

## 15.1 Calculations in finite groups

In this chapter we continue to adopt the *cryptographic perspective* developed in the earlier chapters. This means that we stress the link between mathematical theory and practical calculation which, as we have seen, is fundamental in modern cryptography. The specific system that we consider is based on groups that arise in the theory of elliptic curves, a topic that fascinated mathematicians for over a century before it first found practical application in the 1980s.

From the cryptographic perspective, it is worth stressing that a group consists of two things: a set of elements  $G$ , and an operation  $*$  defined on pairs of elements  $(h, k)$  in  $G$ . When we say that a group  $(G, *)$  is ‘given’, we mean that we know how to represent  $h$  and  $k$  in a definite way, and how to calculate  $h * k$  using this representation. Ultimately, it must be possible to reduce these calculations to operations on strings of bits, although it is usually convenient to use a more familiar notation, such as the standard decimal notation for integers.

For example, suppose we are working in  $\mathbb{F}_p^\times$ , the group of nonzero elements of  $\mathbb{F}_p$ , under multiplication. Then the elements of  $\mathbb{F}_p^\times$  are represented by natural numbers  $1, 2, \dots, p-1$  in decimal notation, and  $h \times k$  can be calculated by applying the familiar ‘long multiplication’ algorithm, followed by ‘long division’ to find the remainder when the result is divided by  $p$ .

### Definition 15.1 (Cyclic group, generator)

The group  $(G, *)$  is a *cyclic group of order  $n$ , with generator  $g$*  if  $|G| = n$  and there is an element  $g \in G$  such that the elements of the group are equal to

$$g, g^2, g^3, \dots, g^n,$$

in some order. (It follows that the group is abelian, and  $g^n$  is the identity element.)

The powers of any element  $h \in G$  are defined recursively by the rule

$$h^1 = h, \quad h^i = h * h^{i-1} \quad (i \geq 2).$$

Although the definition suggests that  $i - 1$  applications of the  $*$  operation are needed in order to calculate  $h^i$ , the repeated squaring algorithm (Section 13.3) allows  $h^i$  to be calculated much more efficiently. Furthermore, if  $G$  has  $n$  elements, every  $h \in G$  is such that  $h^n$  is equal to the identity element. Thus calculating the inverse of  $h$  can, if necessary, be done by using the rule  $h^{-1} = h^{n-1}$ .

The fact that  $\mathbb{F}_p^\times$  is a cyclic group of order  $p - 1$  is a consequence of the famous result that there is a primitive root  $r$  (a generator of  $\mathbb{F}_p^\times$ ) for every prime  $p$ . However, there are two problems. Finding a primitive root  $r$  for a given  $p$  is not trivial, and the correspondence between the powers of  $r$  and the elements of  $\mathbb{F}_p^\times$  is complicated. The latter problem is just the Discrete Logarithm Problem discussed in the previous chapter. As we shall see, both these problems occur more generally in elliptic curve cryptography.

The following example illustrates the fact that, without some additional information, finding a generator for a cyclic group may require ‘brute force’ methods.

### Example 15.2

Let  $*$  denote multiplication of  $2 \times 2$  matrices. Find  $g$  such that the following set of six matrices forms a cyclic group  $(G, *)$  with generator  $g$ .

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \quad \begin{pmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix} \\ \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} \quad \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix} \quad \begin{pmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}$$

*Solution* If we are unaware of the geometrical significance of the matrices, we must proceed by working out the orders of the matrices. The first two matrices have orders 1 and 2 respectively, and clearly they are not generators. However,

if we take the third matrix to be  $g$ , then it turns out that the six given matrices are equal to  $g, g^2, g^3, g^4, g^5, g^6$  (but obviously not in the given order). Thus  $g$  is a generator.

Suppose the problem of finding a generator  $g$  in a cyclic group  $G$  has been solved. Then we might hope to use the correspondence between the elements of  $G$  and the powers of  $g$  to simplify calculations in the group. Thus in order to calculate  $h * k$  we can write  $h = g^i$ , and  $k = g^j$ , calculate  $i + j$  using ordinary addition, and set  $h * k = g^{i+j}$ . But this method assumes that we can find  $i$  and  $j$ , the ‘logarithms’ of  $h$  and  $k$ . That is precisely the Discrete Log Problem (DLP) for  $(G, *)$ :

given a generator  $g \in G$  and any  $h \in G$ , find  $i \in \mathbb{N}$  such that  $g^i = h$ .

In some cases this problem may be easy (Exercise 15.3), but in general it is hard.

## EXERCISES

- 15.1. Show that the operation of multiplying complex numbers makes the following set of numbers into a cyclic group, and find a generator.

$$1, -1, i, -i, \frac{1}{\sqrt{2}}(1+i), \frac{1}{\sqrt{2}}(1-i), \frac{1}{\sqrt{2}}(-1+i), \frac{1}{\sqrt{2}}(-1-i).$$

- 15.2. In Example 14.5 we constructed a table of logarithms to base 2 in the cyclic group  $\mathbb{F}_{11}^\times$ . Explain how the table can be used to show that  $5 \times 10 = 6$  in this group.
- 15.3. Show that, for any positive integer  $n$ , the group  $(\mathbb{Z}_n, +)$  (the integers mod  $n$  under addition) is cyclic, and find a generator. Explain why the DLP is trivial in this case, however large  $n$  may be.

## 15.2 The general ElGamal cryptosystem

The ElGamal systems described in Chapter 14 can be extended to any given cyclic group  $(G, *)$ . Users of the general system are assumed to know that  $G$  is cyclic, and that a certain specified element  $g \in G$  is a generator. It is also assumed that they express plaintext and ciphertext messages as elements of  $G$  in some standard way.

In the general ElGamal cryptosystem, each user, such as Bob, chooses a private key  $b' \in \mathbb{N}$ , and computes his public key  $b \in G$  by the rule  $b = g^{b'}$ . When Alice wishes to send Bob a message  $m \in G$  she chooses a token  $t \in \mathbb{N}$ , and applies the encryption function

$$E_b(m, t) = (g^t, m * b^t).$$

Bob receives ciphertext in two parts: the first part is the ‘leader’  $\ell = g^t$ , and the other part is the encrypted message  $c = m * b^t$ . Bob’s decryption function is

$$D_{b'}(\ell, c) = c * (\ell^{-1})^{b'}.$$

Using essentially the same algebra as in Lemma 14.7, it is easy to check that  $D_{b'}(E_b(m, t)) = m$  for all  $m \in G$ , and all  $t \in \mathbb{N}$ :

$$\begin{aligned} D_{b'}(E_b(m, t)) &= D_{b'}(g^t, m * b^t) &= (m * b^t) * ((g^t)^{-1})^{b'} \\ & &= m * b^t * ((g^{b'})^{-1})^t \\ & &= m * b^t * (b^{-1})^t \\ & &= m. \end{aligned}$$

## EXERCISES

- 15.4. Let  $(G, *)$  be a cyclic group of order 43, with generator  $g$ , and suppose Bob’s private key is 10. What is Bob’s public key, and what is his decryption function? If Alice wishes to send the message  $m \in G$  to Bob, and chooses  $t = 7$ , what ciphertext does Bob receive? Check that his decryption function correctly recovers  $m$ . (All working should be expressed in terms of the ‘variables’  $g$  and  $m$ .)
- 15.5. Alice and Bob are experimenting with an ElGamal system based on the multiplicative group  $G = \mathbb{F}_{17}^\times$ , with generator  $g = 3$ . Bob’s public key is 13. Alice wishes to send the message  $m \in \mathbb{F}_{17}^\times$  to Bob. What encryption function should she use? Find Bob’s private key, write down his decryption function, and verify that it correctly recovers the message  $m$ .
- 15.6. In Exercise 15.3 we noted that  $(\mathbb{Z}_n, +)$  is cyclic group with generator 1. Show that in the corresponding ElGamal system  $b' = b$ , and verify that the decryption function  $D_{b'}$  is the left-inverse of  $E_b$ .

## 15.3 Elliptic curves

In the rest of the book we shall consider fields  $F$  with the property that  $2x = 0$  only if  $x = 0$  (so that  $F \neq \mathbb{F}_2$ , for example). This condition is expressed by the statement that  $F$  does not have *characteristic* 2. The reason for excluding fields with characteristic 2 is that the algebra takes a slightly different form in that case.

### Definition 15.3 (Elliptic curve)

Let  $F$  be a field which does not have characteristic 2. An *elliptic curve* over  $F$  is a set of ‘points’  $(x, y) \in F^2$  that satisfy an equation of the form

$$y^2 = x^3 + \alpha x + \beta \quad (\alpha, \beta \in F),$$

together with one additional ‘point’, which is denoted by  $I$  and called the *point at infinity*.

For cryptographic purposes we shall require that the field  $F$  is finite, but the same constructions can be used over any field  $F$  which does not have characteristic 2, and it is helpful to begin by looking at an example with  $F = \mathbb{R}$ , the field of real numbers. In this case the ‘points’ that form the curve belong to the Euclidean plane  $\mathbb{R}^2$ , and we can sketch the curve in the usual way. The resulting geometrical picture is very useful.

### Example 15.4

Sketch the curve  $y^2 = x^3 - x$  over  $\mathbb{R}$ .

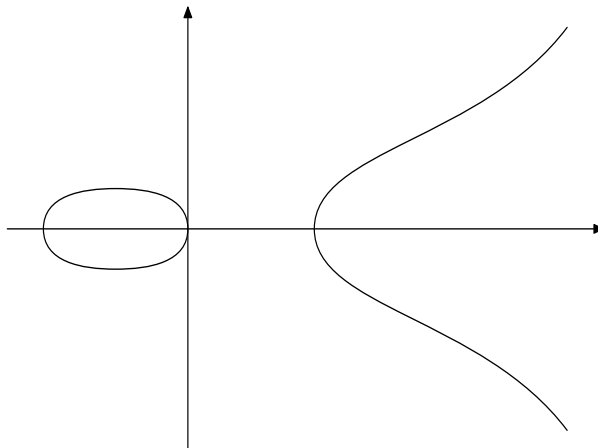
*Solution* The standard method of curve-sketching is to find points on the curve by choosing  $x \in \mathbb{R}$  and calculating the value(s) of  $y$  such that  $y^2 = x^3 - x$ .

When  $x < -1$  and when  $0 < x < 1$  the expression  $x^3 - x$  is negative, and there are no corresponding values of  $y$ , since  $y^2 \geq 0$ .

When  $x = -1, 0, 1$ ,  $x^3 - x = 0$  and  $y = 0$  is the only possibility. Hence the points  $(-1, 0)$ ,  $(0, 0)$ , and  $(1, 0)$  belong to the curve.

Finally, for each remaining value of  $x$  (that is  $-1 < x < 0$  and  $x > 1$ ) the expression  $x^3 - x$  is positive and there are two corresponding values of  $y$ . This means that the curve is symmetrical with respect to the  $x$ -axis: if  $(x, y)$  is on the curve, then  $(x, -y)$  is also on the curve. A sketch is shown in Figure 15.1.

It must be remembered that  $I$ , the ‘point at infinity’, must also be considered. Geometrically, it is helpful to think of  $I$  as a point where all vertical lines meet; that is, an infinitely remote point in the vertical direction.



**Figure 15.1** A sketch of the curve  $y^2 = x^3 - x$  in  $\mathbb{R}^2$

Similar calculations can be used when the field is finite, but of course there is no sensible way of ‘sketching’ the curve.

### Example 15.5

Find all the points on the curve  $y^2 = x^3 + x$  over  $\mathbb{F}_{17}$ .

*Solution* As in the previous example, we consider each value of  $x$  and solve the resulting equation for  $y$ . For example, when  $x = 1$  we require  $y^2 = 2$ , and in  $\mathbb{F}_{17}$  this has two solutions,  $y = \pm 6$ . (Note that  $-6 = 11$  here.)

For each  $x \in \mathbb{F}_{17}$  there are 0, 1, or 2 possible values of  $y$ :

$$\begin{array}{cccccccccc} x = & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ y = & 0 & \pm 6 & - & \pm 9 & 0 & - & \pm 1 & - & - & - \end{array}$$

$$\begin{array}{cccccccc} x = & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ y = & - & \pm 4 & - & 0 & \pm 2 & - & \pm 7 \end{array}.$$

The calculation gives 15 points which, together with  $I$ , the point at infinity, comprise the curve.

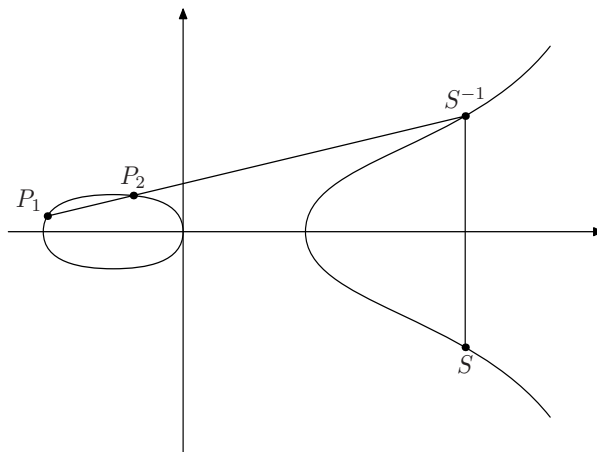
We shall now explain how an operation  $*$  can be defined so that the points of an elliptic curve over a field  $F$  form an abelian group. The definition is based on a geometrical construction and is easy to visualize in the case when  $F = \mathbb{R}$ . But the rules of algebra are the same in any field, so we can translate the construction into familiar coordinate geometry and apply it quite generally.

We begin by specifying that the point at infinity  $I$  is the *identity* element, so  $P * I = I * P = P$  for all points  $P$ . The *inverse* of a point  $P = (x, y)$  is  $P^{-1} = (x, -y)$ : geometrically speaking,  $P^{-1}$  is the reflection of  $P$  in the  $x$ -axis. Note that if  $P$  is on the curve, so is  $P^{-1}$ . Also, if  $Q$  is a point of the form  $(x, 0)$  then  $Q^{-1} = Q$ , so  $Q * Q = I$ .

The crucial part of the construction is the definition of  $P_1 * P_2$ , which depends on the fact that the right-hand side of the equation is a polynomial of degree 3. It follows that a straight line  $y = \lambda x + \mu$  will generally meet the curve in three points. We define

$P_1 * P_2 = S$  if and only if the points  $P_1, P_2$  and  $S^{-1}$  are collinear.

Figure 15.2 shows three collinear points  $P_1, P_2, S^{-1}$  and the point  $S = P_1 * P_2$ .



**Figure 15.2** Illustrating the group operation

We now translate this construction into coordinate geometry. That is, we find equations for the coordinates of  $S = P_1 * P_2$ , given the coordinates of  $P_1$  and  $P_2$ .

### Theorem 15.6

Suppose the points  $P_1 = (x_1, y_1)$  and  $P_2 = (x_2, y_2)$  belong to an elliptic curve  $y^2 = x^3 + \alpha x + \beta$  over a field  $F$  which does not have characteristic 2. Then the point  $S = P_1 * P_2$  is determined by the following rules:

- (i) if  $x_1 = x_2$  and  $y_1 = -y_2$  then  $S = I$ ;

(ii) in all other cases the coordinates  $(x_S, y_S)$  of the point  $S$  are given by

$$x_S = \lambda^2 - x_1 - x_2 \quad y_S = \lambda(x_1 - x_S) - y_1,$$

where  $\lambda$  is defined by

$$\lambda = (y_2 - y_1)(x_2 - x_1)^{-1} \quad \text{if } x_1 \neq x_2;$$

$$\lambda = (3x_1^2 + \alpha)(2y_1)^{-1} \quad \text{if } x_1 = x_2, y_1 = y_2.$$

### Proof

(i) This is the situation when  $P_2 = P_1^{-1}$ , as defined above.

(ii) Suppose that  $x_1 \neq x_2$  and the line through  $P_1$  and  $P_2$  is given by the equation  $y = \lambda x + \mu$ . Then

$$y_1 = \lambda x_1 + \mu \quad \text{and} \quad y_2 = \lambda x_2 + \mu,$$

so that

$$\lambda = (y_2 - y_1)(x_2 - x_1)^{-1}, \quad \mu = \lambda x_1 - y_1.$$

This line meets the curve  $y^2 = x^3 + \alpha x + \beta$  at the points where  $x$  satisfies

$$(\lambda x + \mu)^2 = x^3 + \alpha x + \beta, \quad \text{or} \quad x^3 - \lambda^2 x^2 + (\alpha - 2\lambda\mu)x + (\beta - \mu^2) = 0.$$

We know that two of the roots of this equation are  $x_1$  and  $x_2$ , and since the sum of the roots is  $\lambda^2$ , there is a third root  $x_S$  given by

$$x_S = \lambda^2 - x_1 - x_2.$$

Let  $y_S = -(\lambda x_S + \mu)$  so that the point  $S^{-1} = (x_S, -y_S)$  is on the line  $y = \lambda x + \mu$ , and  $S = (x_S, y_S)$  is the required point  $P_1 * P_2$ . Eliminating  $\mu$  gives

$$y_S = \lambda(x_1 - x_S) - y_1.$$

If  $x_1 = x_2$  the definition of  $\lambda$  will not work, because  $x_2 - x_1 = 0$  has no inverse. In fact if  $x_1 = x_2$  then  $y_1^2 = y_2^2$ , so there are two possibilities,  $y_1 = y_2$  or  $y_1 = -y_2$ . The second possibility has already been dealt with (case (i)).

If  $x_1 = x_2$  and  $y_1 = y_2$  then  $P_1 = P_2$ . In this case, we must determine the line  $y = \lambda x + \mu$  that meets the curve in two coincident points. In coordinate geometry over  $\mathbb{R}$  we call this a *tangent* to the curve, and determine its *slope*  $\lambda$  by calculus. Because the curve has an algebraic equation, the same results hold in any field  $F$ , and the relevant value of  $\lambda$  is as given in the statement of the theorem. The rest of the algebra is as before, with this new value of  $\lambda$ .  $\square$



### Example 15.7

In Example 15.5 we found that the points  $P_1 = (1, 6)$  and  $P_2 = (11, 4)$  belong to the curve  $y^2 = x^3 + x$  over  $\mathbb{F}_{17}$ . Calculate the coordinates of  $S = P_1 * P_2$  and  $T = P_1 * P_1$ .

*Solution* Taking  $P_1 = (1, 6)$  and  $P_2 = (11, 4)$ , the coordinates of  $S = P_1 * P_2$  are given by

$$\lambda = (4 - 6) \times (11 - 1)^{-1} = (-2) \times (10)^{-1} = -2 \times 12 = -24 = 10,$$

$$x_S = 10^2 - 1 - 11 = 88 = 3, \quad y_S = 10(1 - 3) - 6 = -26 = 8.$$

Thus  $S = (3, 8)$ . To find  $T = P_1 * P_1$  we use the alternative form of  $\lambda$ :

$$\lambda = (3 \times 1^2 + 1) \times (2 \times 6)^{-1} = 4 \times 10 = 40 = 6,$$

$$x_T = 6^2 - 1 - 1 = 34 = 0, \quad y_T = 6(1 - 0) - 6 = 0.$$

Thus  $T = (0, 0)$ .

### EXERCISES

15.7. Consider the curve  $y^2 = x^3 + x$  over  $\mathbb{F}_{17}$  discussed in Examples 15.5 and 15.7. Show that  $(1, 6)$  generates a subgroup of order 4.

15.8. Find explicitly all the points on the elliptic curve  $y^2 = x^3 + x$  over  $\mathbb{F}_{13}$ . (There are 20 of them.) Calculate the coordinates of the points

$$(3, 2) * (5, 0), \quad (2, 6) * (2, 6).$$

15.9. Show that a point  $P = (x, y)$  on an elliptic curve has order 2 (that is,  $P * P = I$ ) if and only if  $y = 0$ .

15.10. Taking  $F = \mathbb{R}$ , derive the formula for  $\lambda$  given in Theorem 15.6 for the case  $P_1 = P_2$ .

## 15.4 The group of an elliptic curve

The  $*$  operation endows an elliptic curve with the structure of an abelian group. The relevant properties are almost self-evident, with the exception of the *associative* law:  $(A * B) * C = A * (B * C)$ . Since we have obtained explicit formulae for the group operation, the associative law can, if necessary, be checked by

some rather tedious algebra. (The reader who wants to ‘really’ understand why it is true is advised to study a more theoretical account of elliptic curves.)

Our aim here is to explain how the group of an elliptic curve can be used in practice, specifically as the basis for an ElGamal cryptosystem. In order to do this, we need to identify a suitable cyclic group, which may be a proper subgroup of the full group, and a generator for it. A very simple example follows.

### Example 15.8

For the curve  $y^2 = x^3 + 2x + 4$  over  $\mathbb{F}_5$ , find a cyclic subgroup and a generator of it.

*Solution* We can tabulate the points on the curve in the usual way:

$$\begin{array}{cccccc} x = & 0 & 1 & 2 & 3 & 4 \\ y = & \pm 2 & - & \pm 1 & - & \pm 1 \end{array}$$

Thus, remembering  $I$ , there are seven points. Since 7 is a prime number, the full group must be cyclic, and any element except  $I$  is a generator.

More generally, it would be very useful if we could determine the size and structure of the group of any elliptic curve over a finite field. Sadly, this requires a substantial amount of theory and some nontrivial calculations. But mathematicians have succeed in finding many examples that are suitable for use in practice, and the basic principles are easy to understand.

### Lemma 15.9

Let  $G_E$  be the group of points on an elliptic curve  $E : y^2 = x^3 + \alpha x + \beta$  over a finite field  $F$ . Define

$m_1$  = the number of roots of  $x^3 + \alpha x + \beta = 0$  in  $F$ ;

$m_2$  = the number of  $x \in F$  for which  $x^3 + \alpha x + \beta$  is a non-zero square in  $F$ .

Then

$$|G_E| = m_1 + 2m_2 + 1.$$

### Proof

For each  $x \in F$  we count how many points  $(x, y)$  belong to  $E$ . Since  $F$  is a field, the equation  $y^2 = x^3 + \alpha x + \beta$  has at most two solutions. If  $y = \theta$  is a solution then  $y = -\theta$  is also a solution, so the number of distinct solutions is 0 or 2 unless  $\theta = 0$ , when there is just one solution.

In other words there are two solutions when  $x^3 + \alpha x + \beta$  is a non-zero square in  $F$ , one solution when  $x^3 + \alpha x + \beta = 0$  in  $F$ , and no solutions when  $x^3 + \alpha x + \beta$  is not a square in  $F$ . Adding 1 for the point at infinity, we have the result.  $\square$

The lemma shows that when  $F = \mathbb{F}_p$ , the largest possible value of  $|G_E|$  is  $2p + 1$ , which would occur if  $m_2 = p$ . In fact, one would expect that only about half the values of  $x \in \mathbb{F}_p$  are such that  $x^3 + \alpha x + \beta$  is a square, so that  $|G_E|$  will be approximately equal to  $p$ . Using this idea, Hasse proved in 1933 (long before elliptic curves became part of cryptography) that

$$p + 1 - 2\sqrt{p} \leq |G_E| \leq p + 1 + 2\sqrt{p}.$$

In the most favourable situation,  $|G_E|$  itself is a prime. Then the entire group is a cyclic group, and can be used as framework for systems based on the ElGamal formulae. For example, this happens when  $E$  is the curve

$$y^2 = x^3 + 10x + \beta \quad \text{over } \mathbb{F}_p,$$

where

$$\begin{aligned} p &= 2^{160} + 7 \\ &= 14615016373309029118203684832716283019655932542983 \end{aligned}$$

$$\beta = 1343632762150092499701637438970764818528075565078.$$

It has been shown that

$$\begin{aligned} |G_E| &= 14615016373309029118203683518218126812711137002561 \\ &= p - 13144981562069447795540422, \end{aligned}$$

and it is easy to check (with MAPLE) that  $|G_E|$  is a prime number. It follows that  $G_E$  is a cyclic group, and any non-identity element is a generator. So if we follow the prescription described above, we have the basis for cryptosystem. (Note that  $|G_E|$  differs from  $p$  by a number with 26 digits, whereas  $p$  has 53 digits, in accordance with Hasse's theorem.)

Although this favourable situation cannot be expected to occur very often, in practice it is just as useful to be able to find a large prime dividing  $|G_E|$ . In that case we have a large cyclic subgroup of  $G_E$ .

## EXERCISES

- 15.11. Verify explicitly that  $(2, 1)$  is a generator for the group obtained in Example 15.8.

- 15.12. Consider elliptic curves of the form  $y^2 = x^3 + x + \beta$  over  $\mathbb{F}_{11}$ . Find three values of  $\beta$  for which  $m_1$  (Lemma 15.9) is 0, 1, 3, respectively.
- 15.13. Taking  $\beta = 6$  in the previous exercise, show that the group of the curve is cyclic, and find a generator for it.
- 15.14. Let  $p$  be an odd prime. Show that the group of the elliptic curve  $y^2 = x^3 + x$  over the field  $\mathbb{F}_p$  has even order. Find the number  $m_1$  for this group, distinguishing the cases  $p = 4s + 1$  and  $p = 4s + 3$ .
- 15.15. Any group of order 20 has a cyclic subgroup of order 5. [You are not asked to prove this, but if you are familiar with elementary group theory you may wish to do so.] Determine this subgroup explicitly for the curve described in Exercise 15.8.

## 15.5 Improving the efficiency of exponentiation

From the cryptographic perspective, it remains to consider the problems that arise when we try to implement a cryptosystem based on an elliptic curve.

The most costly operations in the ElGamal scheme are the *exponentiations* – calculating the powers such as  $g^t$  and  $(\ell^{-1})^{b'}$  that occur in the encryption and decryption functions. In order to ensure confidentiality the exponents must be numbers with many digits, and the exponentiations, although feasible by the repeated squaring algorithm, are by no means trivial. In fact, that is the main reason why the ElGamal system is commonly used only to distribute keys for a symmetric key system such as AES, in which the calculations are less costly. (Similar remarks apply to RSA, where exponentiation is also a major part of the system.)

The problem of finding good algorithms for exponentiation is therefore significant. It is easy to see that the repeated squaring algorithm is not optimal: for example, it finds  $g^{15}$  by calculating

$$\begin{aligned} g^2 &= g * g, & g^4 &= g^2 * g^2, & g^8 &= g^4 * g^4, \\ g^{12} &= g^4 * g^8, & g^{14} &= g^2 * g^{12}, & g^{15} &= g * g^{14}. \end{aligned}$$

This procedure involves the sequence of powers 1, 2, 4, 8, 12, 14, 15, which has the property that each term in the sequence except the first is the sum of two (possibly the same) terms that come before it. Any sequence with this property that ends in 15 will produce the the required result.

### Definition 15.10 (Addition chain)

An *addition chain of length  $r$*  for the positive integer  $n$  is a sequence of positive integers  $x_0 = 1, x_1, x_2, \dots, x_r = n$  such that, for  $i = 1, 2, \dots, r$  there exist  $x_j$  and  $x_k$  such that

$$x_i = x_j + x_k \quad (0 \leq j \leq k < i).$$

Clearly, shorter addition chains for  $n$  lead to better methods for calculating  $g^n$ . For example, the repeated squaring method for  $g^{15}$  corresponds to the addition chain of length 6 given above, but there is a shorter addition chain, with length 5: 1, 2, 3, 6, 12, 15. This corresponds to the multiplications

$$\begin{aligned} g^2 &= g * g, & g^3 &= g * g^2, & g^6 &= g^3 * g^3, \\ g^{12} &= g^6 * g^6, & g^{15} &= g^3 * g^{12}. \end{aligned}$$

A further improvement can be made when inversion is a trivial operation. As we shall explain in the next section, this holds true when  $G$  is the group of an elliptic curve. In such cases division (multiplication by a power of  $g^{-1}$ ) is no more costly than multiplication by  $g$ , which motivates the following definition.

### Definition 15.11 (Addition-subtraction chain)

An *addition-subtraction chain of length  $r$*  for the positive integer  $n$  is a sequence of positive integers  $x_0 = 1, x_1, x_2, \dots, x_r = n$  such that, for  $i = 1, 2, \dots, r$  there are  $x_j$  and  $x_k$  such that

$$x_i = \pm x_j \pm x_k \quad (0 \leq j \leq k < i).$$

In other words, each term in the sequence except the first is the sum or difference of two terms that come before it.

The technique of exponentiation using an addition-subtraction chain is best illustrated by an example.

### Example 15.12

Find the optimum method of calculating  $g^{31}$ .

*Solution* The repeated squaring algorithm uses the addition chain 1, 2, 4, 8, 16, 24, 28, 30, 31, which has length 8. It is fairly easy to spot an addition chain of length 7: 1, 2, 3, 5, 10, 11, 21, 31, and some rather tedious analysis will confirm that it is the shortest possible.

However, if subtractions are allowed there is an obvious chain of length 6: 1, 2, 4, 8, 16, 32, and this is optimal. The corresponding method of calculating  $g^{31}$  is

$$\begin{aligned} g^2 &= g * g, & g^4 &= g^2 * g^2, & g^8 &= g^4 * g^4, \\ g^{16} &= g^8 * g^8, & g^{32} &= g^{16} * g^{16}, & g^{31} &= g^{-1} * g^{32}. \end{aligned}$$

A useful technique for finding a good addition-subtraction chain is based on the *non-adjacent form* of an integer (Exercise 15.18). It leads to an algorithm for exponentiation that is about 10% better than repeated squaring, on average.

## EXERCISES

- 15.16. Write down the addition chain for 127 used in the repeated squaring algorithm. This is a chain with length 12. Show that it is not optimal by finding an addition chain with length 10 for 127.
- 15.17. Show that the computation of  $g^{127}$  can be shortened further if addition-subtraction chains are allowed.
- 15.18. Consider representations of an integer in the form

$$\sum c_i 2^i \quad c_i \in \{-1, 0, 1\}.$$

Such a representation is said to be a *non-adjacent form* or *NAF* if  $c_i c_{i+1} = 0$  for all  $i \geq 0$ . Find a NAF for 55 and explain how it can be used to calculate  $g^{55}$ .

- 15.19. Show that every integer has a NAF. [Hint: start from the standard binary representation.] Show also that the NAF is unique.
- 15.20. Why are addition-subtraction chains not useful for the calculation of  $g^n$  when  $g$  is an element of  $\mathbb{F}_p^\times$ ?

## 15.6 A final word

Elliptic curve cryptography is a rapidly growing area of research, and it is possible that future developments will change the picture quite dramatically. Here is a summary of the current state of the art.

- The group of an elliptic curve can be used as the basis for a cryptosystem of the ElGamal type. By making suitable adjustments, elliptic curves can also be used in many other areas of cryptography.
- The ElGamal functions can be calculated fairly efficiently, but the cost of exponentiation (in particular) imposes some constraints in practice.
- It is possible to break an elliptic curve system if there is a method of solving the DLP on the group of the curve but, in general, no such method is known. Other forms of attack may be possible.

We conclude with an explicit example of how the ElGamal formulae can be applied to the group of an elliptic curve. First, we must decide how to represent the elements of the group. For a curve  $E$  defined over a prime field  $\mathbb{F}_p$ , an element of  $G_E$  is a pair  $(x, y)$  with  $x, y \in \mathbb{F}_p$ . So we can regard  $x$  and  $y$  as integers in the range  $0 \leq x, y \leq p - 1$ . Furthermore, when the right-hand side of the equation is a non-zero square there are exactly two values of  $y$  that satisfy the equation, and they can be written uniquely as  $\pm\theta$ , where  $\theta$  satisfies  $1 \leq \theta \leq \frac{1}{2}(p - 1)$ . Since  $\theta$  is determined by  $E$ , in order to store  $(x, y)$  it is only necessary to store  $x$  as an element of  $\mathbb{F}_p$ , together with a single bit that determines whether the relevant sign is  $+$  or  $-$ . Incidentally, this observation justifies the use of addition-subtraction chains for exponentiation, since inversion in  $G_E$  is a trivially easy operation, the inverse of  $(x, y)$  being  $(x, -y)$ .

Let  $E$  denote the curve

$$y^2 = x^3 + x + 4 \quad (x, y \in \mathbb{F}_{23}).$$

We shall use the notation  $x+$  and  $x-$  for the points  $(x, y)$  with  $y = \pm\theta$ ,  $1 \leq \theta \leq 11$ : for example,  $0+$  stands for  $(0, 2)$  and  $0-$  stands for  $(0, -2)$ . Substituting  $x = 0, 1, 2, \dots, 22$  in turn, we find that  $x^3 + x + 4$  is never zero, so that  $m_1 = 0$ , and it is a square when

$$x = 0, 1, 4, 7, 8, 9, 10, 11, 13, 14, 15, 17, 18, 22,$$

so that  $m_2 = 14$ . Hence the order of the group  $G_E$  is  $2 \times 14 + 1 = 29$ . Since this number is prime, the group is cyclic, and any element except  $I$  can be taken as the generator  $g$ .

Conveniently, the group  $G_E$  has the right number of symbols to represent the **english** alphabet, extended to include the comma and full stop. Although this number is far too small to provide security in serious applications, it can be used to send messages that are unintelligible to the vast majority of people. To do this, we need to establish a ‘standard’ correspondence between the 29 elements of the group and the symbols of the extended **english** alphabet. Here is a suitable correspondence.

$I$	0+	0-	1+	1-	4+	4-	7+	7-	8+
$\sqcup$	A	B	C	D	E	F	G	H	I
8-	9+	9-	10+	10-	11+	11-	13+	13-	14+
J	K	L	M	N	O	P	Q	R	S
14-	15+	15-	17+	17-	18+	18-	22+	22-	
T	U	V	W	X	Y	Z	,	.	

Suppose I am using  $G_E$  with generator  $g = 0+$ , and my public key is  $b = 7-$ . If you have read this book carefully, you will be able to construct a table of powers of  $g$ .

$i$	2	3	4	5	6	7	8	9	10	11	12	13	14
$g^i$	13-	11+	1-	7-	9+	15+	14+	4+	22+	10+	17+	8-	18+

Since  $g^{29-i}$  is the inverse of  $g^i$ , and the group is cyclic, this table is sufficient for all calculations in  $G_E$ . In particular, you will quickly see that my private key is  $b' = 5$ . Then, if you intercept some ciphertext intended for me, say

$$(9+, 15-) \quad (11+, 4-) \quad (0+, 18+) \quad (7-, 1+) \quad (14+, 4-) \\ (15+, 7+) \quad (13-, 18+) \quad (1-, 22+)$$

you can apply my decryption function  $(\ell, c) \mapsto c * \ell^{-5}$  and obtain

$$14- \quad 7- \quad 4+ \quad I \quad 4+ \quad 10- \quad 1- \quad 22-$$

which is definitely

THE $\sqcup$ END.

## EXERCISES

- 15.21. The message above was encrypted using a different value of the token  $t$  for each symbol. Find these values.
- 15.22. Karen has agreed to use ElGamal cryptosystem based on the group  $G_E$  defined above, with the ‘standard’ representation of extended **english**. She has chosen the generator  $h = 4-$ , and her public key is  $k = 9+$ . I have sent her the message

$$(7-, 7+) \quad (8-, 9+) \quad (18-, 4-) \quad (10+, 0+) \quad (1-, 8-) \\ (15-, 7+) \quad (8-, 18-) \quad (17-, 10+) \quad (7+, 4-) \quad (8-, 4-) \quad .$$

What does it say?



## Further reading for Chapter 15

There are several books on the mathematical theory of elliptic curves, at various levels of sophistication. From the cryptographic perspective there are two fundamental results: Hasse's theorem on the order of  $G_E$  (Section 15.4), and a theorem that says  $G_E$  can be expressed as the product of at most two cyclic groups. These results are discussed in the books by Silverman [15.5] and Washington [15.6], among others.

The rapidly developing field of elliptic curve cryptography is surveyed in two books by Blake, Seroussi, and Smart [15.1, 15.2]. These books cover many of the implementation issues including the cost of exponentiation (Section 15.5). Further details on addition chains, the NAF, and so on, can be found in the survey by Gordon [15.3], and the famous tome by Knuth [15.4].

- 15.1** I. Blake, G. Seroussi, N. Smart. *Elliptic Curves in Cryptography*. Cambridge University Press (1999).
- 15.2** I. Blake, G. Seroussi, N. Smart. *Advances in Elliptic Curve Cryptography*. Cambridge University Press (2005).
- 15.3** D.M. Gordon. A survey of fast exponentiation algorithms. *J. Algorithms* 27 (1998) 129-146.
- 15.4** D.E. Knuth *The Art of Computer Programming II - Semi-numerical Algorithms*. Addison-Wesley (third edition, 1997).
- 15.5** J.H. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag (1986).
- 15.6** L.C. Washington *Elliptic Curves: Number Theory and Cryptography*. Chapman and Hall / CRC Press (2003).

<http://www.springer.com/978-1-84800-272-2>

Codes: An Introduction to Information Communication  
and Cryptography

Biggs, N.L.

2008, X, 274 p. 36 illus., Softcover

ISBN: 978-1-84800-272-2