Algorithms for Numbers and Public-Key Cryptography

Jean-Sébastien Coron

University of Luxembourg

Course summary

- Algorithms for numbers
  - Describe the basic algorithms for dealing with numbers
  - Implement them on a computer
- Public-key cryptography
  - Describe the basic public-key algorithms
  - and the main cryptanalytical attacks
  - Implement them on a computer

Course organization

- The course is based on lectures and homeworks.
- Homework:
  - Implementation of the basic algorithms described in the lectures.
  - 100% of the final grade.

Basic number theory for cryptography

Jean-Sébastien Coron

University of Luxembourg

Basic number theory for cryptography

- Basic properties
  - Congruence, modular arithmetic, modular exponentiation.
  - GCD, Euclid's algorithm, modular inverse, CRT
  - Euler function, Fermat's little theorem
- The set $\mathbb{Z}_p^*$ for prime p
  - Generators of $\mathbb{Z}_p^*$
  - Quadratic residues, Legendre symbol, Jacobi symbol
  - Computing square roots
- Recommended textbook
  - Victor Shoup, *A Computational Introduction to Number Theory and Algebra*
  - `https://www.shoup.net/ntb/`

Euclidean division and modulo operator

Theorem (Division with remainder)

For $a, b \in \mathbb{Z}$ with $b > 0$, there exist unique $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < b$.

- Quotient
  - $q = \lfloor a/b \rfloor$, where $\lfloor x \rfloor$ denote the greatest integer $\leq x$.
- Modulo operator
  - We write $r = a \bmod b$
  - $a \bmod b = a - b \cdot \lfloor a/b \rfloor$
  - Examples:
    $7 \bmod 3 = 1$
    $10 \bmod 4 = 2$

Basic properties of integers

Theorem (Fundamental theorem of arithmetic)

Every non-zero integer n can be expressed as

$$n = \pm p_1^{e_1} \cdots p_r^{e_r}$$

where the p_i's are distinct primes and the e_i are positive integers. Moreover the decomposition is unique, up to reordering of the primes.

- Proof: existence is easy by induction; unicity: see any standard textbook.

Congruence

- Congruence.
  - Let $n > 0$ and $a, b \in \mathbb{Z}$.
$$a \equiv b \pmod{n} \Leftrightarrow n \,|\, (a - b)$$
  - n is called the *modulus*.
  - Should not be confused with the mod of Euclidean division.
- Examples :
  - $2 \equiv 8 \pmod{3}$, since $3 \,|\, (8 - 2)$.
  - $12 \equiv 2 \pmod{5}$, since $5 \,|\, (12 - 2)$.

Properties

- Basic properties :
  - $a \equiv b \pmod{n} \Leftrightarrow \exists k \in \mathbb{Z}, a = b + k \cdot n$.
  - $a \equiv a \pmod{n}$
  - $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$
  - $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ implies $a \equiv c \pmod{n}$
- When working modulo n, we can always choose a representative between 0 and $n - 1$:
  - Theorem: for any $a \in \mathbb{Z}$, there exists a unique integer $b \in \mathbb{Z}$ such that $a \equiv b \pmod{n}$ and $0 \leq b < n$, namely $b := a \bmod n$.
  - Examples:
    - $23 \equiv 3 \pmod{5}$
    - $25 \equiv 4 \pmod{7}$

Properties

- Congruence is compatible with addition and multiplication
  - If $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, then
  - $a + b \equiv a' + b' \pmod{n}$ and $a \cdot b \equiv a' \cdot b' \pmod{n}$.
- This means that we can work with congruence relations as with ordinary equalities
- When computing modulo n, one can substitute to x a value $x' \equiv x \pmod{n}$:
  - Compute a with $0 \leq a < 7$ such that $a \equiv 83 \cdot 72 \pmod{7}$.
  - First approach: $83 \cdot 72 = 5976$
    $a = 5976 \pmod{7} = 5$.
  - Second approach: $83 \equiv 6 \pmod{7}$,
    $72 \equiv 2 \pmod{7}$,
    $83 \cdot 72 \equiv 6 \cdot 2 \equiv 12 \equiv 5 \pmod{7}$.

Modular exponentiation

- We want to compute $c = a^b \pmod{n}$.
  - Example: RSA
    - $c = m^e \pmod{n}$ where m is the message, e the public exponent, and n the modulus.
- Naive method:
  - Multiplying a in total b times by itself modulo n
  - Very slow: if b is 100 bits, roughly 2^{100} multiplications !
- Example: compute $b = a^{16} \pmod{n}$
  - $b = a \cdot a \cdot \ldots \cdot a \cdot a \pmod{n}$: 15 multiplications
  - $b = (((a^2)^2)^2)^2 \pmod{n}$: 4 multiplications

Square and multiply algorithm

- Let $b = (b_{\ell-1} \dots b_0)_2$ the binary representation of b

$$b = \sum_{i=0}^{\ell-1} b_i \cdot 2^i$$

- Square and multiply algorithm :
  - Input : a, b and n
  - Output : $a^b \pmod{n}$
  - $c \leftarrow 1$

```
for $i = \ell - 1$ down to 0 do
   $c \leftarrow c^2 \pmod{n}$
   if $b_i = 1$ then $c \leftarrow c \cdot a \pmod{n}$
Output $c$
```

Analysis

- Let B_i be the integer with binary representation $(b_{\ell-1} \ldots b_i)_2$, and let

$$c_i = a^{B_i} \pmod{n}$$

- Initialization

$$\begin{cases} B_\ell &= 0 \\ c_\ell &= 1 \end{cases}$$

- Recursive step

$$\begin{cases} B_i &= 2 \cdot B_{i+1} + b_i \\ c_i &= (c_{i+1})^2 \cdot a^{b_i} \pmod{n} \end{cases}$$

- Final step

$$\begin{cases} B_0 &= b \\ c_0 &= a^b \pmod{n} \end{cases}$$

Greatest common divisor

- Greatest common divisor:
  - A common divisor $d \in \mathbb{Z}$ of $a, b \in \mathbb{Z}$ is such that $d|a$ and $d|b$
  - We say that d is a **greatest common divisor** of a and b if $d > 0$ and all other common divisors of a and b divide d.
  - There exists a unique greatest common divisor, so we can write $d = \gcd(a, b)$ and moreover

$$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$$

- Examples
  - $\gcd(9, 6) = 3$
  - $\gcd(7, 5) = 1$.

Property of $\gcd$

- Let $a, b > 0$

$$\gcd(a, b) = \gcd(b, a \bmod b)$$

- Proof. Let $r = a \bmod b = a - q \cdot b$ for some $q \in \mathbb{Z}$.
  - If $d|a$ and $d|b$, then $d|r$, and then $d|\gcd(b, r)$. Then $\gcd(a, b)|\gcd(b, r)$.
  - Similarly $\gcd(b, r)|\gcd(a, b)$, therefore $\gcd(a, b) = \gcd(b, r)$.
- Example:
  - $\gcd(47, 18) = \gcd(18, 11) = \gcd(11, 7) = \gcd(7, 4) = \gcd(4, 3) = \gcd(3, 1) = \gcd(1, 0) = 1$
  - This is Euclid's algorithm

Euclid's algorithm

- Euclid's algorithm with input $a, b > 0$.
  - Let $r_0 = a$ and $r_1 = b$.
  - For $i \geq 0$, one defines the sequence (r_i) and (q_i) such that :

    $$r_i = q_i \cdot r_{i+1} + r_{i+2}$$

    where q_i and r_{i+2} are the quotient and remainder of the division of r_i by r_{i+1}
  - The sequence is decreasing, so $r_k = 0$ for some $k > 0$
  - Then $\gcd(a, b) = r_{k-1}$.
- Proof
  - $\gcd(a, b) = \gcd(r_i, r_{i+1})$ for all $i < k$
  - $$\begin{aligned} \gcd(a, b) &= \gcd(r_{k-1}, r_k) \\ &= \gcd(r_{k-1}, 0) = r_{k-1} \end{aligned}$$

Example of $\gcd$ computation

- Example of $\gcd(a,b)$ with $a = 47$, $b = 18$
  - $r_0 = a = 47$
  - $r_1 = b = 18$
  - $r_i = q_i \cdot r_{i+1} + r_{i+2}$

i	0	1	2	3	4	5	6	7
r_i	47	18	11	7	4	3	1	0

$$\begin{aligned}\gcd(47,18) &= \gcd(18,11) = \gcd(11,7) = \gcd(7,4)\\ &= \gcd(4,3) = \gcd(3,1) = \gcd(1,0) = 1\end{aligned}$$

Modular arithmetic

- Let an integer $n > 1$ called the modulus.
- Modular reduction
  - $r := a \bmod n$, remainder of the division of a by n.
  - $0 \leq r < n$
  - Ex: $11 \bmod 8 = 3$, $15 \bmod 5 = 0$.
- Congruence:
  - $a \equiv b \pmod{n}$ if $n \,|\, (a - b)$.
  - $a \equiv b \pmod{n}$ iif a and b have same remainder modulo n.
  - Ex: $11 \equiv 19 \pmod{8}$.
  - If $r := a \bmod n$, then $r \equiv a \pmod{n}$.

Modular arithmetic

- If $a_0 \equiv b_0 \pmod{n}$ and $a_1 \equiv b_1 \pmod{n}$
  - $a_0 + a_1 \equiv b_0 + b_1 \pmod{n}$
  - $a_0 - a_1 \equiv b_0 - b_1 \pmod{n}$
  - $a_0 \cdot a_1 \equiv b_0 \cdot b_1 \pmod{n}$
- Integers modulo n
  - Integers modulo n are $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$
  - Addition, subtraction or multiplication in $\mathbb{Z}_n$ is done by first doing it in $\mathbb{Z}$ and then reducing the result modulo n.
  - For example in $\mathbb{Z}_7$:
    - $6 + 4 = 3$, $3 - 4 = 6$, $3 \cdot 6 = 4$.

Multiplicative inverse

- Multiplicative inverse :
  - Let $n > 0$ and $a \in \mathbb{Z}$. An integer a' is a *multiplicative inverse* of a modulo n if $a \cdot a' \equiv 1 \pmod{n}$.
- Theorem :
  - Let $n, a \in \mathbb{Z}$ with $n > 0$. Then a has a multiplicatif inverse modulo n iff $\gcd(a, n) = 1$. Moreover such multiplicative inverse is unique modulo n.
  - Proof
    - If $a \cdot a' \equiv 1 \pmod{n}$, then $a \cdot a' = 1 + k \cdot n$ for some $k \in \mathbb{Z}$. Therefore if $d|a$ and $d|n$, then $d|1$. Therefore $\gcd(a, n) = 1$.
    - If $\gcd(a, n) = 1$, then $a\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$,
      so $a \cdot s + n \cdot t = 1$ for some $s, t \in \mathbb{Z}$.
      Therefore $a \cdot s \equiv 1 \pmod{n}$.

Example

- The multiplicative inverse of 5 modulo 7 is 3 because

$$3 \cdot 5 \equiv 15 \equiv 1 \pmod{7}$$

- 2 has no multiplicative inverse modulo 6 :
    - $2 \cdot 1 \equiv 2 \pmod{6}$
    - $2 \cdot 2 \equiv 4 \pmod{6}$
    - $2 \cdot 3 \equiv 0 \pmod{6}$
    - $2 \cdot 4 \equiv 2 \pmod{6}$
    - $2 \cdot 5 \equiv 4 \pmod{6}$

Euclid's extended algorithm

- Euclid's extended algorithm
  - Let $a, b \in \mathbb{Z}$ and $d = \gcd(a, b)$.
  - Computes $u, v \in \mathbb{Z}$ such that $a \cdot u + b \cdot v = d$.
  - Based on computing two sequences u_i, v_i such that $a \cdot u_i + b \cdot v_i = r_i$, where eventually $r_{k-1} = d$.
- Application to computing multiplicative inverse
  - Let a, n with $n > 0$ and $\gcd(a, n) = 1$.
  - With Euclid's extended algorithm, one computes u, v such that
  $$a \cdot u + n \cdot v = 1$$
  - Then $a \cdot u \equiv 1 \pmod{n}$

Euclid's extended algorithm

- Euclid's extended algorithm, for $a > 0$ and $b \geq 0$.
  - $r_0 = a$ and $r_1 = b$.
  - For $i \geq 0$, let $r_i = q_i \cdot r_{i+1} + r_{i+2}$
  - Two additional sequences u_i and v_i.
  - $u_0 := 1,\ v_0 := 0,\ u_1 := 0,\ v_1 := 1$ and for $i \geq 2$, one defines

$$\begin{cases} u_i = u_{i-2} - q_{i-2} \cdot u_{i-1} \\ v_i = v_{i-2} - q_{i-2} \cdot v_{i-1} \end{cases}$$

- There exists $k > 0$ such that $r_k = 0$.
  - $\gcd(a, b) = r_{k-1} = u_{k-1} \cdot a + v_{k-1} \cdot b$

Proof

- We always have
$$r_i = u_i \cdot a + v_i \cdot b$$
- Initialization
  - $r_0 = a = 1 \cdot a + 0 \cdot b.$
  - $r_1 = b = 0 \cdot a + 1 \cdot b.$
- Recursive step:
  - Assume $u_{i-2} \cdot a + v_{i-2} \cdot b = r_{i-2}$
    $u_{i-1} \cdot a + v_{i-1} \cdot b = r_{i-1}$

$$\begin{aligned} u_i \cdot a + v_i \cdot b &= (u_{i-2} - q_{i-2} \cdot u_{i-1}) \cdot a + \\ &\quad (v_{i-2} - q_{i-2} \cdot v_{i-1}) \cdot b \\ &= r_{i-2} - q_{i-2} \cdot r_{i-1} \\ &= r_i \end{aligned}$$

Example of extended gcd computation

- Compute u, v such that $47 \cdot u + 18 \cdot v = 1$
  - $(r_0, r_1) = (47, 18)$
  - $(u_0, u_1) = (1, 0)$
  - $(v_0, v_1) = (0, 1)$

$$\begin{cases} r_{i-2} & = & q_{i-2} \cdot r_{i-1} + r_i \\ u_i & = & u_{i-2} - q_{i-2} \cdot u_{i-1} \\ v_i & = & v_{i-2} - q_{i-2} \cdot v_{i-1} \end{cases}$$

i	0	1	2	3	4	5	6	7
r_i	47	18						
q_i								
u_i	1	0						
v_i	0	1						

Example of extended gcd computation

- Compute u, v such that $47 \cdot u + 18 \cdot v = 1$
  - $(r_0, r_1) = (47, 18)$
  - $(u_0, u_1) = (1, 0)$
  - $(v_0, v_1) = (0, 1)$

$$\begin{cases} r_{i-2} & = & q_{i-2} \cdot r_{i-1} + r_i \\ u_i & = & u_{i-2} - q_{i-2} \cdot u_{i-1} \\ v_i & = & v_{i-2} - q_{i-2} \cdot v_{i-1} \end{cases}$$

i	0	1	2	3	4	5	6	7
r_i	47	18	11					
q_i	2							
u_i	1	0	1					
v_i	0	1	-2					

Example of extended $\gcd$ computation

- Compute u, v such that $47 \cdot u + 18 \cdot v = 1$
  - $(r_0, r_1) = (47, 18)$
  - $(u_0, u_1) = (1, 0)$
  - $(v_0, v_1) = (0, 1)$

$$\left\{ \begin{array}{rcl} r_{i-2} & = & q_{i-2} \cdot r_{i-1} + r_i \\ u_i & = & u_{i-2} - q_{i-2} \cdot u_{i-1} \\ v_i & = & v_{i-2} - q_{i-2} \cdot v_{i-1} \end{array} \right.$$

i	0	1	2	3	4	5	6	7
r_i	47	18	11	7				
q_i	2	1						
u_i	1	0	1	-1				
v_i	0	1	-2	3				

Example of extended gcd computation

- Compute u, v such that $47 \cdot u + 18 \cdot v = 1$
  - $(r_0, r_1) = (47, 18)$
  - $(u_0, u_1) = (1, 0)$
  - $(v_0, v_1) = (0, 1)$

$$\begin{cases} r_{i-2} &= q_{i-2} \cdot r_{i-1} + r_i \\ u_i &= u_{i-2} - q_{i-2} \cdot u_{i-1} \\ v_i &= v_{i-2} - q_{i-2} \cdot v_{i-1} \end{cases}$$

i	0	1	2	3	4	5	6	7
r_i	47	18	11	7	4			
q_i	2	1	1					
u_i	1	0	1	-1	2			
v_i	0	1	-2	3	-5			

Example of extended gcd computation

- Compute u, v such that $47 \cdot u + 18 \cdot v = 1$
  - $(r_0, r_1) = (47, 18)$
  - $(u_0, u_1) = (1, 0)$
  - $(v_0, v_1) = (0, 1)$

$$\begin{cases} r_{i-2} & = & q_{i-2} \cdot r_{i-1} + r_i \\ u_i & = & u_{i-2} - q_{i-2} \cdot u_{i-1} \\ v_i & = & v_{i-2} - q_{i-2} \cdot v_{i-1} \end{cases}$$

i	0	1	2	3	4	5	6	7
r_i	47	18	11	7	4	3		
q_i	2	1	1	1				
u_i	1	0	1	-1	2	-3		
v_i	0	1	-2	3	-5	8		

Example of extended gcd computation

- Compute u, v such that $47 \cdot u + 18 \cdot v = 1$
  - $(r_0, r_1) = (47, 18)$
  - $(u_0, u_1) = (1, 0)$
  - $(v_0, v_1) = (0, 1)$

$$\begin{cases} r_{i-2} & = & q_{i-2} \cdot r_{i-1} + r_i \\ u_i & = & u_{i-2} - q_{i-2} \cdot u_{i-1} \\ v_i & = & v_{i-2} - q_{i-2} \cdot v_{i-1} \end{cases}$$

i	0	1	2	3	4	5	6	7
r_i	47	18	11	7	4	3	1	
q_i	2	1	1	1	1			
u_i	1	0	1	-1	2	-3	5	
v_i	0	1	-2	3	-5	8	-13	

Example of extended gcd computation

- Compute u, v such that $47 \cdot u + 18 \cdot v = 1$
  - $(r_0, r_1) = (47, 18)$
  - $(u_0, u_1) = (1, 0)$
  - $(v_0, v_1) = (0, 1)$

$$\begin{cases} r_{i-2} & = & q_{i-2} \cdot r_{i-1} + r_i \\ u_i & = & u_{i-2} - q_{i-2} \cdot u_{i-1} \\ v_i & = & v_{i-2} - q_{i-2} \cdot v_{i-1} \end{cases}$$

i	0	1	2	3	4	5	6	7
r_i	47	18	11	7	4	3	1	0
q_i	2	1	1	1	1			
u_i	1	0	1	-1	2	-3	5	
v_i	0	1	-2	3	-5	8	-13	

Example of extended gcd computation

- Compute u, v such that $47 \cdot u + 18 \cdot v = 1$
  - $(r_0, r_1) = (47, 18)$
  - $(u_0, u_1) = (1, 0)$
  - $(v_0, v_1) = (0, 1)$

$$\begin{cases} r_{i-2} & = & q_{i-2} \cdot r_{i-1} + r_i \\ u_i & = & u_{i-2} - q_{i-2} \cdot u_{i-1} \\ v_i & = & v_{i-2} - q_{i-2} \cdot v_{i-1} \end{cases}$$

i	0	1	2	3	4	5	6	7
r_i	47	18	11	7	4	3	1	0
q_i	2	1	1	1	1			
u_i	1	0	1	-1	2	-3	5	
v_i	0	1	-2	3	-5	8	-13	

$$47 \cdot 5 + 18 \cdot (-13) = 1$$

Solving linear congruence

- Let $a, n \in \mathbb{Z}$ with $n > 0$ such that $\gcd(a, n) = 1$. Let $b \in \mathbb{Z}$. The equation $a \cdot x \equiv b \pmod{n}$ has a unique solution x modulo n.
  - Let a^{-1} by the multiplicative inverse of a modulo n.

$$a \cdot a^{-1} \cdot x \equiv x \equiv a^{-1} \cdot b \pmod{n}$$

- Example :
  - Find x such that $5 \cdot x \equiv 6 \pmod{7}$
  - 3 is the inverse of 5 modulo 7 because $5 \cdot 3 \equiv 1 \pmod{7}$.
  - $3 \cdot 5 \cdot x \equiv 15 \cdot x \equiv 1 \cdot x \equiv 3 \cdot 6 \equiv 4 \pmod{7}$
  - $x \equiv 4 \pmod{7}$

Chinese remainder theorem

- Chinese remainder theorem
  - Let two integers $n_1 > 1$ and $n_2 > 0$ with $\gcd(n_1, n_2) = 1$.
  - For all $a_1, a_2 \in \mathbb{Z}$, there exists an integer z such that

$$\begin{cases} z \equiv a_1 \pmod{n_1} \\ z \equiv a_2 \pmod{n_2} \end{cases}$$

  - z is unique modulo $n_1 \cdot n_2$.
- Existence :
  - Let $m_1 = (n_2)^{-1} \bmod n_1$ and $m_2 = (n_1)^{-1} \bmod n_2$

$$z := n_2 \cdot m_1 \cdot a_1 + n_1 \cdot m_2 \cdot a_2$$

  - $z \equiv (n_2 \cdot m_1) \cdot a_1 \equiv a_1 \pmod{n_1}$
  - $z \equiv (n_1 \cdot m_2) \cdot a_2 \equiv a_2 \pmod{n_2}$

Euler function

- Definition:
  - $\phi(n)$ for $n > 0$ is defined as the number of integers a comprised between 0 and $n-1$ such that $\gcd(a,n) = 1$.
  - $\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$.
- Equivalently:
  - Let $\mathbb{Z}_n^*$ be the set of integers a comprised between 0 and $n-1$ such that $\gcd(a,n) = 1$.
  - Then $\phi(n) = |\mathbb{Z}_n^*|$.

Properties

- If $p \geq 2$ is prime, then

$$\phi(p) = p - 1$$

- More generally, for any $e \geq 1$,

$$\phi(p^e) = p^{e-1} \cdot (p - 1)$$

- For $n, m > 0$ such that $\gcd(n, m) = 1$, we have:

$$\phi(n \cdot m) = \phi(n) \cdot \phi(m)$$

$\phi(p^e) = p^{e-1} \cdot (p-1)$

- If p is prime
  - Then for any integer $1 \leq a < p$, $\gcd(a, p) = 1$
  - Therefore $\phi(p) = p - 1$
- For $n = p^e$, the integers between 0 and n not co-prime with n are
  - $0, p, 2 \cdot p, \ldots, (p^{e-1} - 1) \cdot p$
  - There are p^{e-1} of them.
  - Therefore, $\phi(p^e) = p^e - p^{e-1} = p^{e-1} \cdot (p-1)$

$\phi(n \cdot m) = \phi(n) \cdot \phi(m)$

- Consider the map:

$$\begin{array}{rcl} f : \mathbb{Z}_{nm} & \rightarrow & \mathbb{Z}_n \times \mathbb{Z}_m \\ a & \rightarrow & (a \bmod n, a \bmod m) \end{array}$$

  - From the CRT, the map is a bijection.
  - Moreover, $\gcd(a, n \cdot m) = 1$ if and only if $\gcd(a, n) = 1$ and $\gcd(a, m) = 1$.
  - Therefore, $|\mathbb{Z}^*_{nm}| = |\mathbb{Z}^*_n| \cdot |\mathbb{Z}^*_m|$
  - This implies $\phi(n \cdot m) = \phi(n) \cdot \phi(m)$.

Theorem

- If $n = p_1^{e_1} \ldots p_r^{e_r}$ is the factorization of n into primes, then :

$$\phi(n) = \prod_{i=1}^{r} p_i^{e_i - 1} \cdot (p_i - 1) = n \prod_{i=1}^{r} (1 - 1/p_i)$$

  - Proof: immediate consequence of the previous properties.
- Example
  - $\phi(45) = \phi(3^2) \cdot \phi(5) = 3 \cdot 2 \cdot 4 = 24$

Euler's theorem

- Theorem
  - For any integer $n > 1$ and any integer a such that $\gcd(a, n) = 1$, we have $a^{\phi(n)} \equiv 1 \mod n$.
- Proof
  - Consider the map $f : \mathbb{Z}_n^* \to \mathbb{Z}_n^*$, with $f(b) = a \cdot b$
  - f is a permutation, therefore :

$$\prod_{b \in \mathbb{Z}_n^*} b = \prod_{b \in \mathbb{Z}_n^*} f(b) = \prod_{b \in \mathbb{Z}_n^*} (a \cdot b) = a^{\phi(n)} \cdot \left(\prod_{b \in \mathbb{Z}_n^*} b \right)$$

  - Therefore $a^{\phi(n)} \equiv 1 \pmod{n}$.

Fermat's little theorem

- Theorem
  - For any prime p and any integer $a \not\equiv 0 \pmod{p}$, we have $a^{p-1} \equiv 1 \pmod{p}$. Moreover, for any integer a, we have $a^p \equiv a \pmod{p}$.
  - Proof: follows from Euler's theorem and $\phi(p) = p - 1$.

Multiplicative order

- The multiplicative order of an integer a modulo n is defined as the smallest integer $k > 0$ such that

$$a^k \equiv 1 \pmod{n}$$

  - Lagrange theorem: we must have $k | \phi(n)$
  - $a \in \mathbb{Z}$ a primitive root modulo n if $k = \phi(n)$
- Example

i	1	2	3	4
$1^i \bmod 5$	1	1	1	1
$2^i \bmod 5$	2	4	3	1
$3^i \bmod 5$	3	4	2	1
$4^i \bmod 5$	4	1	4	1

  - 1 has order 1, 4 has order 2.
  - 2 and 3 have order 4 (primitive roots)

The set $\mathbb{Z}_p^*$ for prime p

- $\mathbb{Z}_p^*$ is a cyclic group
    - There exists $g \in \mathbb{Z}_p^*$ such that

$$\mathbb{Z}_p^* = \{1, g, g^2, \ldots, g^{p-2}\}$$

    - Such a g is called a generator of $\mathbb{Z}_p^*$ (primitive root).
- Example
    - In $\mathbb{Z}_5^*$, $\langle 2 \rangle = \{1, 2, 2^2, 2^3\} = \{1, 2, 4, 3\} = \mathbb{Z}_5^*$
    - But in $\mathbb{Z}_5^*$, $\langle 4 \rangle = \{1, 4\} \neq \mathbb{Z}_5^*$ so 4 is not a generator of $\mathbb{Z}_5^*$.

Quadratic residues

- A quadratic residue modulo n is the square of an integer modulo n

$$\mathrm{QR}_n = \{\, y \,:\, \gcd(y,n) = 1 \wedge \exists x,\ y = x^2 \pmod{n} \,\}$$
$$\mathrm{NQR}_n = \{\, y \,:\, \gcd(y,n) = 1 \wedge \forall x,\ y \neq x^2 \pmod{n} \,\}$$

- Example

$$\mathrm{QR}_{13} = \{1, 3, 4, 9, 10, 12\}$$
$$\mathrm{NQR}_{13} = \{2, 5, 6, 7, 8, 11\}$$

  - because $\{1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2, 10^2, 11^2, 12^2\} \equiv \{1, 3, 4, 9, 10, 12\} \pmod{13}$
- Theorem: let p be a prime number, then $\#\mathrm{QR}_p = \#\mathrm{NQR}_p = (p-1)/2$

Legendre symbol

- For a prime number p, we define the Legendre symbol as

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \in \mathrm{QR}_p \\ -1 & \text{if } a \in \mathrm{NQR}_p \\ 0 & \text{if } p|a \end{cases}$$

- For a prime p number

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$$

  - The Legendre symbol can be efficiently computed

- Let $g \in \mathbb{Z}_p^*$ be a generator of $\mathbb{Z}_p^*$. Let $x = g^r$ for some $r \in \mathbb{Z}$.

$$x \in \mathrm{QR}_p \Leftrightarrow r \text{ is even}$$

  - The Legendre symbol reveals the parity of r.

The Jacobi symbol

- For any integer $n = p_1 \cdot p_2 \cdots p_k$, we define the Jacobi symbol as

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \cdot \left(\frac{a}{p_2}\right) \cdots \left(\frac{a}{p_k}\right)$$

- For m, n odd, positive integers, and for $a, b \in \mathbb{Z}$. From the definition

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right) \quad \left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$$

$$\left(\frac{a}{n}\right) = \left(\frac{a \bmod n}{n}\right)$$

- Other properties

$$\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2} \quad \left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$$

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{(m-1)(n-1)/4}$$

Computing the Jacobi symbol

Algorithm 1 Jacobi(a, n)

```
If $a \leq 1$ then **return** $a$
**if** $a$ is odd **then**                          $\triangleright \left(\frac{a}{n}\right)\left(\frac{n}{a}\right) = (-1)^{(a-1)(n-1)/4}$
    If $a \equiv n \equiv 3 \pmod 4$
        then **return** $-$Jacobi$(n \bmod a, a)$
        else **return** Jacobi$(n \bmod a, a)$
**end if**
**if** $a$ is even **then**                         $\triangleright \left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$
    If $n = \pm 1 \pmod 8$
        then **return** Jacobi$(a/2, n)$
        else **return** $-$Jacobi$(a/2, n)$
**end if**
```

- Example

$$\left(\frac{37}{47}\right) = \left(\frac{10}{37}\right) = -\left(\frac{5}{37}\right) = -\left(\frac{2}{5}\right) = \left(\frac{1}{5}\right) = 1$$

Computing modular square roots

- For a prime number $p \equiv 3 \pmod 4$ and $\alpha \in \mathrm{QR}_p$, we have that a square-root of α can be computed as:

$$\beta = \alpha^{(p+1)/4} \pmod p$$

  - If β is the square root of α then $-\beta$ is also a square root of α modulo p.

- Proof: since $\alpha \in \mathrm{QR}_p$, there exists $\tilde{\beta}$ such that $\tilde{\beta}^2 = \alpha$

$$\beta^2 = \alpha^{(p+1)/2} = \tilde{\beta}^{p+1} = \tilde{\beta}^{p-1} \cdot \tilde{\beta}^2 = \tilde{\beta}^2 = \alpha$$

Solving quadratic equations in $\mathbb{Z}_p$

$$a \cdot x^2 + b \cdot x + c = 0 \pmod{p}$$

- If a solution exists it must be given by

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

- Equation has a solution in $\mathbb{Z}_p$ iff $\Delta \in \mathrm{QR}_p$ where $\Delta = b^2 - 4 \cdot a \cdot c$
  - Compute $\sqrt{\Delta}$ in $\mathbb{Z}_p$ and recover the roots x_1, x_2

Computing square roots modulo $n = pq$

- Given $n = p \cdot q$ for known primes p, q, and given $\alpha \in \mathrm{QR}_n$, we want to find β such that $\beta^2 = \alpha \pmod{n}$
- First solve modulo p and q separately

$$\begin{cases} (\beta_p)^2 & = & \alpha & \pmod{p} \\ (\beta_q)^2 & = & \alpha & \pmod{q} \end{cases}$$

- Solve the simultaneous congruence

$$\begin{cases} \beta & = & \beta_p & \pmod{p} \\ \beta & = & \beta_q & \pmod{q} \end{cases}$$

using the Chinese Reminder Theorem.