# Crypto Maths

San Kho Lin

## 1 Divisibility

An integer $a$ is said to be divisible by a positive integer $b$ and this is written as $b|a$ (i.e. $b$ divides $a$), if $a = bc$ for a third integer $c$ and $c \neq 0$.

1. $a|a$
2. $a|1$ then $a = \pm b$
3. $a|b$ and $b|c$ then $a|c$
4. $a|b$ and $b|a$ then $a = \pm b$
5. $a|b$ and $a|c$ then $a|(bx + cy)$ for some integers $x, y$
6. $a|b$ then $ca|cb$ for any $c$

**Proof (5)**: $a|b$ and $a|c$ then $a|(bx + cy)$ for some integers $x, y$

- Since $a|b$ we have $b = ma$ for some integer m.
- Similarly, $a|c$ we have $c = na$ for some integer n.
- Now consider, $bx + cy = ma.x + na.y = a(mx + ny)$
- Therefore, $a|(bx + cy)$

### 1.1 Division Algorithm

$a = qn + r$ whereas $0 \leq r < n$ and $q = \lfloor a/n \rfloor$

- a = dividend
- n = divisor (modulus)
- q = quotient
- r = remainder (simplest remainder is known as *residue*)

# 2 Prime

## 2.1 Relatively Prime and Co-prime

***Relatively Prime*** *and* ***Co-Prime*** *are the same..* [1]

Two numbers are relatively prime if they have no prime factors in common; that is, their only common divisor is 1. This is equivalent to saying that two numbers are relatively prime if their $\gcd(a, b) = 1$.
finite field set
prime twin-prime co-prime semi-prime
composite numbers

# 3 Euclidean Algorithm

*Euclidean Algorithm* find **Greatest Common Divisor** (GCD) of two positive integers. The greatest common divisor of $a$ and $b$ is the largest integer that divides both $a$ and $b$.

- $gcd(a, b) = max[k]$, such that $k|a$ and $k|b$
- $gcd(0, 0) = 0$
- $gcd(a, 0) = a$
- If $gcd(a, b) = 1$, then $a$ and $b$ are relatively prime

Assume $a \geq b > 0$. Find $gcd(a, b)$ by applying *Division Algorithm* iteratively deducing such that:

$$\begin{aligned}
a &= q_1 b + r_1 \\
b &= q_2 r_1 + r_2 \\
r_1 &= q_3 r_2 + r_3 \\
&. \\
&. \\
r_{n-2} &= q_n r_{n-1} + r_n \\
r_{n-1} &= q_{n+1} r_n + 0
\end{aligned}$$

Therefore, $d = gcd(a, b) = r_n$.
$d = gcd(r_i, r_{i+1})$
$r_{i-2} = q_i r_{i-1} + r_i$

```
Euclid(a,b);
X:=a; y:=b;
while y > 0 do {
  r = x mod y;
  x:=y;
  y:=r; }
return(x);
```

[1] https://en.wikipedia.org/wiki/Coprime_integers

## 3.1 Extended Euclidean Algorithm

XGCD

# 4 Modular Arithmetic

From *Division Algorithm*, we can rewrite $a = \lfloor a/n \rfloor \times n + (a \mod n)$. Therefore, we can rewrite remainder as $r = a \mod n$. We call $r$ is the remainder modulo $n$.

## 4.1 Binary Operations

The rules for ordinary arithmetic involving addition, subtraction, and multiplication carry over into modular arithmetic.

- $[(a \mod n) + (b \mod n)] \mod n = (a + b) \mod n$
- $[(a \mod n) - (b \mod n)] \mod n = (a - b) \mod n$
- $[(a \mod n) \times (b \mod n)] \mod n = (a \times b) \mod n$

**Exponentiation** is performed by repeated multiplication, as in ordinary arithmetic. Technique known as **Repeated Squaring and Multiplying Algorithm**, but work for smaller exponent.
Recall:

$$(x^a)^2 = x^{2a}$$
$$x^{a+b} = x^a x^b$$

## 4.2 Congruence

*...Two numbers are congruent if they are equal to the same thing in mod something...*

Two integers $a$ and $b$ are said to be congruent modulo $n$, if $(a \mod n) = (b \mod n)$ and, can be written as $a \equiv b \pmod{n}$.

1. $a \equiv b \pmod{n}$ if $n|(a - b)$
2. $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$
3. $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ imply $a \equiv c \pmod{n}$

If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ for some integers $a, b, c, d, n$

1. $a \pm c \equiv b \pm d \pmod{n}$ – remainder of sum = sum of remainder
2. $ma \equiv mb \pmod{n}$ – remainder of multiple = multiple of remainder
3. $ac \equiv bd \pmod{n}$ – remainder of product = product of remainder

Note on expression:

- express as **binary operator** that produces a remainder: $a \mod n$

- express as **congruence relation** that shows the equivalence of two integers: $a \equiv b \pmod{n}$

Notation:

$$5 \equiv 3 \pmod{3}$$
$$5 \mod 3 = 2 \mod 3$$

### 4.3 Inverse

**Additive Inverse** = Subtraction
$a - b = a + (-b)$ because $b + (-b) = 0$
$(-b)$ in modulo $m$ is just $(m - b)$.

**Multiplicative Inverses** (and hence Division) are numbers such that when you multiply by multiplicative inverses you get back multiplicative identity, which is 1. We never have multiplicative inverse for 0 i.e. any number times zero will always get 0. 1 will always have multiplicative inverse i.e. $1^{-1} = 1$, but not 2 as $2^{-1} = \frac{1}{2}$ in ordinary arithmetic. But in modular arithmetic, multiplicative inverses exists sometimes... in such that inverse of $a$ exists modulo $m$ wherever $a$ and $m$ have no factor in common. We say this, in terms of *Euclidean Algorithm*:

$a^{-1} \mod m$ exists when $gcd(a, m) = 1$

In other word, the multiplicative inverse of $a \mod m$ is the integer $b$ such that $ab = 1 \mod m$, write $b = a^{-1} \mod m$.

## 5 Euler Totient Function

For $n \geq 1$, let $\phi(n)$ denote the number of integers less than $n$ but are relatively prime to $n$.

$\phi(n) =$ count the number of integers between 1 and $n$ whose gcd with $n$ is 1.

$$\phi(n) = |\{x : 1 \leq x \leq n, \gcd(x, n) = 1\}|$$

Example: $\phi(6) = 2$

$$\gcd(1, 6) = 1$$
$$\gcd(2, 6) = 2$$
$$\gcd(3, 6) = 3$$
$$\gcd(4, 6) = 2$$
$$\gcd(5, 6) = 1$$

Then, $R = \{1, 5\}$. Hence, $\phi(6) = 2$.

**Fact 1:** $\phi(p) = p - 1$ for any prime $p$.
**Fact 2:** $\phi(p) = p^a - p^{a-1} = p^{a-1}(p - 1)$ for any prime $p$ and any integer $a \geq 1$.
**Fact 3:** $\phi(pq) = (p - 1)(q - 1)$ for any pair of primes $p$ and $q$.
**Fact 4:** $\phi(ab) = \phi(a) \times \phi(b)$ if $a$ and $b$ are relatively prime numbers i.e. $\gcd(a, b) = 1$.

Notes:

- Fact 1 to 3 deal with primes.
- Fact 4 is used when any two integers are co-prime.
- And use the first form in Fact 2 which is easier to track! $2^3 - 2^2$

## 6 Fermat's Little Theorem

If [2] $p$ is prime and $a$ is a positive integer not divisible by $p$ , then

$$a^{p-1} \equiv 1 \pmod{p} \tag{1}$$

If $p$ is prime and $a$ is a positive integer, then

$$a^p \equiv a \pmod{p} \tag{2}$$

## 7 Euler's Theorem

For every $a$ and $n$ that are relatively prime (i.e. coprime), then

$$a^{\phi(n)} \equiv 1 \pmod{n} \tag{3}$$

Alternate form: when $a$ does not need to be relatively prime to $n$, then

$$a^{\phi(n)+1} \equiv a \pmod{n} \tag{4}$$

## 8 Trick

When $a$ is one less than $p$.

$$\begin{aligned} 8^{100} &\mod 9 \\ 8 \mod 9 = (-1) &\mod 9 \\ (-1)^{100} &\mod 9 \\ 1 &\mod 9 \end{aligned}$$

When $a$ power is equal to modulo $p$ then answer is just $a$. This is because Fermat's Eq (2).
$3 \equiv 3^{17} \pmod{17}$

[2] In other word: *if a and p are coprime*

Fremat's Lil' Theorem can be used only when modulo $p$ is prime. Otherwise use Euler's Theorem which is more generalized i.e. modulo $n$ does not need to be prime.

Find remainder when $999998 \times 99994$ is divided by 9. In modular group, if a number is divisible means modulo is zero. i.e. $999999 \div 9 = 111111; r = 0$

$$\begin{aligned}
&999998 \times 99994 \\
&= (999999 - 1) \times (99994 - 5) \\
&\equiv (0 - 1) \times (0 - 5) \pmod 9 \\
&\equiv 5 \pmod 9
\end{aligned}$$

## 9 Chinese Remainder Theorem

CRT

## 10 Polynomial

- poly = many, nomial = terms
- a term may have: coefficient, variable and non-negative integer exponent: $Ax^n$
- monomial: 6, which is also $6x^0$ and, $\pi b^5$, $10z^{15}$ – one term
- binomial: $1x^2 + 1$ – two terms, here 1 is known as *constant term* whereas $x^2$ is *variable term*.
- trinomial: $4x^3 + 2x^2 + 7$, $7y^2 - 3y + \pi$ – three terms
- polynomial: $10x^7 - 9x^2 + 15x^3 + 9$, can be also written as $10x^7 - 9x^2 + 15x^3 + 9x^0$
- not a polynomial: $x^{-\frac{1}{2}} + 1$, $9a^{\frac{1}{2}} - 5$ ($\frac{1}{2}$ is fraction, not integer), $9\sqrt{a} - 5$, $9a^a - 5$ (exponent $a$ is variable, not integer)
- polynomial is the sum of finite number of terms
- have a notion of **Degree** such that what is the degree of a given polynomial or what is the degree of a give term of polynomial? – Degree is the power that variable is risen to... i.e. exponent of a term. The highest degree of a give polynomial is the highest exponent of given terms in a polynomial. e.g. $10x^7 - 9x^2 + 15x^3 + 9$ degree is 7 – $7^{th}$ degree polynomial. $x^2 + 1$ is $2^{nd}$ degree binomial. $4x^3 + 2x^2 + 7$ is $3^{rd}$ degree trinomial.
- have a notion of **Standard Form** which is sorted by keeping highest to lowest exponent order and, have a notion of **Leading Term** that is, a term at first position...

# 11 Abstract Algebra

Abstract concept

## 11.1 Set

- A set is a collection of objects.
- These objects are referred to as elements of the set.

## 11.2 Group

- Set of elements : $G = \{a, b, c\}$ (OR) $a, b, c \in G$
- Group has binary operations : $+, \times$
- Closed under operation : Closure – integer times integer get another integer
- Identity $e$ in such that: $a \times e = e \times a = a$
- Identity $e$ in such that: $a + e = a$
- Inverse : $a^{-1}$ exists for all $a \in G$ such that $a \times a^{-1} = e$
- Inverse : $-a$ exists for all $a \in G$ such that $a + (-a) = e$
- Associative : $(a \times b) \times c = a \times (b \times c)$
- Commutative : group is not required to be commutative i.e. possible for $a \times b \neq b \times a$. However, if a group is commutative, it is called *Commutative Group* or **Abelian Group**. Otherwise, it is called *Non-commutative Group*.

## 11.3 Cyclic Group

- A group $G$ is **cyclic** group, if it is generated by **a single element**, $G = \langle x \rangle$.
- If $G = \langle x \rangle$ for some $x$, then we call $G$ a cyclic group.
- e.g. a cyclic group generated by $x$ with operation $\times$, then smallest subgroup of $G$ containing $x$ is: $\langle x \rangle = \{\dots, x^{-1}, 1, x, x^2, x^3, \dots\}$.
- Let $H$ be a group with operation $+$, pick $y \in H$, then group generated by $y$ = smallest subgroup of $H$ containing $y$, such that $\langle y \rangle = \{\dots, -2y, -y, 0, y, 2y, \dots\}$. If $H = \langle y \rangle$ for some $y$, then we call $H$ a cyclic group.
- Example: Group of integers $\mathbb{Z}$ under $+$, claim that $\mathbb{Z} = \langle 1 \rangle$. Then, $\langle 1 \rangle = \{\dots, -2, -1, 0, 1, 2, \dots\}$. This covers all the integers, hence, $\mathbb{Z}$ is a cyclic group. It is an example of **Infinite Cyclic Group**.
- **Finite Cyclic Group** is such that $G$ = Integers mod $n$ under addition. Then, all possible elements are $G = \{0, 1, 2, \dots, n-1\}$. Integers mod $n$ is written like this: $\mathbb{Z}/n\mathbb{Z}$.

## 11.4 Ring

## 11.5 Polynomial Ring

## 11.6 Field

*... Every Field is a Ring. But not every Ring is a Field.*

$Z_p = \{0, 1, ..., p-1\}$
set of reminders obtained by
$Z = (Z_p, +)(Z_p, *)$
0 = identity in addition
$(Zp^*, *)$ = identity in multiplication