Benjamin Fenster
MATH-054 (Puterbaugh)
1 February 2003

Notes – Chapter 3

Elementary Number Theory and Methods of Proof

Definitions

An integer n is <u>even</u> iff there exists an integer k such that n = 2k.
An integer n is <u>odd</u> iff there exists an integer k such that n = 2k + 1
n even $\Leftrightarrow \exists k \in \mathbb{Z} \ni n = 2k$
n odd $\Leftrightarrow \exists k \in \mathbb{Z} \ni n = 2k + 1$

Definitions

An integer n is <u>prime</u> if n > 1 and for all integers r and s, if n = r * s, then r = 1 or s = 1.
An integer n is <u>composite</u> if there exists positive integers r and s such that n = r * s and r 1 and s 1.
Consequence: n composite $\Rightarrow$ n > 1

Theorem

There exists real numbers a and b such that
(1)   (a+b) =   a + b
(2) (a+b)   a + b

Proof

(1) Let a = 1 and b = 0. Then (1 + 0) = 1 = 1 + 0
(2) Let a = 16, b = 9. Then (16 + 9) = 25 = 5. 16 + 9 = 4 + 3   = 7.

Proofs

Existential statements are easy to prove – just need to find one example.
Universal statements are harder. Try the Method of Exhaustion (for all elements in D, show that it works). Method of Direct Proof

Theorem

The sum of any two even integers is even.

Proof

Let m and n be even integers. There exists integers k and l such that m = 2k and n = 2l. The sum is m + n = 2k + 2l = 2(k+l). Since m + n is two times some integer, m + n is even.

Disproof

Disproof by counter-example is easy for universal statements but hard for existentials. For universals, just need to find one x that makes the predicate false.

Disprove

For all positive integers n, if n is prime, then $(-1)^n$ is (-1)

Disproof

Let n = 2, which is prime. $(-1)^2$ = +1 so the conditional is false.

Definitions

A real number r is <u>rational</u> iff there exist integers a and b with $b \neq 0$ such that $r = a / b$. A real number that is not rational is <u>irrational</u>

Theorem

Every integer is a rational number

Proof

Suppose there's an integer; call it n. Since $n = n / 1$ (which is the ratio of two integers), n is rational.

Theorem

The sum of any two rational numbers is rational.

Proof

Let r and s be two rational numbers. There exist integers a, b, c, and d, with $b \neq 0$ and $d \neq 0$ such that $r = a / b$ and $s = c / d$. So $r + s = a/b + c/d = (da + cb)/bd$ which is the ratio of two integers and $bd \neq 0$.

Corollary

Twice a rational number is a rational number.

Justification

Let $r = s$ in the previous proof.

Theorem

The product of any two rational numbers is a rational number.

Proof

Let r and s be rational numbers. There exist integers a, b, c, and d with $b \neq 0$ and $d \neq 0$ such that $r = a/b$ and $s = c/d$. $(rs) = (a/b) * (c/d) = (ac)/(bd)$. Since ac is an integer and bd is an integer not equal to zero, then rs is rational.

Prove or Disprove

The quotient of any pair of rational numbers is rational.

Disproof

1/0 is not rational because it violates the definition.

Prove or Disprove

The sum of two irrational numbers is irrational.

Disproof

$2 + (-2) = 0$

Definition

Let n and d be integers with $d \neq 0$. If there exists an integer k such that $n = dk$, then we say "d divides n," "n is divisible by d," "n is a multiple of d," "d is a factor of n," or "d is a divisor of n." We write $d \mid n$

$d \mid n \Leftrightarrow \exists x \in \mathbb{Z} \ni kd = n$

Theorem

Let a, b, and c be integers such that $a \mid b$ and $b \mid c$. Since $a \mid b$ there exists an integer k such that $ka = b$. Also, since $b \mid c$ there exists an integer m such that $mb = c$. Since $b = ka$, $c = mb = mka = (mk)a$. Since mk is an integer, $a \mid c$.

Theorem

Any positive integer $n > 1$ is divisible by a prime number.

Justification

n is any integer, $n > 1$

Case 1: n is prime. We're done!

Case 2: n is composite

$n = rs$ where $r \neq 1$ and $s \neq 1$ and $r, s \neq n$

If either is prime, we're done.

If neither is prime, pick one and divide it by some other r' and s'

Example

$n = 1800 = 18 * 100 = 18 * (4 * 25) = 18 * ((2 * 2) * 25)$

Theorem

Let a, b, and c be integers such that $a \mid b$ and $a \mid c$. Then $a \mid (b + c)$

Proof

Let a, b, and c be integers such that $a \mid b$ and $a \mid c$. There exist integers k and m such that $ak = b$ and $am = c$. Then $b + c = ak + am = a(k + m)$. Since $k + m$ is an integer, $a \mid (b + c)$

Theorem

The Quotient-Remainder Theorem

Given any integer n and positive integer d, there exist unique integers q and r such that n is equal to $dq + r$ and $0 \quad r < d$

d: Divisor. q: Quotient. r: Remainder

Definition

Given any non-negative integer n and positive integer d, n div d is the integer quotient when n is divided by d.

Also, n mod d is the integer remainder when n is divided by d.

Definition

The <u>parity</u> of an integer is whether it is even or odd.

Theorem

The square of an odd integer can be written in the form $8m + 1$ where m is an integer.

Proof

Let n be an odd integer. There exists an integer k such that $n = 2k + 1$. So $n^2 = (2k + 1)(2k + 1) = 4k^2 + 4k + 1 = 4k(k + 1) + 1$

Case 1:

Let k be even. There exists an integer p such that $k = 2p$. Then

$n^2 = 4(2p)(2p + 1) + 1 = 8p(2p + 1) + 1$ so $m = p(2p + 1)$

Case 2

Let k be odd. Then there exists an integer q such that $k = 2q + 1$ and

$n^2 = 4(2q + 1)(2q + 1 + 1) + 1 = 4(2q + 1)(2q + 2) + 1$

$= 8(2q + 1)(q + 1) + 1$ so $m = (2q + 1)(q + 1)$

Proof by Contradiction

$\sim p \rightarrow c$

$\therefore\ p$

Assume something is true. If it leads to a contradiction, the assumption is false.

Theorem

There is no least positive rational number

Proof

(By contradiction)

Assume there is a smallest positive rational number; call it r. Look at (0.5)r. It is still rational and positive, but (0.5)r < r (a contradiction). Thus there is no smallest rational number.

Proof by Contrapositive

Uses the fact that $p \rightarrow q \equiv \sim q \rightarrow \sim p$

Theorem

Given any positive integer n, if n^2 is odd then n is odd.

Proof

If n is even, then n^2 is even. Let n be an even integer. Then n = 2k for some integer k, so $n^2 = (2k)(2k) = 4k2 = 2(2k^2)$ which is even. Thus if n^2 is odd, n is odd.

Classic Theorem 1

2 is irrational

Proof

Assume that 2 is rational. There exist integers a and b, b $\neq 0$ such that 2 = a / b. Also a and b have no common factors. So b 2 = a or 2b $^2 = a^2$. Since $2b^2$ is even, a^2, and thus a, are even. So there exists an integer k such that a = 2k and $a^2 = 4k^2$. So $2b^2 = a^2 = 4k^2$ and $b^2 = 2k^2$. So b2 is even. Thus, b is even!!! So a and b are both divisible by 2. Thus 2 is irrational.

Theorem

3 + 2 is irrational.

Proof

Assume 3 + 2 is rational. 3 + 2 = a / b. 2 = a / b – 3 so 2 is rational!!!

Lemma

(A baby theorem only useful for proving some other theorem.)

For any integer a, and any prime number p, if p | a then p does not divide (a + 1).

Proof

Assume p | (a + 1). There exists an integer k such that pk = a + 1. Also, since p | a there exists an integer m such that pm = a. Note: 1 = (a + 1) – a = pk – pm = p(k – m), k $\neq$ m. So p | 1. But p > 1, so p cannot divide a + 1.

Classic Theorem 2

There are infinitely many prime numbers.

Proof (by Euclid)

Assume there are a finite number of primes; call them $p_1, p_2, p_3, \ldots, p_n$. Define $P = p_1 * p_2 * p_3 * \ldots * p_n$. Define N = P + 1. Since N > Pi, I = 1, 2, …, n, then N is not prime. There exists a prime number p such that p | N. But $p \mid p_1 * p_2 * p_3 * \ldots * p_n$ so p | P and p | (P + 1). That contradicts the Lemma, so there are infinitely many primes.