INFO-F-405: Introduction to cryptography

Introduction to modular arithmetic

Theoretical background

Euler φ function

The Euler φ function gives the number of integers between 0 and $n-1$ coprime to n. For example, $\varphi(20) = 8$ because only the 8 integers $\{1, 3, 7, 9, 11, 13, 17, 19\}$ are coprime to 20.

A direct consequence of this theorem is that for any p, a prime number, $\varphi(p) = p-1$. More generally, $\varphi(p^m) = p^m - p^{m-1} = (p-1) \cdot p^{m-1}$.

Let us also note this property of φ that if $gcd(m, n) = 1$, then $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.

As a result, it is easy to compute $\varphi(n)$ when we know the prime factors factorization of n. Indeed, if $n = p_1^{m_1} \cdot p_2^{m_2} \cdots p_v^{m_v}$, with all the p_i prime numbers, we have:

$$\varphi(n) = (p_1 - 1)p_1^{m_1-1}(p_2 - 1)p_2^{m_2-1} \cdots (p_v - 1)p_v^{m_v-1} \tag{1}$$

For example $20 = 2^2 \cdot 5$ and $\varphi(20) = (2-1) \cdot 2 \cdot (5-1) = 8$

Additive structure of multiplication

For modulus n of the form p^k, $2p^k$ where p is a prime and $k > 0$, there exists an integer g (called the generator) such that the set of powers of g, $\{g^0, g^1, g^2, \cdots, g^{\varphi(n)-1}\}$ is the set of all integers coprime to n.
For example, if $n = 10$, we have $g = 3$ and $\{1, 3, 9, 27\} \equiv \{1, 3, 7, 9\}$.

Furthermore, $g^{\varphi(n)} \equiv 1 \equiv g^0$, meaning that the exponents of g can be reduced mod $\varphi(n)$. If we multiply two integers $a = g^\alpha$ and $b = g^\beta$ mod n, their exponents add mod $\varphi(n)$: $ab = g^\alpha g^\beta = g^{(\alpha+\beta) \bmod \varphi(n)}$.
For example, modulo 10, $7 \equiv 3^3$ and $9 \equiv 3^2$, hence $7 \cdot 9 = 3^{3+2} \equiv 3^1 = 3$ because $\varphi(10) = 4$.

To compute the multiplicative inverse of an integer $a = g^\alpha$ mod n, one can simply take the additive inverse of the exponent mod $\varphi(n)$. Hence $a^{-1} \equiv g^{(-\alpha) \bmod \varphi(n)}$

Modular exponentiation

Modular exponentiation is the computation of $a^b \mod n$. Working modulo n, if we have a generator g and $a \equiv g^\alpha$, to compute a^b, one can simply compute $(g^\alpha)^b = g^{\alpha \cdot b \mod \varphi(n)}$.
In the same way a multiplication mod n is equivalent to an addition mod $\varphi(n)$ of the exponents, the modular exponentiation mod n is equivalent to a multiplication mod $\varphi(n)$ of the exponents.

Theorem(*Euler*) For all a coprime with n, it holds that:

$$a^{\varphi(n)} \equiv 1 \mod n \tag{2}$$

Multiplicative group of integers modulo n

So far, we have worked with $\mathbb{Z}_n$ with either addition or multiplication. Let us remember that a group requires four properties:

- closure
- associativity
- $\exists$ neutral (identity) element
- all elements of the group have an inverse

Working with the multiplicative group $\mathbb{Z}_8^*$ for instance, we would find that **not** all values in $\mathbb{Z}_8$ have an inverse, as shown in the below table.

	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

We deduce from this table that the elements of $\mathbb{Z}_8^*$ are $\{1, 3, 5, 7\}$ because they have an inverse. More generally, any value a in $\mathbb{Z}_n$ coprime to n is in $\mathbb{Z}_n^*$.

Group order and element order

The order of a group refers to the cardinality of the group, i.e. the number of elements. The order of an element a is the smallest positive integer m such that $a^m = n$ where n is the neutral (or identity) element.

Exercises

Exercise 1

Compute as fast as possible, without writing 78130*8012*700451*19119 mod 20.

Exercise 2

Compute by exhaustive search 23^{-1} in $\mathbb{Z}_{57}$(the answer is a single digit number). Using this result, solve $23x + 52 \equiv 5$ in $\mathbb{Z}_{57}$. Could you solve an equation of the form $19x + a \equiv b$ using the same method?

Exercise 3

Show that $n - 1$ is self inverse in $\mathbb{Z}_n$.

Exercise 4

Show that for $n = pq$, $\varphi(n) = (p - 1)(q - 1)$ for p, q two prime numbers.

Exercise 5

Compute 2^i mod 25 until cycling back to 1(it might take a while but less than 25 steps). Then:

- Deduce the value of $\varphi(25)$.
- Compute $18 * 22$ mod 25 without doing any multiplication using the previous results.
- Solve $16x \equiv 1$ mod 25.
- Compute 17^{2024} mod 25.

Ex. 6 — Asymmetric Cryptography - Euler $\varphi(n)$ Function

1. Compute the Euler $\varphi(n)$ function for all $n \in \{2, 3, 4, 5, 36\}$.

2. Give the results of $2^{32} \bmod 31$, $3^{16} \bmod 32$ and $8^{14} \bmod 25$ without performing the actual exponentiations but by using only the Euler Theorem.

Ex. 7 — Cyclic Groups and Generators
Working with the multiplicative group $\mathbb{Z}_p^*$ for $p = 19$ ...

1. List all the elements of $\mathbb{Z}_{19}^*$ and determine the order of the group.
2. Determine the order $\mathtt{ord}(a)$ of each element $a \in \mathbb{Z}_{19}^*$. Use the following two facts to simplify the amount of calculations:

   Fact (1) If $a \in \mathbb{Z}_p^*$ then $\mathtt{ord}(a)$ divides the order of $\mathbb{Z}_p^*$.

   Fact (2) $\mathtt{ord}(a^k)$ is equal to $\mathtt{ord}(a)/\mathtt{gcd}(\mathtt{ord}(a), k)$.

3. List all the generators of $\mathbb{Z}_{19}^*$.