Math 214 Foundations of Higher Mathematics C.K. Li

Chapter 11 Number Theory

We practice proof techniques using number theory problems.

A goal: Prove the Fundamental Theorem of Arithmetic.

11.1 Divisibility

Definition A positive integer $p \geq 2$ is a prime if 1 and p are the only positiver integer factor (divisor) of p. A positive integer $n \geq 2$ is a composite number if it is not a prime.

Lemma A positive integer $n \geq 2$ is composite if and only if $n = ab$ with $a, b \in \mathbf{N}$ such that $1 < a < n$ and $1 < b < n$.

Theorem Let a, b, c be integers such that $a \neq 0$.

(1) If $a|b$, then $a|bc$. (2) If $a|b$ and $b|c$, then $a|c$. (3) If $a|b$ and $a|c$, then $a|(b + c)$.

Suppose b is also nonzero.

(a) If $a|b$ and $b|a$, then $a = b$ or $a = -b$. (b) If $a|b$, then $|a| \leq |b|$.

11.2 Division Algorithm

Theorem Suppose $a, b \in \mathbf{N}$. Then there are unique integers a and r such that $b = aq + r$ with $0 \leq r < a$.

Proof. Consider $S = \{b - ax : x \in \mathbf{Z}, b - ax \geq 0\}$. Then ....

Corollary (General form of the Division Algorithm) Suppose $a, b \in \mathbf{Z}$ and $a \neq 0$. Then there exist unique integers q and r such that $b = aq + r$ with $0 \leq r < |a|$.

Partition of integers in remainder classes

Definition/notation Let $n \geq 2$ be a positive integers.

$$\mathbf{Z}_n = \{[0], [1], \ldots, [n-1]\}$$

with $[k] = \{nx + k : x \in \mathbf{Z}\}$ is a partition of $\mathbf{Z}$. We say that

$$a \equiv b \pmod{n} \qquad \text{if} \qquad a - b \text{ is divisible by } n.$$

11.3 Greatest common divisors

Definition Suppose $a, b \in \mathbf{Z}$ are not both zero. Then their greatest common divisor is the largest common divisor of a and b.

Theorem Let $a, b \in \mathbf{Z}$ are not both zero. Then the following condition are equivalent.

(1) d is the greatest common divisor of a and b.

(2) d is the smallest element in the set

$$\{ax + by : x, y \in \mathbf{Z}, ax + by \in \mathbf{N}\}.$$

(3) d is a common divisor of a and b, and $c|d$ for any common divisor c of a and b.

11.4 Euclidean Algorithm

Lemma Let $a, b \in \mathbf{N}$. If $b = aq + r$ with $0 \leq r < a$, then $\gcd(a, b) = \gcd(r, a)$.

Consequently, there are positive integers $r_1 > r_2 > r_3 \cdots > r_{n-1}$ such that

$$\gcd(a, b) = \gcd(r_1, a) = \gcd(r_1, r_2) = \cdots = \gcd(0, r_{n-1}) = r_{n-1}.$$

Example: $\gcd(374, 946) =$

11.5 Relatively Prime Integers

Definition Let $a, b \in \mathbf{Z}$, not both zero. Then they are relatively prime if $\gcd(a, b) = 1$.

Theorem Let $a, b \in \mathbf{Z}$, not both zero. Then $\gcd(a, b) = 1$ if and only if there are $x, y \in \mathbf{Z}$ such that $ax + by = 1$.

Question. How to find x and y.

Theorem (Euclid's Lemma) If $a|(bc)$ and $\gcd(a,b) = 1$, then $a|c$.

Corollary Let p is a prime. If $p|bc$, then $p|b$ or $p|c$. More generally, for any integers $a_1, \ldots, a_n$ with $n \geq 2$, if $p|a_1 \cdots a_n$ then $p|a_i$ for some $i \in \{1, \ldots, n\}$.

Theorem Let $a, b, c \in \mathbf{Z}$ such that $ab \neq 0$ and $\gcd(a,b) = 1$. If $a|c$ and $b|c$, then $(ab)|c$.

11.6 The Fundamental Theorem of Arithmetic

Theorem Every integer $n \geq 2$ is a product of primes $p_1 \cdots p_m$. The factorization is uniques up to a rearrangement of $p_1, \ldots, p_m$. That is: if n is a product of primes $q_1 \cdots q_r$, then $r = m$, and $q_1, \ldots, q_m$ is a rearrangement of $p_1, \ldots, p_m$.

Theorem Every integer $n \geq 2$ has a prime factor. If n is not a prime, then there is a prime factor of size not larger than $\sqrt{n}$.

Theorem If $n \in \mathbf{N}$ such that $n \neq k^2$ for some $k \in \mathbf{N}$, then $\sqrt{n}$ is irrational.

Theorem There are infinitely many prime numbers.

Question There are infinitely pair of twin primes, i.e., $(p, p+2)$ pairs such that both p and $p+2$ are primes.

Example $(3, 5), (5, 7), (11, 13)$.

11.7 Sum of divisor

Definition An integer $n \geq 2$ is a perfect number if n is the sum of its proper factors, i.e., factors strictly smaller than n.

Examples $6, 28, 496$.

Questions Is there an odd perfect numbers?

Are there infinitely many even perfect numbers?

Definition A pair of integers $n, n+1$ are Ruth-Aaron pair if the sums of their prime divisors are equal.

Theorem (Erdös) There are infinitely many pairs of Ruth-Aaron pairs.