Intro to modulo arithmetic

$a, b, n, q, r \in \mathbb{Z}$

$n > 1$

$$\boxed{a = nq + r}$$

integer division

$r \in \{0, 1, 2, \dots, n-1\} = \mathbb{Z}_n$

r = remainders at n

q = quotient (sometimes q not specified)

$a \equiv r \mod n$ — a has remainder r at div. with n.

$a - r = nq$ = multiple of n — $n \mid (a-r)$ — n divides $(a-r)$

Examples

- $21 \mod 5 = 1$ — $21 = 5 \cdot q + 1$ — $21 \equiv 1 \mod 5$

  $5 \mid (21-1)$ — 5 divides $21 - 1$

- $24 \equiv 10 \equiv 3 \equiv -39 \mod 7$ — $r \in \mathbb{Z}_7 = \{0 : 6\}$

  $24 = 7 \cdot 3 + 3$

  $3 = 7 \cdot 0 + 3$

  $10 = 7 \cdot 1 + 3$

  $-39 = 7 \cdot (-6) + 3$

Th $a \equiv b \mod n \iff n \mid (a-b)$

iff

<u>proof</u> $a = nq_1 + r_1$

$b = nq_2 + r_2$

$a - b = nq_1 + r_1 - nq_2 - r_2 =$

$= n(q_1 - q_2) + r_1 - r_2$

$a \equiv b \mod n \iff r_1 = r_2 \iff a - b = n \cdot \underbrace{\text{something}}_{(q_1 - q_2)}$

$\iff n \mid (a-b)$

Example $\underbrace{21 \equiv 11 \mod 5}_{\text{true}} \iff \underbrace{5 \mid (21 - 11)}_{\text{true } 10 = 5 \cdot 2}$

mod operations.

- $(a+b) \bmod n = (a \bmod n + b \bmod n) \bmod n$

$$(17+4) \bmod 3 = (17 \bmod 3 + 4 \bmod 3) \bmod 3$$

$$0 \qquad\qquad 2 + 1$$

$$(19+12) \bmod 5 = (19 \bmod 5 + 12 \bmod 5) \bmod 5$$

$$31 \bmod 5 \qquad\qquad 4 + 2$$

$$1$$

- $\underbrace{a}_{= nq_1 + r_1} * \underbrace{b}_{= (nq_2 + r_2)} \bmod n = (\underbrace{a \bmod n}_{r_1} * \underbrace{b \bmod n}_{r_2}) \bmod n$

$nq_1 r_2 + nq_2 r_1 + n^2 q_1 q_2 + r_1 r_2$

$ab \bmod n$

$$17 \cdot 4 \bmod 3 = (17 \bmod 3 * 4 \bmod 3) \bmod 3$$

$$2 \qquad\qquad 2 \quad\; 1$$

$$19 \cdot 12 \bmod 5 = (19 \bmod 5 * 12 \bmod 5) \bmod 5$$

$$3 \qquad\qquad 4 * 2$$

- power

$$a^k \bmod n = (a \bmod n * a \bmod n \ldots * a \bmod n) \bmod n$$

example $13^{100} \bmod 11 = ?$

$$13^{100} \bmod 11 = 13^{64+32+4} \bmod 11 = \left(13^{64} \bmod 11\right) \cdot \left(13^{32} \bmod 11\right) \cdot \left(13^{4} \bmod 11\right) \bmod 11$$

$$\qquad 5 \qquad 4 \qquad 5$$

$$= (5 \cdot 4) \bmod 11 \cdot 5 \bmod 11 = 9 \cdot 5 \bmod 11 = 1$$

Repeated Squaring $a^{2^k} = ?$

$$13 \bmod 11 = 2$$

$$13^2 \bmod 11 = (13 \bmod 11)(13 \bmod 11) = 2 \cdot 2 \bmod 11 = 4$$

$$13^4 \bmod 11 = (13^2 \bmod 11)(13^2 \bmod 11) = 4 \cdot 4 \bmod 11 = 5$$

$$13^8 \bmod 11 = (13^4 \bmod 11)(13^4 \bmod 11) = 5 \cdot 5 \bmod 11 = 3$$

$$13^{16} = \ldots = 3 \cdot 3 \bmod 11 = 9$$

$$13^{32} = \ldots 9 \cdot 9 \bmod 11 = (77+4) \bmod 11 = 4$$

$$13^{64} = \ldots 4 \cdot 4 \bmod 11 = 5$$

Negatives:

$5 \cdot 2 \cdot 4 \mod 11 = (5 \cdot 2) \mod 11 \cdot 4 \mod 11$

$\underset{-1}{}$

$\boxed{10 \equiv -1 \mod 11} \iff 11 \mid (10 - (-1))$

$(-1 \cdot 4) = -4 \mod 11 = 7$

Factorization into primes

$p =$ prime $\in \mathbb{Z}$ divides only with $1, -1$, $p, -p$

$2, 3, 5, 7, 11, 13, 17, 19 \ldots$

Granted: any $n \in \mathbb{Z}^+$ has unique decomposition into primes

ex

$12 = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3$

$48 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 = 2^4 \cdot 3$

$75 = 5 \cdot 5 \cdot 3 = 5^2 \cdot 3$

GCD (a,b) = greatest common divisor (a,b)

def : take all common primes (with min counts) product of

ex $48 = 2^4 \cdot 3$

$36 = 2^2 \cdot 3^2$

$GCD = 2^2 \cdot 3^1 = 12$

$175 = 5^2 \cdot 7$

$98 = 7^2 \cdot 2$

$GCD = 7^1$

$60 = 2^2 \cdot 3 \cdot 5$

$50 = 5^2 \cdot 2$

$GCD = 2^1 \cdot 5^1 = 10$

$GCD\left(\frac{60}{10}, \frac{50}{10}\right) = 1$

(6) (5)

Property $d = GCD(a,b)$

$GCD\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

"Coprimes" = no common factors.

Modulo arithmetic part 2

primes : 2, 3, 5, 7, 11, 13, 17, 19, 23 ...

divide with $1, -1, it, -it$

$\forall n \in \mathbb{N} \Rightarrow$ unique prime decomposition

$a = 12 = 2^2 \cdot 3$

$b = 15 = 3 \cdot 5$

GCD = take common primes (including repetitions in common)

$GCD(12, 15) = 3$

$a = 110 = 2 \cdot 5 \cdot 11$

$b = 66 = 2 \cdot 3 \cdot 11$

$GCD(110, 66) = 2 \cdot 11 = 22$

$a = 128 = 2^7$

$b = 10931 = ?$ no "2"

$GCD(128, 10931) = 1$

no prime in common

GCD properties (theorems)

1) $GCD(a,b)$ = the biggest value $d \in \mathbb{Z}$ divides both

Proof by contradiction

assume $d = GCD(a,b)$ is NOT the biggest common divisor

$\Rightarrow \exists\, g > d \quad g \mid a \quad g \mid b$

$g > d \Rightarrow$ there at least a prime factor p in g more than in d

$\Rightarrow p \mid g \Rightarrow p \mid a,\ p \mid b \Rightarrow p$ also part of GCD.

$\Rightarrow p$ factor of d

contradiction

2) $n \mid a$; $n \mid b$ $\Big\} \Rightarrow n \mid GCD(a,b)$

n = common divisor

proof exercise (use decompositions into primes for n)

$n = p_1^{d_1} \cdot p_2^{d_2} \cdots p_k^{d_k} \Rightarrow \ldots \rightarrow n \mid d = GCD(a,b)$

Euclid Algorithm / Theorem (assume $a > b$)

- $d = GCD(a,b) \Leftrightarrow d = GCD(\underline{a-b}, b)$

  subtract "one" b

$a = 110$ $b = 66$

$a - b = 44$

$gcd(110, 66) = gcd\left(\begin{matrix}66\\44\end{matrix}\right)$

- consequence : subtract all "b"s

$a = b \cdot q + r$ $r \in \{0, \ldots, b-1\}$

$GCD(a,b) = GCD(a - b \cdot q, b)$

$= GCD(r, b)$

$a = 22$ $b = 6$

one b subtract: $(\overset{16}{22-6}, 6)$, $(\overset{10}{16-6}, 6)$ $(\overset{4}{10-6}, 6)$

$(22, 6) = (22 - 3 \cdot 6, 6)$ q r

all of them $22 = 6 \cdot 3 + 4$

Euclid Algorithm

repeat $GCD(a,b) = GCD(b,r)$ $a = bq + r$

untill GCD is found.

a	b	q	r
51	9	5	6
9	6	1	$\boxed{3}$ GCD
6	3	2	0

a	b	q	r
22	6	3	4
6	4	1	$\boxed{2}$ GCD
4	$\boxed{2}$	2	0

$$\left.\begin{array}{l} 51 = 3 \cdot 17 \\ 9 = 3^2 \end{array}\right\} \Rightarrow GCD = 3$$

a	b	q	r
108	60	1	48
60	48	1	$\boxed{12}$ GCD
48	12	4	0

$60 = 2^2 \cdot 3 \cdot 5$

$108 = 2^2 \cdot 3^3$

$GCD = 2^2 \cdot 3$

Modulo - inverse

def inverse of a mod n $= b = a^{-1}$ notation

iff $a \cdot b \equiv 1 \mod n$.

b = inverse of a $\Longleftrightarrow$ a = inverse of b — unique

$b = a^{-1} \mod n$ $\qquad$ $a = b^{-1} \mod n$

Inverse doesn't always exists. $\rightarrow$ iff $\gcd(a,n)=1$
relative prime

ex: $a=4$ $n=9$ want inverse of 4 mod 9

$= 4^{-1} \mod 9 = b$ s.t $4 \cdot b \equiv 1 \mod 9$

$b = 7$ $\qquad 4 \cdot 7 = 28 = 1 \mod 9$

$a = 12 \mod 15$ want $12^{-1} \mod 15$ that is b

doesnot exist!
$\gcd(12,15) = 3$

$12 \cdot b = 1 \mod 15$

Find the inverse using multiplicative group order

req: $\gcd(a, n) = 1$

Look at power(a) group mod n

$a, a^2, a^3, a^4, a^5, \ldots$ mod n until we get 1

$a = 4$ mod $n = 9$

$4, \; 4^2 \bmod 9 = 7, \; 4^3 \bmod 9 = 1$

$4 \cdot 4^2 = 1 \bmod 9$

inverse $4^2 = 7$

$a = 5$ mod 7

$5, \; \underset{\text{mod } 7}{5^2 = 4}, \; 5^3 = 4 \cdot 5 = 6, \; 5^4 = 30 = 2, \; 5^5 = 2 \cdot 5 = 3$

$5^6 = 3 \cdot 5 = 1 \Rightarrow \underset{\text{inverse}}{5^{-1}} = 5^5 = 3 \bmod 7$

$a = 7 \qquad n = 10$

$7,\ 7^2 = 49 = 9 = -1,\ 7^3 = \ldots,\ 7^4 = (7^2)^2 = (-1)^2 = 1$

$7^{-1}_{\text{inverse}} = 7^3$

$a^v \equiv 1 \mod n \qquad v =$ multiplicative order of a

$a^{v-1} =$ inverse because

$a \cdot a^{v-1} = a^v \equiv 1 \mod n.$

Th if $GCD(a, n) = 1$ relatively prime

$\iff \exists\, v$ s.t. $a^v \equiv 1 \mod n$.