Rational Numbers, Divisibility and the Quotient Remainder Theorem

CS 231

Dianna Xu

1

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 ↔ ∃ *a*, *b* ϵ *Z* such that *r* = *a*/*b* and *b* ≠ 0
- *Q* and *R*-*Q*
  - -7/2351?
  - 0.56375631?
  - 0.325325325.....?

2

Prove or Disprove

- Every integer is rational
- ∀*x* ϵ *Z*, *x* ϵ *Q*
- Proof
- Let *x* be a particular but arbitrarily chosen integer
- *x* = *x*/1
- *x*, 1 ϵ *Z* and 1 ≠ 0
- *x* ϵ *Q* ■

3

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* ϵ *Z* and *b* ≠ 0 and *d* ≠ 0
  - *rs* = *ac*/*bd*
  - *ac*, *bd* ϵ *Z* and *bd* ≠ 0
  - *rs* is rational ■

4

Definition: Divisibility

- *n* and *d* are integers and *d* ≠ 0
- *n* is divisible by *d* ↔ ∃ *k* ϵ *Z* such that *n* = *dk*
- *d*|*n*
- If *n*/*d* is not an integer, then $d \nmid n$
- *d* ≤ *n*
- Transitivity: ∀*a*, *b*, *c* ϵ *Z*, *a*|*b* ∧ *b*|*c* → *a*|*c*

5

Example

- ∀*a*, *b*, *c* ϵ *Z*, *a*|*b* ∧ *a*|*c* → *a*|(*b*+*c*)
- Proof
  - let *a*, *b*, *c* be particular but arbitrarily chosen integers such that *a*|*b* ∧ *a*|*c*
  - *a*|*b*: ∃*r* ϵ *Z*, *b* = *ra*
  - *a*|*c*: ∃*s* ϵ *Z*, *c* = *sa*
  - *b*+*c* = *ra* + *sa* = (*r*+*s*)*a*
  - *r*+*s* ϵ *Z*
  - *a*|(*b*+*c*) ■

6

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 = 3.2×10^{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 $n = dq + r$, $0 \leq r < n$
- q is called the quotient and r the remainder
- q = n **div** d ($n\backslash d$) ← Integer Division!
- r = n **mod** d ($n\%d$)
- $n\%d = n - d(n\backslash d)$

12

Example

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

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