Dis 2D: Modular Arithmetic I

Friday, June 26, 2020 1:59 AM

Fundamentals

$\boxed{a \pmod q}$ c.f $\boxed{\text{find remainder of } a \text{ divided by } q}$

$= a - \lfloor \frac{a}{q} \rfloor * q$

$5 \pmod 3 = 5 - \lfloor \frac{5}{3} \rfloor * 3$

$= 5 - 3 = 2$

$a \equiv 0 \pmod q \iff q \mid a$

Unfinished proofs from lecture:

$\boxed{\text{Lem}}$ Let $a = bq + r$, where $a, b, q, r \in \mathbb{Z}$.
Then $\gcd(a,b) = \gcd(b,r)$

$\iff$ i.e $\gcd(a,b) = \gcd(b, a \pmod b)$

Pf: [exercise in discussion]

i) all divisor of a, b also divide b, r

and

ii) all divisor b, r also divide a, b

1) $\forall d \in \{\text{divisor of } a, b\}$, $d \geq 1$

i.e $d \mid a$, $d \mid b$
$\Rightarrow d \mid bq + r$, $d \mid b$
$\Rightarrow d \mid r$, $d \mid b$
$\Rightarrow d \in \{\text{divisor of } b, r\}$

$r \equiv a \pmod b$

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

$a - r = bq$

$\Downarrow$

$b \mid a - r$ $\Rightarrow$

$x, y, z \in \mathbb{Z}$, $\boxed{x \mid y \text{ and } x \mid y + z \Rightarrow x \mid z}$

Extended Euclid's Algorithm

Bezout's identity:

For all integers x, y,
$\boxed{\gcd(x, y) = ax + by,}$ where a, b are integers

Goal of the algorithm = write gcd(x, y) are a linear combination of x, y

Walkthrough

write $\gcd(2328, 440)$ as a lin. comb. of 2328 & 440 i.e find a, b in $\gcd(2328, 440) = (a)(2328) + (b)(440)$

$\gcd(2328, 440)$ $\qquad \gcd(a,b) = \gcd(b, a \pmod b)$

$= \gcd(440, 128)$ $\qquad 440 - \left\lfloor \frac{440}{128} \right\rfloor \times 3$

$= \gcd(128, 56)$ $\qquad = 440 - 384 = 56$ $\qquad 384$

$= \gcd(56, 16)$

$= \gcd(16, 8)$

$= \gcd(8, 0)$ $\qquad 56 - \left\lfloor \frac{56}{16} \right\rfloor * 16 = 8$ $\quad (\to 3)$

$= 8$

Goal: $8 = a\, 2328 + b\, 440$

start from bottom

$(1) 56 + (-3) 16 = 8$

sub. expr. for the smaller int

$(1) 128 - \left\lfloor \frac{128}{56} \right\rfloor * 56 = 16$

$[(1) 128 - (2) * 56] = 16$

$(1) 56 + (-3) [(1) 128 - (2) 56] = 8$

$(7) 56 + (-3) 128 = 8$ $\qquad 56 = (1) 440 -$

$7 \times [440 - 3 * 128] + (-3) 128 = 8$

$128 = [(1)$

$7 \times 440 - 24 \times 128 = 8$

$7 \times 440 - 24 [1 (2328) + (-5) 440] =$

(c) In the same way as just illustrated in the previous two parts, calculate the gcd of 17 and 38, and determine how to express this as a "combination" of 17 and 38.

$\gcd(17, 38) = \gcd(17, 4)$

$= \gcd(4, 1)$ $\qquad 1 = (1) 17 -$

$= \gcd(1, 0) = 1$

$= 17 - 4$

(d) What does this imply, in this case, about the multiplicative inverse of 17, in arithmetic mod 38?

$$(\text{mod } 38) \quad \text{I}$$

x

$$1 \equiv 17x \quad (\text{mod } 38)$$

$$17 \times 9 \equiv 153 \quad (\text{mod } 38) \quad \text{I}$$

$$\equiv 1 \quad (\text{mod } 38)$$

1 Modular Inverses

Recall the definition of inverses from lecture: let $a, m \in \mathbb{Z}$ and $m > 0$; if $x \in \mathbb{Z}$ satisfies $ax \equiv 1$ $(\text{mod } m)$, then we say x is an **inverse of** a **modulo** m.

Now, we will investigate the existence and uniqueness of inverses. (From part a to part d, you are not allowed to use the theorem that will be proved in e and f).

(a) Is 3 an inverse of 5 modulo 10?

$$3 * 5 \equiv 15 \quad (\text{mod } 10)$$

$$\equiv 5 \not\equiv 1 \quad (\text{mod } 10)$$

(b) Is 3 an inverse of 5 modulo 14?

(c) Is each $3 + 14n$ where $n \in \mathbb{Z}$ an inverse of 5 modulo 14?

(d) Does 4 have inverse modulo 8?

exist & uni

If x is a mult. inv of a (mod m)

e) by def^n $ax \equiv 1 \pmod m$

$ax' \equiv 1 \pmod m$

mod arithm $\Rightarrow ax - 1 \equiv 0 \pmod m$

$\Rightarrow ax' - 1 \equiv 0 \pmod m$

divisibility

$m \mid ax - 1$

$m \mid ax' - 1$

$m \mid p$

$m \mid q$

$\Rightarrow m \mid p - q$

$\Downarrow$

$m \mid a(x - x')$

$a \not\equiv 0$

$m \nmid a$

$\Rightarrow m \mid x - x'$

$\Rightarrow x - x' \equiv 0 \pmod m$

suppose $x \equiv$

$\Rightarrow x -$

$ax - ax' \equiv a$

$a(x - x') \equiv a$

$1 - 1 \equiv ab$

$0 \equiv ab$

$\Rightarrow b \equiv 0 \pmod m$

① can

$\forall a,b \in \mathbb{Z}$

(e) + (f) $\Rightarrow$ if $\gcd(a,b) = 1 \Rightarrow$ mu

(e) Suppose $x, x' \in \mathbb{Z}$ are both inverses of a modulo m. Is it possible that $x \not\equiv x' \pmod{m}$?

(f) Prove the following theorem: if $\gcd(a,m) = 1$ and $m > 1$, then an inverse of a modulo m exists. Furthermore, this inverse is unique modulo m. (That is, there is a unique integer $0 \le x < m$ that is an inverse of a modulo m; if $x' \in \mathbb{Z}$ is an inverse of a modulo m, then $x' \equiv x \pmod{m}$.)

(g) Prove the converse of (f) is true: let $a, m \in \mathbb{Z}$ and $m > 1$; if an inverse of a modulo m exists, then a and m are relatively prime.

f) Bezout's identity $\forall x, y \in \mathbb{Z}$ gcc

$1 = \boxed{\gcd(x,y) = ax + by}$ $\Rightarrow$

$\Rightarrow$ Inv of $x \pmod{y} \equiv a$

$A \Rightarrow B$

contradiction is $\neg(A \Rightarrow B)$

i.e assume $\neg(A \Rightarrow B)$

Truth table

$\boxed{A \wedge \neg B}$