2.4: $\mathbb{Z}$ AND ALGORITHMS

EUCLIDEAN ALGORITHM

- efficient method for finding $\gcd(a,b)$
- >2300 yrs. old (in Euclid's Elements - geometry (1000 eds.)

Assume $a, b \in \mathbb{Z}^+$ and $a \geq b$.

The Division Algorithm (2.3) $\Rightarrow$
There are unique $q, r \in \mathbb{Z}$
such that $a = bq + r$.

$$a = b\underbrace{q}_{\text{quotient}} + \underbrace{r}_{\substack{\text{remainder} \\ (0 \leq r < b)}}$$

Ex $57 = 5 \cdot 11 + 2$

Lemma (subresult needed for something bigger)

If $a = bq + r$ ~~($a, b, q, r \in \mathbb{Z}$ in general)~~
then $\gcd(a,b) = \gcd(b, \underset{\substack{\| \\ a \bmod b}}{r})$

gcd

$a = bq + r$

$a = bq + r$

gcd

Ex Find gcd(88,16)

$$\overset{a}{88} = \underbrace{\overset{b}{16}\cdot \underset{\substack{\uparrow \\ \lfloor \frac{88}{16} \rfloor}}{\overset{q}{5}}}_{80} + \overset{r}{8}$$

$$\overbrace{88 = 16}^{\text{gcd}} \cdot 5 + 8$$

$$88 = \underbrace{16 \cdot 5 + 8}_{\text{gcd}} \leftarrow 88 \bmod 16$$

$$\begin{aligned} \gcd(88,16) &= \gcd(16,8) \\ &= 8 \end{aligned}$$

Recursive definition for gcd:

$\gcd(a,b) = \gcd(b, a \bmod b)$ ← Shrink problem
$\gcd(a,0) = a$ ← "Base case"

Proof of Lemma

If $a = bq + r \Rightarrow \gcd(a,b) = \gcd(b,r)$

Show that the common divisors of a and b are the same as those for b and r

$$\{d \in \mathbb{Z} : d | a \text{ and } d | b\} \quad X$$

$$= \{d \in \mathbb{Z} ; d | b \text{ and } d | r\} \quad Y$$

The common gcd is the largest # in this finite set.

Show $X = Y$.

$X \subseteq Y$

Assume $d|a$ and $d|b$. Show $d|r$, also.

$$a = bq + r$$
$$\Rightarrow a - bq = r$$
$$\Rightarrow r = \underset{d|}{a} - \underset{d|}{b}q \quad 2.3$$
$$\Rightarrow d | r$$

$Y \subseteq X$

Assume $d|b$ and $d|r$. Show $d|a$, also.

$$a = \underset{d|}{b}q + \underset{d|}{r} \quad 2.3$$
$$d | a$$

QED

<u>Ex</u> Find gcd(658, 104) $\longrightarrow$

$$658 = 104 \cdot 6 + 34$$
$$104 = 34 \cdot 3 + 2$$
$$34 = 2 \cdot 17 + 0$$

gcd(104, 34)
$\downarrow$
gcd(34, 2)
$\downarrow$
gcd(2, 0)

$= \boxed{2}$ last nonzero remainder

gcd(658, 104) = 2

What's lcm(658, 104)?

$$ab = \gcd(a,b) \cdot \text{lcm}(a,b)$$
$$(658)(104) = (2)\,\text{lcm}$$
$$\Rightarrow \text{lcm} = \boxed{34{,}216}$$

Knuth 515
$\text{lcm}(a,b) = \frac{a}{a \bmod b} \times \text{lcm}(a \bmod b, b)$

Easiest way is through the E.A.!

BINARY REPRESENTATIONS OF INTEGERS

We normally use decimal (base-10) notation

$$4032 = (4032)_{10}$$

$$= 2 \times 10^0 + 3 \times 10^1 + 0 \times 10^2 + 4 \times 10^3$$

Polish computer (base 3, closer to e)

SOU $(5!!)_2$

Binary → Decimal (1-1 corresp. if we eliminate leading "0"s)

$$(101011)_2 = 1 \times 2^0 + 1 \times 2^1 + 0 \times 2^2 + 1 \times 2^3 + 0 \times 2^4 + 1 \times 2^5 = 1 + 2 + 8 + 32 = (43)_{10}$$

Decimal → Binary (different from Rosen)

$(43)_{10}$ What is the highest power of 2 that is ≤ 43?

$32 = 2^5$

Bit Position Value (PV)	Bit Bit=1 if PV $\le$ remainder Bit=0 otherwise	Remainder Start with 43. → If Bit=1, rem. ← rem. − PV → If Bit=0, keep rem.
		43
$2^5=32$	1	$43-32=11$
$2^4=16$	0	11
$2^3=8$	1	$11-8=3$
$2^2=4$	0	3
$2^1=2$	1	$3-2=1$
$2^0=1$	1	$1-1=0$

$(101011)_2$

Hexadecimal (Base-16) Notation

Digits: $0, 1, \ldots, 9, \underset{10}{A}, \underset{11}{B}, \underset{12}{C}, \underset{13}{D}, \underset{14}{E}, \underset{15}{F}$

Ex
$$
\begin{aligned}
(2B)_{16} &= B \times 16^0 + 2 \times 16^1 \\
&= 11 \times 1 + 2 \times 16 \\
&= (43)_{10}
\end{aligned}
$$

2.5

<u>Thm 1</u> If $a, b \in \mathbb{Z}^+$, then
$\exists\, s, t \in \mathbb{Z}$ such that $\gcd(a,b) = \underbrace{sa + tb}_{\substack{\text{some linear combination}\\ \text{of } a,b \\ \text{w/ integer coeffs}}}$

<u>Ex</u> $\gcd(14,10) = 2$
So, $2 = 14\underbrace{s + 10t}_{\in \mathbb{Z} \text{ (multipliers)}}$

Work out Euclidean Algor. until we get $r = 2$.

$$
\begin{aligned}
14 &= 10 \cdot 1 + 4 & \Rightarrow\quad & 4 = 14 - 10 \cdot 1 \\
10 &= 4 \cdot 2 + 2 & \Rightarrow\quad & 2 = 10 - 4 \cdot 2
\end{aligned}
$$

Solve for r

plug in

$$2 = 10 - 4 \cdot 2$$
$$2 = 10 - (14 - 10 \cdot 1) \cdot 2$$
$$2 = 10 - 14 \cdot 2 + 10 \cdot 2$$
$$\boxed{2 = 14(-2) + 10(3)}$$

Don't "absorb" 10s or 14s.

(There are more efficient methods.)

LINEAR CONGRUENCES

Review arithmetic!

Solve: $ax \equiv b \pmod{m}$

We want all $x \in \mathbb{Z}$ that make this true.
(It's like solving an equation for x.)

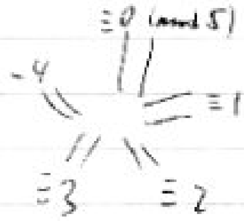
High school:

$$\begin{aligned} ax &= b && (a \neq 0) \\ (\tfrac{1}{a})ax &= (\tfrac{1}{a})b && (\tfrac{1}{a} \text{ is the multiplicative inverse of } a) \\ x &= \tfrac{b}{a} && (\tfrac{1}{a} \cdot a = 1) \end{aligned}$$

Here,

<u>Thm</u> If $\gcd(a,m)=1$ and $m>1$, then there is a unique "inverse class $(\bmod\ m)$" such that $\bar{a} \cdot a \equiv 1 \pmod{m}$ for every integer $\bar{a}$ in the inverse class.

<u>Ex</u> (mod 5)



i.e., there is exactly one congruence class (mod m) of multiplicative inverses for a (mod m).

<u>Ex</u> Solve $3x - 1 \equiv 1 \pmod 5$ — Can $+,-$ same # on both sides.

$\Leftrightarrow \quad 3x \equiv 2 \pmod 5$

Find the inverse class of $3 \pmod 5$. "$\bar{3}$"

Verify $\gcd(5,3) = 1$

I skipped

$5 = 3 \cdot 1 + 2 \Rightarrow 2 = 5 - 3 \cdot 1$

$3 = 2 \cdot 1 + 1 \Rightarrow 1 = 3 - 2 \cdot 1$

$1 = 3 - 2 \cdot 1$
$1 = 3 - (5 - 3 \cdot 1) \cdot 1$
$1 = 3 - 5 + 3$
$1 = 3(2) + 5(-1)$ ← <u>Thm 1</u> form

$1 \equiv 3(2) + 5\cancel{(-1)} \pmod 5$ — $\equiv$ quantities have the same remainder

multiples of $m=5$ act like "0" ("5" = "0")

$3(2) \equiv 1 \pmod 5$

↑ an inverse!

Inverse class $= \{n \in \mathbb{Z} \mid n \equiv 2 \pmod 5\}$
$= \{\ldots, -8, -3, 2, 7, 12, \ldots\}$

Me

$a\bar{a} = 1 + km$, so $a\bar{a}$ must be rel. prime to m (big idea)

$6x = x + 5x$

$6x \equiv x + 5x \pmod 5$

Solve $3x \equiv 2 \pmod 5$

OK to mult. by inverse $\bar{a}$

$\Leftrightarrow (2)3x \equiv (2)(2) \pmod 5$

$\Leftrightarrow 6x \equiv 4 \pmod 5$

$6 \equiv 1 \pmod 5$

$6x = x + \cancel{5x}$

You can replace #s with other members in the same class!

In context of $+ - \times$ $\equiv 4 \pmod 5$

$\Leftrightarrow x \equiv 4 \pmod 5$

Solution set $= \{x \in \mathbb{Z} \mid x \equiv 4 \pmod 5\}$

$= \{\ldots, -6, -1, 4, 9, 14, \ldots\}$

Show your work!

In mod 5 arithmetic, what's $2+3$? "$2+3=0$"

Chinese Remainder Thm deals with solutions of linear congruential systems with pairwise relatively prime moduli. Can be applied to computer arithmetic with large integers — break up into a series of remainders, operate on remainders, then solve a system at the end

SYSTEMS OF LINEAR CONGRUENCES

Gilbert 84

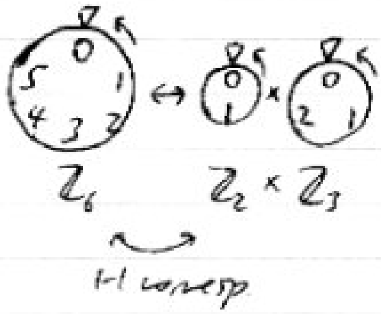
Let $\mathbb{Z}_n$ = the set of integers mod n

$= \{[0]_n, [1]_n, \ldots, [n-1]_n\}$

Let $f: \mathbb{Z}_6 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_3$

defined by $f([a]_6) = ([a]_2, [a]_3)$

$\mathbb{Z}_6$	$\mathbb{Z}_2 \times \mathbb{Z}_3$
$[0]_6$	$([0]_2, [0]_3)$
$[1]_6$	$([1]_2, [1]_3)$
$[2]_6$	$([0]_2, [2]_3)$
$[3]_6$	$([1]_2, [0]_3)$
$[4]_6$	$([0]_2, [1]_3)$
$[5]_6$	$([1]_2, [2]_3)$

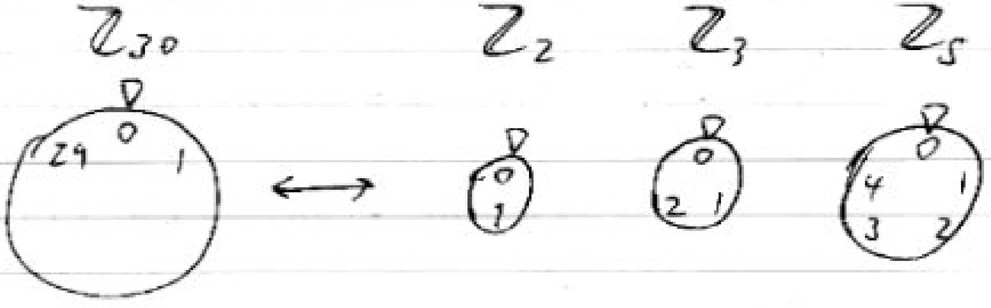


f turns out to be a bijection!

Chinese Remainder Theorem

Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime moduli ($\in \mathbb{Z}^+, \geq 2$).
Let $m = m_1 m_2 \cdots m_n$
Then, $f: \mathbb{Z}_m \to \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \ldots \times \mathbb{Z}_{m_n}$
where $f([a]_m) = ([a]_{m_1}, [a]_{m_2}, \ldots, [a]_{m_n})$
is a bijection.

Ex



This means that the system

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

has a unique solution (mod m)

Ex $\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \end{cases}$

has a unique solution (mod 6), namely $[5]_6$.

Application

Large integers can be broken up into lists of remainders (mod relatively prime moduli). Arithmetic ops. can be performed on these remainders.

The final result corresponds to a linear congruential system which can be solved.