AM 106 - LECTURE 2

Note Title 9/6/2016

TODAY: INTEGERS

- DIVISION, GREATEST COMMON DIVISOR
- PRIMES & UNIQUE FACTORIZATION
- MODULAR ARITHMETIC

———— x ————

READING FOR TODAY'S LECTURE:

GALLIAN, CHAPTER 0

———— x ————

Summary:

- Will study basic properties of integers.
- Multiple Motivations
  1. Proofs
  2. Abstract properties essential to proof
  3. Generalize to other settings.

(if you're getting bored think polynomials & see which properties apply)

DIVISIBILITY

Defn: b divides a (denoted $b|a$) if there exist $q \in \mathbb{Z}$ s.t.

$$a = q \cdot b$$

Fact: $b|a$ & $a, b > 0$ $\Rightarrow$ $a \geq b$

Thm: (DIVISION "ALGORITHM"):

$\forall\ a, b \in \mathbb{Z}$, $b > 0$,

$\exists!\ q \in \mathbb{Z}$ & $0 \leq r < b$ s.t.

$$a = q \cdot b + r$$

(Aside: Notation $\forall \rightarrow$ for all

$\exists \rightarrow$ There exist(s)

$\exists! \rightarrow$ There exists unique.)

Proof: (Existence)

Case: $a \geq 0$:

Prove by strong induction on a:

Base : $0 \le a < b \Rightarrow q = 0,\ r = a$ works

Induction: Assume true for $0 \le a < n$; $n \ge b$

Prove for $a = n$;

By induction $a' = a - b$ expressible as

$$a' = q' \cdot b + r$$

Let $q = q' + 1$; $r = r$

$$a = a' + b = (q' + 1)\, b + r = q \cdot b + r \checkmark$$

Case : $a < 0$ similar

(Uniqueness) :

Suppose $q_1 b + r_1 = q_2 b + r_2$

$0 \le r_2 \le r_1 < b$

Then $r_1 - r_2 = (q_2 - q_1)\, b$

$\Rightarrow 0 \le r_1 - r_2 < b$ & $r_1 - r_2$ is divisible by b.

By Fact, $r_1 - r_2 = 0 \Rightarrow r_1 = r_2$

$\Rightarrow q_1 b = q_2 b \Rightarrow q_1 = q_2$ $\boxtimes$

Food for Thought:

- Which integers divide all integers?
- Which integer is divisible by all integers?

Division "ALGORITHM"?

- Theorem, not algorithm!
- Algorithm implied;
- But extremely inefficient
- Naive algorithm:

$$\left.\begin{array}{l} 0 \le a \le 2^n \\ 0 \le b \le 2^n \end{array}\right\} \begin{array}{l} \text{finding } q, r \\ \text{takes time} \sim 2^n \end{array}$$

- Long Division: takes $\sim O(n^2)$ time

Greatest Common Divisor (GCD)

Defn: For $a, b \in \mathbb{Z} \setminus \{0\}$ their GCD g is the largest positive integer such that

$$g \mid a \quad \& \quad g \mid b$$

Defn: $GCD(a,b) = 1 \Rightarrow$ "a & b relatively prime"

Thm: Let $a, b \neq 0$ with $g = GCD(a,b)$. Then $\exists s, t$ s.t. $s \cdot a + t \cdot b = g$.

Furthermore g is smallest such positive integer.

Assume $a \geq 0$, $b \geq 0$: other cases similar

Proof: (Existence)

- Note: $GCD(a,b) = GCD(a-b, b)$

Proof: $a = \alpha \cdot g$, $b = \beta \cdot g$ $\Rightarrow$ $a - b = (\alpha - \beta) g$, $b = \beta \cdot g$

$\Rightarrow$ Common Divisors $(a,b) \subseteq$ Common Divisors $(a-b, b)$

$\supseteq$ similar

- Induction on $a+b$:

Base: $GCD(a,0) = a$; $a = 1 \cdot a + 0 \cdot 0$

Induction: $g = GCD(a,b) = GCD(a-b, b)$

By induction $g = s'(a-b) + t'b$

$= s' \cdot a + (t' - s') b$

$\Rightarrow g = s \cdot a + t \cdot b$ for

$s = s'$; $t = t' - s'$

- (smallest)

$g = GCD(a,b)$ divides $x \cdot a + y \cdot b$

$\forall x, y$

$\Rightarrow$ it is smaller than every positive
$\leq$
$xa + yb$ ∎

Algorithm? Implied; Inefficient; But can be made efficient using

$$GCD(a,b) = GCD(a \bmod b, b)$$

$a \bmod b = r$ s.t. $0 \leq r < b$ & $\exists q$ s.t.
$a = q \cdot b + r$.

PRIMES & FACTORIZATION

Defn: $p \in \mathbb{Z}$ is prime if $p \neq -1, 0, 1$ & only integers dividing p are ± 1 & $\pm p$.

(Allow neg. integers to be prime. Why?)

Lemma: [Euclid] p prime & $p \mid ab \Rightarrow p \mid a$ or $p \mid b$.

Proof: Suppose $p \nmid a$ & $ab = q \cdot p$

Then ① $GCD(p,a) = 1$

since $GCD(p,a) \mid p$ and only $1, p$ divide p.

② $\Rightarrow \exists\ s, t$ s.t.

$$1 = s \cdot p + t \cdot a$$

③ $$b = b \cdot s \cdot p + t \cdot a \cdot b$$
$$= p(bs + qt)$$

$\Rightarrow$ p divides b.

Fundamental Thm. of Arithmetic

- Every integer $n \notin \{-1, 0, 1\}$ can be expressed as $n = p_1 \cdot p_2 \cdots p_k$ where p_i's are prime
- Furthermore this unique upto ordering & sign ; i.e.
  if $n = q_1 \cdots q_\ell$ where q_i's are prime
  then ① $\ell = k$ &
  ② $\exists$ 1-1 function $\pi : \{1 \dots \ell\} \to \{1 \dots k\}$
  & $\sigma_1 \dots \sigma_\ell \in \{\pm 1\}$
  s.t. $q_i = \sigma_i \cdot p_{\pi(i)}$

Proof: Apply Euclid's Lemma repeatedly.

$\Rightarrow q_1 \mid p_j$ for some j

$\Rightarrow q_1 = \pm p_j$

Recurse on $\frac{n}{q_1}, \frac{n}{\pm p_j}, \dots$ $\boxtimes$

Modular Arithmetic

Division Theorem leads to nice new "algebra"

Defn: $a = q \cdot b + r$: $r \triangleq a \pmod b$

Proposition: $a \bmod b$ (for $a \geq 0$, $b > 0$) is least significant digit of a written in base b.

Examples

$3457 \bmod 10 = 7$

$22 \bmod 4 = 2$

Question: What is $(-a) \bmod b$?

Example Usage USPS money order check digit

Money Order ID = 10 digit number a

Check digit $= a \pmod 9$

Eg. $0897136591 \rightarrow 08971365914$

Questions:

- Why not mod 10?
- Why this scheme?
- if one digit flipped can we detect it?
- Design scheme that detects 1 bit error?
- Will be the simplest "error-correcting code". Will see more later.

Back to Modular Arithmetic

Nice Properties:

- "Homomorphic Properties"

$$((a \bmod n) + (b \bmod n)) \bmod n$$
$$= (a+b) \bmod n$$

$$((a \bmod n) * (b \bmod n)) \bmod n$$
$$= (a * b) \bmod n$$

<u>In fact</u>:

$+_{\text{mod } n}$, $*_{\text{mod } n}$ very nice

- associative, Commutative
- $+_{\text{mod } n}$ has inverse
- $*$ distributes over $+$ ....

just like integers ....

In later lectures:

Abstract these aspects & derive many more properties.