MATH 2513-001 Discrete Mathematics Fall 2009

Elementary Number Theory

The aim of this section of the course is to prove the *Fundamental Theorem of Arithmetic*, and to give some of its applications. We shall also introduce congruences and modular arithmetic.

1. **Theorem.** (Fundamental Theorem of Arithmetic) Every integer $n \geq 2$ can be written as a product

$$n = p_1 \dots p_k$$

of primes p_i. Furthermore, this expression is unique up to rearranging the primes p_i.

Just give a proof of the existence part for now. Use well ordering of $\mathbb{Z}^+$.

2. **Definition.** $p \in \mathbb{Z}^+$ is said to be *prime* if $p \neq 1$ and the only divisors of p are $\pm p$ and ± 1.

3. **Theorem.** (Infinitely many primes) There are infinitely many primes.

4. **Examples.** Use fundamental theorem to prove the following: $\sqrt{2}$ is irrational; the only positive integers n for which $\sqrt{n}$ is rational are the squares; $\log_2(3)$ is irrational; how many zeroes are there at the end of 100!

5. **Definition.** (Divides) Let $a, b \in \mathbb{Z}$. We say that b *divides* a, written $b|a$, if $a = bc$ for some $c \in \mathbb{Z}$. We write $b \not| a$ if b does not divide a.

6. **Theorem.** (Test for primes) Let $n \in \mathbb{Z}^+ - \{1\}$. If $p \not| n$ for each prime $p \leq \sqrt{n}$, then n is prime.

7. **Theorem.** (Properties of divides) Let $a, b, c \in \mathbb{Z}$. Then

   (a) if $a|b$ and $a|c$, then $a|(b + c)$;

   (b) if $a|b$, then $a|bc$ for all $c \in \mathbb{Z}$;

   (c) if $a|b$ and $b|c$, then $a|c$.

8. **Theorem.** (Division Algorithm) Let $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^+$. Then there exist unique $q, r \in \mathbb{Z}$, so that $0 \leq r < b$ and

$$a = bq + r$$

9. **Definition.** (Greatest common divisor) Let $a, b \in \mathbb{Z}$, not both zero. The largest integer d such that $d|a$ and $d|b$ is called the *greatest common divisor of a and b*. It is denoted by $\gcd(a, b)$.

10. **Definition.** (Relatively prime) Say that $a, b \in \mathbb{Z}$ are *relatively prime* if $\gcd(a, b) = 1$.

    In general, we say that integers $a_1, \dots, a_n$ are *relatively prime* if $\gcd(a_i, a_j) = 1$ for all $1 \leq i < j \leq n$.

11. **Theorem.** (gcd is a linear combination) Let $a, b \in \mathbb{Z}^+$. Then there exist $s, t \in \mathbb{Z}$ so that

$$\gcd(a, b) = sa + tb$$

Two proofs. 1. Use back substitution and Euclidean Algorithm. 2. Use well ordering of $\mathbb{Z}^+$.

12. **Lemma.** (Divisibility result) Let $a, b, c \in \mathbb{Z}^+$. If $a|bc$ and $\gcd(a, b) = 1$, then $a|c$.
    This divisibility result is a fundamental application of 11.

13. **Lemma.** If p is prime and $p|a_1 \dots a_n$ then $p|a_i$ for some $i \in \{1, \dots, n\}$.

14. **Application.** Give the proof of the uniqueness part of the Fundamental Theorem.

15. **Lemma.** (Key step of Euclidean Algorithm) Let $a, b \in \mathbb{Z}^+$. If $a = bq + r$ then $\gcd(a, b) = \gcd(b, r)$.

16. **Theorem.** (Euclidean Algorithm. Practical computation of gcd) Let $a, b \in Z^+$. Use the Division Algorithm to write $a = bq_1 + r_1$ for $q_1, r_1 \in \mathbb{Z}$, and $0 \leq r_1 < b$. Then

$$\gcd(a, b) \;=\; \gcd(b, r_1)$$

Continue using the Division Algorithm to get
$b = r_1 q_2 + r_2$, with $0 \leq r_2 < r_1$
$r_1 = r_2 q_3 + r_3$, with $0 \leq r_3 < r_2$
$\vdots$
$r_{n-1} = r_n q_{n+1} + 0$.

Then $r_n = \gcd(a, b)$.

17. **Definition.** (Least common multiple) Let $a, b \in \mathbb{Z}^+$. The *least common multiple of* a *and* b is the smallest positive integer m so that $a|m$ and $b|m$. It is denoted by $\operatorname{lcm}(a, b)$.

18. **Another application of 11.** (lcm, gcd and product) Let $a, b \in \mathbb{Z}^+$. Then

$$ab \;=\; \operatorname{lcm}(a, b)\gcd(a, b)$$

19. **Application of fundamental theorem.** Interpret $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$ in terms of prime decompositions.

20. **Definition.** (Congruence) Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. Say that a *is congruent to* b *modulo* m, written $a \equiv b \pmod{m}$, if $m|(a - b)$.

    Equivalently, $a \equiv b \pmod{m}$ if $a = kb + m$ for some $k \in \mathbb{Z}$.

21. **Theorem.** (Properties of congruence) Let $a, b, c \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. Then

    (a) if $a \equiv a \pmod{m}$;
    (b) if $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$;
    (c) if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

22. **Theorem.** (Further properties of congruence) Let $a, b, c, d \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. Suppose that $a \equiv b \pmod{m}$ and that $c \equiv d \pmod{m}$. Then

    (a) $a + c \equiv b + d \pmod{m}$, and
    (b) $ac \equiv bd \pmod{m}$.