Math 170 Midterm Formula Sheet

October 28, 2008

1 Properties of gcd and Factorization

Definition 1.0.1. Recall a natural number is one of $\{0, 1, 2, 3, \cdots\}$.

Definition 1.0.2. Recall an integer is one of $\{\cdots, -2, 1, 0, 1, 2, 3, \cdots\}$ (i.e. a positive whole number, a negative whole number, or zero).

Theorem 1.0.3 (Fundamental Theorem of Arithmetic)**.** *Every natural number can be uniquely factored as a product of primes.*

In other words, every natural number n is of the form

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot \cdots \cdot p_m^{a_m}$$

Where the $p_1, p_2, \ldots, p_m$ are all prime. Further, up to reordering, there is only one such way to factor n.

Theorem 1.0.4. *If*

- *x divides a*
- *x divides b*

Then x divides $gcd(a, b)$

Theorem 1.0.5 (Division with Remainder)**.** *For all natural numbers $0 < a \leq b$ there exists q, r such that*

- $b = a \cdot q + r$
- $0 \leq r < a$

Theorem 1.0.6 (Uses Extended Euclid's Algorithm)**.** *For all natural numbers a, b there are integers x, y such that*

$$x \cdot a + y \cdot b = gcd(a, b)$$

Definition 1.0.7. Recall that $\phi(n)$ is the number of natural numbers less than or equal to n which do not have any prime factors in common with n

Theorem 1.0.8. *Suppose*

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_m^{a_m}$$

with $p_1, \dots, p_m$ the prime factors of n. Then

$$\phi(n) = n \cdot \frac{p_1 - 1}{p_1} \cdot \frac{p_2 - 1}{p_2} \cdot \dots \cdot \frac{p_m - 1}{p_m}$$

Theorem 1.0.9. *Suppose*

$$n = p_1 \cdot p_2$$

with p_1, p_2 primes. Then

$$\phi(n) = (p_1 - 1)(p_2 - 1)$$

Note this is a special case of 1.0.8

Theorem 1.0.10. *Suppose p is prime then*

$$\phi(p) = (p - 1)$$

Note this is a special case of 1.0.8

2 Properties of Multiplication and Exponents

Theorem 2.0.11. *For all x, y, a, b*

- $(x \cdot y)^a = x^a \cdot y^a$
- $(x^a)^b = x^{a \cdot b}$
- $x^{a+b} = x^a \cdot y^a$

Theorem 2.0.12. *For all integers a, b we have*

$$\frac{1}{\frac{a}{b}} = \frac{b}{a}$$

3 Modular Arithmetic

Definition 3.0.13. $a = b \bmod n$ if the remainder when you divide a by n is the same as the remainder when you divide b by n.

Theorem 3.0.14. *$a = b \ mod \ n$ if and only if $a - b$ is a multiple of n*

Theorem 3.0.15. *Let a, b, n be integers. Then*

- $(a + b) \ mod \ n = (a \ mod \ n) + (b \ mod \ n)$
- $(a \times b) \ mod \ n = (a \ mod \ n) \times (b \ mod \ n)$
- $(a)^m \ mod \ n = (a \ mod \ n)^m$

Theorem 3.0.16 (Fermat's Little Theorem)**.** *If $0 \leq a < p$ and p is prime then*

$$a^{p-1} = 1 \ mod \ p$$

Theorem 3.0.17 (Euler's Theorem)**.** *If* $gcd(a, n) = 1$ *then*

$$a^{\phi(n)} = 1 \ mod \ n$$

Note Fermat's little theorem is a special case of Euler's theorem.

3.1 Bar Codes and Check Digits

Theorem 3.1.1. *Suppose we have a 12 digit bar code:*

$$d_1, d_2, d_3, d_4, d_5, d_6, d_7, d_8, d_9, d_{10}, d_{11}, d_{12}$$

Then we know that

$$3 \cdot d_1 + d_2 + 3 \cdot d_3 + d_4 + 3 \cdot d_5 + d_6 + 3 \cdot d_7 + d_8 + 3 \cdot d_9 + d_{10} + 3 \cdot d_{11} + d_{12} = 0 \ mod \ 10$$

d_{12} *is called the check digit and it is chosen to make the above equation hold.*

4 Misc

Definition 4.0.2. If f is a function.

$$\sum_{i=n}^{m} f(i) = f(n) + f(n+1) + f(n+2) + \cdots + f(m-1) + f(m)$$

Definition 4.0.3. $0! = 1$ and $n! = n \times (n-1)!$ if $n > 0$ or

$$n! = n \times (n-1) \times (n-2) \times \cdots \times 3 \times 2 \times 1 \times 0$$