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

Arithmetic Rules

Assume arithmetic rules for operations $+, *, -$ on the set of integers

- $a(b+c) \; = \; ab+ac$
- $ab \; = \; ba$
- $a(bc) \; = \; (ab)c$
- $a*1 \; = \; a$
- $a*0 \; = \; 0$
- $a+0 \; = \; a$
- $a-a \; = \; 0$
- $a+1 \; > \; a$

The divides operator

Definition

For $a, b \in \mathbb{Z}, a \neq 0$, we say $a \mid b$: (a divides b) if $\exists c \in \mathbb{Z} : b = ac$

- $4 \mid 12$ $\triangleright$ $12 = 4 \cdot 3$
- $3 \mid 12$ $\triangleright$ $12 = 3 \cdot 4$
- $5 \mid 0$ $\triangleright$ $0 = 5 \cdot 0$
- $3 \nmid 7$
- $1 \mid 8$ $\triangleright$ $8 = 1 \cdot 8$
- $-2 \mid 6$ $\triangleright$ $6 = -2 \cdot -3$
- $-6 \mid -12$ $\triangleright$ $-12 = -6 \cdot 2$
- $-4 \nmid 13$

- a is a factor or divisor of b
- b is a multiple of a

Divisibility Facts

1. $\forall n \; 1 \mid n$ $\quad \triangleright \; n = 1 \cdot n$
2. $\forall n \; n \mid n$ $\quad \triangleright \; n = n \cdot 1$
3. $\forall n \; n \mid 0$ $\quad \triangleright \; 0 = n \cdot 0$
4. $\forall n \; -1 \mid n$ $\quad \triangleright \; n = -1 \cdot -n$
5. $\forall n \; -n \mid n$ $\quad \triangleright \; n = -n \cdot -1$

Divisibility Facts

Theorem

For $a, b, c \in \mathbb{Z}$

1. $a \mid b \implies a \mid bc$
2. $a \mid b \wedge b \mid c \implies a \mid c$
3. $a \mid b \wedge a \mid c \implies a \mid b + c$

▷ $3 \mid 6 \implies 3 \mid 6 \cdot 2$

▷ $2 \mid 4 \wedge 4 \mid 8 \implies 2 \mid 8$

▷ $2 \mid 4 \wedge 2 \mid 8 \implies 2 \mid 8 + 4$

Corollary: $a \mid b \wedge a \mid c \implies a \mid mb + nc, \quad m, n \in \mathbb{Z}$

▷ $2 \mid 4 \wedge 2 \mid 8 \implies 2 \mid 3 \cdot 8 + 5 \cdot 4$

Divisibility Facts

Corollary: $a \mid b \wedge a \mid c \implies a \mid mb + nc, \quad m, n \in \mathbb{Z}$

Proof: Number theory proofs generally use definition and basic arithmetic

$$a \mid b \wedge a \mid c \implies \exists x, y : \quad b = ax \quad \wedge \quad c = ay$$

$$mb = m(ax) = a(mx) \implies a \mid mb$$

$$nc = n(ay) = a(ny) \implies a \mid nc$$

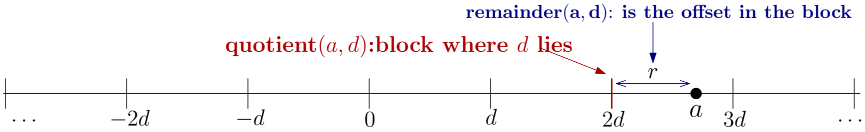
By Theorem part (2) $a \mid mb + nc$

The Division Algorithm

Theorem (The Division Algorithm)

Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \leq r < d$ such that $a = dq + r$

- q : quotient(a, d)
- r : remainder(a, d) ▷ $a \,\%\, d$
- d : divisor
- a : dividend



Clearly with a and $d > 0$, q and r are uniquely defined

Congruence

For $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, $a \equiv_m b$ iff $m \mid (a - b)$

pronounced as *a* is congruent to *b* modulo *m*

▷ Standard notation for $a \equiv_m b$ is $a \equiv b \pmod{m}$

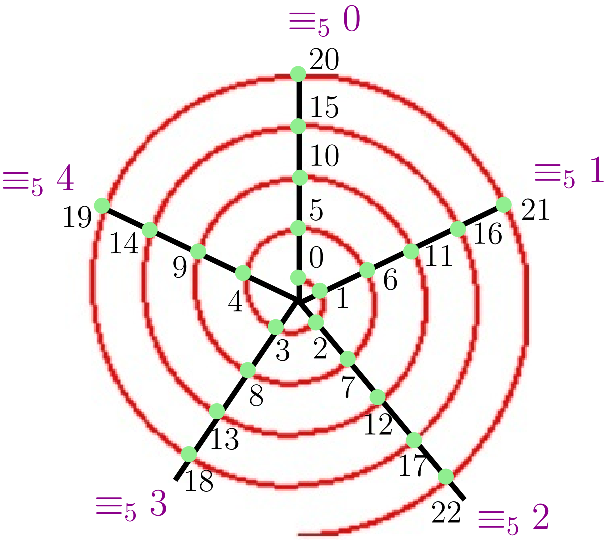
Theorem: Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$.
Then $a \equiv_m b$ iff $a \,\%\, m = b \,\%\, m$

$3 \equiv_3 6$, $3 \equiv_3 3$, $7 \equiv_5 2$ $-3 \equiv_5 2$, $-1 \equiv_3 -4$

To avoid confusion between standard notaitons - $\pmod{m}$ vs $\mathbf{mod}\ m$, we use our notation.

Note that $\%\, m$ is an operator, while $\equiv_m$ is an equivalence relation over $\mathbb{Z}$

Congruence


$\equiv_5 0$
20
15
10
5
0
$\equiv_5 1$
21
16
11
6
1
$\equiv_5 4$
19
14
9
4
$\equiv_5 3$
3
8
13
18
$\equiv_5 2$
2
7
12
17
22

Congruence Facts

Fact

1. $a \equiv_m a$
2. $a \equiv_m b \iff b \equiv_m a$
3. $a \equiv_m b \wedge b \equiv_m c \implies a \equiv_m c$

   ▷ $\equiv_m$ *is an equivalence relation on* $\mathbb{Z}$

4. $a \equiv_m (a \,\%\, m)$

Congruence

Theorem

$a \equiv_m b \iff \exists\, k \in \mathbb{Z} : a = b + km$

▷ $8 \equiv_5 3$ and $8 = 3 + 5(1)$

▷ $16 \equiv_5 1$ and $16 = 1 + 5(3)$

Proof:

$a \equiv_m b$

$\leftrightarrow m|(a - b)$ ▷ by definition

$\leftrightarrow \exists\, k \in \mathbb{Z} : a - b = km$

$\leftrightarrow a = b + km$