CS 2050 Discrete Mathematics February 20th 2024

Lecture 12: Number Theory

Lecturer: Abrahim Ladha

1 Division

Definition 1.1. For any two numbers a, b we say that a divides b (written $a \mid b$) if there exists a number c such that $ac = b$.

You should think that $a \mid b$ to mean that a divides into b evenly, that b/a is some whole.

Theorem 1. If $a \mid b$ and $a \mid c$ then $a \mid (b + c)$

Proof. If $a \mid b$ then there is a d such that $ad = b$. If $a \mid c$ then there is an e such that $ae = c$. Then $b + c = ae + ad = a(e + d)$. So a divides into $b + c$ and we conclude $a \mid (b + c)$ □

Theorem 2. $a \mid b$ then $a \mid bc$ for all numbers c

Proof. Suppose $a \mid b$, so there exists a d such that $ad = b$. So then $bc = (ad)c = a(dc)$. So a divides into bc and we conclude that $a \mid bc$. □

Theorem 3. if $a \mid b$ and $b \mid c$ then $a \mid c$

Proof. If $a \mid b$, then there is a d such that $ad = b$. If $b \mid c$ then there is an e such that $be = c$. Then $c = be = (ad)e = a(de)$. Since a divides into c, then $a \mid c$. □

2 Division Algorithm

Theorem 4. For any number n, there is a a d such that there there exists unique numbers q, r such that $n = dq + r$

Here q is called the quotient, r is called the remainder, and d is called the divisor.

For example, what time will it be after 277 hours if we begin at midnight? We may set $d = 24$ hours in the day, and then compute $r = 277 \pmod{2}4$ to get 13. Then we can compute q by computing $(277 - 13)/24 = 11$. So we know 11 full days will pass, and then 13 hours, so 1pm.

3 Modular Arithmetic

We may define the set $\mathbb{Z}_n = \{0, ..., n - 1\}$. We may further define modular multiplication and modular addition to only compute mod n, and only return elements of $\mathbb{Z}_n$.

$$a \pmod n + b \pmod n \equiv a + b \pmod n$$

$$a \pmod n \cdot b \pmod n \equiv ab \pmod n$$

One way to think about modular arithmetic, is if you are modding out by some n, you can consider only the numbers which are remainders without multiples of this n. That is if $a \equiv r \pmod{n}$, then there is a k such that $a = kn + r$.

Theorem 5. $a \equiv b \pmod{n} \iff n \mid (a - b)$

4 Representing numbers

We write numbers down in base ten simply because we have ten fingers, but there is nothing special about this use of ten. You can represent numbers in base two, base 8, base 16, base 7, or any other base >= 1.

Definition 4.1. A base b representation of a number $n \in \mathbb{N}$ is a sequence $c_k, c_{k-1}, ..., c_1, c_0$ such that

$$n = c_k b^k + ... + c_1 b + c_0$$

where $c_0, ..., c_k \in \{0, ..., b-1\}$.

Representing numbers in base 1 is never quite interesting. This is called unary, and simply looks like a pile of sticks

$$(111111111111)_1 = 12$$

Representing numbers in other bases is far more interesting

$$(1011)_2 = 2^3 + 2^2 + 1 = 13$$

$$0xBEEF = (BEEF)_{16} = (11 \cdot 16^3) + (14 \cdot 16^2) + (14 \cdot 16) + (15 \cdot 16^0) = 48879$$

Theorem 6 (Basis Representation Theorem)**.** For any number $n \in \mathbb{N}$, there exists exactly one representation of n in base b. Each number is uniquely represented in any base.

Proof. Consider $b \geq 2$, as the case $b = 1$ is trivial. Let $f_b(n)$ be the number of ways to represent n in base b. We prove that for any n and for any base b that $f_b(n) = 1$. If n is any number, we know that there is a k such that

$$n = c_k b^k + c_{k-1} b^{k-1} + ... + c_1 b + c_0$$

where $c_0, ..., c_k \in \{0, ..., b-1\}$. Then

$$n - 1 = c_k b^k + ... + (c_t - 1) b^t + \sum_{i=0}^{t-1} (b-1) b^i$$

which is a representation of $n - 1$. We took a representation of n, and showed there must exist a representation of $n - 1$. So every representation of n in base b implies the existence of a a representation of $n - 1$ in base b. We may then deduce $f_b(n) \leq f_b(n-1)$.

We can extend this farther. For any $m \leq n$, it is true that $f_b(m) \geq f_b(n)$. Since

$$f_b(n) \leq f_b(n-1) \leq f_b(n-2) \leq ... \leq f_b(m+1) \leq f_b(m)$$

Notice that b^n has atleast one representation. Also notice that 1 has at most one representation. So since also $b^n > n \geq 1$, we see that

$$1 \leq f_b(b^n) \leq f_b(n) \leq f_b(1) \leq 1$$

It can only be the case that $f_b(n) = 1$ and the proof is complete.

□