Euclidean Algorithm

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

$a = bq_1 + r_2$

$b = r_2 q_2 + r_3$

$\vdots$

$r_{i-2} = r_{i-1} q_{i-1} + r_i$ ← $\gcd(a,b)$

$r_{i-1} = r_i q_i + 0$

Example $\gcd(2048, 728)$

$2048 = 728 \cdot 2 + 528$ (1)

$728 = 528 \cdot 1 + 220$ (2)

$528 = 220 \cdot 2 + 88$ (3)

$220 = 88 \cdot 2 + 44$ (4)

$88 = 44 \cdot 2 + 0$

Let $a = 2048$
$b = 728$

① $528 = a - 2b$.

Plug

② $b = (a-2b) \cdot 2 + 220$

$220 = -a + 3b$

Plug into ③

$a - 2b = (-a+3b) \cdot 2 + 88$

$88 = 3a - 8b$

④ $-a + 3b = (3a-8b) \cdot 2 + 44$

$44 = -7a + 19b$

$\gcd(a,b) = -7a + 19b$

Theorem (Extended Euclidean Algorithm)

Let $a, b \in \mathbb{N}$

Then $\exists\, u, v \in \mathbb{Z}$ s.t.

$\gcd(a,b) = a \cdot u + b \cdot v$.

Pf/ Run Euclidean alg

Sol r_2 in a, b

solve r_3 in b & r_2 ← already in a & b

$\vdots$

Solve r_i in r_{i-1} & r_{i-2}

$\gcd$ ∅

Rmk only needed the # of computations = # divisions in E.A. so still multiple of $\log_2(b)$ comps!

HW Implement.

Def^n a, b are relatively prime if $\gcd(a,b) = 1$.

Corollary *

If $\gcd(a,b) = 1$

$\iff \exists\, u, v \in \mathbb{Z}$ s.t. $au + bv = 1$

HW

Modular Arithmetic

Ex: Clocks

"6 hrs after 9 is 3"

$9 + 6 = 15$ $\xrightarrow{-12}$ 3

"3 hrs before 2 is 11"

$2 - 3 = -1$ $\xrightarrow{+12}$ 11

"$4 + 12 = 16$" $\xrightarrow{-12}$ 4

equivs

$15 \sim 3$

$-1 \sim 11$

$4 \sim 16$

$12 \sim 0$

Difference is a multiple of 12

Def^n $m \in \mathbb{N}$.

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

a is congruent to b modulo m iff

$m \mid (a-b)$ ← $a = b + m \cdot k$

We write

$a \equiv b \mod m$

Ex

$9 + 6 \equiv 3 \mod 12$

$2 - 3 \equiv 11 \mod 12$

Ex $28 \equiv 13 \mod 5$

$28 - 13 = 15 = 5 \cdot 3$

$13 \not\equiv 6 \mod 5$

$13 - 6 = 7$ X

*Goal develop arithmetic in this modular context

Goal (mod 12)

Is 1 & 13 are same

Then $+1$ & $+13$ should do same thing (mod 12)

i.e. $a + 1 \equiv a + 13 \mod 12$

If $a \equiv a' \mod m$ *

$b \equiv b' \mod m$

$a + b \equiv a' + b' \mod m$

Pf/ $a' = a + km$

$b' = b + \ell m$

$a' + b' = a + km + b + \ell m = a + b + (k+\ell)m$

$\implies a + b \equiv a' + b' \mod m$

Prop $a \equiv a' \mod m$

$b \equiv b' \mod m$

* $a + b \equiv a' + b' \mod m$
* $a - b \equiv a' - b' \mod m$
* $a \cdot b \equiv a' \cdot b' \mod m$

Pf/ HW.

Can we divide?

Recall in real #s.

dividing by a

$\iff$ multiplying by $\frac{1}{a} = a^{-1}$

i.e./ a^{-1} is the x s.t. $a \cdot x = 1$

Solve $x = \frac{1}{a}$

a^{-1} is unique.

e.g

$\div 5$ same as $\times 0.2$
$= 5^{-1}$

$5 \cdot 0.2 = 1$

Prop: (division mod m)

$a \in \mathbb{Z}$

1) $\exists\, b \in \mathbb{Z}$ s.t. $ab \equiv 1 \mod m$

$\iff \gcd(a,m) = 1$

2) If $\gcd(a,m) = 1$ &

$ab_1 \equiv ab_2 \equiv 1 \mod m$

Then $b_1 \equiv b_2 \mod m$

Pf/ ($\Leftarrow$)

Assume $\gcd(a,m) = 1$

① Extended E.A. $\exists\, u, v$

s.t. $au + mv = 1$

$\implies au = 1 - mv$

$\equiv 1 \mod m$

Let $b = u$ ← "a^{-1}"

Assume $ab \equiv 1 \mod m$

$ab = 1 - km$

$ab + km = 1$ ←

Let $g = \gcd(a,m)$

Then $g \mid a \implies g \mid ab$

$g \mid m \implies g \mid km$

$\to g \mid (\cancel{ab + km})$ 1

so $g = 1$ ∅

② $ab_1 \equiv 1 \mod m$

$ab_2 \equiv 1 \mod m$

$b_1 \equiv b_1(ab_2) \mod m$

$= (ab_1) b_2$

$\equiv 1 \cdot b_2 \mod m$ ∅

Example: Dividing by 2 mod 5

$\gcd(2,5) = 1 \implies$

2 has an inverse mod 5

$2 \cdot 1 = 2$ x

$2 \cdot 2 = 4$ x

$2 \cdot 3 = 6 \equiv 1 \mod 5$

$\frac{1}{2} \equiv 3 \mod 5$ *

$\frac{3}{2} = 3 \cdot \frac{1}{2} \equiv 3 \cdot 3 = 9$

$\equiv 4 \mod 5$

We can do algebra

$2x \equiv 3 \mod 5$

$\times 3$ $\times 3$

$\cancel{6}x \equiv 9 \mod 5$

$x \equiv 4 \mod 5$

CH

$2x = 2 \cdot 4 = 8 \equiv 3 \mod 5$ ✓

$x = 9$ works

$2 \cdot 9 = 18 \equiv 3$

Remark

Uniqueness of solns to equation or inverses only makes sense mod m. (up to a multiple of m)

$b_1 \neq b_2$ "both work"

but $b_1 \equiv b_2 \mod m$

Rmk

Found $\frac{1}{2}$ by guessing.

If m huge this is too slow.

Fast way to find $a^{-1} \mod m$ is to find u, v s.t. $au + mv = 1$

$\implies a^{-1} = u$

Ext. Euc. Alg implementation

Model for modular arithmetic.

Lemma: $a \in \mathbb{Z}$. $m \in \mathbb{N}$

there is a unique r

w/ $0 \leq r < m$ & $a \equiv r \mod m$

Pf/ $a = mq + r$ long div

gives existence & uniqueness. ∅

Notation

$r = \bar{a}$

reducing out a mod m

Instead of "up to congruence" we can work w/ # $\{0, 1, 2, \dots, m-1\}$.

Def^n.

Let $m \in \mathbb{N}$. Then the ring of integers modulo m is

$\mathbb{Z}/m\mathbb{Z} = \{0, 1, 2, \dots, m-1\}$

w/ addition

$a + b =$ the unique $r \in \mathbb{Z}/m\mathbb{Z}$ congruent to $a+b$.

$\overline{a+b}$

$a - b =$ unique $\overline{a-b} \in \mathbb{Z}/m\mathbb{Z}$

$a \times b =$ unique $\overline{a \times b} \in \mathbb{Z}/m\mathbb{Z}$

$\mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, 3, 4\}$

?

$3 \times 4 = 12$

$\overline{12} = 2$

Practice

Write out $\times$ & $+$ tables for $\mathbb{Z}/5\mathbb{Z}$ & $\mathbb{Z}/6\mathbb{Z}$.