Rational Numbers, Divisibility and the Quotient Remainder Theorem

CS 231

Dianna Xu

Definition: Rational

- A real number is rational iff it can be expressed as a quotient of two integers with a nonzero denominator:
  - r is rational $\leftrightarrow \exists\, a, b \in \mathcal{Z}$ such that $r = a/b$ and $b \neq 0$
- $\mathcal{Q}$ and $\mathcal{R}$-$\mathcal{Q}$
  - -7/2351?
  - 0.56375631?
  - 0.325325325.....?

Prove or Disprove

- Every integer is rational
- $\forall x \in \mathcal{Z}, x \in \mathcal{Q}$
- Proof
  - Let x be a particular but arbitrarily chosen integer
  - $x = x/1$
  - $x, 1 \in \mathcal{Z}$ and $1 \neq 0$
  - $x \in \mathcal{Q}$ ■

Example

- The product of two rational numbers is rational
- Proof
  - let r and s be particular but arbitrarily chosen rational numbers
  - $r = a/b$ and $s = c/d$, $a, b, c, d \in \mathcal{Z}$ and $b \neq 0$ and $d \neq 0$
  - $rs = ac/bd$
  - $ac, bd \in \mathcal{Z}$ and $bd \neq 0$
  - rs is rational ■

Definition: Divisibility

- n and d are integers and $d \neq 0$
- n is divisible by $d \leftrightarrow \exists\, k \in \mathcal{Z}$ such that $n = dk$
- $d|n$
- If n/d is not an integer, then $d \nmid n$
- $d \leq n$
- Transitivity: $\forall a, b, c \in \mathcal{Z}, a|b \wedge b|c \rightarrow a|c$

Example

- $\forall a, b, c \in \mathcal{Z}, a|b \wedge a|c \rightarrow a|(b+c)$
- Proof
  - let a, b, c be particular but arbitrarily chosen integers such that $a|b \wedge a|c$
  - $a|b$: $\exists r \in Z, b = ra$
  - $a|c$: $\exists s \in Z, c = sa$
  - $b+c = ra + sa = (r+s)a$
  - $r+s \in Z$
  - $a|(b+c)$ ■

Unique Factorization of Integers

- Given any integer n>1, there exist
  - a positive integer k,
  - distinct prime numbers $p_1, p_2, \cdots, p_k$
  - positive integers $e_1, e_2, \cdots, e_k$, such that

$$n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k} = \prod_{i=1}^{k} p_i^{e_i}$$

7

Fundamental Theorem of Arithmetic

- A positive integer greater than 1 is either prime or a product of primes

$$999 = 3^3 \times 37$$

$$1000 = 2^3 \times 5^3$$

$$1001 = 7 \times 11 \times 13$$

8

Composite

- If n is a composite integer, then n has a prime divisor less than or equal to the square root of n
- Show that 899 is composite
- Proof
  - Divide 899 by successively larger primes (up to √899 = 29.98), starting with 2
  - We find that 29 (and thus 31) divide 899

9

The Prime Number Theorem

- The number of primes less than x is approximately $x/\ln(x)$
- Consider showing that 2^{650}-1 is prime
  - There are approximately 10^{193} prime numbers less than 2^{650}-1
- How long would it take to test each of those prime numbers?

10

Composite Factors

- Assume a computer can test 1 billion (10^9) per second
  - $10^{193}/10^9 = 10^{184}$ seconds = 3.2 x 10^{176} years!
- There are quicker methods to show a number is prime, but NOT to find the factors
- RSA encryption/decryption relies on the fact that one must factor very large composite n (1200-digit or so) into its component primes

11

Quotient/Remainer

- Given integer n and positive integer d, there exist unique integers q and r such that $n = dq + r$, $0 \le r < n$
- q is called the quotient and r the remainder
- q = n **div** d (n\\d) ← Integer Division!
- r = n **mod** d (n%d)
- n%d = n – d(n\\d)

12

Example

- Given an integer n, if n%13 = 5, what is 6n%13?
  - $n = 13q + 5$
  - $6n = 6(13q+5) = 13\text{x}6\text{x}q + 30$
  - $6n = 13\text{x}6\text{x}q + 13\text{x}2 + 4 = 13\text{x}(6q+2) + 4$
  - $6n$%13 = 4

13

Example

- Prove that if n is any integer not divisible by 5, then n^2 has a remainder of 1 or 4 when divided by 5
  - $n = 5q+1$, $5q+2$, $5q+3$ or $5q+4$
  - $(5q+1)^2 = 25q^2+10q+1 = 5(5q^2+2q) + 1$
  - $(5q+2)^2 = 25q^2+20q+4 = 5(5q^2+4q) + 4$
  - $(5q+3)^2 = 25q^2+30q+9 = 5(5q^2+6q+1) + 4$
  - $(5q+4)^2 = 25q^2+40q+16 = 5(5q^2+8q+3) + 1$

14

Inequality

- Prove $\frac{x+y}{2} \geq \sqrt{xy}, x, y \in R, x \geq 0, y \geq 0$
- Proof
  - $(x-y)^2 \geq 0$
  - $x^2 - 2xy + y^2 \geq 0 \Rightarrow x^2 + 2xy + y^2 \geq 4xy$
  - $\frac{x^2 + 2xy + y^2}{4} \geq xy \Rightarrow \left(\frac{x+y}{2}\right)^2 \geq \left(\sqrt{xy}\right)^2$
  - $\frac{x+y}{2} \geq \sqrt{xy}$ ■

15