< Summary of Number Theory >

Discussed in class:

<u>Definition</u> An integer a divides an integer b (denoted $a|b$) if there is some integer k such that $b = ak$.

<u>Theorem</u> $\prod_{i=0}^{k}(n+i)$ is divisible by k for all positive integers k.

<u>Theorem</u> (The Division Algorithm)
For positive integers a and b, there exist unique integers q and r such that $a = bq + r$ with $0 \leq r < b$.

<u>Definition</u> $[a]_b = r_b^a$ denotes the remainder of a when divided by b.

<u>Theorem</u> (Modular Arithmetic)
Let a, b and c be integers with $c \neq 0$, then

1. $[a+b]_c = [r_c^a + r_c^b]_c$
2. $[a-b]_c = [r_c^a - r_c^b]_c$
3. $[a \cdot b]_c = [r_c^a \cdot r_c^b]_c$

<u>Theorem</u> Given two integers b and n, where n is a $k+1$-place digit that can be expressed as $n = n_0 10^0 + \cdots + n_k 10^k$, n is divisible by b iff

$$[n_0]_b c^0 + \cdots + [n_k]_b c^k$$

where $c = [10]_b$.

<u>Definition</u> A rational number is a number r that can be expressed in the form of $r = \frac{p}{q}$ where p and q are integers such that $q \neq 0$.

<u>Theorem</u> If two integers a and b are rational, then the following are also rational:

1. $a \pm b$
2. $a \cdot b$
3. a/b

<u>Theorem</u> If $d|a$ and $d|b$, then $a|(ax \pm by)$ for all integers x and y.

<u>Definition</u> Two integers a and b are said to share a common factor c if $c|a$ and $c|b$.

<u>Definition</u> The greatest common divisor of a and b (denoted as gcd (a, b)) is the common factor such that $d \leq$ gcd (a, b) for all other common factors d.

<u>Definition</u> Two integers a and b are relatively prime if $\gcd(a, b) = 1$.

<u>Definition</u> An integer p is a prime if its only divisors are 1 and p.

<u>Theorem</u> (Fundamental Theorem of Arithmetic)
Every positive integer n can be decomposed as a product of primes

$$n = {p_1}^{a_1} {p_2}^{a_2} \ldots {p_k}^{a_k}$$

where p_i is the i-th largest prime such that $p_i \neq p_j$ whenever $i \neq j$ and a_i is some integer exponent corresponding to the i-th prime.
Also, the decomposition is unique: Let s and t be two positive integers where $s = {p_1}^{s_1} {p_2}^{s_2} \ldots {p_k}^{s_k}$ and $t = {p_1}^{t_1} {p_2}^{t_2} \ldots {p_k}^{t_k}$. Then, whenever $s = t$, we have $s_i = t_i$ for all $1 \leq i \leq k$.

Theorem $\sqrt{n}$ is rational if and only if $\sqrt{n}$ is an integer.

Theorem If p is a prime, then $\sqrt{p}$ is not an integer.

Corollary If p is a prime, then $\sqrt{p}$ is irrational.
(This result can be generalized to $\sqrt[n]{p}$ where $n \geq 2$.)

Discussed in the textbook:

Theorems 4.1, 4.2 and 4.3 Let a, b, c and d be integers with $a \neq 0$ and $b \neq 0$.

1. If $a|b$ and $b|c$, then $a|c$.
2. If $a|b$ and $c|d$, then $ac|bd$.
3. For all $x, y \in \mathbb{Z}$, if $a|b$ and $a|c$, then $a|(bx + cy)$.

Lemma 11.1 An integer $n \geq 2$ is composite if and only if there exist integers a and b such that $n = ab$ where $1 < a < n$ and $1 < b < n$.

Theorem 11.3 Let a and b be nonzero integers.
i) If $a|b$ and $b|a$, then $a = b$ or $a = -b$.
ii) If $a|b$, then $|a| \leq |b|$.

Definition For integers a and b, an integer of the form $ax + by$, where $x, y \in \mathbb{Z}$, is called a linear combination of a and b.

Theorem 11.7 Let a and b be integers that are not both 0. Then $\gcd(a, b)$ is the smallest positive linear combination of a and b.

Theorem 11.8 Let a and b be two integers not both 0. Then $d = \gcd(a, b)$ if and only if d is the positive integer which satisfies the following two conditions:

1. d is a common divisor of a and b;
2. if c is any common divisor of a and b, then $c|d$.

Lemma 11.9 (The Euclidean Algorithm)
Let a and b be positive integers. If $b = aq + r$ for some integers q and r, then $\gcd(a, b) = \gcd(r, a)$.[I]

Theorem 11.12 Let a and b be integers that are not both 0. Then $\gcd(a, b) = 1$ iff there exist integers s and t such that $as + bt = 1$.[II]

Theorem 11.13 (Euclid's Lemma)
Let a, b and c be integers, where $a \neq 0$. If $a|bc$ and $\gcd(a, b) = 1$, then $a|c$.

Corollary 11.14 Let b and c be integers and let p be a prime. If $p|bc$, then $p|b$ or $p|c$.[III]

[I] In essence, to find the greatest common divisor, first divide b by a (assuming that $a < b$), obtain the first remainder, then use the first remainder to divide a. Repeat the process until $r = 0$, in which case $\gcd(r^*, 0) = r^*$ for some integer r^*. The remainder is guaranteed to converge to zero since $0 \leq r_{i+1} < r_i$ and r_i can only decrease as more divisions are performed.

[II] This is very much a corollary of the linearity of $\gcd(a, b)$.

[III] This result can be extended to products of multiple integers.

Theorem 11.16 Let $a, b, c \in \mathbb{Z}$, where a and b are relatively prime nonzero integers. If $a|c$ and $b|c$, then $ab|c$.

Lemma 11.19 If n is a composite number, then n has a prime factor p such that $p \leq \sqrt{n}$

From assignments:

11.28 Let a and b be integers not both 0. There are infinitely many pairs s, t o f integers such that $\gcd(a, b) = as + bt$.

11.37 If $p \geq 2$ is an integer with the property that for every pair a, b of integers $p|ab$ implies that $p|a$ or $p|b$, then p is prime.[IV]

11.38 a) Every consecutive odd positive integers are relatively prime.

Other Topics:

- Irrationality of $\sqrt{2}$, $\sqrt{3}$, $\sqrt{8}$ and other numbers.
- Infinitude of primes
- Sieve of Eratosthenes

[IV] This is the converse of Theorem 11.14.