E. A. $\gcd(a,b)$ $a \geq b$

$a = bq_1 + r_2$

$b = r_2 q_2 + r_3$

$\vdots$

$r_{n-2} = r_{n-1} q_{n-1} + r_n$ GCD

$r_{n-1} = r_n q_n + 0$

Ex $\gcd(2024, 748)$

$2024 = 748 \cdot 2 + 528$ (1)

$748 = 528 \cdot 1 + 220$ (2)

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

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

$88 = 44 \cdot 2 + 0$

Notice can write 44 in terms of 2024 & 748

$a = 2024$

$b = 748$

1) $528 = a - 2b$

2) $b = (a-2b)\cdot 1 + 220$

$220 = -a + 3b$

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

$88 = 3a - 8b$

4) $-a + 3b = (3a-8b)\cdot 2 + 44$

$\Longrightarrow \underset{\substack{\| \\ GCD(a,b)}}{44} = -7a + 19b$

Extended Euclidean Alg.

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/

$r_2 = a - q_1 b$

$r_3 = b - q_2 r_2$ in a & b

$r_4 = r_2 - q_3 r_3$

$\vdots$

$r_n = r_{n-2} - q_{n-1} r_{n-1}$

$= \gcd(a,b)$ ∅

HW Implement This.

Rmk

Still at most $4\log_2 b + 4$ steps.

Def^n $a, b \in \mathbb{Z}$ are relatively prime if $\gcd(a,b) = 1$.

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

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

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

Pf/ HW

Modular Arithmetic

Example (Clock Arithmetic)

"6 hours after 9 is 3"

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

"3 hours before 2 is 11"

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

"12 hrs past 4 is 4"

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

Equivalence

$15 \sim 3$

$-1 \sim 11$

$16 \sim 4$

$12 \sim 0$

difference is (a multiple of) 12

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

We say $a, b \in \mathbb{Z}$ are congruent modulo m if $m \mid (a-b) \Leftrightarrow a = b + km$

write

$a \equiv b \mod m$

Ex
- $9 + 6 \equiv 3 \mod 12$
- $2 - 3 \equiv 11 \mod 12$
- $4 + 12 \equiv 4 \mod 12$

Ex/ $28 \equiv 13 \mod 5$

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

$13 \not\equiv 7 \mod 5$

$13 - 7 = 6$

Rmk Want arithmetic & algebraic substitution to make sense

e.g/ $1 \equiv 13 \mod 12$

$a * 1 \equiv a * 13 \mod 12$

i.e. Want compatibility w/ arithmetic

Claim

$a \equiv a' \mod m$

$b \equiv b' \mod m$

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

Pf/ $a \equiv a' \mod m \Leftrightarrow a = a' + km$

$b \equiv b' \mod m \Leftrightarrow b = b' + lm$

$a + b = a' + km + b' + lm$

$= a' + b' + (k+l)m$

so $a + b \equiv a' + b' \mod m$ ∅

Prop $a \equiv a' \mod m$

$b \equiv b' \mod m$

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

2) $a - b \equiv a' - b' \mod m$

3) $ab \equiv a' \cdot b' \mod m$

Pf/ HW

Division ($\div$)

Question What is division?

(work in $\mathbb{R}$ = real #s)

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

a^{-1} = the solution to $ax = 1$

This exists & is unique in $\mathbb{R}$

Ex $5^{-1} = \frac{1}{5} = 0.2$

$5 \cdot 0.2 = 1$

$17 \div 5 \Longleftrightarrow 17 \cdot (0.2)$

Remark If I want to divide by a (mod m) need solution (a^{-1}) to

$ax \equiv 1 \mod m$.

Now $(\div a) \Longleftrightarrow (\times a^{-1})$

Prop (Division mod m)

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

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

$\Longleftrightarrow \gcd(a,m) = 1$.

② If $b_1, b_2 \in \mathbb{Z}$ &

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

$\Longrightarrow b_1 \equiv b_2 \mod m$.

Proof

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

so $\exists\, u, v \in \mathbb{Z}$ ✓

$au + mv = 1$

$au = 1 - mv \equiv 1 \mod m$

let $b = u$ & done.

$\Longrightarrow$ Assume $ab \equiv 1 \mod m$

$ab = 1 - km$

$1 = ab + km$

$g = \gcd(a,m)$

$g \mid a \Rightarrow g \mid ab$

$g \mid m \Rightarrow g \mid km$

$\Rightarrow g \mid \underbrace{(ab+km)}_{=1}$

$g \mid 1 \Rightarrow g = 1$ ✓

② $ab_1 \equiv 1 \mod m$ (i)

$ab_2 \equiv 1 \mod m$ (ii)

$b_1 = b_1 \cdot 1 \overset{(ii)}{\equiv} b_1(ab_2) \mod m$

$= (ab_1) b_2$

$\overset{(i)}{\equiv} b_2 \mod m$ ∅

Example Dividing by 2 mod 5

I can always divide by 2 mod 5.

b/c $\gcd(2,5) = 1$

$1 \cdot 2 = 2$ ✗ $2 \cdot 2 = 4$ ✗

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

Fun

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

Do fractions

$\frac{3}{2} = 3 \cdot \frac{1}{2} \equiv 3 \cdot 3 \mod 5$

$\equiv 9 \mod 5$

$\equiv 4 \mod 5$

Do algebra

$\frac{1}{2} \cdot 2x \equiv \frac{3}{2} \mod 5$

$x \equiv \frac{1}{2} \cdot 3 \mod 5$

$\equiv 9 \equiv 4 \mod 5$

check

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

$2 \cdot 9 = 18 \equiv 3$ ✓

Exercise

Find $4^{-1} \mod 15$

Remark We found $2^{-1} \mod 5$ ($4^{-1} \mod 15$) by guessing.

This takes up to m computations!

More efficient to run ext euc. alg & get $au + mv = 1$

then $a^{-1} = u$.

$\sim \log_2 m$

A structure for modular arithmetic.

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

There is a unique r w/ $0 \leq r < m$ s.t.

$a \equiv r \mod m$.

Pf/ Long division $a \div m$

$a = qm + r$ $0 \leq r < m$

existence & uniqueness ∅

Def^n
- The r from the lemma is called the reduction of a mod m denoted $\bar{a}$.
- Replacing a w/ $\bar{a}$ is called reducing mod m.
- $a \% m = \bar{a}$

↑ python.

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

The ring of integers modulo m is

$\mathbb{Z}/m\mathbb{Z} = \{0, 1, 2, 3, \cdots, m-1\}$

With addition, sub

$a + b := \overline{a+b}$

$a - b := \overline{a-b}$

$a \cdot b := \overline{a \cdot b}$

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

$3 \cdot 4 = \overline{12} = 2$

$12 = 2 \cdot 5 + 2$

Exercise

Make + & × table for $\mathbb{Z}/5\mathbb{Z}$ & $\mathbb{Z}/6\mathbb{Z}$

	0	1	2	3	4
0					
1					
2				1	
3					
4			3		