

# Which of these are prime?

	11	21	31
2	12	22	32
3	13	23	33
4	14	24	34
5	15	25	35
6	16	26	36
7	17	27	37
8	18	28	38
9	19	29	39
10	20	30	40

# Sieve of Eratosthenes (3<sup>rd</sup> Century B.C.)

Red: Can't Be Primes  
Eliminating Multiples of 2  
(except 2, itself)

	11	21	31
2	12	22	32
3	13	23	33
4	14	24	34
5	15	25	35
6	16	26	36
7	17	27	37
8	18	28	38
9	19	29	39
10	20	30	40

# Sieve of Eratosthenes (3<sup>rd</sup> Century B.C.)

Red: Can't Be Primes  
Eliminating Multiples of 2 and 3  
(except 2 and 3, themselves)

	11	21	31
2	12	22	32
3	13	23	33
4	14	24	34
5	15	25	35
6	16	26	36
7	17	27	37
8	18	28	38
9	19	29	39
10	20	30	40

# Sieve of Eratosthenes

(3<sup>rd</sup> Century B.C.)

Red: Can't Be Primes  
Eliminating Multiples of 2, 3, and 5  
(except 2, 3, and 5, themselves)

	11	21	31
2	12	22	32
3	13	23	33
4	14	24	34
5	15	25	35
6	16	26	36
7	17	27	37
8	18	28	38
9	19	29	39
10	20	30	40

2.3:  $\mathbb{Z}$  and DIVISION

Ex  $10 \div 2$  is an integer (namely, 5), because  $10 = (2)(5)$

Write:  $2 | 10$

2 divides 10

2 is a factor of 10

10 is a multiple of 2

10 is divisible by 2

Assume  $a, b \in \mathbb{Z}$  and  $a \neq 0$

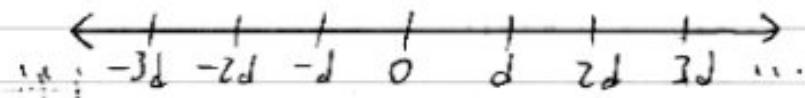
$a$  divides  $b$  ( $a | b$ )  $\Leftrightarrow b \div a$  (or  $\frac{b}{a}$ ) is an integer  
 $\Leftrightarrow \exists c \in \mathbb{Z} : b = ac$

$$\text{Ex } \begin{matrix} \uparrow & \uparrow & \uparrow \\ 5 & 10 & 25 \end{matrix}$$

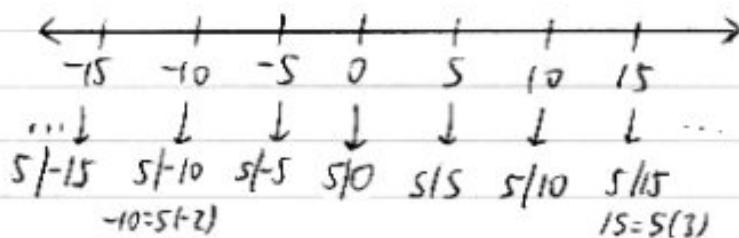
Ex  $4 | 12$  ( $\frac{12}{4} = 3 \in \mathbb{Z}$ )

Ex  $5 \nmid 12$  ( $\frac{12}{5} \notin \mathbb{Z}$ )

If  $d \in \mathbb{Z}^+$ , the multiples of  $d$   
(i.e., the integers divisible by  $d$ ):



Ex  $d=5$ :



(Skip  
too technical) Ex 2 (p. 114)  
 $n, d \in \mathbb{Z}^+$ .

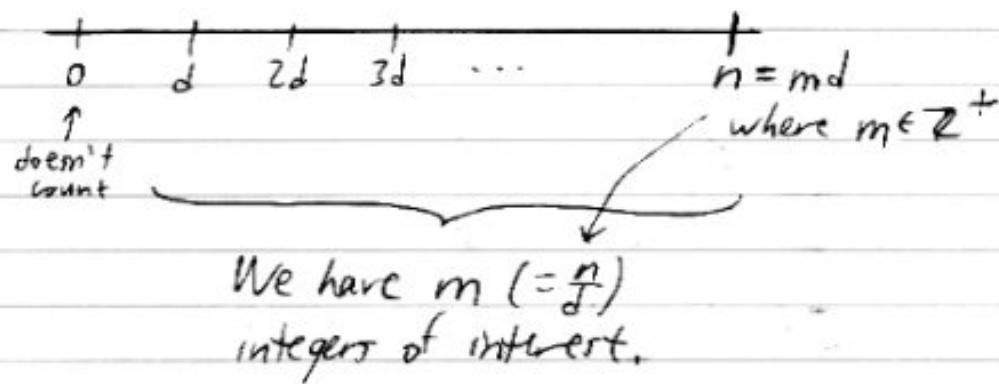
How many positive integers not exceeding  $n$   
are divisible by  $d$ ?

i.e., find  $\left| \{x \mid x \in \mathbb{Z}^+, 1 \leq x \leq n, d|x\} \right|$

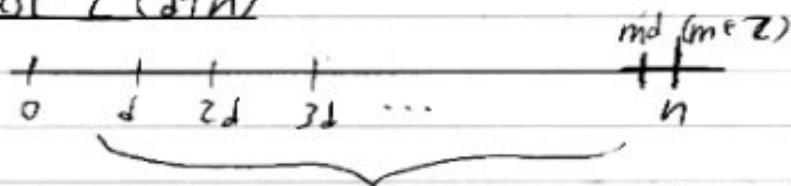
redundant

### Pictures (Optional)

Consider multiples of  $d$   
Case 1 ( $d|n$ )



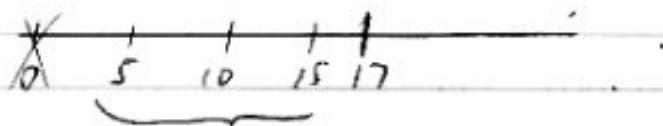
Case 2 ( $d \nmid n$ )



What's  $m$ ?  
It's the highest integer  
such that  
 $md \leq n$  (or  $m \leq \frac{n}{d}$ )  
 $m$  is the highest integer  $\leq \frac{n}{d}$   
So,  $m = \lfloor \frac{n}{d} \rfloor$

In either case, our answer is  $\lfloor \frac{n}{d} \rfloor$ .

Ex How many positive integers not exceeding 17 are divisible by 5?



Answer: 3

$$\lfloor \frac{17}{5} \rfloor = \lfloor \frac{17}{5} \rfloor = \lfloor 3.4 \rfloor = 3$$

Ihm 1 Let  $a, b, c \in \mathbb{Z}$ .

$$\textcircled{1} \quad a|b \text{ and } a|c \Rightarrow a|(b+c)$$

$$\textcircled{2} \quad a|b \Rightarrow \forall c \in \mathbb{Z} \quad a|bc$$

for all  
integers "c"

$$\textcircled{3} \quad a|b \Rightarrow \begin{cases} 3/6, & (c=1) \\ 3/12, & (c=2) \\ 3/18, & (c=3) \\ 3/0, & (c=0) \\ 3/-6, & (c=-1) \\ 3/-12, & (c=-2) \end{cases}, \dots$$

③  $a/b$  and  $b/c \Rightarrow a/c$  (transitivity)

Ex  $3/6$  and  $6/24 \Rightarrow 3/24$

Proof of ①:  $a/b$  and  $a/c \Rightarrow a/(b+c)$

Suppose the condition is true.  
i.e., assume  $a/b$  and  $a/c$ .

(We will show that  $a/(b+c)$  must follow.)

Since  $a/b \Rightarrow \exists s \in \mathbb{Z} (b=as)$

Since  $a/c \Rightarrow \exists t \in \mathbb{Z} (c=at)$



Use a letter other than  $s$ .

$b$  and  $c$  are not

necessarily the same  
multiple of  $a$ ,

(We're asking about  $b+c$ .)

$$b = as \quad \text{Add}$$

$$c = at$$

$$b+c = as + at \quad \text{Distributive Law "in reverse"}$$

$$b+c = a(\underbrace{s+t})$$

This is some integer "u".

$$\Rightarrow \exists u \in \mathbb{Z} (b+c = au)$$

$$\Rightarrow a/(b+c)$$

Short version:

Assume  $a \nmid b$  and  $a \nmid c$ .

$$\Rightarrow \begin{cases} \exists s \in \mathbb{Z} (b = as) \\ \exists t \in \mathbb{Z} (c = at) \end{cases}$$

$$\begin{aligned} \Rightarrow b + c &= as + at \\ \Rightarrow b + c &= a(s + t) \\ &\quad \underbrace{s+t}_{\in \mathbb{Z}} \end{aligned}$$

$$\Rightarrow a \mid (b+c)$$

Prove ②③ in HW #3, 4

### PRIME #s

Assume  $n \in \mathbb{Z}^+, n > 1$ .

$n$  must be divisible by 1 and itself  $(1|n, n|n)$

1 and  $n$  are trivial factors of  $n$ .

$n$  is prime  $\Leftrightarrow n$  has no other divisors (factors)

If  $n$  is not prime, it is composite

0 and 1 are neither prime nor composite.

<u>n</u>	<u>Positive divisors (factors) of n</u>	<u>P=prime C=Composite</u>
2	1, 2	P
3	1, 3	P
4	1, (2), 4	C
5	1, 5	P
6	1, (2, 3), 6	C
7	1, 7	P
8	1, (2, 4), 8	C
9	1, (3), 9	C

odd factor → C

2 is the only even prime.

### Fundamental Theorem of Arithmetic (FTA)

If  $n \in \mathbb{Z}^+$ ,  $n \geq 2$ ,  
then  $n$  is either

- 1) prime, or
- 2) expressible as a product of primes.

This prime factorization is unique up to a reordering of the factors.

$$\text{Ex } 12 = 2 \cdot 2 \cdot 3 = 2 \cdot 3 \cdot 2 = 3 \cdot 2 \cdot 2$$

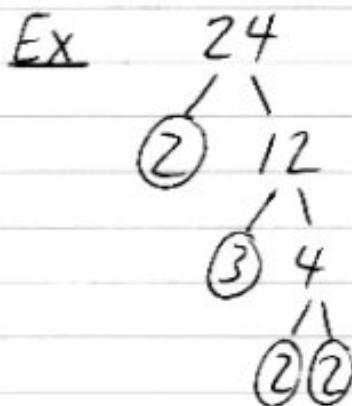
same fac's

$$= 2^2 \cdot 3 \quad \leftarrow \text{exponential notation}$$

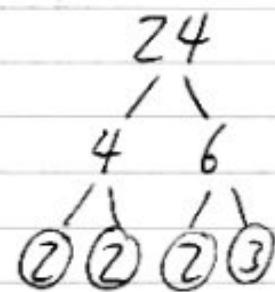
## Factor Tree Method for Finding Prime Fac'n's

Keep splitting factors into smaller factors until all the "leaves" are primes.

Then, the leaves give you the prime fac'n.



$$24 = 2^3 \cdot 3$$



$$24 = 2^3 \cdot 3$$

## Divisibility Tests (aids)

An integer is divisible by...

2  $\Leftrightarrow$  ends in 0, 2, 4, 6, or 8

3  $\Leftrightarrow$  digit sum is divisible by 3

Ex 1431  $\rightarrow$  digit sum is 9  
147,000  $\rightarrow$  12

4  $\Leftrightarrow$  last two digits form a multiple of 4

Ex 35,736  
(100 is div'e by 4)

5  $\Leftrightarrow$  ends in 5 or 0

6  $\Leftrightarrow$  div'e by 2 and 3

7 (no good tricks)

These are div'e  
by 3. What's the  
trick - take a look  
at the digits...

$8 \Leftrightarrow$  last three digits form a multiple of 8

Ex 13, 808

(1000 is divisible by 8)

$9 \Leftrightarrow$  digit sum is divisible by 9

Ex 378  $\rightarrow$  sum digit is 18

$$\begin{array}{r} 9819 \\ 207,000 \end{array} \rightarrow \begin{array}{r} 27 \\ 9 \end{array}$$

$$\begin{array}{r} 207,000 \end{array} \rightarrow \begin{array}{r} 9 \end{array}$$

$10 \Leftrightarrow$  ends in 0

$11 \Leftrightarrow$  alternating sum of digits is divisible by 11

Ex 5467

$$+5 - 4 + 6 - 7 = 0$$

Ex 90,904

$$+9 - 0 + 9 - 0 + 4 = 22$$

Think place value:

$1,100,10000, \dots$  are 1 more than multiples of 11  
 $10,1000, \dots$  less

$12 \Leftrightarrow$  div'ble by 3 and 4

~~If  $m$  and  $n$  are in~~

$n, n \in \mathbb{Z}^+$ .  $m$  and  $n$  are relatively prime if their only common positive factor is 1. Then,  $mn$ -test  $\Leftrightarrow$   $m$ -test and  $n$ -test

Key aid:

If  $n$  is a composite integer,  
then  $n$  has a prime factor  $\leq \sqrt{n}$ .

### Proof

Let  $n$  be a composite integer.

$$\Rightarrow n \text{ has a nontrivial factor } r \quad ((1 < r < n, r \in \mathbb{Z})$$

$$\Rightarrow n = rs$$

$$((1 < s < n, s \in \mathbb{Z}))$$

$$r \leq \sqrt{n} \text{ or } s \leq \sqrt{n}$$

Otherwise,  $r > \sqrt{n}$  and  $s > \sqrt{n}$ .

$$\text{Then, } rs > (\sqrt{n})(\sqrt{n}) = n$$

$$\Rightarrow rs > n$$

This contradicts  $n = rs$ , so this can't happen!

Without loss of generality (w.l.o.g.),  
let's say  $r \leq \sqrt{n}$ .

$$\begin{array}{c} n \\ r \swarrow \searrow \\ (r \leq \sqrt{n}) \end{array}$$

FTA:  
:

Case 1 If  $r$  is prime,  
then  $r$  is our  
desired prime factor  $\leq \sqrt{n}$ .

$p$   
( $p \leq \sqrt{n}$ )

Case 2 Otherwise, by FTA,  
 $r$  has a prime factor  
 $p \leq \sqrt{n}$ .

Contrapositive is true:

If  $n$  does not have a prime factor  $\leq \sqrt{n}$ ,  
then  $n$  is not composite.

$\underbrace{\hspace{10em}}$   
prime  
if  $n \neq 0, 1$

Ex Show that 173 is prime.

Sufficient to show that 173 does not have a prime factor  $\leq \sqrt{173} \approx 13.2$ .

Primes  $p \leq 13$  Does  $p | 173$ ?

2	N
3	N
5	N
7	N (calculator: $\frac{173}{7} \notin \mathbb{Z}$ )
11	N
13	N (calculator $\frac{173}{13} \notin \mathbb{Z}$ )

So, 173 is prime.

Sieve of Eratosthenes

find the prime #'s up to a certain #.

Ex for #'s up to 40, run through the multiples of 2, 3, and 5 and eliminate them (except 2, 3, and 5, themselves)

Overheads

Ex find the prime fac'n of 4575.

$$\begin{array}{c} 4575 \\ \swarrow \quad \searrow \\ 25 \quad 183 \\ \swarrow \quad \searrow \\ 5 \quad 3 \quad 61 \end{array}$$

Verify that 61 is prime

$$\sqrt{61} \approx 7.8$$

$$\begin{array}{r} 2 \nmid 61 \\ 3 \nmid 61 \\ 5 \nmid 61 \\ 7 \nmid 61 \end{array}$$

$$\begin{aligned} 4575 &= 3 \cdot 5 \cdot 5 \cdot 61 \\ &= 3 \cdot 5^2 \cdot 61 \end{aligned}$$

Cryptography - primality testing, factoring

Mersenne primes - primes of the form  $2^p - 1$ .

Great Internet Mersenne Prime Search (GIMPS)

More info: pp. 116-7, Rosen's Web page

116 Web  
Chm (abt 11)

Largest prime so far:

6/1/1999:  $2^{6,972,583} - 1$  ← 38<sup>th</sup> Mersenne prime

has 2M digits (2,098,960)

Previous one only had 909,526 digits. (1998)

19c: #primes  $\leq n \rightarrow \log n$  (Prime Number Thm.)  
1792-stated by Gauss  
1846-proven

So,  $n^{\text{th}}$  prime  $\approx n \log n$

GCDs and LCMs

Let  $a, b \in \mathbb{Z}$  (not both 0)

$\text{gcd}(a, b) =$  greatest common divisor of  $a$  and  $b$   
 $=$  the largest integer that divides  $a$  and  $b$   
 $= \max \{d \in \mathbb{Z} : d | a \text{ and } d | b\}$   
 (Used to reduce fractions)

Ex  $\text{gcd}(90, 100) = 10$

Ex  $\text{gcd}(24, 48) = 24$

Ex  $\text{gcd}(13, 14) = 1$

✓  
relatively prime  $\Leftrightarrow \text{gcd} = 1$

Let  $a, b \in \mathbb{Z}^+$ .

$\text{lcm}(a, b) =$  least common multiple of  $a$  and  $b$   
 $=$  the smallest positive integer  
 divisible by  $a$  and  $b$   
 $= \min \{m \in \mathbb{Z}^+ : a|m \text{ and } b|m\}$   
 (Used to find the LCD.)

Ex  $\text{lcm}(8, 9) = 72$

If  $a, b$  are relatively prime,  
 $\text{lcm}(a, b) = ab$

Ex  $\text{lcm}(4, 12) = 12$

Ex  $\text{lcm}(6, 10) = 30$

## Finding GCDs and LCMs Using Prime Factors

Ex. Find  $\gcd(200, 1500)$

$$\begin{array}{rcl} 200 & = & 2^3 \cdot 5^2 \\ 1500 & = & 2^2 \cdot 3 \cdot 5^3 \end{array}$$

↑ Prime factors  
from factor trees.

Put in 0, 1 exponents:

$$\begin{array}{rcl} 200 & = & 2^3 \cdot 3^0 \cdot 5^2 \\ 1500 & = & 2^2 \cdot 3^1 \cdot 5^3 \\ \hline \gcd & = & 2^2 \cdot 3^0 \cdot 5^2 \\ & = & \boxed{100} \end{array}$$

← for each prime,  
take the smaller  
exponent

In general, to find  $\gcd(a, b)$ :

Find the prime factors of  $a$  and  $b$ .

Let  $p_1, p_2, \dots, p_n$  be the primes that appear in the prime factor of  $a$  or  $b$ .

$$\begin{array}{l} \text{Let } a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} \\ \quad \quad b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n} \end{array} \quad \left\{ \begin{array}{l} a_i, b_i \in \mathbb{Z}^{>0} \end{array} \right.$$

$$\text{Then, } \gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)}$$

$$\begin{aligned} \text{Here, } \gcd(200, 1500) &= 2^{\min(3, 2)}, 3^{\min(0, 1)}, 5^{\min(2, 3)} \\ &= 2^2 \cdot 3^0 \cdot 5^2 \\ &= \boxed{100} \end{aligned}$$

Ex Find  $\text{lcm}(200, 1500)$

$$\begin{aligned} 200 &= \underline{2^3} \cdot 3^0 \cdot 5^2 \\ 1500 &= 2^2 \cdot \underline{3^1} \cdot \underline{5^3} \\ \text{lcm} &= 2^3 \cdot 3^1 \cdot 5^3 \\ &= \boxed{3000} \end{aligned}$$

← for each prime, take the larger exponent

In general, to find  $\text{lcm}(a, b)$ :

same as finding  $\text{gcd}(a, b)$ , except

$$\text{lcm}(a, b) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \dots p_n^{\max(a_n, b_n)}$$

If  $a, b \in \mathbb{Z}^+$ , then  $ab = \text{gcd}(a, b) \cdot \text{lcm}(a, b)$   
 (HW #33)

### Special Case

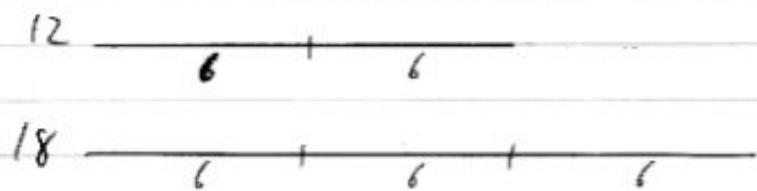
If  $a, b$  are relatively prime

$$\begin{aligned} \text{gcd}(a, b) &= 1 \\ \text{lcm}(a, b) &= ab \end{aligned}$$

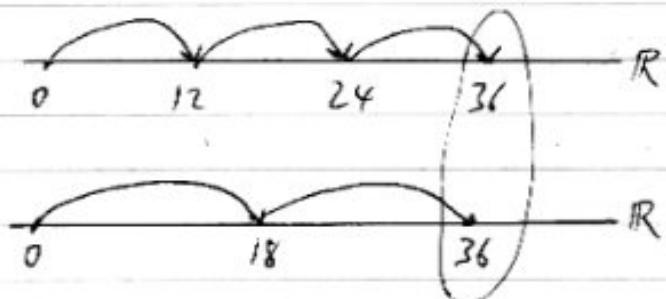
product =  $ab$

Pictures

$$\gcd(12, 18) = 6$$



$$\text{lcm}(12, 18) = 36$$



THE DIVISION "ALGORITHM"

55 is divisible by 5, because

$$55 = 5 \cdot 11$$

57 is not

$$\begin{array}{r} 11 R 2 \\ 5 / 57 \\ -5 \\ \hline 07 \\ -5 \\ \hline 2 \end{array} \quad \begin{array}{r} 57 = 5 \cdot 11 + 2 \\ \uparrow \quad \uparrow \quad \leftarrow \quad \leftarrow \\ \text{dividend} \quad \text{divisor} \quad \text{quotient} \quad \text{remainder} \\ = \lfloor \frac{57}{5} \rfloor \quad (\text{must be } 0, 1, 2, 3, \text{ or } 4 \\ = (11, 4) \quad \text{when } \div \text{ by } 5) \\ \hline \underbrace{1}_{\text{quotient}} \underbrace{2}_{\text{remainder}} \end{array}$$

(i.e.,  $r \in \mathbb{Z}, 0 \leq r < 5$ )

Let  $a \in \mathbb{Z}, d \in \mathbb{Z}^+$

Then, there are unique  $q, r \in \mathbb{Z}$  ( $0 \leq r < d$ ) such that  $a = dq + r$

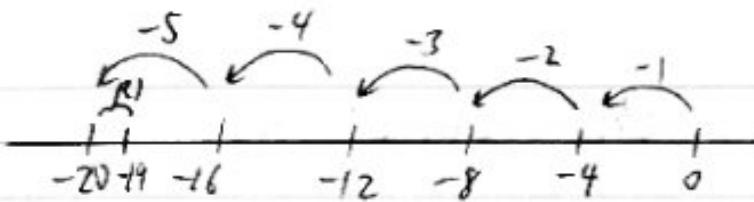
$$d/a \Leftrightarrow r=0$$

↓ dividend (given)    ↓ divisor (given)    ↓ quotient  $= \lfloor \frac{a}{d} \rfloor$     ↓ remainder

Ex What are the quotient and remainder when  $-19$  is divided by  $4$ ?

$$\begin{aligned} \text{quotient} &= \lfloor \frac{-19}{4} \rfloor = \lfloor -4.75 \rfloor = -5 \\ \text{remainder} &= a - dq = -19 - (-5 \cdot 4) \\ -19 &= (4)(-5) + 1 \\ &\quad \overbrace{-20}^{\text{remainder}} \end{aligned}$$

$$q = -5, r = 1$$



Next: Classify integers according to their remainders when you divide by a given divisor.

Ex divisor = "modulus" = 5

Imagine wheel spokes:

$$(R0) \equiv 0 \pmod{5}$$

$$\begin{matrix} 10 \\ | \\ 5 \\ | \\ 0 \end{matrix}$$

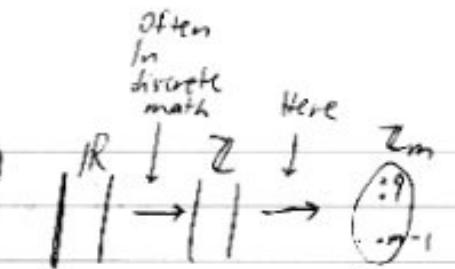
$$\equiv 4 \pmod{5} \quad (R4) \quad 14 \quad 9 \quad 4 \quad -1 \quad (-4) \quad 1 \quad 6 \quad 11 \quad (R1) \equiv 1 \pmod{5}$$

$$\begin{matrix} & -2 & -3 \\ 3 & & 2 \end{matrix}$$

$$\begin{matrix} 8 \\ | \\ 13 \\ (R3) \\ \equiv 3 \pmod{5} \end{matrix}$$

$$\begin{matrix} 7 \\ | \\ 12 \\ (R2) \\ \equiv 2 \pmod{5} \end{matrix}$$

5 congruence classes

MODULAR ARITHMETIC (Gauss)

(a) in notation

Let  $a \in \mathbb{Z}, m \in \mathbb{Z}^+$ .Then,  $a \bmod m$  = the remainder when  $a$  is divided by  $m$ 

$$\text{Ex } 11 \bmod 5 = 1$$

$$11 = 5 \cdot 2 + 1$$

$\begin{array}{r} 1 \\ 9 \\ \hline 5 \\ \hline 1 \end{array}$

$$\text{Ex } -1 \bmod 5 = 4$$

$$\text{Ex } 978 \bmod 7 = ?$$

$$\left\lfloor \frac{978}{7} \right\rfloor = 139, \quad 139 \times 7 = 973$$

largest multiple of  
 $7 \leq 978$

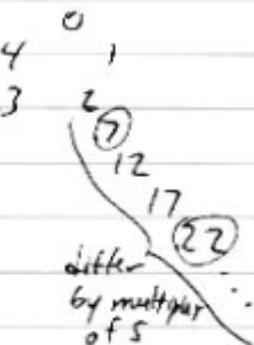
$$r = 978 - 973 = 5.$$

Let  $a, b \in \mathbb{Z}, m \in \mathbb{Z}^+$ . $a$  is congruent to  $b$  modulo  $m$ , or " $a \equiv b \pmod{m}$ " $\Leftrightarrow a \bmod m = b \bmod m$  ( $a, b$  have same  $r$  when  $\div$  by  $m$ ) $\Leftrightarrow m \mid (a-b)$  $\Leftrightarrow \exists k \in \mathbb{Z} (a-b=km) \quad (\text{A}) \quad (\text{spokes: } a, b \text{ can differ by some multiple of } m)$ 

$$\text{Ex } 7 \equiv 2 \pmod{5} \quad \left. \begin{array}{l} 7 \equiv 22 \pmod{5} \\ 22 \equiv 2 \pmod{5} \end{array} \right\} \Rightarrow$$

$$\text{Also: } 5 \mid \overbrace{22-7}^{15}$$

$$\text{Ex } 7 \not\equiv 23 \pmod{5}$$



Prove  $a \equiv b \pmod{m} \Leftrightarrow \exists k \in \mathbb{Z} (a = b + km)$ . (A)

$$\begin{aligned}
 & a \equiv b \pmod{m} \\
 \Leftrightarrow & m \mid (a - b) \\
 \Leftrightarrow & \exists k \in \mathbb{Z} (a - b = km) \\
 \Leftrightarrow & \exists k \in \mathbb{Z} (a = b + km)
 \end{aligned}$$

To be on the same  
spoke,  $a$  and  $b$   
can differ by a  
multiple of  $m$ .

Post-train?  
 Knuth 2/2  
 So,  $a \equiv b \pmod{m}$   
 $\Rightarrow a^2 \equiv b^2 \pmod{m}$   
 $\Leftrightarrow a^2 + b^2 \in \mathbb{Z}$   
 $\Leftrightarrow a^2 + b^2 \equiv 0 \pmod{m}$

If  $a \equiv b \pmod{m}$ , and  
 $c \equiv d \pmod{m}$ , then

$$\begin{aligned}
 a+c &\equiv b+d \pmod{m}, \text{ and} \\
 ac &\equiv bd \pmod{m}
 \end{aligned}$$

(Proofs helpful for HW) p.122 P. 0 +

(mod 3)  
 better  
 do  $6 \times 15$

Ex  $9 \equiv 2 \pmod{7}$

$12 \equiv 5 \pmod{7}$

$$\Rightarrow 9+12 \equiv 2+5 \pmod{7}$$

$$21 \equiv 7 \pmod{7} \quad \checkmark$$

$$\begin{array}{c}
 1+7 \pmod{7} \\
 8 \pmod{7} \\
 \odot 9 \\
 \hline
 2 \pmod{7}
 \end{array}$$

Only the  
remainders matter  
as far as spokes go.

In general,

$$\begin{array}{c}
 5 \pmod{7} \\
 \downarrow \\
 2 \pmod{7}
 \end{array}$$

$$108 \equiv 10 \pmod{7} \quad \checkmark \quad (\text{Both } \equiv 3 \pmod{7})$$

x picture

## APPLICATIONS

### Hashing functions

Storing records that are uniquely identified by a key "k" (e.g., SSN).

#### Division Method:

$$h(k) = k \bmod m$$

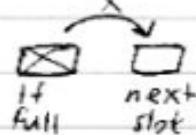
memory location                          # memory locations

"Folding" the list of possible SSNs.

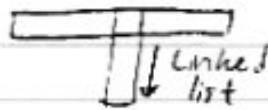
We might get collisions!

#### Resolutions

##### ① Rassen: Linear probing



##### ② Separate chaining



Requires dynamic memory allocation.

Ex Pseudorandom #s (games, simulations, ...)

We want a sequence of  
"random" #s between 0,1.

Most computers use the linear congruential method.

Seed  $x_0$

Recursive def'n:

$$x_{n+1} = (ax_n + c) \pmod{m}$$

Output:  $\frac{x_0}{m}, \frac{x_1}{m}, \frac{x_2}{m}, \dots$

Ex Cryptology

Do p/122 proofs?

2.4:  $\mathbb{Z}$  AND ALGORITHMSEUCLIDEAN ALGORITHM

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

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  $a = bq + r$ .

↑      ↑  
quotient    remainder  
 $0 \leq r < b$

$$\text{Ex } 57 = 5 \cdot 11 + 2$$

Lemma (subresult needed for something bigger)

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

$$\begin{array}{c} \text{gcd} \\ \textcircled{a} = \textcircled{b}q + \textcircled{r} \\ \text{gcd} \end{array}$$

$$\begin{array}{c} a = \textcircled{b}q + \textcircled{r} \\ \text{gcd} \end{array}$$

Ex find  $\gcd(88, 16)$

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

$$\begin{array}{c} \text{gcd} \\ \swarrow \quad \searrow \\ 88 = 16 \cdot 5 + 8 \end{array}$$

$$88 = 16 \cdot 5 + 8 \quad 88 \bmod 16$$

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

Recursive definition for gcd:

$$\begin{aligned} \gcd(a, b) &= \gcd(b, a \bmod b) && \leftarrow \text{shrink problem} \\ \gcd(a, 0) &= a && \leftarrow \text{"base case"} \end{aligned}$$

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 <sup>fin.</sup> set.

Show  $X = Y$ .

$$X \subseteq Y$$

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

$$\begin{aligned} a &= bq + r \\ \Rightarrow a - bq &= r \\ \Rightarrow r &= a - bq \quad \left. \begin{array}{l} \uparrow \quad \uparrow \\ d \mid a \quad d \mid b \end{array} \right\} 2.3 \\ \Rightarrow d &\mid r \end{aligned}$$

$$Y \subseteq X$$

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

$$\begin{aligned} a &= bq + r \\ &\quad \left. \begin{array}{l} \uparrow \quad \uparrow \\ d \mid b \quad d \mid r \end{array} \right\} 2.3 \\ d &\mid a \end{aligned}$$

QED

Ex Find  $\gcd(658, 104)$

$$\begin{aligned} 658 &= 104 \cdot 6 + 34 & \downarrow \gcd(104, 34) \\ 104 &= 34 \cdot 3 + 2 & \downarrow \gcd(34, 2) \\ 34 &= 2 \cdot 17 + 0 & \downarrow \gcd(2, 0) \\ & & = 2 \quad \text{last nonzero remainder} \end{aligned}$$

$$\gcd(658, 104) = 2$$

What's  $\text{lcm}(658, 104)$ ?

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

Knuth SIS

$$\begin{aligned} \text{lcm}(a, b) &= \frac{ab}{\gcd(a, b)} \\ &= \frac{ab}{a \text{ mod } b, b} \end{aligned}$$

Easiest way is through the E.A.!

## BINARY REPRESENTATIONS OF INTEGERS

We normally use decimal (base-10) notation

$$4032 = \underbrace{(4032)}_{\leftarrow}{}_{10}$$

$$\begin{aligned} &= 2 \times 10^0 \\ &\quad + 3 \times 10^1 \\ &\quad + 0 \times 10^2 \\ &\quad + 4 \times 10^3 \end{aligned}$$

Polish  
computer  
base 3,  
— closer  
to e)  
so  
 $(\$11)_2$

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

$$\begin{aligned} \underbrace{(101011)}_{\leftarrow}{}_2 &= 1 \times 2^0 &= 1 &= (43)_{10} \\ &\quad + 1 \times 2^1 &+ 2 & \\ &\quad + 0 \times 2^2 && \\ &\quad + 1 \times 2^3 &+ 8 & \\ &\quad + 0 \times 2^4 && \\ &\quad + 1 \times 2^5 &+ 32 & \end{aligned}$$

Decimal → Binary (different from lesson)

$(43)_{10}$       What is the highest power of 2  
                   that is  $\leq 43$ ?  
 $32 = 2^5$

<u>bit Position</u>	<u>bit</u>	<u>Remainder</u>
<u>Value (PV)</u>	<u>Bit = 1 if <math>PV \leq \text{remainder}</math></u>	<u>start with 43.</u>
	<u>Bit = 0 otherwise</u>	<u><math>\rightarrow</math> If Bit = 1, rem. <math>\leftarrow</math> rem. - PV</u>
		<u><math>\rightarrow</math> If Bit = 0, keep rem</u>
$2^5 = 32$	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, ..., 9,  $A_{10}, B_{11}, C_{12}, D_{13}, E_{14}, F_{15}$

$$\begin{aligned} \text{Ex } \underline{(2B)}_{16} &= 8 \times 16^0 + 2 \times 16^1 \\ &= 11 \times 1 + 2 \times 16 \\ &= (43)_{10} \end{aligned}$$

## 2.5

Thm 1 If  $a, b \in \mathbb{Z}^+$ , then

$\exists s, t \in \mathbb{Z}$  such that  $\gcd(a, b) = sa + tb$

some linear combination of  $a, b$  w/ integer coeffs

$$\text{Ex } \gcd(14, 10) = 2$$

$$\text{So, } 2 = 14s + 10t$$

$\checkmark \in \mathbb{Z}$  (multipliers)

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

$$\begin{aligned} 14 &= 10 \cdot 1 + 4 && \xrightarrow{\text{Solve for } r} 4 = 14 - 10 \cdot 1 \\ 10 &= 4 \cdot 2 + 2 && \Rightarrow 2 = 10 - 4 \cdot 2 \end{aligned} \quad \text{reusing}$$

$$2 = 10 - 4 \cdot 2$$

$$2 = 10 - (14 - 10 \cdot 1) \cdot 2$$

$$2 = 10 - 14 \cdot 2 + 10 \cdot 2$$

$$2 = 14(-2) + 10(3)$$

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:

$$\begin{array}{ll} ax = b & (a \neq 0) \\ \left(\frac{1}{a}\right)ax = \left(\frac{1}{a}\right)b & \left(\frac{1}{a}\right) \text{ is the multiplicative inverse of } a \\ x = \frac{b}{a} & \left(\frac{1}{a} \cdot a = 1\right) \end{array}$$

Here,

Thm 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.

$\bar{x} \pmod{5}$

$$\begin{array}{ccccccc} -4 & & 1 & & 1 & & 1 \\ & \swarrow & & & \searrow & & \\ & 3 & & 2 & & 1 & \end{array}$$

i.e., there is exactly one congruence  
class  $(\bmod m)$  of multiplicative  
inverses for  $a \pmod{m}$ .

Ex Solve  $3x - 1 \equiv 1 \pmod{5}$

$$\Leftrightarrow 3x \equiv 2 \pmod{5}$$

Can +, - same # on both sides.

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

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

$$\begin{aligned} 5 &= 3 \cdot 1 + 2 \Rightarrow 2 = 5 - 3 \cdot 1 \\ 2 &= 3 \cdot 1 + 1 \Rightarrow 1 = 2 - 3 \cdot 1 \end{aligned}$$

$$\begin{aligned} 1 &= 3 - 2 \cdot 1 \\ 1 &= 3 - (5 - 3 \cdot 1) \cdot 1 \\ 1 &= 3 - 5 + 3 \\ 1 &= 3(2) + 5(-1) \quad \leftarrow \text{Thm! form} \end{aligned}$$

$$1 \equiv 3(2) + 5 \cancel{(-1)} \pmod{5}$$

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

= quantities  
have the  
same  
remainder

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

↑  
an inverse!

$$\begin{aligned} \text{Inverse class} &= \{n \in \mathbb{Z} \mid n \equiv 2 \pmod{5}\} \\ &= \{\dots, -8, -3, 2, 7, 12, \dots\} \end{aligned}$$

Solve  $3x \equiv 2 \pmod{5}$

OK to mult.  
by inverse

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

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

$$\begin{array}{l|l} 6 \equiv 1 \pmod{5} & \text{You can replace} \\ 6x = x + 5x & \text{it with other} \\ \Leftrightarrow x \equiv 4 \pmod{5} & \text{members in the} \\ & \text{same class!} \end{array} \quad \begin{array}{l} \text{In} \\ \text{context} \end{array} \equiv 4 \pmod{5} \quad // \quad // \quad //$$

$$\begin{aligned} \text{Solution set} &= \{x \in \mathbb{Z} \mid x \equiv 4 \pmod{5}\} \\ &= \{ \dots, -6, -1, 4, 9, 14, \dots \} \end{aligned}$$

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

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

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

$$\text{defined by } f([a]_6) = ([a]_2, [a]_3)$$

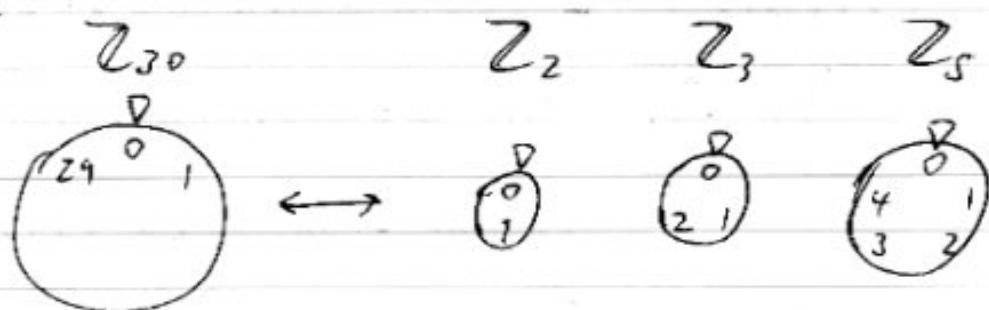
<u><math>\mathbb{Z}_6</math></u>	<u><math>\mathbb{Z}_2 \times \mathbb{Z}_3</math></u>
$[0]_6$	$([0]_2, [0]_3)$
$[1]_6$	$([1]_2, [1]_3)$
$[2]_6$	$([0]_2, [2]_3)$
$[3]_6$	$([1]_2, [0]_3)$
$[4]_6$	$([0]_2, [1]_3)$
$[5]_6$	$([1]_2, [2]_3)$

$\mathbb{Z}_6 \leftrightarrow \mathbb{Z}_2 \times \mathbb{Z}_3$   
 1-1 corresp

f turns out to be a bijection!

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

Ex



This means that the system

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

$$x \equiv a_n \pmod{m_n}$$

has a unique solution  $(\text{mod } m)$

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

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

### Application

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

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