2

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 $\Leftrightarrow \exists a, b \in Z$ such that *r* = *a*/*b* and *b* ≠ 0

- $\cdot Q$ and R-Q

 - 0.325325325....?

- Prove or Disprove
- · Every integer is rational
- ∀x ∈ *Z*, x ∈ *Q*
- Proof
- Let x be a particular but arbitrarily chosen integer
- -x = x/1
- -x, 1 $\in \mathbb{Z}$ and 1 \neq 0
- x ∈ Q ∎

Example

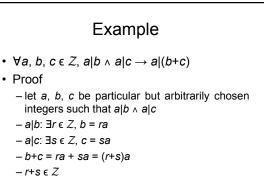
- The product of two rational numbers is rational
- Proof

3

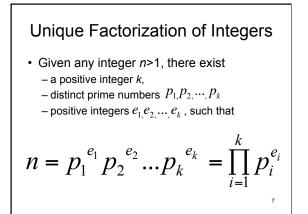
- let *r* and *s* be particular but arbitrarily chosen rational numbers
- -r = a/b and s = c/d, a, b, c, d $\in \mathbb{Z}$ and $b \neq 0$ and $d \neq 0$
- -rs = ac/bd
- -ac, $bd \in Z$ and $bd \neq 0$
- rs is rational ■

Definition: Divisibility

- *n* and *d* are integers and $d \neq 0$
- *n* is divisible by $d \Leftrightarrow \exists k \in \mathbb{Z}$ such that n = dk
- dln
- If *n*/*d* is not an integer, then *d*/*n*
- d ≤ n
- Transitivity: $\forall a, b, c \in \mathbb{Z}, a|b \land b|c \rightarrow a|c$



– a|(b+c) ∎



Fundamental Theorem of Arithmetic

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

 $999 = 3^3 \times 37$ $1000 = 2^3 \times 5^3$ $1001 = 7 \times 11 \times 13$

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 $\sqrt{899}$ = 29.98), starting with 2
 - We find that 29 (and thus 31) divide 899

The Prime Number Theorem

- The number of primes less than *x* is approximately *x*/ln(*x*)
- Consider showing that 2⁶⁵⁰-1 is prime

 There are approximately 10¹⁹³ prime numbers
 less than 2⁶⁵⁰-1
- How long would it take to test each of those prime numbers?

10

12

Composite Factors

- Assume a computer can test 1 billion (10⁹) 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
- $q = n \operatorname{div} d(n \setminus d) \leftarrow \operatorname{Integer Division!}$
- $r = n \mod d (n\%d)$
- $n\%d = n d(n\backslash d)$

Example

- Given an integer *n*, if *n*%13 = 5, what is 6*n*%13? *n* = 13q + 5
 - -6n = 6(13q+5) = 13x6xq + 30
 - -6n = 13x6xq + 13x2 + 4 = 13x(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* = 5*q*+1, 5*q*+2, 5*q*+3 or 5*q*+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

