MATH 415

Modern Algebra I

Lecture 26: Modular arithmetic (continued). RSA encryption.

Theorem The linear congruence $ax \equiv b \mod n$ has a solution if and only if $d = \gcd(a, n)$ divides b. If this is the case then the solution set consists of d congruence classes modulo n that form a single congruence class modulo n/d.

Proof: If the congruence has a solution x, then $ax = b + kn$ for some $k \in \mathbb{Z}$. Hence $b = ax - kn$, which is divisible by $\gcd(a, n)$.

Conversely, assume that d divides b. Then the linear congruence is equivalent to $a'x \equiv b' \mod m$, where $a' = a/d$, $b' = b/d$ and $m = n/d$. In other words, $[a']_m X = [b']_m$, where $X = [x]_m$.

We have $\gcd(a', m) = \gcd(a/d, n/d) = \gcd(a, n)/d = 1$. Hence the congruence class $[a']_m$ is invertible. It follows that all solutions x of the linear congruence form a single congruence class modulo m, $X = [a']_m^{-1}[b']_m$. This congruence class splits into d distinct congruence classes modulo $n = md$.

Corollaries of Lagrange's Theorem

Fermat's Little Theorem If p is a prime number then $a^{p-1} \equiv 1 \bmod p$ for any integer a that is not a multiple of p.

Proof: If a is not a multiple of p then $[a]_p$ is in G_p, the multiplicative group of invertible congruence classes modulo p. Lagrange's Theorem implies that the order of $[a]_p$ in G_p divides $|G_p| = p - 1$. It follows that $[a]_p^{p-1} = [1]_p$, which means that $a^{p-1} \equiv 1 \bmod p$.

Euler's Theorem If n is a positive integer and $\phi(n)$ is the number of integers between 1 and n coprime with n, then $a^{\phi(n)} \equiv 1 \bmod n$ for any integer a coprime with n.

Proof: $a^{\phi(n)} \equiv 1 \bmod n$ means that $[a]_n^{\phi(n)} = [1]_n$. The number a is coprime with n, i.e., $\gcd(a, n) = 1$, implies that the congruence class $[a]_n$ is in G_n. It remains to notice that $|G_n| = \phi(n)$ and apply Lagrange's Theorem.

Problem. Determine the last two digits of 3^{2021}.

The last two digits form the remainder under division by 100.

First let us compute $\phi(100)$. Since $100 = 2^2 \cdot 5^2$, an integer k is coprime with 100 if and only if it is not divisible by 2 or 5. Among integers from 1 to 100, there are $50 = 100/2$ even numbers and $20 = 100/5$ numbers divisible by 5. Note that some of them are divisible by both 2 and 5. These are exactly numbers divisible by 10. There are $10 = 100/10$ such numbers. We conclude that $\phi(100) = 100 - 50 - 20 + 10 = 40$.

By Euler's Theorem, $3^{40} \equiv 1 \bmod 100$. Then

$$
\begin{aligned}
[3^{2021}] &= [3]^{2021} = [3]^{40\cdot 50+21} = ([3]^{40})^{50}\,[3]^{21} = [3]^{21} \\
&= ([3]^5)^4\,[3] = [243]^4\,[3] = [43]^4\,[3] = [(50-7)^2]^2\,[3] \\
&= [7^2]^2\,[3] = [49]^2\,[3] = [(50-1)^2]\,[3] = [1^2]\,[3] = [3].
\end{aligned}
$$

Thus $3^{2021} = \ldots 03$.

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, in particular, to Eve). 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.

$X = \{1, 2, \dots, K\}$, 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 $\{0, 1, 2, \dots, n-1\}$. We need to pick n so that the numbers $1, 2, \dots, K$ 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:

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

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

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

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

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