Office Hours

T,Th: ~~5~~ - 6:30 Pacific
5:30 9/1, 9/8
Mon: 2 - 3 Pacific

Number Theory

Paulin: Abstract Alg
↳ Chap 1
↑ set theory

Study

$\mathbb{N} = \{1, 2, 3, \cdots\}$

Rmk Crypt uses HUGE #s

Notation: Sets

* A set S is a collection of objects
* An element x of a set S is one of those objs.
we write $x \in S$
* Else $x \notin S$
* To define:
$S = \{x_1, x_2, x_3, \cdots\}$
$S = \{\text{objects } x \mid x \text{ satisfies property}\}$

Ex
E = even #s
$= \{2, 4, 6, \cdots\}$
$= \{x \in \mathbb{N} \mid x \text{ is even}\}$

$\mathbb{N} = \{1, 2, 3, \cdots\}$
&
$\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, 3, \cdots\}$
↑ integers

$a, b \in \mathbb{Z}$
* Add: $a + b \in \mathbb{Z}$
* Subtract: $a - b \in \mathbb{Z}$ } Group
* Multiply: $a \times b \in \mathbb{Z}$

Commutative, associative, distributive.
$\mathbb{Z}$ a ring.

Q: Can we $\div$?
.... only sometimes.

Ex $2, 3 \in \mathbb{Z}$
* $2 + 3 = 5 \in \mathbb{Z}$
* $2 - 3 = -1 \in \mathbb{Z}$
* $2 \cdot 3 = 6 \in \mathbb{Z}$
* $2 \div 3 = 2/3 \notin \mathbb{Z} \leftarrow$ X

Question
When can we divide?

Defn:
let a & b be integers ($a, b \in \mathbb{Z}$)
We say b divides a $\quad b \mid a$
or a is divisible by b
if
[idea $\frac{a}{b} = k \in \mathbb{Z}$]
$\exists\, k \in \mathbb{Z}$ s.t. $a = b \cdot k$

Notation
a divides $b \Rightarrow a \mid b$
else $a \nmid b$

Examples
* $2 \mid 6$ b/c $6 = 2 \cdot 3$ ↑ k
* $2 \nmid 3$ b/c $\frac{3}{2} \notin \mathbb{Z}$
$2k$ even
3 odd

Rmk:
$2 \mid n \iff n$ even

Notation
P, Q statements.
$P \iff Q$ (P true if & only if Q true)
$P \Rightarrow Q$ (if P true then Q true)

Ex $4 \mid n \Rightarrow n$ even
Pf/ $4 \mid n \Rightarrow n = 4 \cdot k$
$\Rightarrow n = 2(\underline{2k})$
$\Rightarrow 2 \mid n$
$\Rightarrow n$ even

Propn: $a, b, c \in \mathbb{Z}$
(i) $a \mid b$ & $b \mid c$
Then $a \mid c$
(ii) $a \mid b$ and $b \mid a$
$\Rightarrow a = \pm b$
(iii) $a \mid b$ and $a \mid c$
$\Rightarrow a \mid (b + c)$
$a \mid (b \cdot c) \leftarrow$

Pf/ $a \mid b \Rightarrow b = a \cdot k$ $\quad k, \ell \in \mathbb{Z}$
$b \mid c \Rightarrow c = b \cdot \ell$
so $c = (ak) \cdot \ell$
$= a(k\ell) \leftarrow k\ell \in \mathbb{Z}$
so $a \mid c$. $\varnothing$
(ii) & (iii) on HW.

Defn: $a, b \in \mathbb{Z}$, $a, b \geq 0$
* A common divisor of a & b is an $d \in \mathbb{Z}$ s.t. $d \mid a$ & $d \mid b$.
* The greatest common divisor of a & b is the biggest one.
↑ Denoted $\gcd(a, b)$ or (a, b)

Example $a = 12$ $b = 18$
1) Compute Divisors
$Div(12) = \{1, 2, 3, 4, 6, 12\}$
$Div(18) = \{1, 2, 3, 6, 9, 18\}$
$CDiv(12, 18) = \{1, 2, 3, 6\}$
$\gcd(12, 18) = 6$

Implementation Practice

* divides(a,b)
= true $a \mid b$
= false $a \nmid b$
* getDivisors(a) = returnDiv
* getCommonDivisors(a,b)
= return CDiv
* findGCDslow(a,b)

Example $a = 2024$
$b = 748$

$Div(2024) =$
$\{1, 2, 4, 8, 11, 22, 44, 88, 92, 184, 253, 506, 1012, 2024\}$
$Div(748) =$
$\{1, 2, 4, 11, 17, 22, 34, 44, 68, 187, 374, 748\}$
$\Rightarrow \gcd(2024, 748) = 44$

Why Slow?

| Naive way getDivisors(a) takes a steps.
| clever way getDivisors takes $\sqrt{a}$ steps.
↑ still too slow.

Main tool to speed up computation is Division w/ Remainder (Long Division).

Ex $230 \div 17$

$$\begin{array}{r} 013 \text{ R}9 \\ 17\overline{)230} \\ -17\downarrow \\ 60 \\ -51 \\ \hline 9 \end{array}$$

$230 = 17 \cdot 13 + 9$

Defn
$a, b \in \mathbb{N}$
a divided by b has quotient q & remainder r if
$a = bq + r$ $\quad \underline{0 \leq r < b}$

HW: Implement this.
LongDiv(a,b) =
returns [q,r]

Prop
* q & r exist & are unique.
* $b \mid a \iff \underline{r = 0}$

Remark % - mod in python
$a \% b = r$

You Do
$230 \% 17 = 9$

Check if
$355 \nmid 259948$
$259948 \% 355 = 83$
No!

Lemma: $a, b \in \mathbb{Z}$.
& long divide
$a = bq + r$
$\Rightarrow \gcd(a, b) = \gcd(b, r)$

Pf/ Show common divs of a & b same as those of b & r.
i.e. $d \in \mathbb{Z}$
$d \mid a$ & $d \mid b \iff d \mid b$ & $d \mid r$
($\Rightarrow$) $d \mid a$ & $d \mid b$
$d \mid b$ already! show $d \mid r$.
$r = a - bq$
$d \mid a$ $\quad d \mid bq$
HW $\Rightarrow d \mid (a - bq) = r$ ✓
$\Leftarrow$ Same $\varnothing$

Use to find $\gcd(a, b)$
$a = bq + r$ $\quad r < b$ $\quad \gcd(a,b) = \gcd(b, r)$
$b = rq' + r'$ $\quad = \gcd(r, r')$
⋮ keep going $\quad =$ ⋮
$b > r > r' > \cdots \geq 0$ $\quad = \gcd(r_n, 0)$
$= r_n$

Exercise $a > 0$
$\gcd(a, 0) = a$

Example
$\gcd(2024, 748) =$

$2024 = 748 \cdot 2 + 528$ $\quad \gcd(748, 528)$
$748 = 528 \cdot 1 + 220$ $\quad = \gcd(528, 220)$
$528 = 220 \cdot 2 + 88$ $\quad = \gcd(220, 88)$
$220 = 88 \cdot 2 + 44$ $\quad = \gcd(88, 44)$
$88 = 44 \cdot 2 + \underline{0}$ $\quad = \gcd(44, 0)$
$= 44$

Takeaway
Naive: Thousands
Euclidean: 5 steps.

Thm (Euclidean Alg)
$a, b \in \mathbb{N}$ $\quad a \geq b$. The following computes $\gcd(a, b)$
① $r_0 = a$ $\quad r_1 = b$
② set $i = 1$
③ divide r_{i-1} by r_i get
$r_{i-1} = r_i \cdot q_i + r_{i+1}$
$0 \leq r_{i+1} < r_i$
④ If $r_{i+1} = 0 \Rightarrow$ return r_i
⑤ Else $i = i + 1$ & return to step 3.

Further run step 3 at most
$2 \log_2 b + 2$ times.

Pf/ Correctness
$a = bq_1 + r_2$
$b = r_2 q_2 + r_3$
⋮
$r_{n-1} = r_n q_n + r_{n+1}$ ← 0

Lemma
$\gcd(a,b) = \gcd(b, r_2) = \cdots$
$\cdots = \gcd(r_n, 0) = r_n$ $\varnothing$

Subclaim
$r_{i+2} < \frac{r_i}{2}$
Pf/ 2 cases
① $r_{i+1} \leq \frac{r_i}{2}$
Then $r_{i+2} < r_{i+1}$ ✓
② $r_{i+1} > \frac{r_i}{2} \leftarrow$
$r_i = r_{i+1}(1) + r_{i+2}$
$r_{i+2} = r_i - r_{i+1} < r_i - \frac{r_i}{2} = \frac{r_i}{2}$
$\varnothing$

So
$r_{2k+1} < \frac{1}{2} r_{2k-1} < \cdots < \frac{1}{2^k} r_1 = \frac{1}{2^k} b$
So if $2^k > b$
$\Rightarrow r_{2k+1} = 0$

$\log_2 b = (m$ s.t. $2^m = b$
Let k smallest k s.t. $2^k > b$
$k - 1 \leq m < k$
Done in $2k$ steps
$= 2(k-1) + 2$
$= 2m + 2$
$= 2 \log_2 b + 2$ $\varnothing$

Ex If $b \approx 2^{100}$
$getDiv(b) \approx \sqrt{b} \approx 2^{50}$
$\approx 10^{15}$
Euclid $< 2 \log_2 2^{100} + 2$
$= 2 \cdot 100 + 2 = 202$

Rmk Average
$.85 \log_2 b + .14$