Formula Sheet for Midterm in Math 170 (Fall 2007)

by Nathanael Leedom Ackerman

October 16, 2007

1 Fibonacci Numbers

Let F_n be the nth Fibonacci number. Then

- $F_0 = 0$, $F_1 = 1$
- If $n > 1$ then $F_n = F_{n-1} + F_{n-2}$

2 Properties of gcd and Factorization

Definition 2.0.1. Recall a natural number is one of $\{0, 1, 2, 3, \cdots\}$.

Definition 2.0.2. 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 2.0.3 (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 2.0.4. *If*

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

Then x divides $gcd(a, b)$

Theorem 2.0.5 (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 2.0.6 (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 2.0.7. 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 2.0.8. *Suppose*

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

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

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

Theorem 2.0.9. *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 2.0.8

Theorem 2.0.10. *Suppose* p *is prime then*

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

Note this is a special case of 2.0.8

3 Properties of Multiplication and Exponents

Theorem 3.0.11. *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 3.0.12. *For all integers* a, b *we have*

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

4 Fractions and Real Numbers

Theorem 4.0.13. *Every fraction* $\frac{a}{b}$ *can be written as*

$$\frac{a}{b} = \frac{c}{d}$$

where $gcd(c, d) = 1$*.*

We say $\frac{c}{d}$ *is the fraction in lowest terms*

4.1 Continued Fractions

Recall $[a_1, a_2, \dots]$ is a continued fraction

$$[a_1, a_2, a_3, \dots] = a_1 + \frac{1}{[a_2, a_3, \dots]} = a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{\dots}}}$$

4.2 Decimal Expansions

Definition 4.2.1. Recall that if $a_1, \ldots a_n$ are between 0 and 9 (inclusive) then

$$0.a_1a_2\ldots a_n = \frac{a_1a_2\ldots a_n}{10^n}$$

(here 10^n is a 1 with n 0's after it).

Definition 4.2.2. We then define

$$0.\overline{a_1a_2\ldots a_n} = 0.a_1a_2\ldots a_na_1a_2\ldots a_na_1a_2\ldots a_n\cdots$$

And we showed that

Theorem 4.2.3.

$$0.\overline{a_1a_2\ldots a_n} = \frac{a_1a_2\ldots a_n}{999\ldots 9}$$

where in the denominator there are n 9's.

5 Rational and Irrational Numbers

Definition 5.0.4. Recall that a real number x is Rational if it can be written as $x = \frac{a}{b}$. If a real number isn't rational it is *Irrational*

Definition 5.0.5. Recall that $\sqrt{x}$ is the positive real number y such that $y^2 = x$.

Theorem 5.0.6. *Let n be a natural number such that*

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

Then $\sqrt{n}$ is rational if and only if every a_i is even. (If $\sqrt{n}$ is not rational it is irrational).

Definition 5.0.7. Recall that $\sqrt[m]{x}$ is the positive real number y such that $y^m = x$.

Theorem 5.0.8. *Let n be a natural number such that*

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

Then $\sqrt[m]{n}$ is rational if and only if every a_i is a multiple of m. (If $\sqrt[m]{n}$ is not rational it is irrational).

6 Modular Arithmetic

Definition 6.0.9. $a = b$ mod n if the remainder when you divide a by n is the same as the remainder when you divide b by n.

Theorem 6.0.10. *$a = b$ mod n if and only if $a - b$ is a multiple of n*

Theorem 6.0.11. *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 6.0.12 (Fermat's Little Theorem)**.** *If $0 \leq a < p$ and p is prime then*

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

Theorem 6.0.13 (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.

6.1 Bar Codes and Check Digits

Theorem 6.1.1. *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.*