HAI709I : Fondements cryptographiques de la sécurité, Université de Montpellier, 2023

06/11/2023. Lecture 8.

1 Groups: elementary introduction.

In this section we discuss the algebraic notion of a *group* and its basic properties.

Definition 1. A *group* is a set G (finite or infinite) with a binary operation $*$ (a function $G \times G \mapsto G$) satisfying the following properties

- there exists an $e \in G$ (the neutral element) such that for all $g \in G$
$$g * e = e * g = g$$
- for all $g \in G$ there exists an $h \in G$ such that $g * h = h * g = e$
- for all $g_1, g_2, g_3 \in G$
$$(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3).$$

A group is called *commutative* (or *Abelian*) if for all $g, h \in G$

- $g * h = h * g$.

Examples of groups $(\mathbb{R}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{Z}/n\mathbb{Z}, +)$, $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ for a prime n, the set of all polynomials with real coefficients with the operation of addition, the set of all invertible matrices of size $n \times n$ (with real coefficients) with the operation of multiplication of matrices.

Remark 1. The operation in a group is often denoted as $\cdot$ or $+$.

Exercise 1. Prove that in every group there is only one neutral element.

Definition 2. Let $(G, *)$ be a group with the neutral element e, and let $g \in G$ be its element. The *order* of g is the minimal positive integer number n such that

$$g^n := \underbrace{g * (g * (g * \ldots * (g * g) \ldots))}_{n} = e$$

(or infinity, if for all $n > 0$ the element g^n is not equal to e). For the order of an element $g \in G$ we use the notation $Or(g)$ (the implied group must be clear from the context).

In the class we proved the following proposition.

Proposition 1. *If a group $(G, *)$ if finite (consists of a finite number of elements), then for every $g \in G$ the order of g divides the number of elements in G.*

Corollary 1. *Let $(G, *)$ be a finite group with n elements. Let e be the neutral element of the group. Then for every $g \in G$ we have $g^n = e$.*

Corollary 2. *For a prime number p and for every integer g co-prime with p we have $g^{p-1} = 1 \mod p$.*

2 Modular arithmetic revisited

In this section we discussed properties of certain commutative groups connected with the modular arithmetic.

2.1 Reminder

Theorem 1 (fundamental theorem of arithmetic)**.** *Every integer number n greater than 1 can be represented uniquely as a product of prime numbers, up to the order of the factors.*

We did not prove this theorem in the class. However, we used it to simplify the proofs of several properties of integer numbers:

Proposition 2. *Let x and y be integer numbers. There exist integer numbers v and w such that*

$$v \cdot x + w \cdot y = gcd(x, y),$$

where gcd denote the greatest common divisor*).*

Proposition 3. *If a positive integer number a is co-prime with n then the there exists an integer number b such that $a \cdot b = 1 \mod n$.*

For a prime number p wWe denote by $(\mathbb{Z}/p\mathbb{Z})^{\times}$ the set of integer numbers from $\{1, \dots, p\}$. It is easy to see that this set with the operation of multiplication modulo p is a group.

Theorem 2. *For every prime number p there exists a $g \in \{1, 2, \dots, p-1\}$ such that the order of g in $\big((\mathbb{Z}/p\mathbb{Z})^{\times}, \cdot\big)$ is equal to $p-1$.*

Proof. The core idea of the proof is the fact that in each field a polynomial of degree k cannot have more than k roots. Let us explain this proof in some detail.

Step 1. In this proof, the order of an element $x \in (\mathbb{Z}/p\mathbb{Z})^{\times}$ (denoted $Or(x)$) is the minimal integer number $k \geq 1$ such that $x^k = 1 \mod p$. The theorem claims that for every prime number p there exists a g such that $Or(g) = p-1$.

Step 2. Let g be any element in $(\mathbb{Z}/p\mathbb{Z})^{\times}$. Since the set $\{1, 2, \dots, p-1\}$ is finite, the values

$$g \mod p,\ g^2 \mod p,\ g^3 \mod p, \dots$$

cannot be all different; starting from some moment, this series begins to repeat. Therefore, this sequence (powers of g modulo p) is periodic with some period k. The length of the period (the number k) is in fact equal to the very first position in the sequence where we obtain $g^k = 1 \mod p$. In other words, the period of this sequence modulo p is equal to $Or(g)$.

We know that for every prime number p and for every $g \neq 0 \mod p$ we have $g^{p-1} = 1 \mod p$. Hence, the period of g modulo p must divide the number $p-1$. Our goal is to find a g such that $Or(g)$ not only divides $p-1$ but *is equal to* $p-1$.

Step 3. We proceed with the following lemma.

Lemma 1. *Let k_0 be the least common multiple of*

$$Or(1), Or(2), Or(3), \dots, Or(p-1).$$

Then all element of the field are roots of the equation $x^{k_0} = 1 \mod p$.

Proof. For every $x \in \{1, 2, \ldots, p-1\}$ we have, by definition, $x^{Or(x)} = 1 \mod p$. Since k_0 is a multiple of $Or(x)$, we have $k_0 = \ell \cdot Or(x)$, and

$$x^{k_0} \mod p = x^{\ell \cdot Or(x)} \mod p = (x^{Or(x)})^{\ell} \mod p = 1^{\ell} \mod p,$$

and we are done. □

Thus, the equation

$$x^{k_0} = 1 \mod p$$

has $p-1$ roots in $\mathbb{Z}/p\mathbb{Z}$. It follows that $k_0 \geq p$.

In what follows we will find an element g_0 such that $Or(g_0) = k_0$. The order of every element $\mathbb{Z}/p\mathbb{Z}$ is a factor of $(p-1)$. Thus, we have at once two properties: k_0 is a factor of $p-1$ and $k_0 \geq p-1$. Hence, $k_0 = p-1$, and $Or(g_0) = p-1$.

To conclude the proof of the theorem, it remains to find an element g_0 of order k_0.

Step 4. We need one more lemma:

Lemma 2. *For all $x, y \in (\mathbb{Z}/p\mathbb{Z})^{\times}$ there exists an element $z \in (\mathbb{Z}/p\mathbb{Z})^{\times}$ such that $Or(z)$ is the least common multiple of $Or(x)$ and $Or(y)$.*

Proof. At first, we prove the lemma for a special case, assuming that

$$gcd(Or(x), Or(y)) = 1$$

and, therefore, $lcm(Or(x), Or(y)) = Or(x) \cdot Or(y)$ (here lcm denote *the least common multiplier*).

Since $Or(x)$ and $Or(y)$ are co-prime, we need a z such that

$$Or(z) = lcm(Or(x), Or(y)) = Or(x) \cdot Or(y).$$

We know from the Extended Euclid Algorithm that if the numbers $Or(x)$ and $Or(y)$ are co-prime, then there exist v and w such that

$$v \cdot Or(x) + w \cdot Or(y) = 1.$$

We let $z := x^w \cdot y^v \mod p$.

It is easy to see that $z^{Or(x) \cdot Or(y)} \mod p = 1$. It remains to show that $k = Or(x) \cdot Or(y)$ is the minimal natural number such that $z^k = 1 \mod p$.

It is clear that $Or(z)$ divides $Or(x) \cdot Or(y)$. Hence, if $Or(z) < Or(x) \cdot Or(y)$, then in the sequence

$$z \mod p,\ z^2 \mod p,\ z^3 \mod p,\ \ldots,\ z^{Or(x) \cdot Or(y)} \mod p \tag{1}$$

the *ones* appear in a periodic way, at some positions

$$k', 2k', 3k', \ldots, Or(x) \cdot Or(y).$$

The key observation: if $k' < Or(x) \cdot Or(y)$, then *ones* appear in (1) (among other positions) at some position $Or(x) \cdot \ell$ (for some $\ell < Or(y)$) or at some position $Or(y) \cdot \ell$ (for some $\ell < Or(x)$).

In what follows we show that this is impossible. Indeed, for the number z defined above we have

$$z^{Or(x)} = 1 \cdot y^{u \cdot Or(x)} \mod p = y^{1 - v \cdot Or(y)} \mod p = y \mod p.$$

Hence, the numbers

$$z^{Or(x)},\ z^{2\cdot Or(x)},\ z^{3\cdot Or(x)},\ z^{(Or(y)-1)\cdot Or(x)}$$

coincide with

$$y,\ y^2,\ ,y^3,\ \dots, y^{(Or(y)-1)}$$

modulo p, and they are all *not equal* to 1 modulo p. A similar argument implies that the numbers

$$z^{Or(y)}, z^{2\cdot Or(y)}, z^{3\cdot Or(y)}, z^{(Or(x)-1)\cdot Or(y)}$$

are also not equal to 1 modulo p. Now it is not hard to show that in the list of numbers

$$z,\ z^2,\ z^3,\ \dots,\ z^{Or(x)\cdot Or(y)}$$

only the very last element is equal to 1 modulo p, i.e.,

$$Or(z) = Or(x)\cdot Or(y).$$

It remains to consider the case

$$gcd(Or(x), Or(y)) \neq 1.$$

We reduce the general case to the special case discussed above. We use the following trick. If ℓ is a factor of $Or(y)$, then $Or(y^\ell) = Or(y)/\ell$. So if we can take $\ell := gcd(Or(x), Or(y))$ and let $y' = y^\ell$, then

$$gcd(Or(x), Or(y')) = 1 \text{ and } lcm(Or(x), Or(y')) = lcm(Or(x), Or(y)).$$

It remains to apply the argument explained above to the numbers x and y', and we are done. □

Step 5. Now we iterate an application of Lemma 2. First of all, we let $x_1 = 1$. Now we apply Lemma 2 and find an x_2 such that $Or(x_2)$ is the least common multiple of $Or(x_1)$ and $Or(2)$. Then we apply one more time Lemma 2 and find a x_3 such that $Or(x_3)$ is the least common multiple of $Or(x_2)$ and $Or(3)$. Further, we find a x_4 such that $Or(x_4)$ is the least common multiple of $Or(x_3)$ and $Or(4)$, and so on. Finally, we find an element x_{p-1} such that $Or(x_{p-1})$ is the least common multiple of the orders of x_{p-2} and $p-1$. From this construction it follows that the order of the last final element x_{p-1} is equal to the least common multiple of the orders of *all* elements $1, 2, \dots, p-1$. In other words, we found an element x_{p-1} whose order is equal to the number k_0 from Lemma 1.

Step 5. Since all elements in $\{1, \dots, p-1\}$ satisfy the equation

$$x^{k_0} = 1 \mod p,$$

the number k_0 cannot be smaller than $p-1$ (a polynomial of degree k_0 cannot have more than k_0 roots). On the other hand, we know that $Or(x)$ divides $p-1$ for each x. Thus, k_0 is not less than $p-1$ and not greater than $p-1$. We conclude that $k_0 = p-1$, i.e., we have got an element x_{p-1} such that $Or(x_{p-1})$ is equal to $p-1$. This means that x_0 is a generating element of $(\mathbb{Z}/p\mathbb{Z})^\times$, end we are done. □

3 The RSA scheme

3.1 Modular arithmetic once again.

For a positive integer number n we denote $\varphi(n)$ the numbers between 1 and n that are co-prime with n. For example, $\varphi(5) = 4$, $\varphi(9) = 6$, $\varphi(10) = 4$.

Proposition 4. *(a) if p is a prime number, then $\varphi(p) = p - 1$.*
(b) If p and q are two different prime numbers, then $\varphi(pq) = (p-1)(q-1) = pq - p - q + 1$.

We extend the notation form the previous section and denote by $(\mathbb{Z}/n\mathbb{Z})^\times$ the set of integer numbers from $\{1, \ldots, n\}$ that are co-prime with n. The size of this set is by definition $\varphi(n)$. The set $(\mathbb{Z}/n\mathbb{Z})^\times$ with the operation of multiplication modulo n is a group.

Proposition 5. *For every $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ we have $x^{\varphi(n)} = 1 \mod n$. In particular, if $p \neq q$ are two prime numbers, then $x^{(p-1)(q-1)} = 1 \mod p \cdot q$.*

3.2 Non symmetric cryptography

In the classe started a discussion of the *asymmetric* encryption scheme RSA (suggested by Rivest, Shamir, and Adleman). In contrast with the schemes that we have discussed before, in RSA we need two *different* keys: one for encoding and another for decoding messages.

The scheme is defined as follows. Let p and q be prime numbers, $n = p \cdot q$. Let $k, d \in (\mathbb{Z}/\varphi(n)\mathbb{Z})^\times$ such that $d \cdot k = 1 \mod \varphi(n)$.

public key: (k, n)

secret key: (d, n)

We assume that the open and the encrypted messages are represented by integer numbers from $(\mathbb{Z}/n\mathbb{Z})^\times$.

encryption: $Enc(m) = m^k \mod n$

decryption: $Dec(e) = e^d \mod n$

Correctness of the scheme: let us show that the operations Enc and Dec are mutually inverse, i.e., $Dec(Enc(m)) = m$ for all m co-prime with n.

$$(m^k)^d = m^{k \cdot d} = m^{1+\ell\varphi(n)} = m \cdot (m^{\varphi(n)})^\ell = m \cdot 1^\ell \mod n = m \mod n.$$

If the public key is available to everyone, then everyone can encrypt a message. But only the holder of the private key can decode the encrypted message.

Observe that given p and q we can easily compute the product $n = pq$, but not vice-versa (the problem of integer factorisation is believed to be hard). The numbers p and q are needed to prepare the pair of elements d and k that are inverse to each other modulo $\varphi(n)$. When the private and the public key are fixed, the numbers p and q can be discarded. These numbers should never become made public. Indeed, given the numbers p and p, and the public key, one can effectively compute the private key.

The encoding and decoding algorithms in the scheme RSA require to compute $x^k \mod n$ for very large numbers k and n. (In practice it is often recommended to use numbers with at least two thousands of binary digits). In the class we discussed an efficient exponentiation algorithm: we can compute $x^k \mod n$ in time that polynomially depends on *the number of binary digits* in x, k, n.

References

[1] J. Katz, Y. Lindell. Introduction to modern cryptography, CRC Press, 2021

[2] B. Martin. Codage, cryptologie et applications. PPUR presses polytechniques, 2004