Elliptic Curves in Cryptography

Diana Mocanu

Abstract

1. Group Theory Basics

In a nutshell, group theory is the study of symmetries.

Definition 1.1. A **group** is a set G together with a binary operation:

$$(a,b) \to a*b\colon G\times G\to G$$

satisfying the following conditions:

G1: (associativity) for all $a,b,c\in G$ we have that

$$(a*b)*c=a*(b*c);$$

G2: (existence of a neutral element) there exists an element $e\in G$ such that

$$e*a=a=a*e$$

for all $a\in G$;

G3: (existence of inverses) for each $a\in G$, there exists an element denoted a^{-1} such that

$$a*a^{-1}=e=a^{-1}*a.$$

We usually abbreviate $(G,*)$ to G. Also, we usually write ab for $a*b$ and 1 for e; alternatively, we write $a+b$ for $a*b$ and 0 for e. In the first case, the group is said to be **multiplicative**, and in the second, it is said to be **additive**. The convention when talking about abstract groups is to use multiplicative notation.
The convention of this course will be to denote by G^* the additive group G without 0 if not otherwise stated.

Definition 1.2.

- The **order** of a group G is simply the number of elements in G. We denote it by $|G|$.
- The **order** of an element $a\in G$ is the smallest integer $m\neq 0$ such that $a^m=e$. If no such integer exists, we say a has **infinite order**.

Definition 1.3. Let G be a group such that the following additional axiom holds:

G4: $a*b=b*a$ for all $a,b\in G$.

Then, we say G is **abelian** or **commutative**.

Example 1.4. $(\mathbb{Z},+)$, $(\mathbb{Z}^*,\times)$, $(\mathbb{Q},+)$, $(\mathbb{Q}^*,\times)$ $(\mathbb{R},+)$, $(\mathbb{R}^*,\times)$, $(\mathbb{C},+)$, $(\mathbb{C}^*,\times)$ are all groups.

Example 1.5. Historically, the concept of a group got formalized while people were studying the symmetries of a fixed set S (i.e. **the group of symmetries** of S).
More precisely, think of the **permutation group** S_n of the set $S := \{1,2\dots n\}$ i.e. the self-bijections of S. What is the group operation? Can you compute its order?

Example 1.6. For those of you who came across matrix operations, you might want to check that if we take GL_n to be the invertible $n\times n$ matrices with matrix multiplication, we get a group. (Here, we consider matrices with entries in any field $\mathbb{F}$, for example $\mathrm{GL}_n(\mathbb{Q})$ are invertible matrices with entries in $\mathbb{Q}$).

Example 1.7. Lastly, we present a key example for this course which you might have encountered before as "modular arithmetic".
Consider the integers a,b,m. we say

$$a \equiv b \mod m$$

if $a-b$ is a multiple of m. That is if $a-b=im$ for some integer i.
For any integer $n\in\mathbb{Z}$ there is a unique integer r in $\{0,1,\cdots,m-1\}$ such that $n\equiv r \mod m$. Then r is called the residue of n modulo m, and by slight abuse of notation we will refer to it as $n \mod m$. One can find the residue of a number n by taking the remainder when dividing by m.
Recall that to define a group, we need a set and an operation satisfying **G1, G2, G3**. The set we consider will be $\mathbb{Z}_m := \{0,1,\cdots,m-1\}$. We will define the binary operations $\oplus,\otimes$ as follows. For $a,b\in\mathbb{Z}_m$ we define $a\oplus b$ to be to be the residue of $(a+b)$ modulo m. Similarly, $a\otimes b$ is defined to be the residue of $(a\times b)$ modulo m.
By an abuse of notation, we will denote the set of invertible elements with respect to $\otimes$ by $\mathbb{Z}_m^*$.

Problems

1.1. In Example 1.7:

- compute the set $\mathbb{Z}_m^*$ of invertible elements with respect to $\otimes$ (i.e. all of the elements $a\in\mathbb{Z}_m$ such that there exists an a^{-1} with the property $a\otimes a^{-1}=1=a^{-1}\otimes a$);
- show that $(\mathbb{Z}_m,\oplus)$ and $(\mathbb{Z}_m^*,\otimes)$ are groups by checking that $\oplus,\otimes$ are well defined operations and that **G1, G2, G3** hold. Compute their orders.

1.2. Which of the above examples represent abelian groups? Try to prove your claims formally using Definition 1.3 or provide a counter-example (i.e. two elements which do not commute).

1.3. Compute the order of the groups in the above examples.

1.4. Take $n=1517$. Compute the inverse of $a=100$ in Z_n^*. *Hint*: You might find it useful to use Euclid Algorithm to find $b,c\in\mathbb{Z}$ such that $ab+cn=1$, as $\gcd(a,n)=1$.

Definition 1.8. A **subgroup** of $(G,*)$ is a subset $H\subseteq G$ which is also a a group with respect to the same operation. This is equivalent with the following two conditions:

S1: $a,b\in H$ implies $a*b\in H$;

S2: $a\in H$ implies $a^{-1}\in H$.

Example 1.9. The most basic example is the subgroup generated by an element. Let G be a group and $a \in G$. We denote $\langle a \rangle := \{1, a, a^2, a^3, \cdots\}$ to be the **subgroup generated by** a. Prove this is a subgroup (i.e. satisfies **S1, S2**).

Example 1.10. The **center** of a group G is defined to be the set of all commuting elements, more precisely:

$$Z(G) := \{a \in G \text{ such that } ag = ga \text{ for all } g \in G\}.$$

Prove that $Z(G)$ is a subgroup of G (i.e. satisfies **S1, S2**).

Theorem 1.11 (Lagrange's Theorem)**.** Suppose $|G|$ is finite, and H is a subgroup of G. Then $|H|$ divides $|G|$.

Problems

1.5. Think of how you can create new groups out of existing ones.
Hint: What happens if:

- you intersect two subgroups of a given group; what about reunions?
- you form a direct product of two groups.

1.6.
1. Apply Lagrange's Theorem for G, a finite group and $H = \langle a \rangle$, where $a \in G$. What relation can you deduce about the order of a and $|G|$.
2. Now, prove that with the notation in 1. we have that for each $a \in G$, $a^{|G|} = e$, where e is the identity.
3. Write down what you get when applying 2. to $G = \mathbb{Z}_p^*$ where p is a prime number. This is known as **Fermat's little theorem** and it is essential for the rest of this course.
4. Write down what you get when applying 2. to $G = \mathbb{Z}_n^*$ for any n (make use of Exercise 1.1). This is known as **Euler's theorem**.

1.7. Compute $Z(GL_n(\mathbb{Q}))$. *Hint:* Consider matrices of the form $I_n + E_{ij}$, where I_n is the identity w.r.t. matrix multiplication and E_{ij} is the matrix which has 1 in position ij and 0 everywhere else.

2. Rings and Fields

Definition 2.1. A structure $(R, +, \times)$ is a **ring** if R is a non-empty set and $+$ and $\times$ are binary operations such that:

1. $(R, +)$ is an abelian group;
2. $\times$ is associative (i.e. **G1** holds for $(R, \times)$);
3. multiplication distributes over addition i.e. the following holds:
   D: $a \times (b + c) = a \times b + a \times c$ and $(a + b) \times c = a \times c + b \times c$ for all $a, b, c \in R$.

Moreover, we say R is **commutative** if **G4** holds for $(R, \times)$ and that R **has unity** if **G2** holds for $(R, \times)$.

Example 2.2. $(\mathbb{Z},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$, $(\mathbb{C},+,\times)$ are all rings.

Example 2.3. Matrix Rings: Let M_n be the matrices with the component-wise addition and matrix multiplication. This is a ring. Make sure you know how to prove this.
Is M_n commutative? Does it have unity? (As before, we consider matrices with entries in any field $\mathbb{F}$, for example $\mathrm{M}_n(\mathbb{Q})$ are matrices with entries in $\mathbb{Q}$)

Example 2.4. Polynomial rings Polynomials with coefficients in a field $\mathbb{F}$ (for example $\mathbb{R}[x]$) form a ring. Can you define the two operations $+,\times$. Is it commutative? Does it have unity?

Definition 2.5. A **field** is a ring where $(R^*,\times)$ is an abelian group.

Example 2.6. $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$, $(\mathbb{C},+,\times)$ are all fields.

Definition 2.7. The **characteristic** of a field $\mathbb{F}$ is the smallest positive number n such that:

$$\underbrace{1+1+1...+1}_{n \text{ times}}=0$$

If no such n exists, we say $\mathbb{F}$ has characteristic 0. You should think of the characteristic as the additive order of 1.

Problems

2.1. Show that the integers modulo an integer m ($\mathbb{Z}_m$) form a ring with the usual addition and multiplication.

2.2. For what integers m is it true, that the integers modulo m ($\mathbb{Z}_m$) form a field? Compute its characteristic.
In this is the case we denote this field by $\mathbb{F}_m$. These are called **Finite fields** and they are unique in some sense (up to isomorphism).

2.3. Give an example of a ring without unity.

3. Elliptic Curves

There is an extensive literature on elliptic curves, as they are both geometric and algebraic objects which arise very naturally in different areas of Mathematics. Recently, they have been used as a theoretical tool in the proof of Fermat Last Theorem and since then, they are heavily studied in the context of solving Diophantine equations. However, this is outside the scope of this course, but I would be happy to talk about it in the office hours with the interested students.
Perhaps the most applied context in which elliptic curves have been used so far is Cryptography. Our aim in the remaining of this course is to try to understand briefly and intuitively what role elliptic curves play in cryptography.
Firstly, we need to go through some basic theory of elliptic curves which I tried to simplify for our purpose. We will start by defining elliptic curves over rational numbers, study their group law briefly, and then generalize the concepts over finite fields.

Definition 3.1. An **elliptic curve over** $\mathbb{Q}$ consists of solutions (x,y) to an equation of the form:

$$E: Y^2 = X^3 + aX + b$$

where $a, b \in \mathbb{Q}$. Moreover, we require that the following quantity, (called the discriminant) is non-zero $\Delta = 4a^3 + 27b^2 \neq 0$ (in more advanced terms, we require the curve to be non-singular). We think of the elliptic curve E as having a distinguished point called the **POINT AT INFINITY** and denoted by $\underline{O}$.

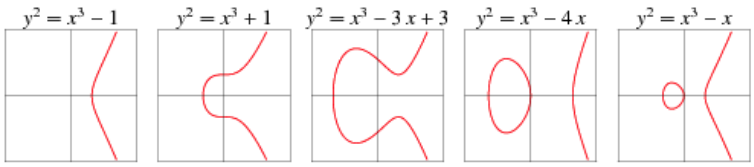
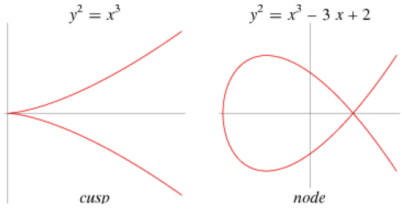


Figure 3.1: Elliptic curves for various values of a and b.

REMARK 3.2. 1. The $\Delta \neq 0$ condition assures that we do not have "unsmoothness" (cusps) or "self-intersections" (nodes):



2. The point at infinity comes from the fact that our curve is formally defined in something called the "projective space", but this is outside the scope of the course. Pictorially, you should think of this as "everything above the curve" together with "everything below the curve". I apologize for this sloppy description. We will cover this in classes in more detail.

DEFINITION 3.3.
- A point $P = (x, y)$ is a **rational point** on E if P lies on E (i.e. (x, y) is a solution to the equation describing E) and $x, y \in \mathbb{Q}$.
- We write $E(\mathbb{Q})$ for the rational points together with the point at infinity $\underline{O}$.

EXAMPLE 3.4. In the first curve in Figure 1 we can easily see that $P_1 = (1, 0)$ is a rational point. Can you give an example of one (or more) rational point for each of the curves in this figure?

We present the following surprising result, based on a remarkably beautiful geometric construction.

THEOREM 3.5 (The Group Law)**.** The set $E(\mathbb{Q})$ forms an abelian group with the binary operation $\oplus$ defined as follows.
Let $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ be two rational points, i.e. $P, Q \in E(\mathbb{Q})$. The line joining P and Q must intersect the curve in a third point, say R [1]. The point R will also be rational, as both the line and the cubic curve E are defined over $\mathbb{Q}$. If then we reflect R to the x-axis we obtain another rational point which we call $P \oplus Q$.

[1] This statement is not trivial, it comes from Bezout Theorem applied for a projective line and a projective cubic curve. However, this is out of the scope of this course, so we will take it for granted.

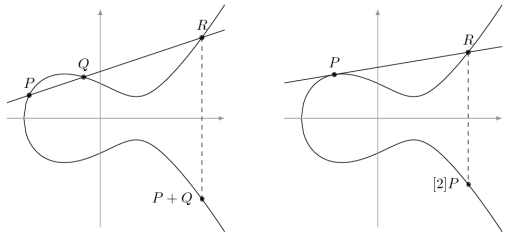


Figure 3.2: The Group law on an elliptic curve.

PROOF. We will sketch the proof in class. Note that $\underline{O}$ is the identity! □

REMARK 3.6. There are some subtleties to address:

1. when we add a point P with itself, we take the tangent to the curve at P as shown in the above figure. Such a line will intersect the curve in exactly one other point R.[2] Again, we take the reflection of R in the x-axis to obtain a point which we call $[2]P = P \oplus P$.

2. if the line through P and Q is vertical, (or the tangent through P is vertical), we consider the third point of intersection to be $\underline{O}$. This will get us $P \oplus Q = \underline{O}$, in other words Q is the inverse of P w.r.t. $\oplus$ (or $[2]P = \underline{O}$ i.e. P has order 2).

3. points on a line add up to $\underline{O}$, for example $P+Q+R = \underline{O}$.

4. observe the symmetry to the x-axis.

LEMMA 3.7. Let $P = (x,y) \in E(\mathbb{Q})$. Then, $-P = (x,-y)$.

PROOF. Given a point $P = (x,y)$, if we take the line through P and $\underline{O}$ then this is the vertical line. So, the third point of intersection is $(x,-y)$, which must then be $-P$ as points on a line add up to $\underline{O}$. □

Thus, this lemma gives an easy rule to find inverses of points.

EXAMPLE 3.8. Let

$$E : Y^2 = X^3 + 1.$$

Let us compute $P \oplus Q$, where $P = (-1,0)$ and $Q = (0,1)$. The line through P and Q, which we denote by $l_{P,Q}$ is

$$l_{P,Q} : Y = X + 1.$$

Substituting this into E we see that x-coordinate of any point of intersection satisfies: $(x+1)^2 = x^3 + 1$, and so

$$x^3 - x^2 - 2x = 0 \tag{3.1}$$

We are looking for (x_R, y_R), the third point of intersection of E and $l_{P,Q}$. We first find x_R; note that x_P, x_Q and x_R must be the roots of (3.1). Factorise (3.1) to give: $x(x+1)(x-2)$, whose roots are: $0, -1, 2$. Two of these are the already known $x_P = -1, x_Q = 0$, and so x_R must be the remaining root: $x_R = 2$. Having found x_R, we use the equation of $l_{P,Q}$ to compute $y_R = x_R + 1 = 3$. In summary: E and $l_{P,Q}$ intersect at: $(-1,0), (0,1), (2,3)$, and so $(-1,0)+(0,1)+(2,3) = \underline{O}$. Finally, this gives: $(-1,0)+(0,1) = -(2,3) = (2,-3)$, using the rule that negation is given by

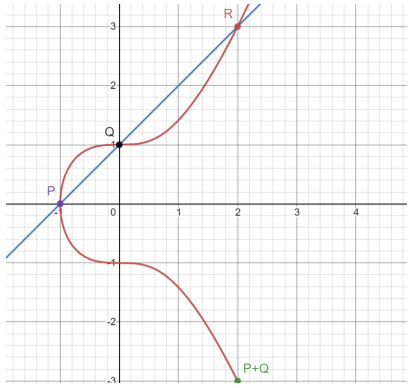


Figure 3.3: Drawn in Desmos.

reflection in the x-axis. Note that by Lemma 3.7 we get that $P=-P$. Hence, we can deduce that $[2]P=P+P=\underline{O}$. Alternatively, we could have used the same methos as above, by first computing the tangent line $l_{P,P}$ and then follow the above steps. Make sure you know how to do this!

Problems

3.1. Give examples of one (or more) rational points on each of the curves in Figure 1.

3.2. Let $E: Y^2=X^3-X$. Let $P=(1,0)$, $Q=(-1,0)$. Compute $P+Q$, $[2]P$, $[2]Q$.

3.3. Let $E: Y^2=X^3+1$. Let $P=(0,1)$. First compute $[2]P$. Then, find the order of P in $E(\mathbb{Q})$.

3.4. Show that the point $(2,4)$ is of order 4 on $E: Y^2=X^3+4X$, defined over $\mathbb{Q}$.

We will now generalize the above notions over prime finite fields. More precisely, we will replace $\mathbb{Q}$ with $\mathbb{F}_p$, for p a prime number and see what changes.

Definition 3.9. An **elliptic curve over** $\mathbb{F}_p$ with $p\neq 2,3$ consists of solutions (x,y) to an equation of the form:

$$E: Y^2=X^3+aX+b$$

where $a,b\in\mathbb{F}_p$. Moreover, we require that the following quantity, (called the discriminant) is non-zero $\Delta=4a^3+27b^2\neq 0 \mod p$.
We think of the elliptic curve E as having a distinguished point called the **point at infinity** and denoted by $\underline{O}$.
We define $P=(x,y)$ to be an $\mathbb{F}_p$**-rational point** if P lies on E and $x,y\in\mathbb{F}_p$ and take $E(\mathbb{F}_p)$ to be the all of the $\mathbb{F}_p$-rational points, together with the point at infinity.

Remark 3.10. This curves will look very different from the ones over $\mathbb{Q}$. The main difference is that $E(\mathbb{F}_p)$ is always finite and we picture it as a discrete set as shown in Figure 3.10. So, a natural question to ask is: how big is $E(\mathbb{F}_p)$? The following theorem will give us a hint:

[2]This is because we consider the tangent at P to intersect the elliptic curve twice. In technical terms, we say it has intersection multiplicity 2.

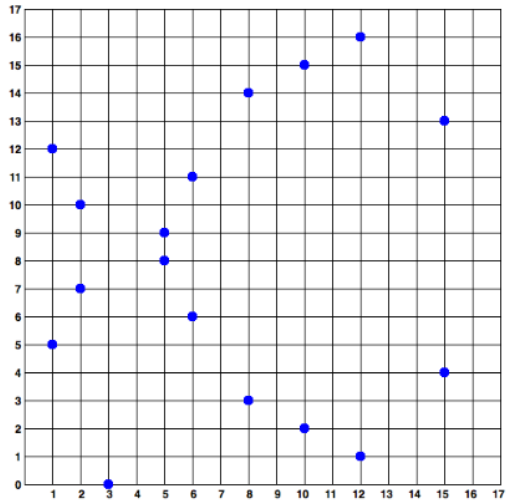


Figure 3.4: $E: Y^2 = X^3 + 7$ over $\mathbb{F}_{17}$

Observe the x-axis symmetry again.

Theorem 3.11 (Hasse Bound)**.** Let E be an elliptic curve over $\mathbb{F}_p$. Let $N_p = |E(\mathbb{F}_p)|$ where, as usual, $E(\mathbb{F}_p)$ should be taken to including $\underline{O}$ [so that N_p is the number of points (x,y) on E with $x,y \in \mathbb{F}_p$, plus 1, to include the point at infnity $\underline{O}$]. Then:

$$|N_p - (p+1)| \leq 2\sqrt{p}$$

Proof. The proof is outside the scope of the course, but we will provide the following intuition for why we expect N_p to be approximately $p+1$.
Let $E: Y^2 = X^3 + aX + b$. Each of the p possible x-coordinates $0, \cdots, p-1$ has about a 50% chance of making $X^3 + aX + b$ a square modulo p. When $X^3 + aX + b$ is not a square, there are no corresponding y-coordinates. When $X^3 + aX + b$ is a square, there are at most two corresponding y- coordinates. So, one might expect 'on average' about p points of the form (x,y), that is, about $p+1$ points, including the one at infinity. □

Theorem 3.12 (The Group Law)**.** As before, $E(\mathbb{F}_p)$ is a group together with $\oplus$, where $\oplus$ is defined exactly as in the rational case.

I hope that the following example will make it clear how this works:

Example 3.13. Let $E: Y^2 = X^3 + 7$ over $\mathbb{F}_{17}$. Take $P = (2,10)$ and $Q = (5,9)$. The line through P and Q is $l_{P,Q}: y = 11X + 5 \mod 17$. Hence, to find the third point of intersection R between E and $l_{P,Q}$ we need to solve

$$(11x+5)^2 = x^3 + 7 \mod 17.$$

By rearranging and reducing modulo 17 we het $(x-2)(x-15)(x-12) = 0 \mod 17$. Hence the $x_R = 12$ and $y = 11 \cdot 12 + 5 = 1 \mod 17$. So, $R = (12,1)$ and its reflection, $P \oplus Q = (12,-1) = (12,16)$.

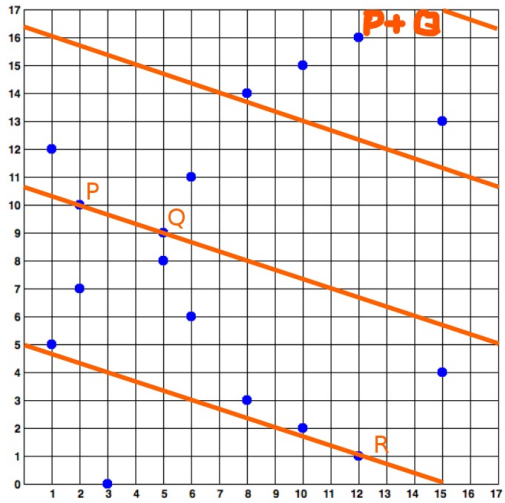


Figure 3.5: Here $P=(2,10), Q=(5,9)$ and $P+Q=(12,16)$ and E is an in 3.10

Problems

3.5. For each of the following elliptic curves, find all the points (including, as always, the point at infinity) over $\mathbb{F}_5$. Draw a complete group table in each case and describe each group as a product of cyclic groups.

1. $E: Y^2 = X^3 + 2X$;
2. $E: Y^2 = X^3 + 1$.

3.6. Let $p \equiv 2(\mod 3)$ be prime and let $A \in F_p^*$. Show that the number of points (including the point at infinity) on the curve $Y^2 = X^3 + A$ over $\mathbb{F}_p$ is exactly $p+1$.

3.7. Let $E: Y^2 = X^3 + 4X + 1$, defined over $\mathbb{F}_{13}$. Then show that $E(\mathbb{F}_{13})$ has a point of order greater than 2. *Hint:* Use Hasse's Theorem to get a bound for $E(\mathbb{F}_{13})$, then observe that all points (x,y) of order 2 have $y=0$.

4. Cryptography

Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents, even if the communication channel is compromised. We will present two public-key cryptographic systems: RSA and ECDH.

4.1. RSA

The RSA Public Key Cryptosystem, invented by Rivest, Shamir and Adleman in 1977 allows messages to be sent securely without the need to exchange a "key" secretly.
Following tradition, let us suppose that we have two people named Alice and Bob, and that Alice

wants to send a message to Bob. A malicious eavesdropper will appear later by the name of Eve. We have the following steps:

1. **PUBLIC KEY** Bob chooses two large primes p and q and an integer e such that $\gcd(e,\phi(n))=1$. (Note that $\phi(n)=(p-1)(q-1)$, so this is equivalent to $\gcd(e,p-1)=\gcd(e,q-1)=1$.) Typically p,q have hundreds of digits each. It is best not to choose them to have any particular structure. We will discuss in class how to do this. Bob forms the product $n=pq$ and announces the numbers n and e publicly. He **does not** publish p or q separately.

2. **ENCRYPTION** Now we describe how Alice sends her message. Suppose the message is written in English. First it must be converted to numerical form. This is done using a suitable numerical substitution scheme such as $A\to 01$, $B\to 02$, etc. This string of numerals is then split into chunks, each of which is a number smaller than n. Each of these chunks is then transmitted separately.

   If M is one of the chunks, it is transmitted as follows. Alice computes $M^e(\mod n)\in\{0,1,\dots n-1\}$ and sends this to Bob.

3. **DECRYPTION** Now Bob has the encrypted message $M^e(\mod n)$. How does he decrypt it? Since Bob knows p and q, he can compute $\phi(n)=(p-1)(q-1)$. Since, by assumption, e is coprime to $\phi(n)$, he can find d such that

   $$de=1 \mod \phi(n)$$

   for example by Euclid Algorithm, as you did in Problem 1.4. Say $de=k\phi(n)+1$. But then

   $$(M^e)^d=(M^{\phi(n)})^k M.$$

   By the Euler theorem, this is $\equiv M(\mod n)$. However, the unencrypted message M is known to be a natural number $<n$, and so this allows it to be recovered uniquely. There is an issue here if it happens that M is not coprime to n. However, since $n=pq$ with p and q large primes, this is exceptionally unlikely to happen.

4. **SECURITY** The decryption method we presented above depends on having the number d to hand. To calculate this, we needed $\phi(n)$. Eve, the eavesdropper, could read the message if she had $\phi(n)$.
   However, knowledge of $\phi(n)$ is equivalent to knowledge of the factorisation $n=pq$, which is widely believed to be hard.

Problem

4.1. For classes: we will split in pairs and one person will encrypt a message using 2. above and the second person will decrypt it using 3. above.

4.2. ECDH

Note that RSA security relies on the hardness of **FACTORISATION** i.e. it is computationally very hard for a given integer n, to find its prime factorisation. However, there have been few algorithms (e.g. Quadratic Sieve, General Number Field Sieve, Shor's quantum algorithm) which can break factorisation.

Hence, we would like to construct cryptosystems which rely on harder to break mathematical problems. One of them is the Diffie-Hellman Key Exchange, which relies on the **DISCRETE LOGARITHM PROBLEM**.

DEFINITION 4.1. In its most standard form, the **DISCRETE LOGARITHM PROBLEM** in a finite group G can be stated as follows: given $a \in G$ and $b \in \langle a \rangle$, find the least positive integer x such that $a^x = b$.

EXAMPLE 4.2. The discrete logarithm problem is easy when $G = (\mathbb{R}^*, \times)$ as it will reduce to finding $\log_\alpha \beta$ which is a well known real function.

EXAMPLE 4.3. In $G = \mathbb{Z}_p^*$ the discrete logarithm problem has infinite solutions. This can be seen by regarding the "logarithm" as the inverse of exponentiation in $\mathbb{F}_p$. For example, consider the equation $3^x \equiv 13 \pmod{17}$ for x. One solution is $x = 4$, but it is not the only solution. Since $3^{16} \equiv 1 \pmod{17}$—as follows from Fermat's little theorem—it also follows that if n is an integer then $3^{4+16n} \equiv 3^4 \times (3^{16})^n \equiv 13 \times 1^n \equiv 13 \pmod{17}$. Hence the equation has infinitely many solutions of the form $4 + 16n$. Moreover, because 16 is the smallest positive integer m satisfying $3m \equiv 1 \pmod{17}$, these are the only solutions.

EXAMPLE 4.4. If $G = E(\mathbb{F}_p)$, it turns out that the discrete logarithm problem is very hard. This is why this section is dedicated to Elliptic-Curve Diffie–Hellman (ECDH), a cryptosystem based on the hardness of this problem.

PROBLEM

4.2. Phrase the discrete logarithm problem for $E(\mathbb{F}_p)$. Be careful as we use the additive notation for this example as opposed to multiplicative notation in the case of $\mathbb{R}$ and $\mathbb{F}_p$.

The Diffie-Hellman method proceeds by allowing Alice and Bob to exchange a common secret key via an unsecure channel. We have the following steps:

1. **INITIALIZATIONS** They both have access to the following public available information: $E : Y^2 = X^3 + AX + B$ over a fixed field $\mathbb{F}_p$, where p is a prime, a fixed point $G \in E(\mathbb{F}_p)$ and n the order of G.

2. **PRIVATE KEY CREATION** Alice chooses a random element $d_A \in \{1, 2, \ldots n-1\}$ and computes $Q_A := [d_A]G := \underbrace{G \oplus G \oplus G \cdots \oplus G}_{d_A \text{ times}}$. Alice's secret key is d_A and her public key is Q_A
   Similarly, Bob chooses a random element $d_B \in \{1, 2, \ldots n-1\}$ and computes $Q_B := [d_B]G := \underbrace{G \oplus G \oplus G \cdots \oplus G}_{d_B \text{ times}}$. Bob's secret key is d_B and his public key is Q_B.

3. **PUBLIC KEY EXCHANGE** Alice sends her public key Q_A to Bob.
   Bob sends his public key Q_B to Alice.

4. **COMPUTING THE SHARED KEY/SECRET** Alice computes $P := d_A Q_B = d_A d_B G$. Bob computes $Q := d_B Q_A = d_B d_A G$. By commutativity, both Alice and Bob now share $P = Q$, so for example they can take the x-coordinate of P, denoted $x_P \in \mathbb{F}_p$, to be their shared key, which they can then use to encrypt a message.

5. **SECURITY** In order for Eve to read the encoded message, she needs to find out x_P. She has access to the initial information: $E, \mathbb{F}_p, G, n$. She can intercept Q_A and Q_B. However, in order to compute P (and hence x_P) she needs to know d_A or d_B. Well, this is equivalent to solving the discrete logarithm problem for $G = E(\mathbb{F}_p)$, which we know to be very hard to solve.

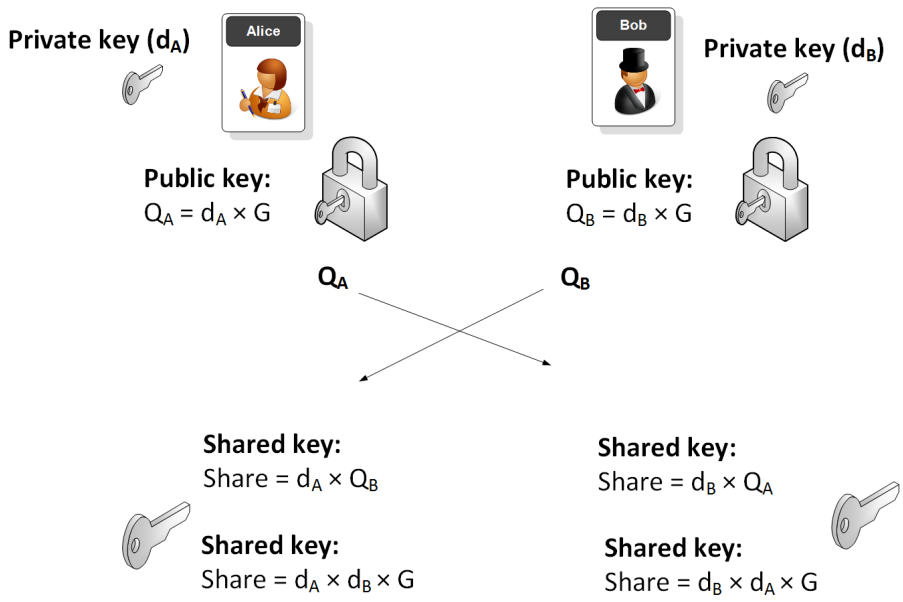


Figure 4.1: ECDH: credits "A security site.com"

Problem

For classes: we will split in pairs and each pair will perform ECDH key exchange between them.

4.3. RSA vs ECDH

The main difference between RSA vs ECDH is in the encryption strength. Elliptic-Curve Diffie-Hellman (ECDH) provides an equivalent level of encryption strength as RSA algorithm with a shorter key length. Therefore the security offered by an ECDH is higher than an RSA for Public Key Infrastructure (PKI).
However, due to the fact that RSA is simple, it may run faster. But along with increased computational power (for example, along with the emergence of quantum computers), running time won't be a problem anymore and security is the main concern.
Nowadays, even more sophisticated Elliptic Curves cryptosystems have emerged and there is a huge research area on the topic. Most common ideas are to use supersingular elliptic curves over finite fields (i.e. elliptic curves with a big endomorphism ring) and to look at special homomorphisms between them (called isogenies). One can create a graph where the elliptic curves are the vertices and the isogenies are edges. It is possible to create shared keys by making (and composing) walks on this graph. To find out more about this google "SIDH Cryptography".

References

[1] I. Blake, Hewlett-Packard Laboratories, Palo Alto, California, G. Seroussi, Hewlett-Packard Laboratories, Palo Alto, California, N. Smart. *Elliptic Curves in Cryptography.* Hewlett-Packard Laboratories, Bristol.

[2] Cryptography Stack Exchange. `https://crypto.stackexchange.com/questions/66589/elliptic-curves-on-finite-fields`

[3] E.V. Flynn. *Elliptic Curves. HT 2016/17.* University of Oxford Lecture Notes Part C, HT 2016/17.

[4] M. Goemans. *Modular Arithmetic and Elementary Algebra.* MIT lectures.

[5] B. Green. *Part A Number Theory 2020.* University of Oxford Lecture Notes Part A, TT 2020.

[6] J.S. Milne. *Group Theory.* `https://www.jmilne.org/math/CourseNotes/GT.pdf`