Number Theory

> *Mathematics is the queen of sciences and number theory is the queen of mathematics.*
>
> – Carl Friedrich Gauss

But why is it computer science?

- It turns out to be critical for cryptography!

Division

For $a, b \in Z$, $a \neq 0$, a *divides* b if there is some $c \in Z$ such that $b = ac$.

- Notation: $a \mid b$
- Examples: $3 \mid 9$, $3 \not\mid 7$

If $a \mid b$, then a is a *factor* of b, b is a *multiple* of a.

Theorem 1: If $a, b, c \in Z$, then

1. if $a \mid b$ and $a \mid c$ then $a \mid (b + c)$.
2. If $a \mid b$ then $a \mid (bc)$
3. If $a \mid b$ and $b \mid c$ then $a \mid c$ (divisibility is transitive).

Proof: How do you prove this? Use the definition!

Division

For $a, b \in Z$, $a \neq 0$, a *divides* b if there is some $c \in Z$ such that $b = ac$.

- Notation: $a \mid b$
- Examples: $3 \mid 9$, $3 \not\mid 7$

If $a \mid b$, then a is a *factor* of b, b is a *multiple* of a.

Theorem 1: If $a, b, c \in Z$, then

1. if $a \mid b$ and $a \mid c$ then $a \mid (b + c)$.
2. If $a \mid b$ then $a \mid (bc)$
3. If $a \mid b$ and $b \mid c$ then $a \mid c$ (divisibility is transitive).

Proof: How do you prove this? Use the definition!

- E.g., if $a \mid b$ and $a \mid c$, then, for some d_1 and d_2,

$$b = ad_1 \text{ and } \; c = ad_2.$$

- That means $b + c = a(d_1 + d_2)$
- So $a \mid (b + c)$.

Other parts: homework.

Division

For $a, b \in Z$, $a \neq 0$, a *divides* b if there is some $c \in Z$ such that $b = ac$.

- Notation: $a \mid b$
- Examples: $3 \mid 9$, $3 \not\mid 7$

If $a \mid b$, then a is a *factor* of b, b is a *multiple* of a.

Theorem 1: If $a, b, c \in Z$, then

1. if $a \mid b$ and $a \mid c$ then $a \mid (b + c)$.
2. If $a \mid b$ then $a \mid (bc)$
3. If $a \mid b$ and $b \mid c$ then $a \mid c$ (divisibility is transitive).

Proof: How do you prove this? Use the definition!

- E.g., if $a \mid b$ and $a \mid c$, then, for some d_1 and d_2,

$$b = ad_1 \text{ and } \; c = ad_2.$$

- That means $b + c = a(d_1 + d_2)$
- So $a \mid (b + c)$.

Other parts: homework.

Corollary 1: If $a \mid b$ and $a \mid c$, then $a \mid (mb + nc)$ for all $m, n \in Z$.

The division algorithm

Theorem 2: For $a \in Z$ and $d \in N$, $d > 0$, there exist unique $q, r \in Z$ such that $a = q \cdot d + r$ and $0 \leq r < d$.

- r is the remainder when a is divided by d

Notation: $r \equiv a \pmod{d}$; $a \bmod d = r$

The division algorithm

Theorem 2: For $a \in Z$ and $d \in N$, $d > 0$, there exist unique $q, r \in Z$ such that $a = q \cdot d + r$ and $0 \leq r < d$.

- r is the remainder when a is divided by d

Notation: $r \equiv a \pmod{d}$; a mod $d = r$

Examples:

- Dividing 101 by 11 gives a quotient of 9 and a remainder of 2, so $101 \equiv 2 \pmod{11}$ and $101 \bmod 11 = 2$.
- Dividing 18 by 6 gives a quotient of 3 and a remainder of 0, so $18 \equiv 0 \pmod{6}$ and $18 \bmod 6 = 0$.

The division algorithm

Theorem 2: For $a \in Z$ and $d \in N$, $d > 0$, there exist unique $q, r \in Z$ such that $a = q \cdot d + r$ and $0 \leq r < d$.

- r is the remainder when a is divided by d

Notation: $r \equiv a \pmod{d}$; $a \bmod d = r$

Examples:

- Dividing 101 by 11 gives a quotient of 9 and a remainder of 2, so $101 \equiv 2 \pmod{11}$ and $101 \bmod 11 = 2$.
- Dividing 18 by 6 gives a quotient of 3 and a remainder of 0, so $18 \equiv 0 \pmod{6}$ and $18 \bmod 6 = 0$.

Proof: The proof is constructive: We define q, r expicitly:
Let $q = \lfloor a/d \rfloor$ and define $r = a - q \cdot d$.

- So $a = q \cdot d + r$ with $q \in Z$ and $0 \leq r < d$ (since $q \cdot d \leq a$).

But why are q and d unique?

The division algorithm

Theorem 2: For $a \in Z$ and $d \in N$, $d > 0$, there exist unique $q, r \in Z$ such that $a = q \cdot d + r$ and $0 \leq r < d$.

- r is the remainder when a is divided by d

Notation: $r \equiv a \pmod{d}$; $a \bmod d = r$

Examples:

- Dividing 101 by 11 gives a quotient of 9 and a remainder of 2, so $101 \equiv 2 \pmod{11}$ and $101 \bmod 11 = 2$.
- Dividing 18 by 6 gives a quotient of 3 and a remainder of 0, so $18 \equiv 0 \pmod{6}$ and $18 \bmod 6 = 0$.

Proof: The proof is constructive: We define q, r expicitly:
Let $q = \lfloor a/d \rfloor$ and define $r = a - q \cdot d$.

- So $a = q \cdot d + r$ with $q \in Z$ and $0 \leq r < d$ (since $q \cdot d \leq a$).

But why are q and d unique?

- Suppose $q \cdot d + r = q' \cdot d + r'$ with $q', r' \in Z$ and $0 \leq r' < d$.
- Then $(q' - q)d = (r - r')$ with $-d < r - r' < d$.
- The lhs is divisible by d so $r = r'$ and we're done.

Primes

- If $p \in N$, $p > 1$ is *prime* if its only positive factors are 1 and p.
- $n \in N$ is *composite* if $n > 1$ and n is not prime.
  - If n is composite then $a \mid n$ for some $a \in N$ with $1 < a < n$
  - Can assume that $a \leq \sqrt{n}$.
    - **Proof:** By contradiction:
      Suppose $n = bc$, $b > \sqrt{n}$, $c > \sqrt{n}$. But then $bc > n$, a contradiction.

Primes: $2, 3, 5, 7, 11, 13, \ldots$
Composites: $4, 6, 8, 9, \ldots$

Primality testing

How can we tell if $n \in N$ is prime?

Primality testing

How can we tell if $n \in N$ is prime?

The naive approach: check if $k \mid n$ for every $1 < k < n$.

- But at least 10^{m-1} numbers are $\leq n$, if n has m digits
  - 1000 numbers less than 1000 (a 4-digit number)
  - 1,000,000 less than 1,000,000 (a 7-digit number)

So the algorithm is *exponential time*!

We can do a little better

- Skip the even numbers
- That saves a factor of 2 $\longrightarrow$ not good enough
- Try only primes (Sieve of Eratosthenes)
  - Still doesn't help much

Primality testing

How can we tell if $n \in N$ is prime?

The naive approach: check if $k \mid n$ for every $1 < k < n$.

- But at least 10^{m-1} numbers are $\leq n$, if n has m digits
  - 1000 numbers less than 1000 (a 4-digit number)
  - 1,000,000 less than 1,000,000 (a 7-digit number)

So the algorithm is *exponential time*!

We can do a little better

- Skip the even numbers
- That saves a factor of 2 $\longrightarrow$ not good enough
- Try only primes (Sieve of Eratosthenes)
  - Still doesn't help much

We can do much better:

- There is a polynomial time *randomized* algorithm
  - We will discuss this when we talk about probability
- In 2002, Agarwal, Saxena, and Kayal gave a (nonprobabilistic) polynomial time algorithm
  - Saxena and Kayal were undergrads in 2002!

The Fundamental Theorem of Arithmetic

Theorem 3: Every natural number $n > 1$ can be uniquely represented as a product of primes, written in nondecreasing size.

- Examples: $54 = 2 \cdot 3^3$, $100 = 2^2 \cdot 5^2$, $15 = 3 \cdot 5$.

Proving that that n can be written as a product of primes is easy (by strong induction):

- Base case: 2 is the product of primes (just 2)
- Inductive step: If $n > 2$ is prime, we are done. If not, $n = ab$.
  - Must have $a < n$, $b < n$.
  - By I.H., both a and b can be written as a product of primes
  - So n is product of primes

Proving uniqueness is harder.

- We'll do that in a few days ...