Number Theory & Cryptography

- Divisibility and Congruence
- Modular Arithmetic and its Applications
- GCD, (Extended) Euclidean Algorithm, Relative Prime
- The Caesar Cipher and Affine Cipher, Modular Inverse
- The Chinese Remainder Theorem
- Fermat's Little Theorem and Modular Exponentiation
- Private and Public Key Cryptography, The RSA Cryptosystem

Imdad ullah Khan

Modular Arithmetic Applications: Cryptography

Cryptography encoding and decoding messages

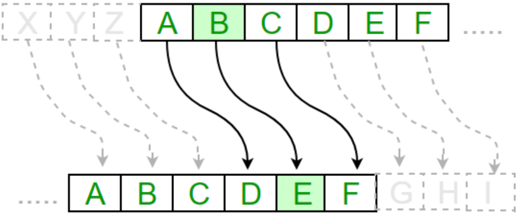
- Cipher: A method for encoding messages
- Plaintext: The original message to be encoded
- Ciphertext: The encoded message
- Encryption: The process of encoding messages
- Decryption: The process of decoding messages

The Caesar Cipher

Cryptography: encoding and decoding messages

The Caesar Cipher (Substitution): Substitute each letter of the message by the letter coming three letters after it in the alphabet

How about x, y and z?



The Caesar Cipher

Cryptography: encoding and decoding messages

The Caesar Cipher (Substitution): Substitute each letter of the message by the letter coming three letters after it in the alphabet

Replace 3 with some other integer s

Encryption

$c \leftarrow (p + s) \ \% \ 26$

Decryption

$p \leftarrow (c - s) \ \% \ 26$

Even further $\quad c \leftarrow (tp + s) \ \% \ 26 \quad$ ▷ Affine Cipher

Affine Cipher

Affine Cipher:

Encryption

$c \leftarrow (tp + s) \;\%\; 26$

Decryption

$p \leftarrow \dfrac{(c - s)}{t} \;\%\; 26$

$$tp \;=\; (c - s) \;\%\; 26 \quad\Longrightarrow\quad p \;=\; t^{-1}(c - s) \;\%\; 26$$

a^{-1} (multiplicative inverse): $a \cdot a^{-1} = 1 \;\%\; 26$

If $t = 3$, then $3 \cdot 9 = 27 \;\%\; 26 = 1$ $\quad \triangleright \; 9 = 3^{-1}$

If $t = 5$, then $5 \cdot 21 = 105 \;\%\; 26 = 1$ $\quad \triangleright \; 21 = 5^{-1}$

Not every integer has an inverse

What is inverse of 4 modulo 26?

Modular Inverse

Definition

b is the inverse of a modulo m iff $a \cdot b \equiv_m 1$

For real numbers, every $x \neq 0 \in \mathbb{R}$ has an inverse

For integers, only 1 has an inverse

What if we were doing modular arithmetic?

Interesting property: integers also have inverses (at least some of them)

Modular Inverse

Definition

b is the inverse of a modulo m iff $a \cdot b \equiv_m 1$

Z_5	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Z_6	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

Modular Inverse

Definition

b is the inverse of a modulo m iff $a \cdot b \equiv_m 1$

Theorem

a has an inverse modulo m iff a and m are relatively primes

Equivalently, inverse of a modulo m exists iff $\text{GCD}(a, m) = 1$

$\text{GCD}(3, 7) = 1$ $\quad 3 \cdot 5 \,\%\, 7 = 1$

$\text{GCD}(4, 11) = 1$ $\quad 4 \cdot 3 \,\%\, 11 = 1$

$\text{GCD}(8, 9) = 1$ $\quad 8 \cdot 8 \,\%\, 9 = 1$

Modular Inverse

Theorem

a has an inverse modulo m iff $\text{GCD}(a, m) = 1$

Proof:

$\text{GCD}(a, m) = 1$

$\implies sa + tm = 1$

$\implies tm = 1 - sa \implies m \mid 1 - sa$

$\implies 1 - sa \equiv_m 0$

$\implies sa \equiv_m 1$

We can find s and t from Extended Euclidean Algorithm

Modular Arithmetic: Cancellation

If $a \equiv_m b$, then $a + c \equiv_m b + c$

If $a \equiv_m b$, then $ac \equiv_m bc$

Just as in '$=$' for real numbers

if $ac \equiv_m bc$, then IS $a \equiv_m b$?

$3 \cdot 4 \equiv_8 1 \cdot 4$ but $3 \not\equiv_8 1$

$4 \cdot 3 \equiv_9 1 \cdot 3$ but $4 \not\equiv_9 1$

$2 \cdot 4 \equiv_{12} 5 \cdot 4$ but $2 \not\equiv_{12} 5$

We cannot cancel two "equal" values on both side of a congruence

Modular Arithmetic: Cancellation

Lemma

Let $\operatorname{GCD}(a, m) = 1$*. If* $ab \equiv_m ac$*, then* $b \equiv_m c$

$\operatorname{GCD}(a, m) = 1 \implies \exists\, a^{-1} : aa^{-1} \equiv_m 1$

$ab \equiv_m ac$

$\implies aba^{-1} \equiv_m aca^{-1}$

$\implies b \equiv_m c$

Typically modulus is a prime $\implies$ an inverse exists for every integer.

Modulo a prime, integers behave "like" real numbers

Solving Congruence

Finding $a^{-1} \% m$ is solving the congruence $ax \equiv_m 1$

How about solving other congruences!

Solve $2x \equiv_7 3$

$\mathrm{GCD}(2,7) = 1$ and $2 \cdot 4 \equiv_7 1$ so 4 is 2^{-1}

$2x \equiv_7 3 \implies 2x \cdot 4 \equiv_7 3 \cdot 4$

$\implies x \equiv_7 12 \equiv_7 5$

Verify that all integers of the form $5 + 7t$ satisfy this congruence

Solving Congruence

Finding a^{-1} % m is solving the congruence $\quad ax \equiv_m 1$

How about solving other congruences!

Solve $3x \equiv_6 2$

Going through all numbers % 6, no x satisfy this congruence

We say

$$3x \equiv_6 2 \quad \text{has no solutions}$$