Number Theory: Divisibility

Freeman Cheng

Erindale Secondary School

October 22, 2018

Outline

Methods of Proof

- We will briefly cover direct proof and proof by contradiction.

Direct Proof

Example

Prove that the sum of two even numbers is even.

Proof by Contradiction

Example

Prove that $\sqrt{2}$ is irrational.

Introduction

(1.1) Definition

Let a and b be two integers, a being nonzero. We can say that a is a divisor of b if there exist an integer x such that $ax = b$.

- We use the notation $a|b$ to represent this.
- For example, $12|48$.

Properties

(Taken from Number Theory: Structures, Examples, and Problems by Dorin Andrica and Titu Andreescu).

1. If $a|b$ and $b \neq 0$, then $|a| \leq |b|$;
2. If $a|b$ and $a|c$, then $a|sb + tc$ for any integers s and t;
3. If $a|b$ and $a|b \pm c$, then $a|c$;
4. $a|a$;
5. If $a|b$ and $b|c$, then $a|c$;
6. If $a|b$ and $b|a$, then $|a| = |b|$.

Example

Problem 1

Find all positive integers n such that $n^2 + 1$ is divisible by $n + 1$ (W. Sierpinski).

Solution

Let a and b be integers, with a nonzero. Note that if $a|b$, then $a|b-ka$ for some integer k. Thus, it follows that

$$\begin{aligned} &n+1|n^2+1-(n-1)(n+1), \\ &n+1|n^2+1-(n^2-1), \\ &n+1|2. \end{aligned}$$

Since $n+1|2$ and $n>0$, we can conclude that $\boxed{n=1}$.

Problem

Problem 2

Let n be a positive integer divisible by 3. Explain why the sum of the digits of n is also divisible by 3.

- Use the same strategy as the previous problem.

Problem

Problem 3

Find all positive integers n for which the number obtained by erasing the last digit is a divisor of n.

Solution

Let the number after erasing the last digit be a and the last digit be b. Thus,

$$n = 10a + b.$$

It follows that

$$\begin{aligned} a &| n, \\ a &| 10a + b, \\ a &| b. \end{aligned}$$

Thus any number which ends in 0 will satisfy the conditions. If $b \neq 0$, then we can manually list out all n: 11, 12, 13, 14, 15, 16, 17, 18, 19, 22, 24, 26, 28, 33, 36, 39, 44, 48, 55, 66, 77, 88, 99.

Division Algorithm

(1.2) Division Algorithm

Let a and b be integers, with a positive. There must exist unique integers q and r such that $b = qa + r$ with $0 \leq r < a$.

- Note that q is the quotient and r is the remainder.

Proof (Optional)

The well-ordering principle is a prerequisite for this proof.

(1.3) Well-Ordering Principle

Every non-empty set of non-negative integers contains a least element.

First we prove that there must exist such a remainder. Given integers a and b and varying q, consider the set

$$S = \{b - qa \text{ such that } b - qa \geq 0\}.$$

Let the minimum of this set occur when $q = q_1$. For the sake of contradiction, let $r = b - q_1 a \geq a$. We arrive at a contradiction since

$$b - q_1 a \geq a \implies b - q_1(a + 1) \geq 0$$

(we get a new minimum). Thus, there will always exist such a remainder. (Inspired by Justin Stevens' book).

Greatest Common Divisor

(1.4) Definition

The greatest common divisor of two integers a and b is the largest number which is a divisor of both.

- We will use $\gcd(a, b)$ to represent greatest common divisor.
- We can find the GCD of two numbers by comparing prime factors. For example, find $\gcd(84, 98)$.
- If $\gcd(a, b) = 1$, we say that a and b are relatively prime.

Division Algorithm and GCD

Problem 4

Given integers b, q, a, r such that $b = qa + r$, prove

$$\gcd(b, a) = \gcd(a, r).$$

Solution

Suppose there is some integer c such that $c|b$ and $c|a$. It follows that

$$c|b - qa \implies c|r.$$

Now suppose that there is some integer d such that $d|a$ and $d|r$. It follows that

$$d|qa + r \implies d|b.$$

The pairs of integers (b, a) and (a, r) share the same common divisors, thus $\gcd(b, a) = \boxed{\gcd(a, r)}$.

Euclidean Algorithm

Problem 5

Explain why $\gcd(a, b) = \gcd(a, b - ka)$ for integers a, b, k.

- This is called the Euclidean Algorithm.
- Use the result of the previous problem to prove this.

A Problem From The First IMO

Problem 6

Prove that for all positive integers n, the fraction

$$\frac{21n+4}{14n+3}$$

is irreducible.

Solution 1

Our goal is to prove that $\gcd(21n+4, 14n+3) = 1$. We apply the Euclidean Algorithm. We have

$$\gcd(21n+4, 14n+3) = \gcd(7n+1, 14n+3) = \gcd(7n+1, 1) = 1.$$

Our proof is complete.

Solution 2

Notice that if $d|a$ and $d|b$ then $d|sa + tb$ for any integers s, t. Since

$$(-2)(21n + 4) + (3)(14n + 3) = 1,$$

the two numbers share no common factor other than 1, implying that the fraction is irreducible.

More Problems

Problem 7

Prove that $n^5 - 5n^3 + 4n$ is divisible by 120.

Problem 8

What is the largest positive integer n such that $n^3 + 100$ is divisible by $n + 10$ (AIME).

Problem 9

Show that for any natural number $n \geq 2$, one can find three distinct natural numbers a, b, c between n^2 and $(n+1)^2$ such that $a^2 + b^2$ is divisible by c.

Next Week

- We will do more problems.
- Introduce the relation between GCD and LCM.