Number theory

Study of numbers

integers

positive integers

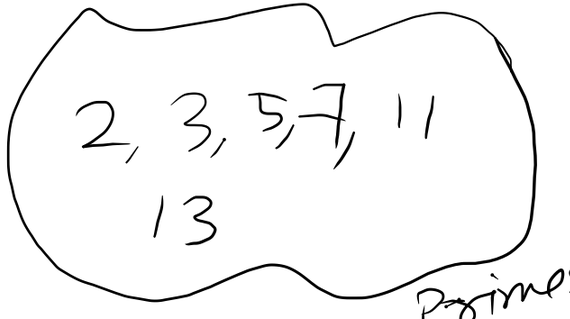
$$\mathbb{Z} = \{-\infty, \ldots, -1, 0, 1, 2, \ldots \infty\}$$

$$\mathbb{Z}^+ = \{1, 2, \ldots, \infty\}$$

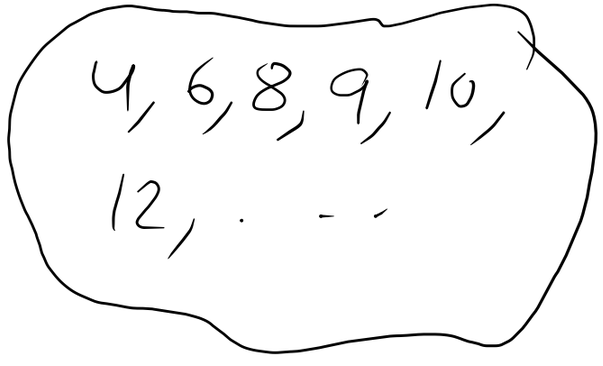
Divisibility Theory

positive integers classes.

Unit



primes



composites.

Division

Let a, b be integers with $a \neq 0$ then a divides b $(a \mid b)$ if $\exists$ an integer c such that

$$b = a \cdot c$$

$a \leftarrow$ factor / divisor

$b \leftarrow$ multiple of a.

Ex^{m} $9 \mid 27$, $7 \mid 49$.

$a \nmid b \leftarrow$ a does not divides b.

Properties: Let a, b, c be integers $a \neq 0$ then

a) if $a \mid b$ and $a \mid c$ then $a \mid (b+c)$

b) If $a \mid b$, then $a \mid bc$ for all integers c.

c) If $a \mid b$ and $b \mid c$ then $a \mid c$

d) $a \mid b$ and $a \mid c$ then

$$a \mid (mb + nc)$$ m, n are integers.

Division theorem

Let a and d be two integers with $d > 0$
then $\exists$ integers q and r such that

$$a = qd + r \quad \text{where} \quad 0 \leq r < d$$

$d \leftarrow$ divisor
$a \leftarrow$ divident
$q \leftarrow$ quotient
$r \leftarrow$ remainder

Ex^{m}

$$34 = 8 \cdot 4 + 2$$
$$a \quad q \quad d \quad r$$

congruence relation

Let a and b be integers and m be a positive integer, then a is congruent to b modulo m if $m \mid (a-b)$

notation : $a \equiv b \bmod m$.

$a \not\equiv b \bmod m$: a is not congruent to b modulo m.

$5 \equiv 1 \bmod 2$

modulo 3.

0, 3, 6, 9, 12, . . . $\equiv 0 \mod 3$

1, 4, 7, 10, 13 . . . $\equiv 1 \mod 3$

2, 5, 8, 11, 14, ... $\equiv 2 \mod 3$

Properties: Let m be a positive integer, The integers a, and b where a is b congruent modulo m iff there is an integer k such that $a = b + km$

Proof

$$a \equiv b \bmod m$$

$$\Rightarrow m \mid (a-b)$$

$$\Rightarrow a - b = m \cdot k$$

$$\Rightarrow a = b + km.$$

- Let m be a positive integer. If $a \equiv b \bmod m$ and $c \equiv d \bmod m$ then
  - $\rightarrow (a+c) \equiv b+d \bmod m$
  - $\rightarrow ac \equiv bd \bmod m$.

H.W.

- If $a \equiv b \bmod m$ then
  - $\rightarrow ca \equiv cb \bmod m$
  - $\rightarrow c+a \equiv c+b \bmod m$

where c is an integer.

– Let m be a positive integer and a, b are integers

then

$$(a+b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m.$$

$$ab \bmod m = ((a \bmod m) \cdot (b \bmod m)) \bmod m.$$

Primes: A positive integer > 1 is a prime if it is divisible by 1 and the number itself.

otherwise it is a composite.

The fundamental theorem of arithmatic

Every integer can be written as the the product of primes.

$$n = \pm p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

Where p_i's are k distinct primes and

e_i's are integers with $e_i > 0$

Greatest common divisor (gcd)

It is the positive divisor of both a and b

i.e, $gcd(a, b) = d$ means.

$d \mid a$ and $d \mid b$.

Exm $gcd(12, 33) = 3$ as $3 \mid 12$ and $3 \mid 33$

Relatively prime

Two integers a and b are relatively prime.
if gcd (a, b) = 1

Ex^m

12, 31 gcd (12, 31) = 1

8, 9 ← relatively prime.

Finding gcd

gcd (a, b)

$$a = p_1^{e_1} \cdot p_2^{e_2} \cdots p_K^{e_K} \qquad e_i \geq 0$$

$$b = p_1^{f_1} \cdot p_2^{f_2} \cdots p_K^{f_K} \qquad f_i \geq 0.$$

$$\gcd(a,b) = p_1^{\min(e_1,f_1)} \cdot p_2^{\min(e_2,f_2)} \cdots p_K^{\min(e_K,f_K)}$$

This method is not efficient.

as prime factorization is not efficient.

Least common multiple (lcm)

$lcm(a,b) = l$ means $a \mid l$ and $b \mid l$

l is the smallest integer.

Finding lcm

$$lcm(a,b) = p_1^{\max\{e_1,f_1\}} \; p_2^{\max\{e_2,f_2\}} \cdots p_x^{\max\{e_x,f_x\}}$$

Let a, b be integers, then

$$ab = gcd(a,b) \times lcm(a,b)$$

Properties of gcd

$$gcd(a,b) = gcd(b,a)$$

$$gcd(a,a) = a$$

$$gcd(a,b) = gcd(a-b,b)$$

$$gcd(a,0) = a$$

Euclid's algorithm for finding gcd

Input: two integers a, b

output: $\gcd(a, b)$

Ex^m $\gcd(138, 256)$

$\gcd(256, 138)$

```
Euclid (a, b)
while b ≠ 0
    r ← a mod b
    a ← b
    b ← r
return a
```

$\equiv a = bq + r$

$b = 138$

$\begin{cases} r \leftarrow 118 \\ a = 138 \\ b = 118 \end{cases}$

$\begin{cases} r \leftarrow 20 \\ a \leftarrow 118 \\ b \leftarrow 20 \end{cases}$

$\begin{cases} r \leftarrow 18 \\ a \leftarrow 20 \\ b \leftarrow 18 \end{cases}$

$\begin{cases} r \leftarrow 2 \\ a \leftarrow 18 \\ b \leftarrow 2 \end{cases}$

$\begin{cases} r \leftarrow 0 \\ a \leftarrow 2 \\ b \leftarrow 0 \end{cases}$

$\boxed{\gcd(256, 138) = 2}$

correctness

~~let~~ $a = bq + r$ where a, b, q, r are integers with $r \geq 0$ then

$$\gcd(a, b) = \gcd(b, r).$$

Proof $d = \gcd(a, b) \Rightarrow d \mid a$ and $d \mid b$

also $a = bq + r$

$\Rightarrow a - bq = r$

if $d \mid a$ and $d \mid b \Rightarrow d \mid a - bq$

$\Rightarrow d \mid r$.

Exm gcd (1244, 324)

$= \gcd(324, 272)$

$= \gcd(272, 52)$

$= \gcd(52, 12)$

$= \gcd(12, 4)$

$= \gcd(4, 0)$

$= 4.$