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.

Answer of exercise 1

Working modulo 20, we can ignore multiples of 100 and hence keep only the two last digits of each numbers. We see that $78130 \equiv 30 \equiv 10$ and $8012 \equiv 12$. Since $12 \cdot 10$ is an obvious multiple of 20, the whole product is 0.

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?

Answer of exercise 2

- $23 \cdot 5 = 115 \equiv 1 \mod 57$.
- $x \equiv (5 - 52) \cdot 23^{-1} \equiv 50$
- No because 19 is not invertible as $57 = 19 \cdot 3$ (not coprime)

Exercise 3

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

Answer of exercise 3

$(n-1)^2 = n^2 - 2n + 1 \equiv 1 \mod n$

Exercise 4

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

Answer of exercise 4

Let S_1 be the multiples of p less than pq and let S_2 be the multiples of q less than pq. Total number of coprimes $\varphi(pq) = pq - 1 - |S_1| - |S_2|$ since only multiples of p or q can divide pq. Since $|S_1| = q - 1$ and $|S_2| = p - 1$, we have $\varphi(pq) = pq - 1 - q + 1 - p + 1 = pq - p - q + 1 = (p - 1) \cdot (q - 1)$

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.

Answer of exercise 5

```
0 -> 1        11 -> 23
1 -> 2        12 -> 21
2 -> 4        13 -> 17
3 -> 8        14 -> 9
4 -> 16       15 -> 18
5 -> 7        16 -> 11
6 -> 14       17 -> 22
7 -> 3        18 -> 19
8 -> 6        19 -> 13
9 -> 12       20 -> 1
10 -> 24
```

- $\varphi(25) = 20$
- $18 \cdot 22 = 2^{15} \cdot 2^{17} = 2^{32} \equiv 2^{12} \equiv 21$ (remember we compute the exponent mod $\varphi(25) = 20$)
- $x \equiv 16^{-1}$
  $\Leftrightarrow x \equiv 2^{4^{-1}} \equiv 2^{-4}$
  $\Leftrightarrow x \equiv 2^{-4} \cdot 1 \equiv 2^{-4} \cdot 2^{20} \equiv 2^{16} \equiv 11$

- $17^{2024} \equiv 17^4 \equiv 2^{13 \cdot 4} \equiv 2^{52} \equiv 2^{12} \equiv 21$

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

Answer of exercise 6

1.
   - $\varphi(2) = 2^1 - 2^0 = 2 - 1 = 1$
   - $\varphi(3) = 3^1 - 3^0 = 3 - 1 = 2$
   - $\varphi(4) = \varphi(2^2) = 2^1 - 2^1 = 4 - 2 = 2$
   - $\varphi(5) = 5^1 - 5^0 = 5 - 1 = 4$
   - $\varphi(36) = \varphi(2^2 3^2) = \varphi(2^2) \cdot \varphi(3^2) = (2^2 - 2^1) \cdot (3^2 - 3^1) = 2 \cdot 6 = 12$

2.
   - According to Euler Theorem we have $2^{30} = 2^{\varphi(31)} = 1 \mod 31$.
     Therefore, we can compute $2^{32} \mod 31 = 2^2 \cdot 2^{30} \mod 31 = 4 \cdot 1 \mod 31 = 4 \mod 31$.
     We conclude that $2^{30} \equiv 4 \pmod{31}$.
   - Similarly, according to Euler Theorem we have $3^{16} = 3^{\varphi(2^5)} = 3^{\varphi(32)} = 1 \mod 32$.
     Therefore, $3^{16} \equiv 1 \pmod{32}$.
   - Since 8 and 25 are coprime, we can apply Euler's theorem. Let us first compute $\varphi(25)$. $\varphi(25) = \varphi(5^2) = 5^2 - 5^1 = 20$
     Because the exponent is lower than $\varphi(25)$, it is difficult to actually compute anything. However, we can still lower the exponent base to increase the exponent to a value greater than $\varphi(25)$: $8^{14} = (2^3)^{14} = 2^{42}$.
     We can now apply Euler's theorem: $2^{42} = 2^{20} \cdot 2^{20} \cdot 2^2 \equiv 1 \cdot 1 \cdot 2^2 \mod 25 \equiv 4 \mod 25$.

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 $\mathbb{Z}_{19}^*$.

Answer of exercise 7

1. Since p is prime, the order of the group $\mathbb{Z}_p^* = p - 1 = 19 - 1 = 18$. The elements of $|\mathbb{Z}_{19}^*|$ are $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18\}$.

2. Recall that the order of an element $a \in \mathbb{Z}_p^*$ is the smallest number i such that $a^i \mod p = 1$ where $1 \leq i \leq |\mathbb{Z}_p^*|$.

   Obviously, the order $\mathtt{ord}(1) = 1$.

   For any other value $a \neq 1$, we need to explore a wider range of possibilities. From Fact (1), we know that i divides $\mathtt{ord(}\mathbb{Z}_{19}^*\mathtt{)} = 18$. As a result, the candidates for i are $\{1, 2, 3, 6, 9, 18\}$.

   Using Fact (2) we know that computing $\mathtt{ord}(2)$ will enable us to easily calculate $\mathtt{ord}(4)$, $\mathtt{ord}(8)$ and $\mathtt{ord}(16)$. Similarly, computing $\mathtt{ord}(3)$ will enable us to easily calculate $\mathtt{ord}(9)$.

   Finally, let us not forget that we from Euler's theorem, $a^{18} \equiv 1 \mod 19$ since $\varphi(19) = 18$.

   To sum up, what we need to do is to compute the order for the elements $a \in \{2, 3, 5, 6, 7, 10, 11, 12, 13, 14, 15, 17\}$ by finding the smallest integer $i \in \{2, 3, 6, 9\}$ such that

   $$a^i \mod 19 = 1.$$

   If such integer i doesn't exist then the order of a equals automatically to 18 (which is the order of the group $\mathbb{Z}_{19}^*$) from Euler's theorem.

   For 2:

   - $2^2 = 4$
   - $2^3 = 8$
   - $2^6 = 64 \equiv 7 \mod 19$
   - $2^9 = 2^3 \cdot 2^6 = 8 \cdot 7 = 56 \equiv 18 \mod 19$
   - Since none of the values worked, we deduce from Euler's theorem that $2^{18} \equiv 1 \mod 19$ and that $\mathtt{ord(2)} = 18$.

   This enables us to compute 4, 8 and 16 easily:

   - $4 = 2^2 \Leftrightarrow 2^{18} = (2^2)^9 \Rightarrow \mathtt{ord}(4) = 9$
   - $8 = 2^3 \Leftrightarrow 2^{18} = (2^3)^6 \Rightarrow \mathtt{ord}(8) = 6$

- $16 = 2^4$. From Fact (2) we know that $\mathtt{ord}(2^4) = \frac{18}{\mathtt{gcd}(\mathtt{ord}(2),4)} = \frac{18}{\mathtt{gcd}(18,4)} = \frac{18}{2} = 9$:

The complete list of $\mathtt{ord}(a)$ can be found in the below table.

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\mathtt{ord}(a)$	1	18	18	9	9	9	3	6	9	18	3	6	18	18	18	9	9	2

3. Since $\mathbb{Z}_{19}^*$ is a cyclic group (because 19 is a prime) the number of generators can be determined by computing $|\mathbb{Z}_{\varphi(p)}^*|$. Hence we need to calculate $|\mathbb{Z}_{\varphi(19)}^*| = |\mathbb{Z}_{18}^*|$. Applying Euler phi function this results in $|\mathbb{Z}_{18}^*| = \varphi(18) = 6$.