MAT310: Number Theory Overview

Abstract

We've been over a lot of terrain in this course. Some themes have, however, been appearing over and over. Well-ordering, the division algorithm, prime factorizations, Diophantine equations, various proof techniques (including contradiction and induction), and certainly math history have had important roles in this course.

I hope that you have a better sense of where mathematics has come from (and maybe even where it's going!). One thing we've seen is that, in spite of number theory's purity, it is also absolutely essential to some modern applications of mathematics (e.g. information security). Pythagorean triples arose from an application, and then formed the basis of Fermat's last theorem.

1 Section 1.1

Some useful preliminaries:

- **Well-Ordering Principle**
- **Archimedean property**
- **First Principle of Finite Induction**
- **Second Principle of Finite Induction**
- **Binomial Theorem**
- **Pascal's rule**

2 Section 2.1

- **Division Algorithm**: Given integers a and b, with $b > 0$, there exist unique integers q and r satisfying

  $$a = qb + r$$

  with $0 \leq r < b$. q is called the **quotient**, and r is called the **remainder**.

  Corollary: Given integers a and b, with $b \neq 0$, there exist unique integers q and r satisfying

  $$a = qb + r$$

  with $0 \leq r < |b|$.

3 Section 2.2

- **common divisor**
- **greatest common divisor**
- **relatively prime**:
- **Theorem 2.2**: For integers a, b, c, the following hold:
  1. $a|0$, $1|a$, $a|a$
  2. $a|1$ if and only if $a = \pm 1$
  3. If $a|b$ and $c|d$, then $ac|bd$.
  4. If $a|b$ and $b|c$, then $a|c$.
  5. $a|b$ and $b|a$ if and only if $a = \pm b$
  6. If $a|b$ and $b \neq 0$, then $|a| \leq |b|$.
  7. If $a|b$ and $a|c$, then $a|(bx + cy)$ for arbitrary integers x and y.

- **Theorem 2.3**: Given integers a and b, not both zero, there exists integers x and y such that

$$\gcd(a, b) = ax + by$$

Corollary: If a and b are given integers, not both zero, then the set

$$T = \{ax + by | x, y \text{ are integers}\}$$

is precisely the set of all multiples of $d = \gcd(a, b)$.

- **Theorem 2.4**: Let a and b be integers, not both zero. Then a and b are relatively prime if and only if there exist integers x and y such that $1 = ax + by$.

Corollary 1: If $\gcd(a, b) = d$, then $\gcd(a/d, b/d) = 1$.

Corollary 2: If $a|c$ and $b|c$, with $\gcd(a, b) = 1$, then $ab|c$.

- **Theorem 2.5 (Euclid's lemma)**: If $a|bc$, with $\gcd(a, b) = 1$, then $a|c$.

- **Theorem 2.6**: Let a and b be integers, not both zero. For a positive integer d, $d = \gcd(a, b)$ if and only if

1. $d|a$ and $d|b$, and
2. Whenever $c|a$ and $c|b$, then $c|d$.

4 Section 2.3

- **least common multiple**

- **Lemma**: If $a = qb + r$, then $\gcd(a, b) = \gcd(b, r)$

- **Euclidean Algorithm**:

$$\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \ldots = \gcd(r_{n-1}, r_n) = r_n$$

(i.e. $r_n | r_{n-1}$, so the final remainder is 0). Then $\gcd(a, b) = r_n$.

- **Theorem 2.7**: if $k > 0$, then $\gcd(ka, kb) = k\gcd(a, b)$.

  Corollary: if $k \neq 0$, then $\gcd(ka, kb) = |k|\gcd(a, b)$.

- **Theorem 2.8**: For positive integers a and b

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

  Corollary: For positive integers a and b

$$\text{lcm}(a, b) = ab \iff \gcd(a, b) = 1$$

5 Section 2.4

- **Diophantine equation**

- **Theorem 2.9**: The linear Diophantine equation $ax + by = c$ has a solution iff $d|c$, where $d = \gcd(\text{a,b})$. If (x_0, y_0) is any particular solution of this equation, then all other solutions are given by

$$x = x_0 + \left(\frac{b}{d}\right)t \qquad y = y_0 - \left(\frac{a}{d}\right)t$$

  for integral values of t.

  Corollary: If $1 = \gcd(\text{a,b})$, and (x_0, y_0) is any particular solution of the equation $ax + by = c$, then all other solutions are given by

$$x = x_0 + bt \qquad y = y_0 - at$$

  for integral values of t.

6 Section 3.1

- **prime, composite**
- **Theorem 3.1**: If p is prime and $p|ab$, then $p|a$ or $p|b$.

  Corollary 1: If p is prime and $p|a_1a_2\ldots a_n$, then $p|a_k$ for some k, $1 \leq k \leq n$.

  Corollary 2: If $p, q_1, q_2, \ldots, q_n$ are all prime and $p|q_1q_2\ldots q_n$, then $p = q_k$ for some k, $1 \leq k \leq n$.
- **Theorem 3.2 (Fundamental Theorem of Arithmetic)**: Every positive integer $n > 1$ can be expressed as a product of primes uniquely (up to the order of the primes in the product).

  Corollary: Any positive integer $n > 1$ can be written uniquely in a *canonical form*

  $$n = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$$

  where, for $i = 1, 2, ..., r$ each k_i is a positive integer and each p_i is a prime, with $p_1 < p_2 < \cdots < p_r$.
- **Theorem 3.3 (Pythagoras)**: $\sqrt{2}$ is irrational.

7 Section 3.2

- The sieve of Eratosthenes
- **Theorem 3.4 (Euclid)**: The primes are infinite in number.
- **Theorem 3.5**: If p_n is the n^{th} prime, then $p_n \leq 2^{2^{n-1}}$.

  Corollary: For $n \geq 1$, there are at least $n + 1$ primes less than 2^{2^n}.

8 Section 3.3

- Various famous interesting conundrums, mysteries, conjectures, etc. are discussed, including
  - The Goldbach Conjecture;
  - Twin Primes, and other gaps between primes;
  - Dirichlet's primes of the form $a + kb$, with $\gcd(a, b) = 1$; and
  - Primes of various forms given by the division algorithm.
- **Lemma**: The product of two or more integers of the form $4n + 1$ is of the same form.
- **Theorem 3.6**: There are infinitely many primes of the form $4n + 3$.
- **Theorem 3.7 (Dirichlet)**: If a and b are relatively prime positive integers, then the arithmetic progression

  $$a,\ a + b,\ a + 2b,\ a + 3b, \ldots$$

  contains infinitely many primes.
- **Theorem 3.8**: If all the $n > 2$ terms of the arithmetic progression

  $$p,\ p + d,\ p + 2d,\ \ldots, p + (n - 1)d$$

  are prime numbers, then the common difference d is divisible by every prime $q < n$.

9 Section 4.2

- **congruence modulo** n
- **complete set of residues**
- **Theorem 4.1**: For arbitrary integers a and b, $a \equiv b (\mathrm{mod}\ n)$ if and only if a and b leave the same nonnegative remainder when divided by n.

- **Theorem 4.2**: Let $n > 1$ be fixed and a, b, c, and d be arbitrary integers. Then the following properties hold:

  1. $a \equiv a (\text{mod } n)$
  2. If $a \equiv b (\text{mod } n)$, then $b \equiv a (\text{mod } n)$.
  3. If $a \equiv b (\text{mod } n)$ and $b \equiv c (\text{mod } n)$, then $a \equiv c (\text{mod } n)$.
  4. If $a \equiv b (\text{mod } n)$ and $c \equiv d (\text{mod } n)$, then $a + c \equiv b + d (\text{mod } n)$, and $ac \equiv bd (\text{mod } n)$.
  5. If $a \equiv b (\text{mod } n)$, then $a + c \equiv b + c (\text{mod } n)$, and $ac \equiv bc (\text{mod } n)$.
  6. If $a \equiv b (\text{mod } n)$, then $a^k \equiv b^k (\text{mod } n)$ for any positive integer k.

- **Theorem 4.3**: If $ca \equiv cb (\text{mod } n)$, then $a \equiv b (\text{mod } n/d)$, where $d = \gcd(c, n)$.

  Corollary 1: If $ca \equiv cb (\text{mod } n)$ and $\gcd(c, n) = 1$, then $a \equiv b (\text{mod } n)$.

  Corollary 2: If $ca \equiv cb (\text{mod } p)$ (p prime), and p does not divide c, then $a \equiv b (\text{mod } p)$.

- Problem #13: If $a \equiv b (\text{mod } n_1)$ and $a \equiv b (\text{mod } n_2)$, then $a \equiv b (\text{mod n})$, where $n = \text{lcm}(n_1, n_2)$. Hence, whenever n_1 and n_2 are relatively prime, $a \equiv b (\text{mod } n_1 n_2)$.

10 Section 4.3

- *base b place-value notation*

- **Theorem**: Given any integer $b > 1$, any integer may be written uniquely in base b place-value notation.

- **Theorem 4.4**: Let $P(x) = \sum_{k=0}^{m} c_k x^k$ be a polynomial function of x with integral coefficients c_k. If $a \equiv b (\text{mod n})$, then $P(a) \equiv P(b) (\text{mod n})$.

  Corollary: If a is a solution of the **congruence** $P(x) \equiv 0 (\text{mod n})$, and $a \equiv b (\text{mod n})$, then b is also a solution.

- **Theorem 4.5/4.6**: Let

$$N = a_m 10^m + a_{m-1} 10^{m-1} + \cdots + a_2 10^2 + a_1 10 + a_0$$

be the decimal expansion of positive integer N, $0 \leq a_k < 10$, and let $S = a_0 + a_1 + \ldots + a_m$. Then

  - $9|N \iff 9|S$.
  - Let $T = a_0 - a_1 + a_2 - \ldots + (-1)^m a_m$. Then $11|N \iff 11|T$.

11 Section 4.4

- **linear congruence**
- **Theorem 4.7**: The linear congruence $ax \equiv b(\text{mod n})$ has a solution if and only if $d|b$, where $d = \gcd(a, n)$. If $d|b$, then the linear congruence has d mutually incongruent solutions modulo n.

  Corollary: If $\gcd(a, n) = 1$, then the inear congruence $ax \equiv b(\text{mod n})$ has a unique solution modulo n.
- **Theorem 4.8 (The Chinese Remainder Theorem):** Let $n_1, n_2, \ldots, n_r$ be positive integers such that $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then the system of linear congruences

$$\begin{aligned} x &\equiv a_1 (\text{mod } n_1) \\ x &\equiv a_2 (\text{mod } n_2) \\ &\vdots \\ x &\equiv a_r (\text{mod } n_r) \end{aligned}$$

has a simultaneous solution which is unique modulo $N = n_1 n_2 \cdots n_r$. The unique solution is of the form

$$\overline{x} = a_1 N_1 x_1 + \ldots + a_r N_r x_r$$

where $N_k = \frac{N}{n_k}$ and x_k is the unique solution to the linear congruence $N_k x \equiv 1(\text{mod } n_k)$.

- **Theorem 4.9**: The system of linear congruences

$$ax + by \equiv r(\text{mod n})$$
$$cx + dy \equiv s(\text{mod n})$$

has a unique solution whenever $\gcd(ad - bc, n) = 1$.

12 Section 5.3

- **Theorem 5.1 (Fermat's Theorem)**: Let p be prime and suppose that p does not divide a. Then $a^{p-1} \equiv 1(\text{mod p})$.

  Corollary: If p is a prime, then $a^p \equiv a(\text{mod p})$ for any integer a.

- **Lemma**: If p and q are distinct primes with $a^p \equiv a(\text{mod q})$ and $a^q \equiv a(\text{mod p})$, then $a^{pq} \equiv a(\text{mod pq})$.

13 Section 5.4

- **Theorem 5.4 (Wilson's Theorem)**: If p is prime, then

$$(p-1)! \equiv -1(\text{mod p})$$

  Converse to Wilson's Theorem): If

$$(p-1)! \equiv -1(\text{mod p})$$

  then p is prime.

- **Theorem 5.5**: The quadratic congruence $x^2 + 1 \equiv 0(\text{mod p})$, where p is an odd prime, has a solution if and only if $p \equiv 1(\text{mod } 4)$.

14 Section 6.1

- $$\tau(n) = \sum_{d|n} 1$$

  and

  $$\sigma(n) = \sum_{d|n} d$$

- A number-theoretic function is said to be **multiplicative** if

  $$f(mn) = f(m)f(n)$$

  whenever $\gcd(m, n) = 1$.

- **Theorem 6.1** If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorization of $n > 1$, then the positive divisors of n are precisely those integers of the form $d = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, where $0 \leq a_i \leq k_i$ for i in $\{1, \ldots, r\}$.

- **Theorem 6.2** If $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorization of $n > 1$, then

  1. $$\tau(n) = (k_1 + 1)(k_2 + 1) \cdots (k_r + 1)$$

     and

  2. $$\sigma(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \frac{p_2^{k_2+1} - 1}{p_2 - 1} \cdots \frac{p_r^{k_r+1} - 1}{p_r - 1}$$

- $$\tau(n) = \prod_{i=1}^{r} (k_i + 1)$$

  and

  $$\sigma(n) = \prod_{i=1}^{r} \frac{p_i^{k_i+1} - 1}{p_i - 1}$$

- **Theorem 6.3** The functions τ and σ are multiplicative functions.
- **Lemma** If $\gcd(m, n) = 1$, then the set of positive divisors of mn consists of all products $d_1 d_2$, where $d_1|m$, $d_2|n$, and $\gcd(d_1, d_2) = 1$; furthermore these products are all distinct.

  Theorem 6.4 If f is a multiplicative function and F is defined by

$$F(n) = \sum_{d|n} f(d)$$

  then F is also multiplicative.

15 Section 7.2

- **Euler's** ϕ: For $n \geq 1$, let $\phi(n)$ denote the number of positive integers not exceeding n that are relatively prime to n.
- **Theorem 7.1**: If p is prime and $k > 0$, then

$$\phi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right)$$

- **Lemma**: Given integers a, b, c, $\gcd(a, bc) = 1$ if and only if $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$.

  Theorem 7.2: The function ϕ is a multiplicative function.
- **Theorem 7.3**: If the integer $n > 1$ has the prime factorization $p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, then

$$\phi(n) = (p_1^{k_1} - p_1^{k_1 - 1})(p_2^{k_2} - p_2^{k_2 - 1}) \cdots (p_r^{k_r} - p_r^{k_r - 1}) = n \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

- **Theorem 7.4**: For $n > 2$, $\phi(n)$ is an even integer.

16 Section 7.3

- **Theorem 7.5 (Euler)**: If $n \geq 1$ and $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 (\text{mod n})$.
  Corollary: Fermat's Little theorem

17 Section 7.5

- *Cipher* – the code
- *Plaintext* – the message to be encrypted
- *Ciphertext* – the encrypted message
- *Frequency Analysis* – using the known distribution of letters (or words) to break a code.
- **Caesar Cypher (circa 50 B.C.)**
- **Vigenère Cypher (1586)**
- **Hill's cipher (1929)**

18 Section 7.5b

- The RSA algorithm

19 Section 10.2

- **perfect number**
- **Mersenne number**: $M_n = 2^n - 1$, with $n \geq 1$. If M_n is prime, then it's called a **Mersenne prime**
- **Theorem 10.1**: If $2^k - 1$ is prime ($k > 1$), then $n = 2^{k-1}(2^k - 1)$ is perfect, and every even perfect number is of this form.
- The test of a perfect number is if

$$\sigma(n) = 2n$$

20 Section 11.1

- **Pythagorean triple**
- **Lemma 1**: If x, y, z is a primitive Pythagorean triple, then one of the integers x or y is even, while the other is odd.

  Lemma 2: If $ab = c^n$, where $\gcd(a, b) = 1$, then a and b are n^{th} powers. That is, there exist positive integers a_1 and b_1 for which $a = a_1^n$ and $b = b_1^n$.

  Theorem 11.1: All solutions of the Pythagorean equation

$$x^2 + y^2 = z^2$$

  satisfying the conditions

$$\gcd(x, y, z) = 1 \quad 2|x \quad x, y, z > 0$$

  are given by the formulas

$$x = 2st \quad y = s^2 - t^2 \quad z = s^2 + t^2.$$

  For integers $s > t > 0$ such that $\gcd(s, t) = 1$ and $s \not\equiv t (\text{mod } 2)$.

21 Section 11.2

- **Theorem 11.3**: The Diophantine equation $x^4+y^4 = z^2$ has no solution in the positive integers x, y, and z.

  Corollary: The equation $x^4 + y^4 = z^4$ has no solution in the positive integers x, y, and z.

  Corollary: The equation $x^{4k}+y^{4k} = z^{4k}$ has no solution in the positive integers x, y, and z.

- **Theorem 11.4**: The Diophantine equation $x^4-y^4 = z^2$ has no solution in the positive integers x, y, and z.

22 Section 13.1

- **Fibonacci numbers**:

  $$u_n = u_{n-1} + u_{n-2}$$

  for $n \geq 3$, where $u_1 = u_2 = 1$.

- **Theorem 13.1**: For the Fibonacci sequence, $\gcd(u_n, u_{n+1}) = 1$ for every $n \geq 1$.

- **Theorem 13.2**: For $m \geq 1$ and $n \geq 1$, $u_m | u_{mn}$.

- **Lemma**: If $m = qn + r$, then $\gcd(u_m, u_n) = \gcd(u_r, u_n)$

  Theorem 13.3: The greatest common divisor of two Fibonacci numbers is again a Fibonacci number; specifically $\gcd(u_m, u_n) = u_d$ where $d = \gcd(m, n)$.

  Corollary: In the Fibonacci sequence, $u_m | u_n$ if and only if $m|n$ for $n \geq m \geq 3$.

23 Section 13.2

- **Theorem 13.4**: Any positive integer N can be expressed as a sum of distinct Fibonacci numbers, no two of which are consecutive; that is,

  $$N = u_{k_1} + u_{k_2} + \ldots + u_{k_r}$$

  where $k_i \geq 2$ and $k_{i+1} > k_i + 2$ for $i = 1, 2, \ldots, r$ (the **Zeckendorf** representation).

- $$u_{2k}^2 = u_{2k+1}u_{2k-1} - 1$$