CS 40
FOUNDATIONS OF CS

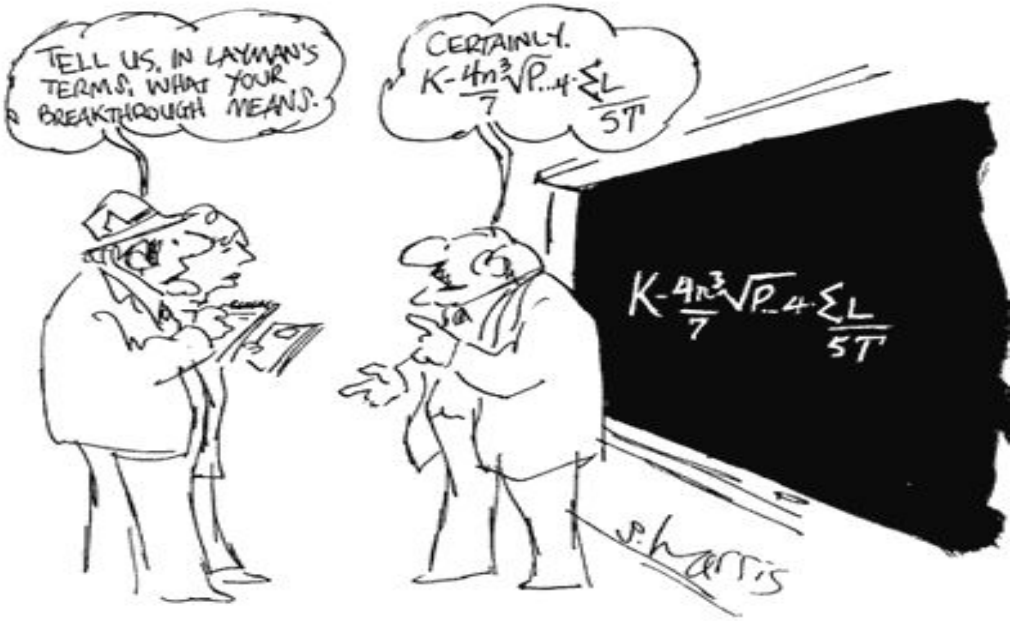
Summer 2024
Session A
Week ~~2 & 3~~ 4

Learning goals

Netflix example: tuples.

→ Represent Numbers?

Multiple Representations



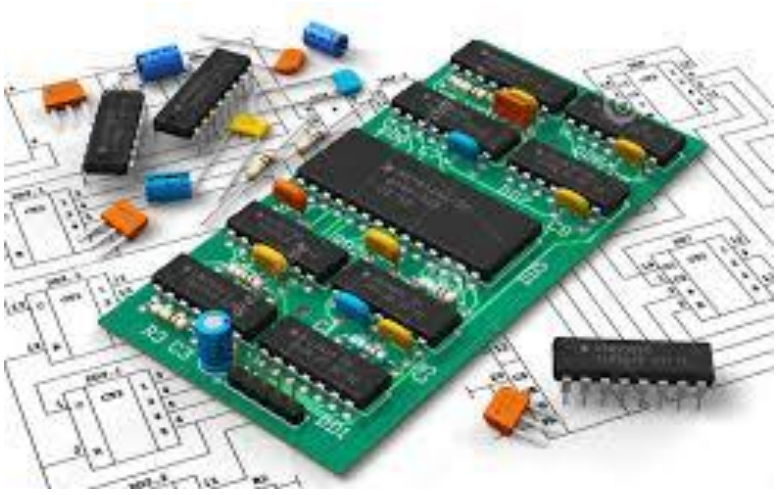
Thursday's learning goals

- Represent numbers in different ways (base expansions and prime factorization)
- Define the base expansion of a positive integer, specifically decimal, binary, hexadecimal, and octal.
- Convert between expansions in different bases of a positive integer.
- Define and use the **div** and **mod** operators.
- Trace an algorithm specified in pseudocode.
- Another way of representing numbers (prime factorization)

Integer representations

Different contexts call for different representations.

Base 10



Base 2

Base b expansion of n

zyBook 6.3, Rosen p. 246

Also known as **positional representation** of positive integers

Definition (Rosen p. 246) For b an integer greater than 1 and n a positive integer, the **base b expansion of n** is

$$(a_{k-1} \cdots a_1 a_0)_b$$

where k is a positive integer, $a_0, a_1, \ldots, a_{k-1}$ are nonnegative integers less than b, $a_{k-1} \neq 0$, and

$$n = a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$$

Alternatively, the base b expansion of n is a string over the alphabet $\{x \in \mathbb{N} \mid x < b\}$ and whose leftmost character is nonzero.

Base b expansion

In what base **could** this expansion be

$(1401)_?$

A. Binary (base 2) → each digit should be 0 or 1

B. Octal (base 8)

C. Decimal (base 10)

D. Hexadecimal (base 16)

E. More than one of the above

say $(1101)_2 = 1\times2^0 + 0\times2^1 + 1\times2^2 + 1\times2^3$

$= 1 + 4 + 8$

$= 13$

$(1401)_8$

$= 1\times8^0 + 4\times8^2 + 1\times8^3$

$= 1 + 4\times64 + \underbrace{64\times8}_{512}$

Base b expansion

In what base **could** this expansion be

$(1401)_?$

A. Binary (base 2)

B. Octal (base 8) $(1401)_8 = 1*8^3+4*8^2+1=(769)_{10}$

C. Decimal (base 10) $(1401)_{10} =1*10^3+4*10^2+1=1401$

D. Hexadecimal (base 16) $(1401)_{16} =1*16^3+4*16^2+1=5121$

E. More than one of the above

Ternary representation of 17

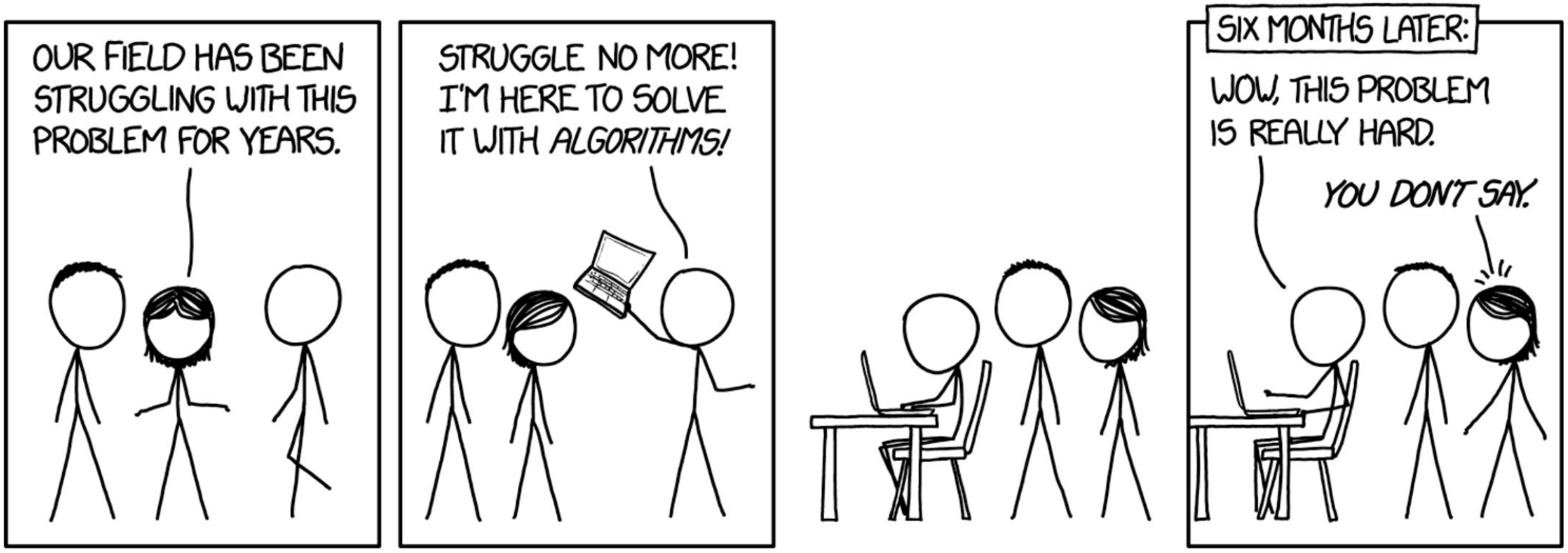
A. $(17)_3$
B. $(211)_3$
C. $(122)_3$ ✓
D. $(221)_3$
E. $(112)_3$

$= 2 \times 3^0 + 2 \times 3^1 + 1 \times 3^2 = 2 + 6 + 9 = 17$

we are the rep

But do we directly find the rep?

Converting between bases

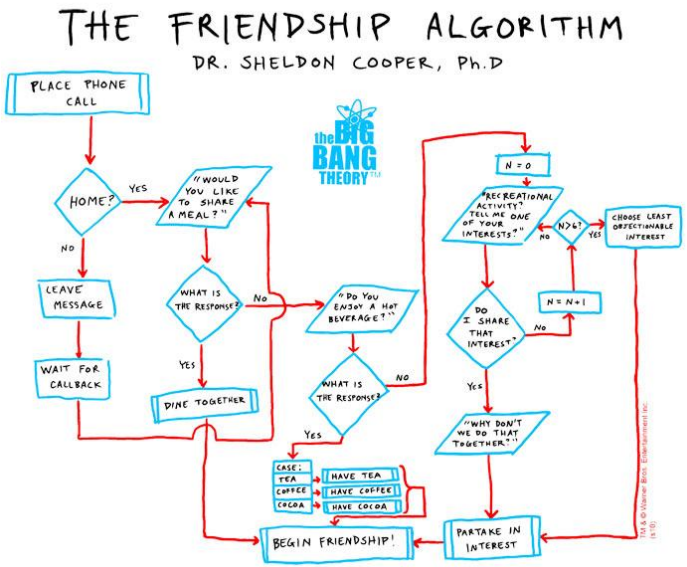


xkcd

Algorithm?

zyBook 6.1, Rosen 3.1 p. 191,

Finite sequence of precise instructions for solving problem.



Algorithm: Pseudocode

Notation: zyBook 6.1

Finite sequence of precise instructions for solving problem.

```
1  procedure log(n: a positive integer)
2  r := 0
3  while n > 1
4    r := r + 1
5    n := n div 2
6  return r {r holds the result of the log operation}
```

procedure name

i/p for the procedure

align

return i/p statement

o/p specification

:= define

r := 0 → r is set to 0

code: r=0 → r is set to 0

r == 0 → is r equal to 0?

At the end of running *log(6)* what values are in the variables *r* and *n*?

A. r = 6, n = 0
B. r = 6, n = 6
C. r = 2, n = 0
D. r = 2, n = 1
E. None of the above.

What is this algorithm doing?

→ Do a run through the pseudocode

n	r	n>1?
6	0	yes
3	1	yes
1	2	NO

= ⌈log 6⌉ ← returned r

does the algorithm return:

a) $\log n$

b) $\lceil \log n \rceil$ ← ceil ← round up

c) ~~$\lfloor \log n \rfloor$~~ ← floor ← round down

Algorithm: constructing base b expansion

Input n,b **Output** k, coefficients in expansion

- English description.

Alg 2: $17 \cdot 1/3 = \boxed{2}$ $17/3 = 5$ $5 \cdot 1/3 = \boxed{2}$ $5/3 = 1$ $1 \cdot 1/3 = \boxed{1}$

a_0 a_1 a_2

$(17)_3 \hookrightarrow (122)_3$

$a_2 a_1 a_0$

- Pseudocode.

Alternate greedy alg:

Think of filling buckets greedily

→ $\log n$ → we know how to compute $\lfloor \log n \rfloor$

Given n, b → what can be the max i s.t the coeff of 2^i is non zero in the $\left[\exp_b n\right]$

$$a_i \times 2^i + \ldots + a_2 \times 2^2 + a_1 \times 2^1 + a_0 \times 2^0$$

↳ what is the max possible i s.t $a_i \neq 0$ · ↳ $\lfloor \log_b n \rfloor$

$n = 6$

$b = 2$

$\lfloor \log_2 6 \rfloor = 2$

can a_3 be non zero.

$a_3 \cdot 2^3$

↓

can this be > 0 ?

$2^{\lfloor \log_b n \rfloor + 1} > n$ *

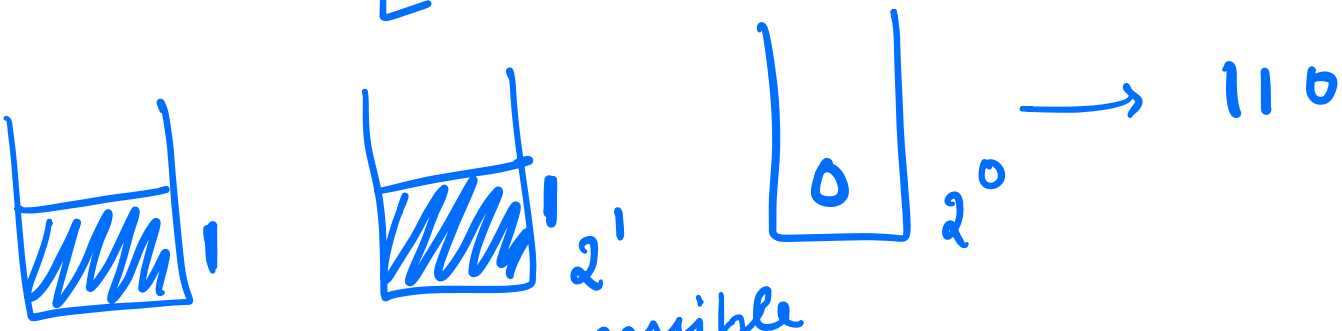
Compute the expansion left to right:

$$a_k\, a_{k-1} \cdots a_2\, a_1\, a_0$$

for $i = \lfloor \log_b n \rfloor$ to 0

set a_i to maximum possible

$n = 6, \; b = 2 \quad \lfloor \log_2 6 \rfloor = 2$



$\longrightarrow$ 1 1 0

fill 2^2 as much as possible

$= 4$

n

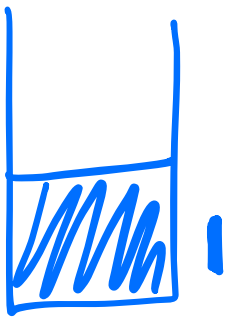
$n = 6 - 4 = 2$

$n = 2 - 2 = 0$

$(17)_3$

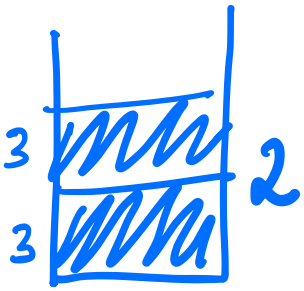
$n = 17$, $b = 3$

$\lfloor \log_b n \rfloor = \lfloor \log_3 17 \rfloor = 2$



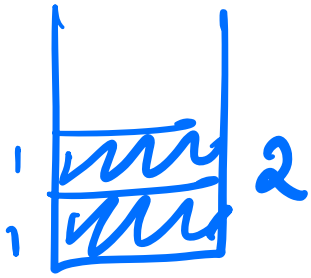
$3^2 = 9$

$17/9 = 1$



$3^1 = 3$

$n = 17 - 9 = 8$



$3^0 = 1$

$n = 8 - 6 = 2$

$(122)_3$

Algorithm 1: constructing base b expansion

Input n,b **Output** k, coefficients in expansion

- English description.

Initialize value remaining to be n

Find biggest power of b that is less than or equal to value remaining.

Increment appropriate coefficient.

Update value remaining by subtract this power of b from it.

Repeat until value remaining is 0.

Algorithm 1: constructing base b expansion

Calculating base b expansion, from left

```
1  procedure baseb1(n, b: positive integers with b > 1)
2  v := n
3  k := logb(n, b) + 1
4  for i := 1 to k
5     a_{k-i} := 0
6     while v ≥ b^{k-i}
7        a_{k-i} := a_{k-i} + 1
8        v := v − b^{k-i}
9  return (a_{k-1}, ..., a_0){(a_{k-1} ... a_0)_b is the base b expansion of n}
```

$k = \lfloor \log_b n \rfloor + 1$

for i = 1 to k

k-i : k-1 to 0

$\lfloor \log_b n \rfloor$

$a_{k-i} = 0$ → initially coeff is 0

a_{k-1} is coefficient of biggest power of b that is less than n
Thus: k is 1 more than integer part of $\log_b n$

Trace the pseudo code for:

$n = 17$

$b = 3$

$k = \lfloor \log_b n \rfloor + 1$

$= \lfloor \log_3 17 \rfloor + 1 = 2 + 1 = 3$

$v = n = 17$

$\boxed{k = 3}$

for $i = 1$ to 3

i	k-i = 3-i	a_{k-i}	v
1	2	1	8
2	1	2	2
3	0	2	0

$(1\ 2\ 2)_3$ output

$a_{k-i} = 1$

$v = 8$

$v > 3^{k-i}$

$= 3^2$

$8 >= 9$ X

$a_1 = 0$

$a_1 = 1$

$v = 8 - 3$

$= 5$

$v > 3$

$a_2 = 2$

$v = 5 - 3$

$= 2$ $\quad 2 > 3$ X

0 | 17

1 | $17 - 3^2$

$+ 9$

8

Algorithm 2: constructing base b expansion

Input n,b **Output** k, coefficients in expansion

Idea: Find smallest digit first, then next smallest, etc.

…. **but how?**

Rosen p. 249

Bases and Divisibility

zyBook 6.2-6.3, Rosen p. 237-239

Division algorithm: For n an integer and d a positive integer, there are unique integers q and r with $0 \le r < d$ and $n = dq + r$. *(zyBook 5.2)*

Notation: $q = n$ **div** d and $r = n$ **mod** d

rounding down

q: quotient → reminder

When k>1

$$n = a_{k-1}b^{k-1} + \ldots + a_1 b + a_0$$

$$n = b(a_{k-1}b^{k-2} + \ldots + a_1) + a_0$$

d

$q = n$ div d

$q = n$ div b

$r = n$ mod b

$r = n$ mod d

$$q = a_{k-1} b^{k-2} + \cdots + a_2 b + a_1$$

$$b\left(a_{k-1} b^{k-3} + \cdots + a_2\right) + a_1$$

q div b $\qquad$ q mod b

Algorithm 2: constructing base b expansion

Input n,b **Output** k, coefficients in expansion

Idea: Use n **mod** b to compute least significant digit.

Use n **div** b to compute new integer whose expansion we need. Repeat.

Algorithm 2: constructing base b expansion

2nd algorithm

Calculating base b expansion, from right

```
1  procedure baseb2(n,b: positive integers with b>1)
2  q := n
3  k := 0
4  while q ≠ 0
5     a_k := q mod b
6     q := q div b
7     k := k+1
8  return (a_{k-1},...,a_0){(a_{k-1},...,a_0)_b is the base b expansion of n}
```

$17 = (1\,2\,2)_3$

n	b	q	k	a_k	$q \neq 0$?
17	3	17	0	2	NO
	3	5	1	2	NO
	3	1	2	1	NO
		0			YES ✓

$a_2 = 1 \bmod 3 = 1$

$a_k = 17 \bmod 3 = 2$

$q = 17 \operatorname{div} 3 = 5$

$a_1 = 5 \bmod 3 = 2$

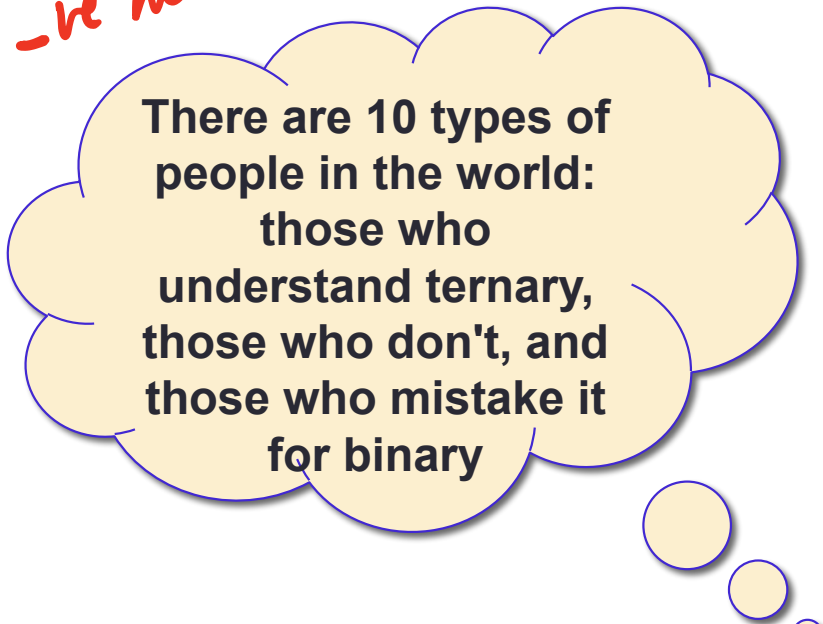
$q = 5 \operatorname{div} 3 = 1$

q = 1 div 3 = 0

Representing more

- Base b expansions can express any **positive integers**

- What about
  - Zero?
  - negative integers? → Exercise (think about -ve numbers :))
  - rational numbers?
  - other real numbers?



Bases and Divisibility

zyBook 6.2-6.3, Rosen

p. 237-239

Division algorithm: For n an integer and d a positive integer, there are unique integers q and r with $0 \le r < d$ and $n = dq + r$. (*zyBook 5.2*)

Notation: $q = n$ **div** d and $r = n$ **mod** d

What is result of each of the following?

11 div 4 = 2

11 mod 4 = 3

-11 div 4 = -3 → div still a smaller integer

$-11 = -3 * 4 + 1$

$= -12 + 1$

$= -11$

-11 mod 4 = 1

-11 div -4 X

-11 mod -4 X → usually not used (div: integral div)

$-11/4 = -2.75$

↓ integral div = -3

$-11/-4 = 11/4 = 2.75$

Tuesday's learning goals

- Another way of representing numbers (prime factorization)
- Calculating greatest common divisor of two numbers in multiple ways (prime factorization and Euclid's algorithm)
- Modular Arithmetic and applications
- Finding the inverse of a number mod n

A different way to represent positive integers

Fundamental Theorem of Arithmetic: Every positive integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of nondecreasing size.

which of these fit the theorem

Let's try some example prime factorizations. Which of these match the definitions?

A. 3 = 3
B. 100 = (1)(2)(2)(5)(5)
C. 20 = (4)(5)
D. 9 = (3)(3)
E. All of the above.

1 is neither prime nor composite

non decreasing

(1)(3)(5) ?

(3)(1)(0) ?

(1)(2)(2)(3)(5) ?

Greatest common divisor

- **Definition**: Let *a* and *b* be integers, not both zero. The largest positive integer *d* such that *d* | *a* and also *d* | *b* is called the greatest common divisor of *a* and *b*. The greatest common divisor of *a* and *b* is denoted by gcd(*a*,*b*).

- gcd(24, 36) = ? 12
- gcd(17,22) = ? 1

Finding gcd using prime factorization

- $24 = 2^3 \cdot 3$
- $36 = 2^2 \cdot 3^2$

- $120 = 2^3 \cdot 3 \cdot 5$
- $500 = 2^2 \cdot 5^3$

$\gcd(24, 36) = 12 = 2^{\min(2,3)} \cdot 3^{\min(1,2)}$

$2^3 \cdot 3 \quad 2^2 \cdot 3^2$

$= 2^2 \cdot 3 = 4 \cdot 3 = 12$

$\gcd(120,500) = 2^{\min(2,3)} \cdot 5^{\min(1,3)} = 2^2 \cdot 5 = 4 \cdot 5 = 20$

Can someone tell me a formula for computing gcd(c,d) using prime factorization of c & d.

Finding gcd using prime factorization

- Suppose the prime factorizations of *a* and *b* are:

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, \qquad b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n},$$

- where each exponent is a nonnegative integer, and where all primes occurring in either prime factorization are included in both. Then:

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

Least common multiple

Definition: The least common multiple of the positive integers *a* and *b* is the smallest positive integer that is divisible by both *a* and *b*. It is denoted by lcm(*a*,*b*).

- $24 = 2^3 \cdot 3$
- $36 = 2^2 \cdot 3^2$

$\text{lcm}(24, 36) = 2^{\max(2,3)} \cdot 3^{\max(2,1)}$

$= 2^3 \cdot 3^2 = 8 \cdot 9 = 72$

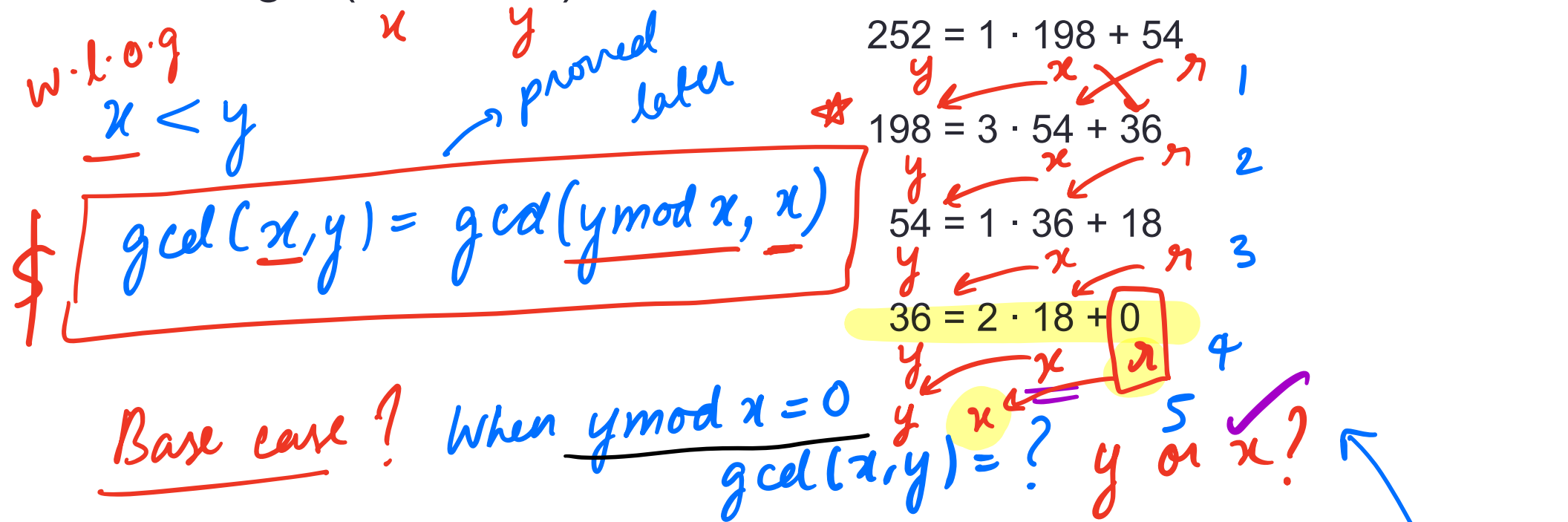
- $120 = 2^3 \cdot 3 \cdot 5$
- $500 = 2^2 \cdot 5^3$

$\text{lcm}(120,500) = 2^{\max(2,3)} \cdot 3^{\max(1,0)} \cdot 5^{\max(1,3)}$

$= 2^3 \cdot 3 \cdot 5^3 =$

Euclid's algorithm

- Euclid's algorithm is an efficient method for computing gcd
- Find gcd(198, 252): = 18



Euclid's algorithm in pseudocode

procedure *gcd*(*x*, *y*: positive integers and x < y)

a := *x*

b := *y*

while a ≠ 0

r := *b* **mod** *a*

b := *a*

a := *r*

return b {gcd(x,y) is b}

code 1>

code 2>

another way

if r == 0

break

Trace gcd(198, 252)

a = 18

b = 36

in this case o/p a

setting y to old x

setting x to r

Finally b = 18, a = 0

Goal: Prove gcd(x,y) = gcd(y mod x, x)

Properties of Divisibility

Theorem 1: Let a, b, and c be integers, where $a \neq 0$.

i. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$

ii. If $a \mid b$, then $a \mid bc$ for all integers c

iii. If $a \mid b$ and $b \mid c$, then $a \mid c$

Rephrase (ii)? If $a|b$ then a divides all multiples of b.

Theorem 5.2.1: Divisibility and linear combinations.

Let x, y, and z be integers. If x|y and x|z, then x|(sy + tz) for any integers s and t.

Exercise: use theorem 1.1 & 1.2 to prove Theorem 5.2.1

x divides any linear combination of y & z

Proof [Theorem 1.1]: If $a|b$ & $a|c$ then $a|b+c$

Let $a, b, c \in \mathbb{Z}$, $a \neq 0$

& $a|b$ & $a|c$

We use a direct proof to show that $a|b+c$

Since $a|b$, $b = ax$ for some $x \in \mathbb{Z}$

$a|c$, $c = ay$ for some $y \in \mathbb{Z}$

$\therefore b + c = a(x+y)$

since $x, y \in \mathbb{Z}$, $x+y \in \mathbb{Z}$

Thus $a|b+c$

This completes the proof

Theorem 1.3: If $a|b$ & $b|c$ then $a|c$

Let $a, b, c \in \mathbb{Z}$, $a \neq 0$

& $a|b$, $b|c$

We use a direct proof to show $a|c$

Since $a|b$, $b = ax$ for some $x \in \mathbb{Z}$

$b|c$, $c = by$ for some $y \in \mathbb{Z}$

$\Rightarrow c = by = (ax)y = a(xy)$

since $x, y \in \mathbb{Z}$, $xy \in \mathbb{Z}$

$\therefore$ since $c = a(xy)$

$\Rightarrow a \mid c$

This completes the proof.

Correctness of Euclid's algorithm

GCD Theorem:

Let x and y be two positive integers. Then gcd(x, y) = gcd(y mod x, x).

y x y mod x

Earlier we showed: 54 = 1 · 36 + 18

Which of the following claims is a direct application of the above theorem?

A. gcd(18, 54) = gcd(18, 36)

B. gcd(36, 54) = gcd(18, 36)

C. gcd(18, 36) = 18

D. All of the above

E. None of the above

Correctness of Euclid's algorithm

GCD Theorem:

Let x and y be two positive integers. Then gcd(x, y) = gcd(y mod x, x).

Earlier we showed: $54 = 1 \cdot 36 + 18$

Do you agree or disagree with the following strategy?

To prove the GCD theorem, we need to show that if a number is a common divisor of (y mod x) and x, then it is a common divisor of x and y.

$\Longrightarrow$

We can then conclude that gcd(y mod x, x) is the same as gcd(x, y)

A. Agree
B. Disagree

↓
Enough to show: $d \in \mathbb{Z}$
if $d \mid y \bmod x \wedge d \mid x$
then $d \mid y \wedge d \mid x$

$(d \mid x \wedge d \mid y \bmod x) \longleftrightarrow (d \mid x \wedge d \mid y)$

If we prove: $\forall d \in \mathbb{Z}^+$ can conclude $\gcd(x, y \bmod x) = \gcd(x, y)$

GCD Theorem:

Let x and y be two positive integers. Then gcd(x, y) = gcd(y mod x, x).

Proof: We are going to use Theorem 2, 5.2.1

If $\forall d \in \mathbb{Z}^+ \quad d|x \wedge d|y \bmod x \iff d|x \wedge d|y$

Then since gcd of two nos is the greatest divisor of those two nos, we have $\gcd(x, y \bmod x) = \gcd(x, y)$

To complete the proof we need to show:

$\forall d \in \mathbb{Z}^+ \quad d|x \wedge d|y \bmod x \iff d|x \wedge d|y$

Let d be an arbitrary $+^{ve}$ integer,

(i) $d|x \wedge d|y \bmod x \longrightarrow d|x \wedge d|y$

Need to show $d|y$

First write x w.r.t y

$y = xq + r \longrightarrow r = y \bmod x$

To show that, $d|xq + r$

We know, $d|x$ ∴ by Theorem 1 $d|xq$

$d|y \bmod x \Rightarrow d|r$

Again by Theorem 1 we have

$d|xq + r$

OR

simpler $d|x$ & $d|r$ ∴ by Theorem 2

$d|\underbrace{xq + r}_{\text{linear comb of } x \& r} \Rightarrow d|y$

(ii) $d|x \wedge d|y \longrightarrow d|y \bmod x \wedge d|x$

We need to show

$d \mid y \bmod x$ assuming $d \mid x \wedge d \mid y$

Let, $y = xq + r \Rightarrow r = y - xq$

We know $d \mid y$ & $d \mid x$

Need to show $d \mid r$

$r = y - xq$

By Theorem 2,

since $d \mid y$ & $d \mid x$

$\Rightarrow d \mid y - qx \Rightarrow d \mid r$

$[d \mid sy + tx]$

$s = 1 \quad t = -q$

$s, t \in \mathbb{Z}$

This completes the proof.

By (i) & (ii), we know that

$\forall d \in \mathbb{Z}^+$

$\therefore d \mid x \wedge d \mid y \iff d \mid x \wedge d \mid y \bmod x$

$\therefore \gcd(x, y) = \gcd(y \bmod x, x)$

This completes the proof

Modular Arithmetic

Arithmetic on a ring of integers $\mathbb{Z}_m = \{0, 1, \ldots m-1\}$

Addition modulo m ($+_m$) : $102 +_5 48 = (102 + 48)\ mod\ 5 =$

Multiplication modulo m ($\cdot_m$): $(7 \cdot_5 10) = (7 \cdot 10)\ mod\ 5 =$

The operations $+_m$ and $\cdot_m$ satisfy many of the same properties as ordinary addition and multiplication:
Closure, Associativity, Commutativity, Identity, Distributivity, Additive Inverses

Summary:

Task: compute gcd

→ Came up with Euclid's alg

→ Pseudo code

→ Example, run through pseudo code

→ Proved some helper theorems (Theorem 1, 5.2.1)

→ Proved Euclid's alg correctness

Application: Cycling

How many minutes past the hour are we at? *Model with* $+15$ **mod** 60

Time:	12:00pm	12:15pm	12:30pm	12:45pm	1:00pm	1:15pm	1:30pm	1:45pm	2:00pm
"Minutes past":	0	15	30	45	0	15	30	45	0

Caeser Cipher with shift value 15

Encrypt: "ALP"

Replace each English letter by a letter that's fifteen ahead of it in the alphabet *Model with* $+15$ **mod** 26

Original index:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Original letter:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Shifted letter:	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Shifted index:	15	16	17	18	19	20	21	22	23	24	25	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

Application: Pseudorandom numbers

$$x_{n+1} = (7x_n + 4) \bmod 9, \text{ with } x_0 = 3.$$

$$\begin{aligned}
x_1 &= 7x_0 + 4 \bmod 9 = 7 \cdot 3 + 4 \bmod 9 = 25 \bmod 9 = 7,\\
x_2 &= 7x_1 + 4 \bmod 9 = 7 \cdot 7 + 4 \bmod 9 = 53 \bmod 9 = 8,\\
x_3 &= 7x_2 + 4 \bmod 9 = 7 \cdot 8 + 4 \bmod 9 = 60 \bmod 9 = 6,\\
x_4 &= 7x_3 + 4 \bmod 9 = 7 \cdot 6 + 4 \bmod 9 = 46 \bmod 9 = 1,\\
x_5 &= 7x_4 + 4 \bmod 9 = 7 \cdot 1 + 4 \bmod 9 = 11 \bmod 9 = 2,\\
x_6 &= 7x_5 + 4 \bmod 9 = 7 \cdot 2 + 4 \bmod 9 = 18 \bmod 9 = 0,\\
x_7 &= 7x_6 + 4 \bmod 9 = 7 \cdot 0 + 4 \bmod 9 = 4 \bmod 9 = 4,\\
x_8 &= 7x_7 + 4 \bmod 9 = 7 \cdot 4 + 4 \bmod 9 = 32 \bmod 9 = 5,\\
x_9 &= 7x_8 + 4 \bmod 9 = 7 \cdot 5 + 4 \bmod 9 = 39 \bmod 9 = 3.
\end{aligned}$$

General recursive generator

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

$2 \le a < m,$
$0 \le c < m,$
$0 \le x_0 < m$

The sequence generated is
3,7,8,6,1,2,0,4,5,3,7,8,6,1,2,0,4,5,3,...
It repeats after generating 9 terms.

Commonly, computers use a linear congruential generator with increment $c = 0$. This is called a *pure multiplicative generator*. Such a generator with modulus $2^{31} - 1$ and multiplier $7^5 = 16{,}807$ generates $2^{31} - 2$ numbers before repeating.

Computing Arithmetic Expressions mod m

Which of the following are true?

A. $(102 + 48) \bmod 5 = (102 \bmod 5) + (48 \bmod 5)$

B. $(7 \cdot 10) \bmod 5 = (7 \bmod 5) \cdot (10 \bmod 5)$

C. $(2^5) \bmod 3 = \left((2 \bmod 3)^{(5 \bmod 3)} \right) \bmod 3$

D. More than one of the above

E. None of the above

Multiplicative inverse mod n (key step in the RSA cryptosystem)

Definition 5.5.1: Multiplicative inverse mod n.

A ***multiplicative inverse mod n*** (or just ***inverse mod n***) of an integer x, is an integer $s \in \{1, 2, \ldots, n-1\}$ such that $sx \bmod n = 1$.

Multiplicative inverses don't always exist

For example, there is no multiplicative inverse of 2 mod 6.

Multiplicative inverse of x mod n exists

if and only if x and n are relatively prime.

The operations $+_n$ and $\cdot_n$ satisfy many of the same properties as ordinary addition and multiplication: *Closure, Associativity, Commutativity, Identity, Distributivity, Additive Inverses* *BUT NOT DIVISION: Multiplicative inverses don't always exist*

Finding Multiplicative inverses mod n (when they exist)

Theorem 5.5.2: Expressing gcd(x, y) as a linear combination of x and y.

Let x and y be integers, then there are integers s and t such that

$$\gcd(x, y) = sx + ty$$

$$\gcd(6,14) = 2 = (-2)\cdot 6 + 1\cdot 14$$

Finding inverses

- Extension of Euclidean algorithm
- Find an inverse of 3 modulo 7.
  - Using the Euclidian algorithm: $7 = 2 \cdot 3 + 1$.
  - Write gcd(3, 7) as $s \cdot 3 + t \cdot 7$

$$1 = -2 \cdot 3 + 1 \cdot 7$$

  - Hence, -2 is an inverse of 3 modulo 7.
  - To get a value within $\mathbb{Z}_7$ add 7

Finding inverses: Extended Euclid's

- **Example**: Find an inverse of 31 modulo 43.
- **Solution**: First use the Euclidian algorithm to show that gcd(31,43) = 1.

$43 = 1 \cdot 31 + 12$

$31 = 2 \cdot 12 + 7$

$12 = 1 \cdot 7 + 5$

$7 = 1 \cdot 5 + 2$

$5 = 2 \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$

Finding inverses: Extended Euclid's

- **Example**: Find an inverse of 31 modulo 43.
- **Solution**: First use the Euclidian algorithm to show that gcd(31,43) = 1.
- Working Backwards to express gcd(x, y) as a linear combination of x and y

$$43 = 1\cdot 31 + 12$$
$$31 = 2\cdot 12 + 7$$
$$12 = 1\cdot 7 + 5$$
$$7 = 1\cdot 5 + 2$$
$$5 = 2\cdot 2 + 1$$
$$2 = 2\cdot 1 + 0$$

$$12 = 43 - 1\cdot 31$$
$$7 = 31 - 2\cdot 12$$
$$5 = 12 - 1\cdot 7$$
$$2 = 7 - 1\cdot 5$$
$$1 = 5 - 2\cdot 2$$

$$\begin{aligned}
1 &= 5 - 2\cdot 2 \\
&= 5 - 2\cdot (7 - 1\cdot 5) \\
&= 3\cdot 5 - 2\cdot 7 \\
&= 3\cdot (12 - 1\cdot 7) - 2\cdot 7 \\
&= 3\cdot 12 - 5\cdot 7 \\
&= 3\cdot 12 - 5\cdot (31 - 2\cdot 12) \\
&= 13\cdot 12 - 5\cdot 31 \\
&= 13\cdot (43 - 1\cdot 31) - 5\cdot 31 \\
&= 13\cdot 43 - 18\cdot 31
\end{aligned}$$

multiplicative inverse of 31 mod 43 is