

Math 4573: Number Theory

Lecturer: **James Cogdell**

Notes by: Farhan Sadeek

Spring 2025

1 January 8, 2025

Dr. Cogdell explained the logistics of the class and also took attendance.

1.1 Conjectures in Number Theory

- A number is divisible by 3 if the sum of its digits is divisible by 3.
- **Fermat's Last Theorem:** There are no three positive integers a , b , and c that satisfy the equation $a^n + b^n = c^n$ for any integer value of n greater than 2.
- There are infinitely many primes.
- $\sqrt{2}$ is irrational.
- π is irrational.
- Every number can be written as the sum of four squares (Lagrange's Four Square Theorem). For example, $1000 = 10^2 + 30^2 + 0^2 + 0^2$ and $999 = 30^2 + 9^2 + 3^2 + 3^2$.
- The polynomial $n^2 - n + 41$ produces prime numbers for $n = 0, 1, 2, \dots, 40$, but not for $n = 41$.
- Euler conjectured that no n^{th} power can be written as the sum of two n^{th} powers for $n > 2$. This was proven false by the counterexample $144^5 = 27^5 + 84^5 + 110^5 + 133^5$.
- **Goldbach's Conjecture:** Every even integer greater than 2 can be written as the sum of two primes. For example, $4 = 2 + 2$, $6 = 3 + 3$, $8 = 3 + 5$, $10 = 5 + 5$, $12 = 5 + 7$, $14 = 7 + 7$, $16 = 3 + 13$, $18 = 7 + 11$. This has been verified for numbers up to 100,000 but remains unproven.

Number theory is related to **Abstract Algebra**, but also intersects with other domains such as **Combinatorics**, **Analysis**, and **Topology**. We will accept a few fundamental facts about **Number Theory**.

Fact 1

If S is a non-empty set of positive integers, then S contains a smallest element. This is known as the Well-Ordering Principle.

1.2 Divisibility

This concept has been known since the time of Euclid.

Definition 2

An integer b is divisible by an integer $a \neq 0$ if there is an integer x such that $b = ax$. We write this as $a \mid b$. If b is not divisible by a , we write $a \nmid b$.

There are two derivative notions:

- If $0 < a < b$, then a is called a **proper divisor** of b .
- If $a^k \parallel b$, it means $a^k \mid b$ and $a^{k+1} \nmid b$.

Theorem 3

Let a , b , and c be integers. Then the following are true:

- If $a \mid b$, then $a \mid bc$.
- If $a \mid b$, then $a \mid b + c$.
- If $a \mid b$ and $a \mid c$, then $a \mid b + c$.
- If $a \mid b$ and $b \mid a$, then $a = b$ or $a = -b$.
- If $a \mid b$ and $a > 0$ and $b > 0$, then $a \leq b$.
- If $m \neq 0$ and $a \mid b$, then $am \mid bm$.
- If $a \mid b_1, a \mid b_2, \dots, a \mid b_n$, then $a \mid \sum_{i=1}^n b_i x_i$ for any integers x_i .

Theorem 4 (The Division Algorithm)

Given integers a and b with $a > 0$, there exist unique integers q and r such that

$$b = qa + r, \quad 0 \leq r < a.$$

If $a \nmid b$, then r satisfies the stronger inequality

$$0 < r < a.$$

Proof. Consider the arithmetic progression $\dots, b-3a, b-2a, b-a, b, b+a, b+2a, b+3a, \dots$. In this sequence, select the smallest non-negative member. This defines r and satisfies the inequalities of the theorem. Since r is in the sequence, it can be written as $b - qa$. To prove the uniqueness of q and r , suppose there is another pair q_1 and r_1 that satisfies the same conditions. We first prove that $r = r_1$. If not, assume $r < r_1$, so $0 < r_1 - r < a$. But $r_1 - r = a(q - q_1)$, meaning $a \mid (r_1 - r)$, which contradicts the fact that $0 < r_1 - r < a$. Thus, $r = r_1$ and $q = q_1$. \square

Fact 5

If $a \mid b$, then r satisfies the stronger inequality $0 \leq r < a$.

Fact 6

The Division Algorithm can be stated without the assumption $a > 0$. Given integers a and b with $a \neq 0$, there exist integers q and r such that $b = qa + r$ with $0 \leq |r| < |a|$.

Definition 7 (Common Divisor)

The integer a is a **common divisor** of b and c if $a \mid b$ and $a \mid c$. Since there is only a finite number of divisors of any non-zero integer, there is only a finite number of common divisors of b and c except in the case $b = c = 0$.

If at least one of b and c is not 0, the **greatest common divisor** is called the **gcd** $\gcd(b, c)$ (*greatest common divisor of b and c*), and is denoted by (b, c) . Similarly, we have the greatest common divisor g of the integers b_1, b_2, \dots, b_n (*not all 0*) denoted by (b_1, b_2, \dots, b_n) .

Theorem 8

If g is the **gcd** of b and c , then there exist integers x_0 and y_0 such that

$$g = bx_0 + cy_0$$

2 January 10, 2025

Dr. Cogdell takes attendance so I will have to be in class every single day.

Definition 9 (Common Divisor)

The integer a is a common divisor of b and c if $a \mid b$ and $a \mid c$. Since there is only a finite number of divisors of any nonzero integer, there is only a finite number of common divisors of b and c , except in the case $b = c = 0$. If at least one of b and c is not 0, the greatest among their common divisors is called the greatest common divisor of b and c and is denoted by (b, c) . Similarly, we denote the greatest common divisor g of the integers b_1, b_2, \dots, b_n , not all zero, by (b_1, b_2, \dots, b_n) .

Theorem 10

If g is the greatest common divisor of b and c , then there exist integers x_0 and y_0 such that $g = (b, c) = bx_0 + cy_0$.

Fact 11

Another fundamental way to state this is that the linear combination of b and c is with integral multipliers x_0 and y_0 . This assertion holds for any finite collection.

Proof. Consider the following linear combinations $\{bx + cy\}$ where x and y are all integers. Note this also contains $x = y = 0$. Choose $bx_0 + cy_0$ is the least positive integer l in the set.

We need to prove that $l \mid b$ and $l \mid c$. We will do this via indirect proof. If we assume that $l \nmid b$, we will obtain a contradiction. From $l \nmid b$, there are integers q and r such that $b = lq + r$ where $0 < r < l$. Since l is the least positive integer in the set, we can write $r = bx_1 + cy_1$ for some integers x_1 and y_1 . So we have

$$r = b - lq = b - q(bx_0 + cy_0) = b(1 - qx_0) + c(-qy_0)$$

and this r is in the set $bx + cy$. This contradicts the fact that l is the least positive integer in the set $\{bx + cy\}$. Thus, we have shown that $l \mid b$.

Since g is the greatest common divisor of b and c , we may write $l = bx_0 + cy_0 = g(Bx_0 + Cy_0)$. Then, $g \mid l$ and by parts of theorem 1.1, we have shown $g \leq l$. Now, $g < l$ is impossible since, g is the greatest common divisor, so $g = l = bx_0 + cy_0$. \square

Theorem 12

The greatest common divisor g of b and c can be characterized in the following two ways:

- It is the least positive value of $bx + cy$ where x and y range over all integers.
- It is the positive common divisor of b and c that is divisible by every common divisor.

Proof. Part 1 follows from the proof of Theorem 1.3. To prove part 2, we observe that if d is any common divisor of b and c , then $d \mid g$ by part 3 of Theorem 1.1. Moreover, there cannot be two distinct integers with property 2, because of Theorem 1.1, part 4. \square

Remark 13. If an integer d is expressible in the form $d = bx + cy$, then d is not necessarily the $\gcd(b, c)$. However, it does follow from such an equation that (b, c) is a divisor of d . In particular, if $bx + cy = 1$ for some integers x and y , then $(b, c) = 1$.

Theorem 14

Given any integers b_1, b_2, \dots, b_n not all zero, with greatest common divisor g , there exist integers x_1, x_2, \dots, x_n such that

$$g = (b_1, b_2, \dots, b_n) = \sum_{j=1}^n b_j x_j.$$

Furthermore, g is the least positive value of the linear form $\sum_{j=1}^n b_j y_j$ where the y_j range over all integers; also g is the positive common divisor of b_1, b_2, \dots, b_n that is divisible by every common divisor.

Proof. Consider the set $S = \left\{ \sum_{j=1}^n b_j y_j \mid y_j \in \mathbb{Z} \right\}$. Since not all b_j are zero, there exists a non-zero integer in S . Let g be the smallest positive integer in S . Then g can be written as $g = \sum_{j=1}^n b_j x_j$ for some integers x_j .

We claim that g is the greatest common divisor of b_1, b_2, \dots, b_n . First, we show that g is a common divisor of b_1, b_2, \dots, b_n . For each b_i , we have

$$b_i = \sum_{j=1}^n b_j \delta_{ij},$$

where δ_{ij} is the Kronecker delta. Since g divides each term on the right-hand side, it follows that $g \mid b_i$ for all i .

Next, we show that g is the greatest common divisor. Let d be any common divisor of b_1, b_2, \dots, b_n . Then $d \mid \sum_{j=1}^n b_j x_j$, so $d \mid g$. Therefore, g is the greatest common divisor of b_1, b_2, \dots, b_n .

Finally, we show that g is the least positive value of the linear form $\sum_{j=1}^n b_j y_j$. Suppose there exists a positive integer h such that $h = \sum_{j=1}^n b_j z_j$ and $h < g$. Then h is in S , which contradicts the minimality of g . Therefore, g is the least positive value of the linear form.

Thus, we have shown that $g = (b_1, b_2, \dots, b_n) = \sum_{j=1}^n b_j x_j$ and g is the least positive value of the linear form $\sum_{j=1}^n b_j y_j$ where the y_j range over all integers. Also, g is the positive common divisor of b_1, b_2, \dots, b_n that is divisible by every common divisor. \square

Theorem 15

For any positive integer m we have

$$(ma, mb) = m(a, b)$$

Proof. By Theorem 1.4 we have

$$\begin{aligned} (ma, mb) &= \text{least positive value of } max + mby \\ &= m \cdot \{\text{least positive value of } ax + by\} \\ &= m(a, b). \end{aligned}$$

\square

Theorem 16

If $d \mid a$ and $d \mid b$, $d > 0$, then

$$\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d}(a, b)$$

If $(a, b) = g$, then

$$\left(\frac{a}{g}, \frac{b}{g}\right) = 1$$

Proof. The second assertion is the special case of the first obtained by using the greatest common divisor g of a and b in the role of d . The first assertion in turn is a direct consequence of Theorem 1.6 obtained by replacing m, a, b in that theorem by $d, \frac{a}{d}, \frac{b}{d}$ respectively. \square

Theorem 17

If $(a, m) = (b, m) = 1$, then $(ab, m) = 1$

Proof. By Theorem 1.3, there exist integers x_0, y_0, x_1, y_1 such that

$$1 = ax_0 + my_0 = bx_1 + my_1.$$

Thus, we may write

$$ax_0 - bx_1 = m(y_1 - y_0).$$

Let $y_2 = y_1 - y_0$. Then we have

$$ax_0 - bx_1 = my_2.$$

From the equation $ax_0 - bx_1 = my_2$, we note, by part 3 of Theorem 1.1, that any common divisor of a and b is a divisor of m . Hence, $(a, b, m) = 1$. □