Aug31

Wednesday, August 18, 2021 10:17 AM

Number Theory

The study of the natural numbers

$$\mathbb{N} = \{1, 2, 3, 4, \dots\}$$

Rmk

Crypto use HUGE numbers

$\approx 10^{200}$ or so...

Notation: Set Theory

Reference:

Paulin: Abstract Algebra
Chapter 1

* A set S is a collection of (mathematical) objects.

* An object x is in the set $\rightsquigarrow x \in S$

or not in the set ⇝ $x \notin S$

* We write

$$S = \{x_1, x_2, x_3, \dots\}$$

$$= \{x \mid x \text{ satisfies some property}\}$$

Examples

- $\mathbb{N} = \{x \mid x \text{ is a positive whole number}\}$
- $3 \in \mathbb{N} \qquad \frac{1}{2} \notin \mathbb{N}$
- $\mathbb{E} = \{x \in \mathbb{N} \mid x \text{ is even}\}$

Back to number theory

Define the set of integers

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, 3, \dots\}$$

Question:

what structures does $\mathbb{Z}$ have?

what can we do to integers?

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

- Add: $a + b$
- Subtract: $a - b$
- Multiply: $a \times b$

Group

Ring

⇝ Associativity

⇝ Commutativity of $+$ & $\times$

⇝ Distributive law.

Question

Can we divide??

.... only sometimes.

Ex $2, 3 \in \mathbb{Z}$

$$2 + 3 = 5 \in \mathbb{Z}$$

$$2 - 3 = -1 \in \mathbb{Z}$$

$$2 \cdot 3 = 6 \in \mathbb{Z}$$

$$2 \div 3 = \frac{2}{3} \notin \mathbb{Z}$$ ← cant

But...

$$6 \div 3 = 2 \in \mathbb{Z} \leftarrow \text{can.}$$

Rmk

The question of when we can divide is central to Number Theory & Crypto.

Defn

Let $a, b \in \mathbb{Z}$. We say a divides b (denoted $a \mid b$) if $\left(\overset{\text{idea}}{\downarrow}\ \frac{b}{a} \in \mathbb{Z}\right)$ there exists an integer $k \in \mathbb{Z}$ s.t. $b = a \cdot k$

If a doesn't divide b write

$$a \nmid b$$

Examples

- $2 \mid 6$ bc $6 = 2 \cdot \underset{}{\overset{k=3}{3}}$
- n is even $\overset{\Rightarrow}{\Longleftrightarrow}$ $n = 2 \cdot k$

$\Longleftrightarrow 2|n$

Aside (Paulin 1)

P & Q logical statements

$$P \Longrightarrow Q$$

.... If P is true, so is Q

$$P \Longleftrightarrow Q$$

... P true if and only if Q is

$(P \Rightarrow Q$ AND $Q \Rightarrow P)$

Example

If $4/n$ then n is even.

Proof

$4/n \Longrightarrow n = 4 \cdot k$ some $k \in \mathbb{Z}$

$\Longrightarrow n = 2 \cdot (2k)$

$\Longrightarrow 2/n$

$\Longrightarrow n$ even ∅

Prop: (Properties of divisibility)

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

a) if $a|b$ & $b|c$, then $a|c$

b) if $a|b$ & $b|a$, then $a = \pm b$

c) if $a|b$ & $a|c$, then $a|(b \pm c)$

d) if $a|b$, then $a|b \cdot c$

Proof

(a) $a|b \implies b = k \cdot a$ some $k \in \mathbb{Z}$

$b|c \implies c = l \cdot b$ some $l \in \mathbb{Z}$

$$c = l \cdot b = l \cdot (k \cdot a)$$

$$= (lk) \cdot a \quad \& \quad lk \in \mathbb{Z}$$

$\implies a|c$ by def. ∅

(b) & (c),(d) are HW.

Important Def^n

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

- A divisor of a is an integer d s.t. $d \mid a$.
- A common divisor of a & b is an integer d s.t. $d \mid a$ & $d \mid b$.
- The greatest common divisor of a & b is the largest of all the common divisors.

  Denoted $\gcd(a,b)$

  or (a,b)

Example $a = 12$ $b = 18$

(Positive) divisors of a & b.

$$Div(12) = \{1, 2, 3, 4, 6, 12\}$$

$$Div(18) = \{1, 2, 3, 6, 9, 18\}$$

write common divisors.

$$CDiv(12, 18) = \{1, 2, 3, 6\}$$

Biggest one?

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

Exercise: Open up a Jupyter NB
write functions

* getDivisors (a):
return positive divisors of a.

- do it in a or $\sqrt{a}$ steps
- Use % operation

↪ a%b = remainder of b/a w/ long division.

* getCommonDivisors (a, b):
return CDiv.

* findGCDSlow (a, b):
return GCD by computing CDIV & looking for biggest

* Do it for gcd (748, 2024) = 44

Div (748) =

{1, 2, 4, 11, 17, 22, 34, 44, 68, 187, 374, 748}

$\mathrm{Div}(2024) =$

$\{1, 2, 4, 8, 11, 22, 23, 44, 88, 92, 184, 253, 506, 1012, 2024\}$

Observe

Slow Part: getDivisors(a)

a or $\sqrt{a}$ steps.

Cryptographic #s are $\approx 10^{200}$

so $\sqrt{a} \approx \underbrace{10^{100}}$

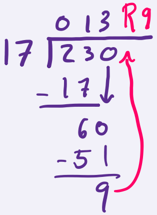
↑ too many steps!!

Speed it up!!

Tool: Long Division.

Example

$230 \div 17 = 13$ w/ Remainder of 9.



$230 = 17 \cdot 13 + 9$

Rmk $230 \% 17 = 9$ ←

Def^n $a, b \in \mathbb{N}$. we say a divided by b has quotient q & remainder r if

- $a = b \cdot q + r$
- $0 \leq r < b$

Prop:

- q & r exist and are unique.
- $b \mid a \iff r = 0$

Proof: Exercise.

HW: Implementation of long division.

```
longDivide(a, b):
    return [q, r]  s.t.
        $a = bq + r$  &  $0 \leq r < b$.
```

(use % & // ← integer division)

Lemma

Suppose $a, b \in \mathbb{N}$ long divide to

$$a = bq + r$$

Then $\gcd(a, b) = \gcd(b, r)$.

Proof

Strategy: Show common divisors are the same!

Goal

d a common divisor of a & b

$\iff$ d a common div of b & r

$(\Longrightarrow)$ $d \mid a$ & $d \mid b$.

Show $d \mid b$ ✓ & $d \mid r$ ✓

$a = bq + r \Longrightarrow r = a - bq \leftarrow$

$d \mid b \overset{HW}{\Longrightarrow} d \mid bq$

$d \mid a$

$\overset{HW}{\Longrightarrow} d \mid a - bq$ ✓

$(\Longleftarrow)$ identical.

we win!

Strategy to compute gcd of a & b.

Want $\gcd(a, b)$ ←

=

Long divide $a = bq + r$

Suffice to compute $\gcd(b, r)$

Long divide $\quad b = r \cdot q_1 + r_1 \quad \updownarrow =$

Suffice to compute $\gcd(r, r_1)$

$\vdots$ keep going.

$b > r > r_1 > r_2 > \dots \geq 0$

stop somewhere!

$$r_n = q_n \cdot r_{n+1} + 0$$

$$\begin{aligned} \gcd(a,b) &= \gcd(b, r_1) \\ &= \gcd(r_1, r_2) \\ &= \dots \\ &= \gcd(r_n, r_{n+1}) \\ &= \gcd(r_{n+1}, 0) \\ \longrightarrow &= r_{n+1} \end{aligned}$$

Exercise

$\gcd(a, 0) = a \quad \forall \quad a \geq 0.$

Example

$\gcd(2024, 748)$

Rmk get Div thousands of divisions

(clever, hundreds).

$\gcd(2024, 748)$: $2024 = 748 \cdot 2 + 528$.

$= \gcd(748, 528)$: $748 = 528 \cdot 1 + 220$.

$= \gcd(528, 220)$: $528 = 220 \cdot 2 + 88$.

$= \gcd(220, 88)$: $220 = 88 \cdot 2 + 44$.

$= \gcd(88, 44)$: $88 = 44 \cdot 2 + 0$.

$= \gcd(44, 0) = \boxed{44}$

5 steps instead of thousands!!

Theorem (Euclidean Algorithm)

$a \geq b \geq 0$. The following algorithm computes $\gcd(a, b)$.

1) Set $r_0 = a$, $r_1 = b$
2) Set $i = 1$
3) Divide r_{i-1} by r_i :

$$r_{i-1} = r_i \cdot q_i + r_{i+1}$$

4) if $r_{i+1} = 0$, return

$$\gcd(a,b) = r_i$$

5) Else, set $i = i+1$ & return to step 3.

Furthermore, step 3 occurs @ most $2\log_2 b + 2$ times. ←

Proof

Correctness

$a = bq_1 + r_2$ $\qquad r_2 > r_3 > r_4 > \dots \geq 0$

$b = r_2 q_2 + r_3$ $\qquad$ stops when

$r_2 = r_3 q_3 + r_4$ $\qquad r_{n+1} = 0$

$\vdots$

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

Lemma

$$\gcd(a,b) = \gcd(b, r_2) = \gcd(r_2, r_3)$$

$$= \dots = \gcd(r_n, 0) \underset{\substack{\uparrow \\ \text{HW.}}}{=} r_n$$

SubClaim: $r_{i+2} < \frac{1}{2} r_i$

Proof of subclaim

2 cases

Case 1: $r_{i+1} \le \frac{1}{2} r_i$

Then $r_{i+2} < r_{i+1} \le \frac{1}{2} r_i$ we win.

Case 2: $\underline{r_{i+1} > \frac{1}{2}} r_i$

$$r_i = \underline{r_{i+1}} \cdot q + r_{i+2}$$

If $q \ge 2$ $r_{i+1} \cdot q > r_i$ ↯

So $q = 1$

$$r_i = r_{i+1} + r_{i+2}$$

Solve

$$r_{i+2} = r_i - r_{i+1} < r_i - \frac{1}{2} r_i = \frac{1}{2} r_i$$

we win. ✓

$$r_{2k+1} < \frac{1}{2} r_{2k-1} < \frac{1}{4} r_{2k-3}$$

$$< \dots < \frac{1}{2^k} r_1 = \frac{1}{2^k} \cdot b$$

So, if $2^k \geq b$

know $r_{2k+1} < \frac{b}{2^k} \leq 1$

so $r_{2k+1} = 0$ & we're done.

If $2^k > b$, perform $\leq 2k$ divisions

<u>Recall</u>

$$\log_2 b = (m : 2^m = b)$$

If $2^k > b \geq 2^{k-1}$

$$\Longrightarrow \underline{\underline{k-1}} \leq \underline{\underline{m}} < k$$

$$\begin{aligned} 2k &= 2(k-1)+2 \\ &\leq 2m + 2 \\ &= \underbrace{2\log_2 b + 2}_{\text{Fewer than this many steps}} \end{aligned}$$

<u>E.g.:</u> $b \approx 2^{100}$

GetDivisors $= \sqrt{b} = 2^{50} \approx \underline{10}^{15}$ steps

Euclid takes $2(\log_2 2^{100}) + 2$

$$\underline{\underline{= 202}} \quad \text{steps}$$

< 100 usually.

HW: Implement this algorithm.

Rmk • Careful analysis gives

$< 1.45 \log_2 b + 1.68$ steps

• Average time is

$.85 \log_2(b) + .14$ steps.

Next time **In person!!**

Extended Euclidean Algorithm gives a way to express

$$\gcd(a,b) = a \cdot u + b \cdot v$$

for $u, v \in \mathbb{Z}$.