MATH 433

Applied Algebra

Lecture 6:
Euler's totient function.
Public key systems.

Finite multiplicative order

$\mathbb{Z}_n$: the set of all congruence classes modulo n.
G_n: the set of all invertible congruence classes modulo n.

Theorem A nonzero congruence class $[a]_n$ is invertible if and only if $\gcd(a, n) = 1$.

A congruence class $[a]_n$ has **finite order** if $[a]_n^k = [1]_n$ for some integer $k \geq 1$. The smallest k with this property is called the **order of** $[a]_n$. We also say that k is the **order of** a **modulo** n.

Theorem A congruence class $[a]_n$ has finite order if and only if it is invertible.

Proposition Let k be the order of an integer a modulo n. Then $a^s \equiv 1 \bmod n$ if and only if s is a multiple of k.

Proof: If $s = kt$, where $t \in \mathbb{Z}$, then

$$[a]_n^s = ([a]_n^k)^t = [1]_n^t = [1]_n.$$

Conversely, let $[a]_n^s = [1]_n$. We have $s = kq + r$, where q is the quotient and r is the remainder of s by k. Then

$$[a]^r = [a]^{s-kq} = [a]^s([a]^k)^{-q} = [1].$$

Since $0 \leq r < k$, it follows that $r = 0$.

Fermat's Little Theorem Let p be a prime number. Then $a^{p-1} \equiv 1 \bmod p$ for every integer a not divisible by p.

Euler's Theorem Let $n \geq 2$ and $\phi(n)$ be the number of elements in G_n. Then $a^{\phi(n)} \equiv 1 \bmod n$ for every integer a coprime with n.

Corollary Let a be an integer coprime with an integer $n \geq 2$. Then the order of a modulo n is a divisor of $\phi(n)$.

Euler's totient function

The number of elements in G_n, the set of invertible congruence classes modulo n, is denoted $\phi(n)$. In other words, $\phi(n)$ counts how many of the numbers $1, 2, \ldots, n$ are coprime with n.

$\phi(n)$ is called **Euler's ϕ-function** or **Euler's totient function**.

Proposition 1 If p is prime, then $\phi(p^s) = p^s - p^{s-1}$.

Proposition 2 If $\gcd(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.

Theorem Let $n = p_1^{s_1} p_2^{s_2} \ldots p_k^{s_k}$, where $p_1, p_2, \ldots, p_k$ are distinct primes and $s_1, \ldots, s_k$ are positive integers. Then

$$\phi(n) = p_1^{s_1-1}(p_1 - 1)p_2^{s_2-1}(p_2 - 1) \ldots p_k^{s_k-1}(p_k - 1).$$

Sketch of the proof: The proof is by induction on k. The basis of induction is Proposition 1. The induction step relies on Proposition 2.

Proposition If $\gcd(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.

Proof: Let $\mathbb{Z}_m \times \mathbb{Z}_n$ denote the set of all pairs (X, Y) such that $X \in \mathbb{Z}_m$ and $Y \in \mathbb{Z}_n$. We define a function $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ by the formula $f([a]_{mn}) = ([a]_n, [a]_m)$. Since m and n divide mn, this function is well defined (does not depend on the choice of the representative a). Since $\gcd(m, n) = 1$, the Chinese remainder theorem implies that this function establishes a one-to-one correspondence between the sets $\mathbb{Z}_{mn}$ and $\mathbb{Z}_m \times \mathbb{Z}_n$.

Furthermore, an integer a is coprime with mn if and only if it is coprime with m and with n. Therefore the function f also establishes a one-to-one correspondence between G_{mn} and $G_m \times G_n$, the latter being the set of pairs (X, Y) such that $X \in G_m$ and $Y \in G_n$. It follows that the sets G_{mn} and $G_m \times G_n$ consist of the same number of elements. Thus $\phi(mn) = \phi(m)\phi(n)$.

Examples. $\phi(11) = 10$,
$\phi(25) = \phi(5^2) = 5 \cdot 4 = 20$,
$\phi(27) = \phi(3^3) = 3^2 \cdot 2 = 18$,
$\phi(100) = \phi(2^2 \cdot 5^2) = \phi(2^2)\phi(5^2) = 2 \cdot 20 = 40$,
$\phi(1001) = \phi(7 \cdot 11 \cdot 13) = \phi(7)\phi(11)\phi(13)$
$= 6 \cdot 10 \cdot 12 = 720$.

Problem. Determine the last two digits of 7^{404}.

The last two digits are the remainder under division by 100. Since $\phi(100) = 40$, we have

$$7^{40} \equiv 1 \bmod 100.$$

Then $[7^{404}] = [7]^{404} = [7]^{40 \cdot 10 + 4} = ([7]^{40})^{10} [7]^4$
$= [7]^4 = [343][7] = [43][7] = [301] = [1]$.
Hence the last two digits are 01.

Public key encryption

Suppose that Alice wants to obtain some confidential information from Bob, but they can only communicate via a public channel (meaning all that is sent may become available to third parties). How to organize secure transfer of data in these circumstances?

The **public key encryption** is a solution to this problem.

Public key encryption

The first step is **coding**. Bob digitizes the message and breaks it into blocks $b_1, b_2, \ldots, b_k$ so that each block can be encoded by an element of a set $X = \{1, \ldots, K\}$, where K is large. This results in a **plaintext**. Coding and decoding are standard procedures known to public.

Next step is **encryption**. Alice sends a **public key**, which is an invertible function $f : X \to Y$, where Y is an equally large set. Bob uses this function to produce an encrypted message (**ciphertext**): $f(b_1), f(b_2), \ldots, f(b_k)$. The ciphertext is then sent to Alice.

The remaining steps are **decryption** and **decoding**. To decrypt the encrypted message (and restore the plaintext), Alice applies the inverse function f^{-1} to each block. Finally, the plaintext is decoded to obtain the original message.

Trapdoor function

For a successful encryption, the function f has to be the so-called **trapdoor function**, which means that f is easy to compute while f^{-1} is hard to compute unless one knows special information ("trapdoor").

The usual approach is to have a family of fuctions $f_\alpha : X_\alpha \to X_\alpha$ (where $X \subset X_\alpha$) depending on a parameter α (or several parameters). For any function in the family, the inverse also belongs to the family. The parameter α is the trapdoor.

An additional step in exchange of information is **key generation**. Alice generates a pair of **keys**, i.e., parameter values, α and β such that the function f_β is the inverse of f_α.
α is the **public key**, it is communicated to Bob (and anyone else who wishes to send encrypted information to Alice).
β is the **private key**, only Alice knows it.

The encryption system is efficient if it is virtually impossible to find β when one only knows α.

RSA system

The **RSA (Rivest-Shamir-Adleman)** system is a public key system based on the modular arithmetic.

$X = \{1, 2, \ldots, K\}$, where K is a large number (say, 2^{128}).

The **key** is a pair of integers (n, α), **base** and **exponent**. The domain of the function $f_{n,\alpha}$ is G_n, the set of invertible congruence classes modulo n, regarded as a subset of $\{0, 1, 2, \ldots, n-1\}$. We need to pick n so that the numbers $1, 2, \ldots, K$ are all coprime with n.

The function is given by $f_{n,\alpha}(a) = a^\alpha \bmod n$.

Key generation: First we pick two distinct primes p and q greater than K and let $n = pq$. Secondly, we pick an integer α coprime with $\phi(n) = (p-1)(q-1)$. Thirdly, we compute β, the inverse of α modulo $\phi(n)$.

Now the public key is (n, α) while the private key is (n, β).

By construction, $\alpha\beta = 1 + \phi(n)k$, $k \in \mathbb{Z}$. Then

$$f_{n,\beta}(f_{n,\alpha}(a)) = [a]_n^{\alpha\beta} = [a]_n([a]_n^{\phi(n)})^k,$$

which equals $[a]_n$ by Euler's theorem. Thus $f_{n,\beta} = f_{n,\alpha}^{-1}$.

Efficiency of the RSA system is based on impossibility of efficient prime factorisation (at present time).

Example. Let us take $p = 5$, $q = 23$ so that the base is $n = pq = 115$. Then $\phi(n) = (p-1)(q-1) = 4 \cdot 22 = 88$.

Exponent for the public key: $\alpha = 29$. It is easy to observe that -3 is the inverse of 29 modulo 88:

$$(-3) \cdot 29 = -87 \equiv 1 \mod 88.$$

However the exponent is to be positive, so we take $\beta = 85$ $(\equiv -3 \mod 88)$.

Public key: $(115, 29)$, private key: $(115, 85)$.

Example of plaintext: 6/8 (two blocks).

Ciphertext: 26 ($\equiv 6^{29} \mod 115$), 58 ($\equiv 8^{29} \mod 115$).