ of $E[\ell]$ gives us a matrix $(\phi_q)_\ell$, as in Section 3.1. Since $P \in E(\mathbf{F}_q)$, we have $\phi_q(P) = P$. Let $\phi_q(Q) = bP + dQ$. Then

$$(\phi_q)_\ell = \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix}.$$

From Theorem 4.10, we know that

$$\text{Trace}((\phi_q)_\ell) \equiv a = q + 1 - \#E(\mathbf{F}_q) \pmod{\ell}.$$

Since $\#E(\mathbf{F}_q) \equiv 0 \pmod{\ell}$ by assumption, we have

$$1 + d \equiv q + 1 \pmod{\ell},$$

so $d \equiv q \pmod{\ell}$. An easy induction shows that

$$\begin{pmatrix} 1 & b \\ 0 & q \end{pmatrix}^m = \begin{pmatrix} 1 & b\frac{q^m-1}{q-1} \\ 0 & q^m \end{pmatrix}.$$

Since $q \not\equiv 1 \pmod{\ell}$, by assumption, we have

$$\phi_q^m = 1 \text{ on } E[\ell] \iff (\phi_q)_\ell^m \equiv I \pmod{\ell} \iff q^m \equiv 1 \pmod{\ell}.$$

Since $E[\ell] \subseteq E(\mathbf{F}_{q^m})$ if and only if $\phi_q^m = 1$ on $E[\ell]$, by Lemma 4.5, this proves the proposition. ∎

If we have $E[n] \subseteq E(\mathbf{F}_{q^m})$, then we can use the MOV attack or we can use the Tate-Lichtenbaum pairing to reduce discrete log problems in $E(\mathbf{F}_{q^m})$ to discrete log problems in $\mathbf{F}_{q^m}^\times$. The Tate-Lichtenbaum pairing is generally faster (see [44]). In both cases, we pick arbitrary points R and compute their pairings with P and kP. With high probability (as in Section 5.3.1), we obtain k after using only a few values of R.

5.4 Anomalous Curves

The reason the MOV attack works is that it is possible to use the Weil pairing. In order to avoid this, it was suggested that elliptic curves E over $\mathbf{F}_q$ with

$$\#E(\mathbf{F}_q) = q$$

be used. Such curves are called **anomalous**. Unfortunately, the discrete log problem for the group $E(\mathbf{F}_q)$ can be solved quickly. However, as we'll see below, anomalous curves are potentially useful when considered over extensions of $\mathbf{F}_q$, since they permit a speed-up in certain calculations in $E(\overline{\mathbf{F}}_q)$.

The Weil pairing is not defined on $E[p]$ (or, if we defined it, it would be trivial since $E[p]$ is cyclic and also since there are no nontrivial pth roots of unity in characteristic p; however, see [10] for a way to use a Weil pairing in this situation). Therefore, it was hoped that this would be a good way to avoid the MOV attack. However, it turns out that there is a different attack for anomalous curves that works even faster for these curves than the MOV attack works for supersingular curves.

In the following, we show how to compute discrete logs in the case $q = p$. Procedures for doing this have been developed in [95], [102], and [115]. Similar ideas work for subgroups of p-power order in $E(\mathbf{F}_q)$ when q is a power of p (but in Proposition 5.6 we would need to lift E to a curve defined over a larger ring than $\mathbf{Z}$).

Warning: The property of being anomalous depends on the base field. If E is anomalous over $\mathbf{F}_q$, it is not necessarily anomalous over any $\mathbf{F}_{q^n}$ for $n \geq 2$. See Exercises 5.5 and 5.6. This is in contrast to supersingularity, which is independent of the base field and is really a property of the curve over the algebraic closure (since supersingular means that there are no points of order p with coordinates in the algebraic closure of the base field).

The first thing we need to do is lift the curve E and the points P, Q to an elliptic curve over $\mathbf{Z}$.

PROPOSITION 5.6

Let E be an elliptic curve over $\mathbf{F}_p$ and let $P, Q \in E(\mathbf{F}_p)$. We assume E is in Weierstrass form $y^2 = x^3 + Ax + B$. Then there exist integers $\tilde{A}, \tilde{B}, x_1, x_2, y_1, y_2$ and an elliptic curve $\tilde{E}$ given by

$$y^2 = x^3 + \tilde{A}x + \tilde{B}$$

such that $\tilde{P} = (x_1, y_1)$, $\tilde{Q} = (x_2, y_2) \in \tilde{E}(\mathbf{Q})$ and such that

$$A \equiv \tilde{A}, \quad B \equiv \tilde{B}, \quad P \equiv \tilde{P}, \quad Q \equiv \tilde{Q} \pmod{p}.$$

PROOF Choose integers x_1 and x_2 such that $x_1, x_2 \pmod p$ give the x-coordinates of P, Q. First, assume that $x_1 \not\equiv x_2 \pmod p$. Choose an integer y_1 such that $\tilde{P} = (x_1, y_1)$ reduces to $P \bmod p$. Now choose y_2 such that

$$y_2^2 \equiv y_1^2 \pmod{x_2 - x_1} \text{ and } (x_2, y_2) \equiv Q \pmod p.$$

This is possible by the Chinese Remainder Theorem, since $\gcd(p, x_2 - x_1) = 1$ by assumption.

Consider the simultaneous equations

$$y_1^2 = x_1^3 + \tilde{A}x_1 + \tilde{B}$$
$$y_2^2 = x_2^3 + \tilde{A}x_2 + \tilde{B}.$$

We can solve these for $\tilde{A}, \tilde{B}$:

$$\tilde{A} = \frac{y_2^2 - y_1^2}{x_2 - x_1} - \frac{x_2^3 - x_1^3}{x_2 - x_1}, \quad \tilde{B} = y_1^2 - x_1^3 - \tilde{A}x_1.$$

Since $y_2^2 - y_1^2$ is divisible by $x_2 - x_1$, and since x_1, x_2, y_1, y_2 are integers, it follows that $\tilde{A}$, and therefore $\tilde{B}$, are integers. The points $\tilde{P}$ and $\tilde{Q}$ lie on the curve $\tilde{E}$ we obtain.

If $x_1 \equiv x_2 \pmod p$, then $P = \pm Q$. In this case, take $x_1 = x_2$. Then choose y_1 that reduces mod p to the y-coordinate of P. Choose an integer $\tilde{A} \equiv A \pmod p$ and let $\tilde{B} = y_1^2 - x_1^3 - \tilde{A}x_1$. Then $\tilde{P} = (x_1, y_1)$ lies on $\tilde{E}$. Let $\tilde{Q} = \pm\tilde{P}$. Then $\tilde{Q}$ reduces to $\pm P = Q \bmod p$.

Finally, $4\tilde{A}^3 + 27\tilde{B}^2 \equiv 4A^3 + 27B^2 \not\equiv 0 \pmod p$, since E is an elliptic curve. It follows that $4\tilde{A}^3 + 27\tilde{B}^2 \neq 0$. Therefore $\tilde{E}$ is an elliptic curve. ∎

REMARK 5.7 If we start with $Q = kP$ for some integer k, it is very unlikely that this relation still holds on $\tilde{E}$. In fact, usually $\tilde{P}$ and $\tilde{Q}$ are independent points. However, if they are dependent, so $a\tilde{P} = b\tilde{Q}$ for some nonzero integers a, b, then $aP = bQ$, which allows us to find k (unless $bP = \infty$). The amazing thing about the case of anomalous curves is that even when $\tilde{P}$ and $\tilde{Q}$ are independent, we can extract enough information to find k. ∎

Let $a/b \neq 0$ be a rational number, where a, b are relatively prime integers. Write $a/b = p^r a_1/b_1$ with $p \nmid a_1 b_1$. Define the **p-adic valuation** to be

$$v_p(a/b) = r.$$

For example,

$$v_2(7/40) = -3, \quad v_5(50/3) = 2, \quad v_7(1/2) = 0.$$

Define $v_p(0) = +\infty$ (so $v_p(0) > n$ for every integer n).

Let $\tilde{E}$ be an elliptic curve over $\mathbf{Z}$ given by $y^2 = x^3 + \tilde{A}x + \tilde{B}$. Let $r \geq 1$ be an integer. Define

$$\tilde{E}_r = \{(x, y) \in \tilde{E}(\mathbf{Q}) \mid v_p(x) \leq -2r,\ v_p(y) \leq -3r\} \cup \{\infty\}.$$

These are the points such that x has at least p^{2r} in its denominator and y has at least p^{3r} in its denominator. These should be thought of as the points that are close to ∞ mod powers of p (that is, p-adically close to ∞).

THEOREM 5.8

Let $\tilde{E}$ be given by $y^2 = x^3 + \tilde{A}x + \tilde{B}$, with $\tilde{A}, \tilde{B} \in \mathbf{Z}$. Let p be prime and let r be a positive integer. Then

1. *$\tilde{E}_r$ is a subgroup of $\tilde{E}(\mathbf{Q})$.*
2. *If $(x, y) \in \tilde{E}(\mathbf{Q})$, then $v_p(x) < 0$ if and only if $v_p(y) < 0$. In this case, there exists an integer $r \geq 1$ such that $v_p(x) = -2r$, $v_p(y) = -3r$.*
3. *The map*

$$\begin{aligned} \lambda_r : \tilde{E}_r/\tilde{E}_{5r} &\to \mathbf{Z}_{p^{4r}} \\ (x, y) &\mapsto p^{-r}x/y \pmod{p^{4r}} \\ \infty &\mapsto 0 \end{aligned}$$

   is an injective homomorphism (where $\mathbf{Z}_{p^{4r}}$ is a group under addition).

4. *If $(x, y) \in \tilde{E}_r$ but $(x, y) \notin \tilde{E}_{r+1}$, then $\lambda_r(x, y) \not\equiv 0 \pmod{p}$.*

This will be proved in Section 8.1. The map λ_r should be regarded as a logarithm for the group $\tilde{E}_r/\tilde{E}_{r+1}$ since it changes the law of composition in the group to addition in $\mathbf{Z}_{p^{4r}}$, just as the classical logarithm changes the composition law in the multiplicative group of positive real numbers to addition in $\mathbf{R}$.

We need one more fact, which is contained in Corollary 2.33: the reduction mod p map

$$\begin{aligned} \mathrm{red}_p : \tilde{E}(\mathbf{Q}) &\longrightarrow \tilde{E} \pmod{p} \\ (x, y) &\mapsto (x, y) \pmod{p} \quad \text{when } (x, y) \notin \tilde{E}_1 \\ \tilde{E}_1 &\to \{\infty\} \end{aligned}$$

is a homomorphism. The kernel of red_p is $\tilde{E}_1$.

We are now ready for a theoretical version of the algorithm. We start with an elliptic curve E over $\mathbf{F}_p$ in Weierstrass form, and we have points P and Q on E. We want to find an integer k such that $Q = kP$ (assume $k \neq 0$). The crucial assumption is that E is anomalous, so $\#E(\mathbf{F}_p) = p$. Perform the following steps.

1. Lift E, P, Q to $\mathbf{Z}$ to obtain $\tilde{E}, \tilde{P}, \tilde{Q}$, as in Proposition 5.6.
2. Let $\tilde{P}_1 = p\tilde{P}, \tilde{Q}_1 = p\tilde{Q}$. Note that $\tilde{P}_1, \tilde{Q}_1 \in \tilde{E}_1$ since $\text{red}_p(p\tilde{P}) = p \cdot \text{red}_p(\tilde{P}) = \infty$ (this is where we use the fact that E is anomalous).
3. If $\tilde{P}_1 \in \tilde{E}_2$, choose new $\tilde{E}, \tilde{P}, \tilde{Q}$ and try again. Otherwise, let $\ell_1 = \lambda_1(\tilde{P}_1)$ and $\ell_2 = \lambda_1(\tilde{Q}_1)$. We have $k \equiv \ell_2/\ell_1 \pmod{p}$.

Why does this work? Let $\tilde{K} = k\tilde{P} - \tilde{Q}$. We have

$$\infty = kP - Q = \text{red}_p(k\tilde{P} - \tilde{Q}) = \text{red}_p(\tilde{K}).$$

Therefore $\tilde{K} \in \tilde{E}_1$, so $\lambda_1(\tilde{K})$ is defined and

$$\lambda_1(p\tilde{K}) = p\lambda_1(\tilde{K}) \equiv 0 \pmod{p}.$$

Therefore,

$$k\ell_1 - \ell_2 = \lambda_1(k\tilde{P}_1 - \tilde{Q}_1) = \lambda_1(kp\tilde{P} - p\tilde{Q}) = \lambda_1(p\tilde{K}) \equiv 0 \pmod{p}.$$

This means that $k \equiv \ell_2/\ell_1 \pmod{p}$, as claimed.

Note that the assumption that E is anomalous is crucial. If $E(\mathbf{F}_p)$ has order N, we need to multiply by N to put $\tilde{P}, \tilde{Q}$ into $\tilde{E}_1$, where λ_1 is defined. The difference $\tilde{K} = k\tilde{P} - \tilde{Q}$ gets multiplied by N, also. When N is a multiple of p, we have $\lambda_1(N\tilde{K}) \equiv 0 \pmod{p}$, so the contribution from $\tilde{K}$ disappears from our calculations.

If we try to implement the above algorithm, we soon encounter difficulties. If p is a large prime, the point $\tilde{P}_1$ has coordinates whose numerators and denominators are too large to work with. For example, the numerator and denominator of the x-coordinate usually have approximately p^2 digits (see Section 8.3). However, we are only looking for $x/y \pmod{p}$. As we shall see, it suffices to work with numbers mod p^2. (It is also possible to use the "dual numbers" $\mathbf{F}_p[\epsilon]$, where $\epsilon^2 = 0$; see [10].)

Let's try calculating on $\tilde{E} \pmod{p^2}$. When we compute $(x, y) = \tilde{P}_1 = p\tilde{P}$, we run into problems. Since $\tilde{P}_1 \in \tilde{E}_2$, we have p^2 in the denominator of x, so $\tilde{P}_1$ is already at ∞ mod p^2. Therefore, we cannot obtain information directly from calculating $\lambda_1(\tilde{P}_1)$. Instead, we calculate $(p-1)\tilde{P} \pmod{p^2}$, then add it to $\tilde{P}$, keeping track of p in denominators.

The procedure is the following.

1. Lift E, P, Q to $\mathbf{Z}$ to obtain $\tilde{E}$, $\tilde{P} = (x_1, y_1)$, $\tilde{Q} = (x_2, y_2)$, as in Proposition 5.6.
2. Calculate
$$\tilde{P}_2 = (p-1)\tilde{P} \equiv (x', y') \pmod{p^2}.$$
The rational numbers in the calculation of $\tilde{P}_2$ should not have p in their denominators, so the denominators can be inverted mod p^2 to obtain integers x', y'.

3. Calculate $\tilde{Q}_2 = (p-1)\tilde{Q} \equiv (x'', y'') \pmod{p^2}$.

4. Compute
$$m_1 = p\frac{y' - y_1}{x' - x_1}, \quad m_2 = p\frac{y'' - y_2}{x'' - x_2}.$$

5. If $v_p(m_2) < 0$ or $v_p(m_1) < 0$, then try another $\tilde{E}$. Otherwise, $Q = kP$, where $k \equiv m_1/m_2 \pmod{p}$.

Example 5.5
Let E be the elliptic curve given by $y^2 = x^3+108x+4$ over $\mathbf{F}_{853}$. Let $P = (0, 2)$ and $Q = (563, 755)$. It can be shown that $853P = \infty$. Since 853 is prime, the order of P is 853, so $853|\#E(\mathbf{F}_{853})$. Hasse's theorem implies that $\#E(\mathbf{F}_{853}) = 853$, as in Section 4.3.3. Therefore, E is anomalous. Proposition 5.6 yields

$$\tilde{E}: \ y^2 = x^3 + 7522715x + 4, \quad \tilde{P} = (0, 2), \quad \tilde{Q} = (563, 66436).$$

We have

$$\tilde{P}_2 = 852\tilde{P} \equiv (159511, 58855) \pmod{853^2}$$
$$\tilde{Q}_2 = 852\tilde{Q} \equiv (256463, 645819) \pmod{853^2}.$$

Note that even with a prime as small as 853, writing $\tilde{P}_2$ without reducing mod 853^3 would require more than 100 thousand digits. We now calculate

$$m_1 = 853\frac{58855 - 2}{159511 - 0} = \frac{58853}{187} \text{ and } m_2 = 853\frac{645819 - 66436}{256463 - 563} = \frac{58853}{187}.$$

Therefore, $k \equiv m_1/m_2 \equiv 234 \pmod{853}$. □

Let's prove this algorithm works (the proof consists mostly of keeping track of powers of p, and can be skipped without much loss). The following notation is useful. We write $O(p^k)$ to represent a rational number of the form $p^k z$ with $v_p(z) \geq 0$. Therefore, if $a, b \in \mathbf{Z}$ and $k > 0$, then $a = b + O(p^k)$ simply means that $a \equiv b \pmod{p^k}$. But we are allowing rational numbers and we are allowing negative k. For example,

$$\frac{1}{49} = \frac{23}{98} + O(7^{-1})$$

since

$$\frac{23}{98} = \frac{1}{49} + \frac{1}{7}\frac{3}{2}.$$

The following rule is useful:

$$\frac{a}{b + O(p^k)} = \frac{a}{b} + O(p^k) \text{ when } v_p(b) = 0, \ v_p(a) \geq 0, \text{ and } k > 0.$$

To prove it, simply rewrite the difference $\frac{a}{b+p^k z} - \frac{a}{b}$. (*Technical point:* This actually should say that $a/(b+O(p^k))$ can be changed to $(a/b)+O(p^k)$. The problem with "=" is that the right side sometimes cannot be changed back to the left side; for example, let the right side be 0 with $a = -p^k$.)

Write $\tilde{P}_2 = (p-1)\tilde{P} = (u, v)$, with $u, v \in \mathbf{Q}$ (this is not yet mod p^2). Then

$$u = x' + O(p^2), \quad v = y' + O(p^2).$$

Let

$$(x, y) = \tilde{P}_1 = p\tilde{P} = \tilde{P} + \tilde{P}_2 = (x_1, y_1) + (u, v).$$

Then

$$x = \left(\frac{v - y_1}{u - x_1}\right)^2 - u - x_1 = \left(\frac{y' - y_1 + O(p^2)}{x' - x_1 + O(p^2)}\right)^2 - u - x_1.$$

We have $\tilde{P}_1 \in \tilde{E}_1$ and usually we have $\tilde{P}_1 \notin \tilde{E}_2$. This means that $x' - x_1$ is a multiple of p, but not of p^2 (note: $y' \not\equiv y_1 \pmod{p}$ since otherwise $(p-1)P = P$, which is not the case). We'll assume this is the case. Then

$$\begin{aligned}
\frac{y' - y_1 + O(p^2)}{x' - x_1 + O(p^2)} &= \frac{1}{p}\left(\frac{y' - y_1 + O(p^2)}{\frac{x'-x_1}{p} + O(p)}\right) \\
&= \frac{1}{p}\left(\frac{y' - y_1}{\frac{x'-x_1}{p}} + O(p)\right) \\
&= \frac{1}{p}m_1 + O(p^0).
\end{aligned}$$

Note that $v_p(m_1) = 0$. Since $v_p(u) \geq 0$ and $v_p(x_1) \geq 0$, we obtain

$$x = \left(\frac{1}{p}m_1 + O(p^0)\right)^2 - u - x_1 = \frac{m_1^2}{p^2} + O(p^{-1}).$$

Similarly, the y-coordinate of $\tilde{P}_1$ satisfies

$$y = -\frac{m_1^3}{p^3} + O(p^{-2}).$$

Therefore,

$$\ell_1 = \lambda_1(\tilde{P}_1) = \lambda_1(x, y) = p^{-1}\frac{x}{y} = -\frac{1}{m_1} + O(p) \equiv -\frac{1}{m_1} \pmod{p}.$$

Similarly,

$$\ell_2 = \lambda_1(\tilde{Q}_1) \equiv -\frac{1}{m_2} \pmod{p}.$$

If $v_p(m_2) < 0$, then $\tilde{Q}_1 \in \tilde{E}_2$ by Theorem 5.8, hence either $\tilde{P}_1 \in \tilde{E}_2$ or $k = 0$. We are assuming these cases do not happen, and therefore the congruence just obtained makes sense. Therefore,

$$k \equiv \frac{\ell_2}{\ell_1} \equiv \frac{m_1}{m_2} \pmod{p},$$

as claimed. This shows that the algorithm works.

Anomalous curves are attractive from a computational viewpoint since calculating an integer multiple of a point in $E(\overline{\mathbf{F}}_q)$ can be done efficiently. In designing a cryptosystem, one therefore starts with an anomalous curve E over a small finite field $\mathbf{F}_q$ and works in $E(\mathbf{F}_{q^k})$ for a large k. Usually it is best to work with the subgroup generated by a point whose order ℓ is a large prime number. In particular, ℓ will be much larger than p, hence not equal to p. Therefore, the above attack on anomalous curves does not apply to the present situation.

Let E be an elliptic curve over $\mathbf{F}_q$ such that $\#E(\mathbf{F}_q) = q$. Then the trace of the Frobenius ϕ_q is $a = 1$, so

$$\phi_q^2 - \phi_q + q = 0.$$

This means that $q = \phi_q - \phi_q^2$. Therefore

$$q(x, y) = (x^q, y^q) + (x^{q^2}, -y^{q^2}) \text{ for all } (x, y) \in E(\overline{\mathbf{F}}_q).$$

The calculation of x^q, for example, can be done quickly in a finite field. Therefore, the expense of multiplying by q is little more than the expense of one addition of points. The standard method of computing $q(x, y)$ (see Section 2.2) involves more point additions (except when $q = 2$; but see Exercise 5.8). To calculate $k(x, y)$ for some integer k, expand $k = k_0 + k_1 q + k_2 q^2 + \cdots$ in base q. Compute $k_i P$ for each i, then compute $q^i k_i P$. Finally, add these together to obtain kP.

5.5 Other Attacks

For arbitrary elliptic curves, Baby Step/Giant Step and the Pollard ρ and λ methods seem to be the best algorithms. There are a few cases where index calculus techniques can be used in the jacobians of higher genus curves to solve discrete logarithm problems on certain elliptic curves, but it is not clear how generally their methods apply. See [45], [46], [79]. See also [113] for a discussion of some other index calculus ideas and elliptic curves.

An interesting approach due to Silverman [112] is called the **xedni calculus**. Suppose we want to find k such that $Q = kP$ on a curve E over $\mathbf{F}_p$.

Proposition 5.6 shows that we can lift E, P, and Q to an elliptic curve $\tilde{E}$ over $\mathbf{Z}$ with points $\tilde{P}$ and $\tilde{Q}$. If we can find k' with $\tilde{Q} = k'\tilde{P}$, then $Q = k'P$. However, it is usually the case that $\tilde{P}$ and $\tilde{Q}$ are independent, so no k' exists. Silverman's idea was to start with several (up to 9) points of the form $a_iP + b_iQ$ and lift them to a curve over $\mathbf{Q}$. This is possible: Choose a lift to $\mathbf{Z}$ for each of the points. Write down an arbitrary cubic curve containing lifts of the points. The fact that a point lies on the curve gives a linear equation in the coefficients of the cubic equation. Use linear algebra to solve for these coefficients. This curve can then be converted to Weierstrass form (see Section 2.5.2). Since most curves over $\mathbf{Q}$ tend to have at most 2 independent points, the hope was that there would be relations among the lifted points. These could then be reduced mod p to obtain relations between P and Q, thus solving the discrete log problem. Unfortunately, the curves obtained tend to have many independent points and no relations. Certain modifications that should induce the curve to have fewer independent points do not seem to work. For an analysis of the algorithm and why it probably is not successful, see [55].

Exercises

5.1 Suppose G is a subgroup of order N of the points on an elliptic curve over a field. Show that the following algorithm finds k such that $kP = Q$:

(a) Fix an integer $m \geq \sqrt{N}$.

(b) Compute and store a list of the x-coordinates of iP for $0 \leq i \leq m/2$.

(c) Compute the points $Q - jmP$ for $j = 0, 1, 2, \cdots, m-1$ until the x-coordinate of one of them matches an element from the stored list.

(d) Decide whether $Q - jmP = iP$ or $= -iP$.

(e) If $\pm iP = Q - jmP$, we have $Q = kP$ with $k \equiv \pm i + jm \pmod{N}$.

This requires a little less computation and half as much storage as the baby step, giant step algorithm in the text. It is essentially the same as the method used in Section 4.3.4 to find the order of $E(\mathbf{F}_q)$.

5.2 Let G be the additive group $\mathbf{Z}_n$. Explain why the discrete logarithm problem for G means solving $ka \equiv b \pmod{n}$ for k and describe how this can be solved quickly. This shows that the difficulty of a discrete logarithm problem depends on the group.

5.3 Let E be the elliptic curve $y^2 = x^3 + 3$ over $\mathbf{F}_7$.
(a) Show that $4(1, 2) = (4, 5)$ on E.

(b) Show that the method of the proof of Proposition 5.6, with $P = (1, 2)$ and $Q = (4, 5)$, produces the points $\tilde{P} = (1, 2)$ and $\tilde{Q} = (4, 5)$ on $\tilde{E} : y^2 = x^3 - 14x + 17$ (which is defined over $\mathbf{Q}$).
(c) Show that $2(1, 2) = (1, -2)$ and $3(1, 2) = \infty$ on $\tilde{E}$ mod 73.
(d) Show that there is no integer k such that $k(1, 2) = (4, 5)$ on $\tilde{E}$.
This shows that lifting a discrete log problem mod p to one on an elliptic curve over $\mathbf{Q}$ does not necessarily yield a discrete log problem that has a solution.

5.4 Let G be a group and let p be a prime. Suppose we have a fast algorithm for solving the discrete log problem for elements of order p (that is, given $g \in G$ of order p and $h = g^k$, there is a fast way to find k). Show that there is a fast algorithm for solving the discrete log problem for elements of order a power of p. (This is essentially what the Pohlig-Hellman method does. Since Pohlig-Hellman works with small primes, the fast algorithm for elements of order p in this case is simply brute force search.)

5.5 Let $p \geq 7$ be prime. Show that if E is an elliptic curve over $\mathbf{F}_p$ such that $E(\mathbf{F}_p)$ contains a point of order p, then $\#E(\mathbf{F}_p) = p$.

5.6 Show that if E is anomalous over $\mathbf{F}_q$ then it is not anomalous over $\mathbf{F}_{q^2}$.

5.7 Show that if E is anomalous over $\mathbf{F}_2$ then it is anomalous over $\mathbf{F}_{16}$.

5.8 Suppose E is anomalous over $\mathbf{F}_2$, so $\phi_2^2 - \phi_2 + 2 = 0$. Show that

(a) $4 = -\phi_2^3 - \phi_2^2$
(b) $8 = -\phi_2^3 + \phi_2^5$
(c) $16 = \phi_2^4 - \phi_2^8$

These equations were discovered by Koblitz [63], who pointed out that multiplication by each of 2, 4, 8, 16 in $E(\overline{\mathbf{Q}})$ can be accomplished by applying suitable powers of ϕ_2 (this is finite field arithmetic and is fast) and then performing only one point addition. This is faster than successive doubling for 4, 8, and 16.

5.9 Let E be defined over $\mathbf{F}_q$.

(a) Show that a map from $E(\mathbf{F}_q)$ to itself is injective if and only if it is surjective.

(b) Show that if $E(\mathbf{F}_q)$ has no point of order n, then $E(\mathbf{F}_q)/nE(\mathbf{F}_q) = 0$ (in which case, the Tate-Lichtenbaum pairing is trivial).

5.10 (a) Let ψ be a homomorphism from a finite group G to itself. Show that the index of $\psi(G)$ in G equals the order of the kernel of ψ.

(b) Let E be defined over $\mathbf{F}_q$ and let $n \geq 1$. Show that $E(\mathbf{F}_q)[n]$ and $E(\mathbf{F}_q)/nE(\mathbf{F}_q)$ have the same order. (When $n|q-1$, this can be proved from the nondegeneracy of the Tate-Lichtenbaum pairing; see Lemma 11.28. The point of the present exercise is to prove it without using this fact.)

5.11 This exercise gives a way to attack discrete logarithms using the Tate-Lichtenbaum pairing, even when there is a point of order ℓ^2 in $E(\mathbf{F}_q)$ (cf. Lemma 5.4). Assume ℓ is a prime such that $\ell|\#E(\mathbf{F}_q)$ and $\ell|q-1$, and suppose that the ℓ-power torsion in $E(\mathbf{F}_q)$ is cyclic of order ℓ^i, with $i \geq 1$. Let P_i have order ℓ^i and let P have order ℓ.

(a) Show that $\tau_\ell(P, P_i)$ is a primitive ℓth root of unity.

(b) Suppose $Q = kP$. Show how to use (a) to reduce the problem of finding k to a discrete logarithm problem in $\mathbf{F}_q^\times$.

(c) Let $N = \#E(\mathbf{F}_q)$. Let R be a random point in $E(\mathbf{F}_q)$. Explain why $(N/\ell^i)R$ is very likely to be a point of order ℓ^i. This shows that finding a suitable point P_i is not difficult.

5.12 Let E be defined by $y^2 + y = x^3 + x$ over $\mathbf{F}_2$. Exercise 4.7 showed that $\#E(\mathbf{F}_2) = 5$, so E is supersingular and $\phi_2^2 + 2\phi_2 + 2 = 0$.

(a) Show that $\phi_2^4 = -4$.

(b) Show that $E[5] \subseteq E(\mathbf{F}_{16})$.

(c) Show that $\#E(\mathbf{F}_4) = 5$ and $\#E(\mathbf{F}_{16}) = 25$.

This example shows that Proposition 5.3 can fail when $a \neq 0$.