Math 4573: Number Theory

Lecturer: **Professor James Cogdell**
Notes by: Farhan Sadeek

Spring 2025

1 January 8, 2025

Dr. Cogdell explained the logistics of the class and also took attendance. This class will be no exams and graded based on only homeworks.

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 $n = 0, 1, 2, \ldots, 40$, 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 $\mathcal{S}$ is a non-empty set of positive integers, then $\mathcal{S}$ 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 $a \mid b_1, a \mid b_2, \ldots, a \mid b_n$, 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 $\ldots, b-3a, b-2a, b-a, b, b+a, b+2a, b+3a, \ldots$. 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 $q = q_1$. □

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 $b_1, b_2, \ldots, b_n$ (*not all* 0) denoted by $(b_1, b_2, \ldots, b_n)$.

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 $b_1, b_2, \ldots, b_n$, not all zero, by $(b_1, b_2, \ldots, b_n)$.

Fact 10

Another fundamental way to to state this is that the linear combination of b and c is with integgral multipliers x_0 and y_0. This assertion of 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 we have shown $g \leq l$. Now, $g < l$ is impossible since, $g$is the greatest common divisor, so $g = l = bx_0 + cy_0$. □

Theorem 11

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 8. 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 3. Moreover, there cannot be two distinct integers with property 2, because of Theorem 3, part 4. □

Remark 12. *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 13

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

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

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 $b_1, b_2, \ldots, b_n$ 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. □

Theorem 14

For any positive integer$m$ we have

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

Proof. By Theorem 11 we have

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

□

Theorem 15

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

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

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

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

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 14 obtained by replacing m, a, b in that theorem by $d, \frac{a}{d}, \frac{b}{d}$ respectively. □

Theorem 16

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

Proof. By Theorem 8, 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 Theorem 3, that any common divisor of a and b is a divisor of m. Hence, $(a,b,m)=1$. □

Theorem 17

For any integers a and b, the following equalities hold:

$$(a,b) = (b,a) = (a,-b) = (a, b+ax).$$

Proof. The equality $(a,b)=(b,a)$ follows from the definition of the greatest common divisor, as the order of the arguments does not affect the set of common divisors.

The equality $(a,b)=(a,-b)$ holds because the set of common divisors of a and b is the same as the set of common divisors of a and $-b$.

To prove $(a,b)=(a,b+ax)$, we note that any common divisor of a and b is also a divisor of $b+ax$ (since $b+ax = b + a\cdot x$). Conversely, any common divisor of a and $b+ax$ is also a divisor of b (since $b = (b+ax) - a\cdot x$). Therefore, the set of common divisors of a and b is the same as the set of common divisors of a and $b+ax$, which implies that $(a,b)=(a,b+ax)$. □

Theorem 18

If $c \mid ab$ and $(b,c)=1$, then $c \mid a$.

Proof. Since $(b,c)=1$, there exist integers x and y such that $bx+cy=1$. Multiplying both sides by a, we get

$$abx + acy = a.$$

Since $c \mid ab$, there exists an integer k such that $ab = ck$. Substituting this into the equation, we get

$$ckx + acy = a.$$

Factoring out c from the left-hand side, we get

$$c(kx+ay) = a.$$

Therefore, $c \mid a$. □

3 January 13, 2025

3.1 Euclidean Algorithm

Given two integers b and c, now we can generate the greatest common divisor. There is no algorithm to this problem, but there is an algorithm.

Question 19. *Given a set of integers $(bx + cy)$ how to find the greatest common divisor?*

Consider the case $b = 963$ and $c = 657$. If we divide c into b, we get the quotient $q = 1$ and the remainder $r = 306$. We can write this as $b = qc + r$ or $r = b - cq$. In particular, $306 = 963 - 1 \cdot 657$. Now $(b, c) = (b - cq, c)$ by replacing a and x by c and $-q$ in Theorem 17, so we see that

$$(963, 657) = (963 - 1 \cdot 657, 657) = (306, 657).$$

The integer 963 has been replaced by the smaller integer 306, and this suggests that the procedure be repeated. So we divide 306 into 657 to get a quotient 2 and a remainder 45, and

$$(306, 657) = (306, 657 - 2 \cdot 306) = (306, 45).$$

Next, 45 is divided into 306 with quotient 6 and remainder 36, then 36 is divided into 45 with quotient 1 and remainder 9. We conclude that

$$(963, 657) = (306, 657) = (306, 45) = (45, 36) = (36, 9).$$

Thus $(963, 657) = 9$, and we can express 9 as a linear combination of 963 and 657 by sequentially writing each remainder as a linear combination of the two original numbers:

$$\begin{aligned}
306 &= 963 - 657, \\
45 &= 657 - 2 \cdot 306 = 657 - 2 \cdot (963 - 657) = 3 \cdot 657 - 2 \cdot 963, \\
36 &= 306 - 6 \cdot 45 = (963 - 657) - 6 \cdot (3 \cdot 657 - 2 \cdot 963) = 13 \cdot 963 - 19 \cdot 657, \\
9 &= 45 - 36 = 3 \cdot 657 - 2 \cdot 963 - (13 \cdot 963 - 19 \cdot 657) = 22 \cdot 657 - 15 \cdot 963.
\end{aligned}$$

In terms of Theorem 8, where $g = (b, c) = bx_0 + cy_0$, beginning with $b = 963$ and $c = 657$ we have used a procedure called the Euclidean algorithm to find $g = 9$, $x_0 = -15$, $y_0 = 22$. Of course, these values for x_0 and y_0 are not unique: $-15 + 657k$ and $22 - 963k$ will do where k is any integer.

To find the greatest common divisor (b, c) of any two integers b and c, we now generalize what is done in the special case above. The process will also give integers x_0 and y_0 satisfying the equation $bx_0 + cy_0 = (b, c)$. The case $c = 0$ is special: $(b, 0) = |b|$. For $c \neq 0$, we observe that $(b, c) = (b, -c)$ by Theorem 17, and hence, we may presume that c is positive.

Theorem 20 (The Euclidean Algorithm)

Given integers b and $c > 0$, we make a repeated application of the division algorithm, Theorem 4, to obtain a series of equations:

$$\begin{aligned} b &= cq_1 + r_1, \quad 0 < r_1 < c, \\ c &= r_1 q_2 + r_2, \quad 0 < r_2 < r_1, \\ r_1 &= r_2 q_3 + r_3, \quad 0 < r_3 < r_2, \\ &\vdots \qquad\qquad\qquad \vdots \\ r_{j-2} &= r_{j-1} q_j + r_j, \quad 0 < r_j < r_{j-1}, \\ r_{j-1} &= r_j q_{j+1}. \end{aligned}$$

The greatest common divisor (b, c) of b and c is r_j, the last nonzero remainder in the division process. Values of x_0 and y_0 in $(b, c) = bx_0 + cy_0$ can be obtained by writing each r_i as a linear combination of b and c.

Proof. The chain of equations is obtained by dividing c into b, r_1 into c, r_2 into r_1, and so on, until r_j into r_{j-1}. The process stops when the division is exact, that is, when the remainder is zero. Thus, in our application of Theorem 4, we have written the inequalities for the remainder without an equality sign. For example, $0 < r_1 < c$ instead of $0 \leq r_1 < c$, because if r_1 were equal to zero, the chain would stop at the first equation $b = cq_1$, in which case the greatest common divisor of b and c would be c.

We now prove that r_j is the greatest common divisor g of b and c. By Theorem 17, we observe that

$$(b, c) = (c, r_1) = (r_1, r_2) = \cdots = (r_{j-1}, r_j) = (r_j, 0) = r_j.$$

To see that r_j is a linear combination of b and c, we argue by induction that each r_i is a linear combination of b and c. Clearly, r_1 is such a linear combination, and likewise r_2. In general, r_i is a linear combination of r_{i-1} and r_{i-2}. By the inductive hypothesis, we may suppose that these latter two numbers are linear combinations of b and c, and it follows that r_i is also a linear combination of b and c. □

4 January 15, 2025

Example 21

We will find the g.c.d of 42823 and 6409.

Solution. *We apply the Euclidean algorithm to divide c into b, where $b = 42823$ and $c = 6409$. We obtain a quotient $q_1 = 6$ and a remainder $r_1 = 4369$. Continuing, if we divide 4369 into 6409, we get a quotient $q_2 = 1$ and a remainder $r_2 = 2040$. Dividing 2040 into 4369 gives $q_3 = 2$ and $r_3 = 289$. Dividing 289 into 2040 gives $q_4 = 7$ and $r_4 = 17$. Since 17 is an exact divisor of 289, the solution is that the g.c.d is 17.*

We can write this in tabular form:

$$\begin{aligned}
42823 &= 6 \cdot 6409 + 4369, \\
6409 &= 1 \cdot 4369 + 2040, \\
4369 &= 2 \cdot 2040 + 289, \\
2040 &= 7 \cdot 289 + 17, \\
289 &= 17 \cdot 17.
\end{aligned}$$

Thus, $(42823, 6409) = (6409, 4369) = (4369, 2040) = (2040, 289) = (289, 17) = 17$*.*

Example 22

Find integers x and y such that $42823x + 6409y = 17$.

Solution. *We find integers x and y such that $42823x + 6409y = 17$.*

Here it is natural to consider $i = 1, 2, \ldots$, but to initiate the process we also consider $i = 0$ and $i = -1$. We put $r_{-1} = 42823$, and write

$$42823 \cdot 1 + 6409 \cdot 0 = 42823.$$

Similarly, we put $r_0 = 6409$, and write

$$42823 \cdot 0 + 6409 \cdot 1 = 6409.$$

We multiply the second of these equations by $q_1 = 6$, and subtract the result from the first equation, to obtain

$$42823 \cdot 1 + 6409 \cdot (-6) = 4369.$$

We multiply this equation by $q_2 = 1$, and subtract it from the preceding equation to find that

$$42823 \cdot (-1) + 6409 \cdot 7 = 2040.$$

We multiply this by $q_3 = 2$, and subtract the result from the preceding equation to find that

$$42823 \cdot 3 + 6409 \cdot (-20) = 289.$$

Next we multiply this by $q_4 = 7$, and subtract the result from the preceding equation to find that

$$42823 \cdot (-22) + 6409 \cdot 147 = 17.$$

On dividing 17 into 289, we find that $q_5 = 17$ and that $289 = 17 \cdot 17$. Thus r_4 is the last positive remainder, so that $g = 17$, and we may take $x = -22$, $y = 147$. These values of x and y are not the only ones possible. In Section 5.1, an analysis of all solutions of a linear equation is given.

Remark 23. *Section 5.1 on Analysis*

Definition 24

The integers $a_1, a_2, \ldots, a_n$ all different from zero, have a common b if $a_i \mid b$ for $i = 1, 2, \ldots, n$. The least positive multiple is is called **least common multiple** and it's denoted $[a_1, a_2, \ldots, a_n]$

Theorem 25

If b is any common multiple of $a_1, a_2, \ldots, a_n$, then $[a_1, a_2, \ldots, a_n] \mid b$. This is the same as saying that if h denotes $[a_1, a_2, \ldots, a_n]$, then $0, \pm h, \pm 2h, \pm 3, \ldots$ comprise all the common multiples of $a_1, a_2, \ldots, a_n$.

Proof. Let m be any common multiple and divide m by h. By Division Algorithm, there is a quotient q and a remainder r such that $m = qh + r$, where $0 \leqslant r < h$. We must prove that $r = 0$. If $r \neq -$, we argue as follows. For each $i = 1, 2, \ldots, n$, we know that $a_i \mid h$ and $a_i \mid m$, so that $a_i \mid r$. Thus r is a positive common multiple of $a_1, a_2, \ldots, a_n$ contrary to the fact that h is the least of all common positive multiple. □

Theorem 26

If $m > 0$ $[ma, mb] = m[a, b]$. Also, $[a, b] \cdot (a, b) = |ab|$

Proof. Let $H = [ma, mb]$ and $h = [a, b]$. Then mh is a multiple of ma and mb, so that $mh \mid H$. Also, H is a multiple of both ma and mb, so H/m is a multiple of a and b. Thus, $H/m \mid h$, from which it follows that $mh = H$, and this establishes the first part of the theorem.

It will suffice to prove the second part for positive integers a and b, since $[a, -b] = [a, b]$. We begin with the special case where $(a, b) = 1$. Now $[a, b]$ is a multiple of a, say ma. Then $b \mid ma$ and $(a, b) = 1$, so by Theorem 18 we conclude that $b \mid m$. Hence $b \mid m$, $ba \mid ma$. But ba, being a positive common multiple of b and a, cannot be less than the least common multiple, so $ba = ma = [a, b]$.

Turning to the general case where $(a, b) = g > 1$, we have $(a/g, b/g) = 1$ by Theorem 15. Applying the result of the preceding paragraph, we obtain

$$\left[\frac{a}{g}, \frac{b}{g}\right] = \frac{ab}{g^2}.$$

Multiplying by g^2 and using Theorem 14 as well as the first part of the present theorem, we get $[a, b](a, b) = ab$. □

5 January 17, 2025

Definition 27

An integer $p > 1$ is called a **prime number** or **prime** in case there is no divisor of d of p satisfying $1 < d < p$. An integer $a > 1$ is not a prime, it is called **composite number**.

Example 28

$2, 3, 5, 7$ are primes, but $4, 6, 8, 9$ are composite.

Theorem 29

Every integer n greater than 1 can be expressed as a product of primes.

Proof. If the integer n is a prime, then the integer itself stands as a 'product' with a single factor. Otherwise, n it can be factored into say n_1, n_2, where $1 < n_1 < n$ and $1 < n_2 < n$. If n_1 is prime then let it stand. Otherwise, it will factor into say $n_3, n4$ where $1 < n_3 < n$ and $1 < n_4 < n$. Simliarly, for n_2. The process of writing each composite number that arises as a product of factors must termiate because the factors are smaller than the composite itself, yet each factor is an integer greater than 1. Thus we can conclude n as a product of q primes, and since the prime factors are not necessarily so the result can be written in the form

$$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_n^{\alpha_n}$$

where the $p_1, p_2, p_3, \dots, p_n$ are distinct primes and $\alpha_1, \alpha_2, \dots, \alpha_n$ are positive □

Fact 30

This representation of n as a product of primes is called the canonical factoring of n into prime numbers. It turns out that the representation is unique in the sense that, for a fixed n any other representation is merely a reordering, or a perumtation of factors, nevertheles it requires proof.

Theorem 31

If $p \mid ab$, p being a prime, then $p \mid a$ or $p \mid b$. More generally, if $p \mid a_1 a_2$, then p at least one factor of a_1.

Proof. If $p \nmid b$, since $(a, p) = 1$, by a previous theorem, $p \mid b$. We may regard as a proof of the general cae of the statement mathematical induction. So we assume that the property holds when n divides a factor with fewer than n primes. Now, if $p \mid a_1 a_2 \dots a_n$, that is $p \mid ac$, where $c = a_1 a_2 \dots a_n$, then $p \mid a_1$ or $p \mid c$.If $p \mid c$, we apply the induction hypthesis to conclude that $p \mid i$, for some subscript $i = 1, 2, \dots, n$. □

Theorem 32 (The Fundamental Theorem of Arithmetic or the Unique Factorization Theorem)

The facoring of $n > 1$ into primes is unique and apart from the order of the primes.

Proof. Suppose there is an integer n with two different factorizations. Dividing out any primes common to the two representations, we would have an equality of the form

$$p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_s$$

where the factors p_i and q_j are primes, not necessarily all distinct, but where no prime on the left side occurs on the right side. But this is impossible because $p_1 \mid q_1 q_2 \cdots q_s$, so by Theorem 31, p_1 is a divisor of at least one of the q_j. That is, p_1 must be identical with at least one of the q_j. This contradicts our assumption that no prime on the left side occurs on the right side. Therefore, the factorization of n into primes is unique. □

In the applications of the fundamental theorem, we frequently write the integer $a > \leqslant 1$, in the form,

$$a = \prod_{i=1}^{n} p_i^{\alpha_i}$$

where $\alpha(p)$ is a non-negative integer for all sufficiently large primes, p. If $a = 1$, then $\alpha(p) = 0$, for all primes, p and the product may be considered to be empty. We may write $a = \prod p^{\alpha}$

It $a = \prod_p p^{\alpha(p)}$, $b = \prod_p p^{\beta(p)}$, $c = \prod_p p^{\beta(p)}$ and $a = b = c$ then $\alpha(p) + \beta(p) = \gamma(p)$ for all p. So, $a \mid c$, we must note that $\alpha(p) \leqslant \gamma(p)$ for all p that we may define an integer $b = \prod_p p^{\beta(p)}$ with $\beta = \gamma(p) - \alpha(p)$. So $a \mid c$. Note that the greatest common divisor and least common multiple can be written as

$$(a, b) = \prod_p p^{\min(\alpha(p), \beta(p))}$$

$$[a, b] = \prod_p p^{\min(\alpha(p), \beta(p))}$$

Example 33

$a = 108, b = 225$, then $a = 2^2 \cdot 3^3 \cdot 5^0$ and $b = 2^0 \cdot 3^2 \cdot 5^2$. So $(a, b) = 2^0 \cdot 3^2 \cdot 5^0 = 9$, and $[a, b] = 2^2 \cdot 3^3 \cdot 5^2 = 2700$.

Definition 34

a is a **square (or perfect square)** if it can be written as n^2

Remark 35. *a is auare free if 1 is the largest square dividing a. So $\alpha(p)$ is square free if the only numbers are 0 and 1.*

Theorem 36 (Euclid)

The number of primes is inifite. i.e. there is no end to the sequence of primes.

$$2, 3, 5, 7, 11, 13, \ldots$$

Proof. Suppose that $p_1, p_2, \ldots, p_n$ are the first r primes. Then form the number

$$n = 1 + p_1 p_2 \ldots p_r$$

Note that n is not divisible by p_1 or p_2 or $\ldots$, or p_r Hencce, ayny prime divisor is distinct from $p_1, p2, \ldots, p_r$. Since n is neither a prime or has a prime factor factor p. This impl □

6 January 22, 2025

Theorem 37

There are arbitrarily large gapes in the series of primes stated otherwise, given any k, there exit k consequetive composite integers.

Proof. Consider the integers

$$(k+1)!+2, (k+1)!+3\dots, (k+1)!+k, (k+1)!+k+1$$

Every one of these composite because j divides $(k+1)!$ and $j \leqslant k$. □

The primes are spaced rather irregularly, as the last theorem suggests. If we denote the number of pirmes that do not exceed x by $\pi(x)$, but we may ask about the nature of this function. Because of this irregular occurence of primes, we cannnot expect a simple formula for $\pi(x)$, but we may week to estimate the rate of it's growth.

Theorem 38

For any real number $y \geqslant 2$, we have

$$\sum_{p \leqslant y} \frac{1}{p} \log\log y - 1$$

6.1 The Binomial Theorem

We first define the `binomial coefficients` and describe them combinatorially.

Definition 39

Let α be any real number, and let k be a non-negative integer. Then the binomial coefficient $\binom{\alpha}{k}$ is given by the formula:

$$\binom{\alpha}{k} = \frac{\alpha(\alpha-1)(\alpha-2)\cdots(\alpha-k+1)}{k!}$$

Suppose that n and k are both integers. From the formula, we see that if $0 \leq k \leq n$, then

$$\binom{n}{k} = \frac{n!}{k!(n-k)!},$$

whereas if $n < k$, then

$$\binom{n}{k} = 0.$$

Here we employ the convention $0! = 1$.

Theorem 40

Let $\mathbb{S}$ be a set containing exactly n elements. For any non-negative integer k, the number of subsets $\mathbb{S}$ containing precisely k elements $\binom{n}{k}$.

Proof. Let $\mathbb{S}$ be a set containing exactly n elements. For any non-negative integer k, the number of subsets $\mathbb{S}$ containing precisely k elements is $\binom{n}{k}$.

Suppose that $\mathbb{S} = \{1, 2, \ldots, n\}$. These numbers may be listed in various orders, called permutations, here denoted by π. There are $n!$ of these permutations π, because the first term may be any one of the n numbers, the second term any one of the $n-1$ remaining numbers, the third term any one of the still remaining $n-2$ numbers, and so on.

We count the permutations in a way that involves the number X of subsets containing precisely k elements. Let N be a specific subset of $\mathbb{S}$ with k elements. There are $k!$ permutations of the elements of N, each permutation having k terms. Similarly, there are $(n-k)!$ permutations of the $n-k$ elements not in N. If we attach any one of these $(n-k)!$ permutations to the right end of any one of the $k!$ previous permutations, the ordered sequence of n elements thus obtained is one of the permutations π of $\mathbb{S}$. Thus we can generate $k!(n-k)!$ of the permutations π in this way. To get all the permutations π of $\mathbb{S}$, we repeat this procedure with N replaced by each of the subsets in question. Let X denote the number of these subsets. Then there are $k!(n-k)!X$ permutations π, and equating this to $n!$ we find that

$$X = \frac{n!}{k!(n-k)!}.$$

We now see that the quotient $\frac{n!}{k!(n-k)!}$ is an integer, because it represents the number of ways of doing something. In this way, combinatorial interpretations can be useful in number theory. □

Theorem 41

The product of any k consecutive integers is divisible by $k!$.

Proof. Let's write the product as $n(n-1)\cdots(n-k+1)$. If $n \geq k$, then we write this in the form $\binom{n}{k} \cdot k!$ and note that $\binom{n}{k}$ is an integer, by Theorem 40. If $0 \leq n < k$, then one of the factors of our product is 0, so the product vanishes, and is therefore a multiple of $k!$ in this case also. Finally, if $n < 0$, we note that the product may be written as

$$(-1)^k(-n)(-n+1)\cdots(-n+k-1) = (-1)^k\binom{-n+k-1}{k}k!.$$

Note that in this case the upper member $-n+k-1$ is at least k, so that by Theorem 40 the binomial coefficient is an integer.

In the formula for the binomial coefficients we note a symmetry:

$$\binom{n}{k} = \binom{n}{n-k}.$$

□

Theorem 42 (The Binomial Theorem)
For any integer $n \geqslant 1$, and any real numbers x and y, we have

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

Proof. We first consider the product and obtain

$$\prod_{i=1}^{n} (x_i + y_i)$$

On multiplying this out, we obtain 2^n monomial terms of the form

$$\prod_{i \in \mathbb{A}} x_i \prod_{j \in \mathbb{A}} y_j$$

where $\mathbb{A}$ is any subset of {1, 2, ..., n}. For each fixed $k, 0 \leqslant k \leqslant n$, we consider the monomial terms obtained from those subsets of $\mathbb{A}$ of {1, 2, 3, ..., n} having exactly k elements. The number of such subsets is $\binom{n}{k}$, and the set $x_i = x$ and $y_i = y$ for all i and note that such a monomial has a value of $x^k y^{n-k}$ for the subsets in question. Since there are $\binom{n}{k}$ □

7 January 24, 2025

The binomial theorem can also be proved analytically by appealing the following simple results.

Lemma 43
Let $P(z) = \sum_{k=0}^{n} a_k z^k$ be a polynomial with real coefficients. Then $a_r = \frac{P^{(r)}(0)}{r!}$ for $r = 0, 1, 2, \ldots, n$, where $P^{(r)}(0)$ denotes the r^{th} derivative of $P(z)$ evaluated at $z = 0$.

The binomial coefficients arise in many identities, The simplest relations is the recurrence relation

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$$

Maybe used in many ways, for example to construct the Pascal's Triangle which is the infinite array of numbers. The pascal's triangle could be used to expand the binomial theorem, for example $(x+y)^5 = 1x^5 + 5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4 + 1y^5$

$$\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1
\end{array}$$

This is also obtained by the proceeding row, just to left and just to the right. In general the n^{th} row is the coefficients of the expansion of $(x+y)^{n-1}$

7.1 Congruences

7.1.1 Congruences

A congruence is nothing more than the statement about divisibility.

Definition 44

If an integer $m \neq 0$, divide the difference $a - b$, then we say that a is congruent to b modulo m, and write we will write $a \equiv (b \bmod m)$. If $a - b$ is not divisible by n, we say that a is not congruent to b modulo m, and write $a \not\equiv b \bmod m$.

Fact 45

Since $a - b$ is divisible by m, if $a - b$ is divisible by $-m$, we generally take the remainder to be the smallest positive integer.

Theorem 46

Let $a, b, c, d \in \mathbb{Z}$. Then

1. $a \equiv b \pmod{m}$, $b \equiv a \pmod{m}$, and $a - b \equiv 0 \pmod{m}$ are equivalent statements.
2. If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.
3. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.
4. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.
5. If $a \equiv b \pmod{m}$ and $d \mid m$, $d > 0$, then $a \equiv b \pmod{d}$.
6. If $a \equiv b \pmod{m}$, then $ac \equiv bc \pmod{mc}$ for $c > 0$.

Theorem 47

Let f denote a polynomial with integral coefficients. If $a \equiv b \pmod{m}$, then $f(a) \equiv f(b) \pmod{m}$.

Proof. We can suppose $f(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_0$ where the c_i are integers. Since $a \equiv b \pmod{m}$, we can apply Theorem 46, part 4, repeatedly to find $a^2 \equiv b^2$, $a^3 \equiv b^3$, ..., $a^n \equiv b^n \pmod{m}$, and then $c_j a^j \equiv c_j b^j \pmod{m}$ and finally $c_n a^n + c_{n-1}a^{n-1} + \cdots + c_0 \equiv c_n b^n + c_{n-1}b^{n-1} + \cdots + c_0 \pmod{m}$. □

Theorem 48

For $a, b, m \in \mathbb{Z}$, $m > 0$, the situations hold:

- $ax \equiv ay \pmod{m}$ if an only if $x \equiv y \pmod{\frac{m}{(a,m)}}$
- If $ax \equiv ay \pmod{m}$ and $(a, m) = 1$, then $x \equiv y \pmod{m}$.
- $x \equiv y \pmod{m_i}$ for $i = 1, 2, \ldots, r$ if and only if $x \equiv y \pmod{[m_1, m2, \ldots, m]}$

Proof.

- If $ax \equiv ay \pmod{m}$, then $ay - ax = mz$ for some integer z. Hence we have

$$a(y - x) = mz,$$

and thus

$$\frac{a}{(a,m)}(y - x) = \frac{m}{(a,m)}z.$$

But $\left(\frac{a}{(a,m)}, \frac{m}{(a,m)}\right) = 1$ by Theorem 15 and therefore $\frac{m}{(a,m)} \mid (y - x)$ by Theorem 18. That is,

$$x \equiv y \pmod{\frac{m}{(a,m)}}.$$

- Conversely, if $x \equiv y \pmod{\frac{m}{(a,m)}}$, we multiply by a to get $ax \equiv ay \pmod{a \cdot \frac{m}{(a,m)}}$ by use of Theorem 46, part 6. But (a, m) is a divisor of a, so we can write $ax \equiv ay \pmod{m}$ by Theorem 46, part 5.

For example, $15x \equiv 15y \pmod{10}$ is equivalent to $x \equiv y \pmod{2}$, which amounts to saying that x and y have the same parity. □

Proof.

- If $x \equiv y \pmod{m_i}$ for $i = 1, 2, \ldots, r$, then $m_i \mid (y - x)$ for $i = 1, 2, \ldots, r$. That is, $y - x$ is a common multiple of $m_1, m_2, \ldots, m_r$, and therefore (see Theorem 25) $[m_1, m_2, \ldots, m_r] \mid (y - x)$. This implies $x \equiv y \pmod{[m_1, m_2, \ldots, m_r]}$.
- If $x \equiv y \pmod{[m_1, m_2, \ldots, m_r]}$, then $x \equiv y \pmod{m_i}$ by Theorem 46 part 5, since $m_i \mid [m_1, m_2, \ldots, m_r]$.

□

8 January 27, 2025

In deadling with integers modulo m, we are essentially peforming the aritmetic but are disregarding the multiples of m. In a sense, not disregarding between a and $a + mx$, where $x \in \mathbb{Z}$. Given any integer, a, let

q and r be the quotient and the remainder on m; thus $a = qm + r$. Now $a \equiv r \pmod{m}$), and since r satistifies the inequalities $0 \leqslant r < m$, we see that every integer is congruent modulo m to one of the values $0, 1, 2, \ldots, m - 1$. Also, it is clear that no two of these m integers are congruent modulo m. These m values constitute a complete residue system modulo m, and we now give a general definition of this term.

Definition 49

If $x \equiv y \pmod{m}$ then y is called a residue of x **modulo** m. A set $x_1, x_2, \ldots, x_m$ is called a complete residue system modulo m if for every integer y there is one and only x_j such that $y \equiv x_j \pmod{m}$.

It is obvious that there are infinitely many complete residue systems **modulo** m, the set $1, 2, \ldots, m-1, m$ being another example.

A set of m integers forms a complete residue system modulo m if and only if no two integers in the set are congruent modulo m.

For fixed integer $x \equiv a \pmod{m}$ is the arithmetic progression

$$\ldots, a - 3m, a - 2m, a - m, a, a + m, a + 2m, a + 3m, \ldots$$

This set is called a **residue class** or **congruence class** modulo m. There are m distinct residue classe modulo m, obtained from taking $a = 0, 1, 2, \ldots, m$.

Theorem 50

If $b \equiv c \pmod{m}$, then $(b, m) = (c, m)$.

Proof. We have $c = b + mx$ for some $x \in \mathbb{Z}$. Let $d = (b, m)$. Then $d \mid b$ and $d \mid m$. Since $d \mid m$, we have $d \mid mx$. Therefore, $d \mid (b + mx)$, which implies $d \mid c$. Thus, d is a common divisor of c and m, so $d \leq (c, m)$.

Conversely, let $d' = (c, m)$. Then $d' \mid c$ and $d' \mid m$. Since $c = b + mx$, we have $d' \mid (b + mx)$. But $d' \mid m$, so $d' \mid b$. Thus, d' is a common divisor of b and m, so $d' \leq (b, m)$.

Therefore, $(b, m) = (c, m)$. □

Definition 51

A **reduced residue system** modulo m is a set of integers r_i such that $(r_i, m) = 1, r_i \not\equiv r_j \pmod{m}$ if $i \neq j$, and such that every x prime to m is congruent modulo m to some member r_i of the set.

Remark 52. *In view of the preceding theorem, it is clear that a reduced residue system modulo m can be obtained by deleting from a complete residue system modulo m and those members that are not relatively prime to m. Furthermore, all reduced residue system modulo m have the same number of members, namely $\phi(m)$. This is called **Euler's ϕ function**, sometimes called the **totient function**. By applying the definition of $\phi(m)$, we can see that $\phi(p) = p - 1$ for any prime p.*

Theorem 53

The number $\phi(m)$ is the number of positive integers less than or equal to m that are relatively prime to m.

Euler's function $phi(m)$ is of considerable interest. We will consider that in further sections.

Theorem 54

Let $a, m = 1$. Let $r_1, r_2, \ldots, r_n$ be a complete, or a reduced residue system modulo m. Then $ar_1, ar_2, \ldots, ar_n$ is a complete, or a reduced, residue system, respectively, modulo m.

Proof. If $r_i, m = 1$, then $ar_i, m = 1$. There are the same number of $ar_1, ar_2, \ldots, ar_n$ as of $r_1, r_2, \ldots, r_n$. Therefore, we need to only show that $ar_i \not\equiv ar_j \pmod{m}$ if $i \neq j$. But Theorem 48 shows that $ar_i \equiv ar_j \pmod{m}$ implies $r_i \equiv r_j \pmod{m}$, hence $i = j$. □

Example 55

For example, since $1, 2, 3, 4$ is a reduced residue system modulo 5, so also is $2, 4, 6, 8$. Since $1, 3, 7, 9$ is a reduced residue system modulo 10, so also is $3, 9, 21, 27$.

Theorem 56 (Fermat's Little Theorem)

If $p \nmid a$, then $(a, p) = 1$ and $a^{p-1} \equiv 1 \pmod{p}$. To find $\varphi(p)$, we refer to Theorem 53. All the integers $1, 2, \ldots, p-1$ are relatively prime to p. Thus we have $\varphi(p) = p - 1$, and the first part of Fermat's theorem follows. The second part is now obvious.

9 January 29, 2025

Theorem 57 (Euler's generalization of Fermat's Theorem)

If $(a, m) = 1$ then

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

Proof. Let $r_1, r_2, \ldots, r_{\varphi(m)}$ be a reduced residue system modulo m. Then by Theorem 54, $ar_1, ar_2, \ldots, ar_{\varphi(m)}$ is also a reduced residue system modulo m. Hence, corresponding to each r_i there is one and only one ar_j such that $r_i \equiv ar_j \pmod{m}$. Furthermore, different r_i will have different corresponding ar_j. This means that the numbers $ar_1, ar_2, \ldots, ar_{\varphi(m)}$ are just the residues modulo m of $r_1, r_2, \ldots, r_{\varphi(m)}$, but not necessarily in the same order. Multiplying and using Theorem 46, part 4, we obtain

$$\prod_{j=1}^{\varphi(m)} ar_j \equiv \prod_{i=1}^{\varphi(m)} r_i \pmod{m},$$

and hence

$$a^{\varphi(m)} \prod_{j=1}^{\varphi(m)} r_j \equiv \prod_{j=1}^{\varphi(m)} r_j \pmod{m}.$$

Now $(r_j, m) = 1$, so we can use Theorem 48, part 2, to cancel the r_j and we obtain $a^{\varphi(m)} \equiv 1 \pmod{m}$. □

Theorem 58

If $(a, m) = 1$. then there is an x such that $ax = 1 \pmod{m}$ and any two such x are congruent $pmodm$. If $(a, m) > 1$, then there is no such x.

Proof. If $a, m = 1$, then there exist x and y such that $ax + my = 1$ That is. $ax \equiv 1$, Conversely, if $ax \equiv 1 \pmod{m}$, then there is a y such that $ax + by = 1$, so that $(a, m) = 1$. Thus if, $ax_1 \equiv ax_2 \equiv 1 \pmod{m}$, then $(a, m) = 1$, and that follows from Theorem 48, part 2. □

Note 59. *The relation $ax \equiv 1 \pmod{m}$ asserts that there is a residue system x that is multiplicative inverse of the class a. To avoid confusion rational number $a^{-1} = \frac{1}{m}$, we denote that this residue $\bar{a}$. The value of $\bar{a}$ is quickly found by employing the Eucledian Algorithm, as asserted. The existence of $\bar{a}$ is also evident from Theorem 54, if $(a, m) = 1$ then the members $a, 2a, \ldots, ma$ form a complete system of residues, which is to say, that is one of them is $\equiv 1 \pmod{m}$. In additional it can be inferred in the form $\bar{a} = a^{\varphi(m)} - 1$*

Lemma 60

Let p be a prime number. Then $x^2 \equiv 1 \pmod{m} \iff x = \pm 1 \pmod{m}$. In a later section, we will establish a more general result which the following is easily derived, but we are giving a direct proof for now, because the observation has many useful applications.

Proof. This is a quadratic congruence. It may be expressed as $x^2 - 1 \equiv 0 \pmod{m}$. That is $(x-1)(x-2) \equiv 0 \pmod{p}$, which is to say that $\mid (x-1)(x-1) \mid$. By Theorem 31 it follows that $p \mid (x-1)$ or $p \mid (x+1)$. So $x \equiv 1 \pmod{m}$ or $x \equiv -1 \pmod{m}$ .Conversely, it either □

Theorem 61 (Wilson's Theorem)

If p is a prime, then $(p-1) \equiv -1 \pmod{m}$

10 January 31, 2025

Proof. If $p = 2$ or $p = 3$, the congruence is easily verified. Thus we may assume that $p \geq 5$. Suppose that $1 \leq a \leq p - 1$. Then $(a, p) = 1$, so that by Theorem 58 there is a unique integer $\bar{a}$ such that $1 \leq \bar{a} \leq p - 1$ and $a\bar{a} \equiv 1 \pmod{p}$. By a second application of Theorem 58 we find that if a is given then there is exactly one $\bar{a}$, $1 \leq \bar{a} \leq p - 1$, such that $a\bar{a} \equiv 1 \pmod{p}$. Thus a and $\bar{a}$ form a pair whose combined contribution to $(p-1)!$ is $\equiv 1 \pmod{p}$. However, a little care is called for because it may happen that $a = \bar{a}$. This is equivalent to the assertion that $a^2 \equiv 1 \pmod{p}$, and by Lemma 60 we see that this is in turn equivalent to $a \equiv 1$ or $a \equiv p - 1$. That is, $\bar{1} = 1$ and $\overline{p-1} = p - 1$, but if $2 \leq a \leq p - 2$ then $a \neq \bar{a}$. By pairing these latter residues in this manner we find that $\prod_{a=2}^{p-2} a \equiv 1 \pmod{p}$, so that $(p-1)! \equiv 1 \cdot \prod_{a=2}^{p-2} a \cdot (p-1) \equiv -1 \pmod{p}$. □

Theorem 62

Let p denote a prime. Then $x^2 \equiv -1 \pmod{m}$ has solution $\iff p = 2$ or $p \equiv 1 \pmod{4}$

Proof. If $p = 2$, we have the solution $x = 1$. FOr any odd prime p, we can write Wilson's theorem in the form

$$\left(1 \cdot 2 \ldots j \ldots \frac{p-1}{2}\right)\left(\frac{p+1}{2} \ldots (p-j) \ldots (p-2)(p-1)\right) \equiv -1 \pmod{p}$$

The product on the left has divided into two parts, each with the same number of factors. Pairing off j in the first half with $p - j$ in the second half, we can rewrite the congruence in the form

$$\prod_{j=1}^{\frac{p-1}{2}} j(p-j) \equiv \quad \pmod{p}$$

But $j(p-j) \equiv -j^2 \pmod{p}$, and so the above is

$$\prod_{j=1}^{\frac{p-1}{2}} (-j^2) \equiv (-1)^{\frac{p-1}{2}} \left(\prod_{j=1}^{\frac{p-1}{2}} j \pmod{p}.\right)$$

If $p \equiv 1 \pmod{4}$ then the first factor on the right is 1, and we see that $x = (\frac{p-1}{2})!$ is a solution of $x^2 \equiv -1 \pmod{p}$.

Suppose, conversely, that there is an x such that $x^2 \equiv -1 \pmod{p}$. We note that for such an $x, p \nmid x$. We suppose that $p > 2$, and raise both sides of the congruence to the power $\frac{p-1}{2}$ to see that

$$(-1)^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} = x^{p-1} \pmod{p}$$

.

By Fermat's congruence, the right side here is $\equiv 1 \pmod{p}$. The left hand side is ± 1. Since $-1 \not\equiv 1 \pmod{m}$, we deduce that

$$(-1)^{\frac{p-1}{2}} = 1.$$

Thus $\frac{p-1}{2}$ is even; that is, $p \equiv 1 \pmod{4}$.

In the case $p \equiv 1 \pmod{4}$, we have expilcitly constructed a solution of the congruence, $x^2 \equiv -1 \pmod{p}$. However, the amout of calculation required to evaluate $\frac{p-1}{2}! \pmod{p}$ is no smaller than the exhausting $x = 1, x2, \ldots, x = \frac{p-1}{2}$. In a later section, we will develop a method by which the desired x can be quickly determined. □

11 February 3, 2025

Theorem 62 provides a key piece of information needed to determine which integers can be written as the sum of two squares. We began by showing that a a class of prime numbers can be represented in this manner.

Lemma 63

If p is a prime numebr and $p \equiv 1 \pmod 4$ then there exist positive integers a and b such that $a^2 + b^2 = p$. This was first stated in 1632 by Albert Girard on the basis of numericla evidence. The first proof was given by Fermat in 1654.

Lemma 64

Let q be prime of the form $a^2 + b^2$. If $q \equiv 3 \pmod 4$. then $q \mid a$ and $q \mid b$.

Theorem 65 (Fermat)

Write the canonical factorization of n in the form

$$n = 2^\alpha \prod_{p \equiv 1(4)} p^\beta \prod_{p \equiv 3(4)} q^\gamma$$

Then n can be expressed as a sum of the two squres $\Longleftrightarrow$ all exponents γ are there.

Note 66. *We note that the identity holds:*

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ac + bc)^2$$

The Theorem of Fermat is the first of many such theorems. The object of constructing a coherent theorey of quadratic forms was the primary in the instance on research for seveveral centuries. This first setep in the theory is to generate Theorem 62. This is accomplished in the law of quadratic reciprocity, whcih we study in the initial chapters of the following chapters. With this tool in hand, we deelop some of the few fundamentals concerting quadratic forms in the latter part of Chapter 3. In particular, in sections, we apply the general theory of the sum of two squares, to give not only a proof of Theorem 65 but also some further results.

11.1 Solutions of Congruences

Let $f(x)$ denote a polynomial with the integer coefficients

$$f(x) = a_n x^n + a_{n+1} x^{n-1} + \cdots + a_0.$$

If n is an integer such that $f(u) \equiv 0 \pmod m$ we say that it is a solution of the congruence $f(x) \equiv 0 \pmod m$. Whether or not an integer a is a solution of a congruence depends on the modulo m.

If the integer u is a solution of $f(x) \equiv 0 \pmod m$ and if $v \equiv u \pmod m$, then Theorem 47 shows that v is also a solution. Because of this we shall say that $f(x) \equiv 0 \pmod m$ meaning that every integer congruent to $u \pmod m$ satisfies $f(x) \equiv 0 \pmod m$.

Example 67

The congruence $x^2 - x + 4 \equiv 0 \pmod{10}$ has the solution $x = 3$ and the solution $x = 8$. It also has solutions $x = 13$ and $x = 18$ and all other numbers obtained by adding and subtracting 10 as often as we wish. In counting the number of solutions of a congruence, we can restrict our attention to complete residue system belong to the modolus. In the example $x^2 - x + 4 \equiv 0 \pmod{10}$ because $x = 3$ and $x = 8$ are the only numbers among $0, 1, 2, \ldots, 9$ that are solutions. The two solutions can be written in the form $x = 3$ or $x = 8$ on in congruence from $x \equiv 3 \pmod{10}$ and $x \equiv 8 \pmod{10}$.

Example 68

The congruence

$$x^2 - 7x + 2 \equiv 0 \pmod{10}$$

has exactly 4 solutions, $x = 3, 4, 8, 9$. The reason for counting the number of solutions in this way is that if $f(x) \equiv 0 \pmod{m}$ has a solution $x = a$, then it follows that all integers x satisfying $x \equiv a \pmod{m}$ are automatically solutions, so this entire congruenec class is counted as a single solution.

Definition 69

Let $r_1, r_2, \ldots, r_m$ denote a complete system of residues $\pmod{m}$ Then the number of solutions of $f(x) \equiv 0 \pmod{m}$ is the number of solutions r_i such that $f(r_1) \equiv 0 \pmod{m}$.

12 February 5, 2025

Example 70

$x^2 + 1 = 0 \pmod{7}$ has no solutions.
$x^2 + 1 = 0 \pmod{5}$ has two solutions.
$x^2 - 1 = 0 \pmod{8}$ has 4 solutions.

Definition 71

Let

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$$

If $a_n \not\equiv 0 \pmod{m}$, then the degree of the congruence $f(x) = 0 \pmod{m}$ is degree n.
If $a_n \equiv 0 \pmod{m}$. Then let j be the largest integer such that $a_j \not\equiv 0 \pmod{m}$.
If there is no such j, so all coefficients are multiples of m, then the degree is not defined to the congruence.
It should be noted that the degree of the congruence $f(x) \equiv 0 \pmod{m}$ is not the same as the degree fo the polynomial $f(x)$.
The degree of the congruence depends on the modulus m and the coefficients of the polynomial $f(x)$.

Example 72

If

$$g(x) = 6x^3 + 3x^2 + 1$$

then $g(x) \equiv 0 \pmod 5$ has degree three but $g(x) \equiv 0 \pmod 2$ has degree 2 where as $g(x)$is of degree 3.

Theorem 73

If $d \mid m, d > 0$, and if the solution of $f(x) \equiv 0 \pmod m$ then it is a solution of $f(x) \equiv 0 \pmod d$.

Proof. This follows directly from Theorem 46, part 5 □

This is a distinction mode in the theory of algebraic congruence equations that has an analogy for congruences. A conditional equation such as $x^2 - 5x + 6 = 0$ is true only for certain values of x, namely $x = 2$ and $x = 3$. An identity of identical equations, such as $(x-2)^2 = x^2 - 4x + 4$ holds for all real numbers of complex numbers. Similarly, we say $f(x) \equiv 0 \pmod m$ is an **identical congruence** if all polynomials all of those coefficients are divisble by all whose coefficients are divisible by $f(x) \equiv 0 \pmod m$ is an identical congruence. A different type of identical congruence is also illustrated by $x^p \equiv x \pmod p$ which is trye by Fermat's theorem.

So before, considering congruences of higher degree, we first descibe the solutions in the linear case.

Theorem 74

Let a^b, and $m > 0$ be integers. Put $g = (a, m)$and now the congruence $ax \equiv b \pmod m$ has a solution $\Leftrightarrow g \mid b$. If the condition is met, then the solution from an arithmetic property progressoin with common differnece m/g, giving the solutions $\pmod m$.

Proof. The question is whether there exist integers x and y such that $ax + my = b$. Since g divides the left side, for such integers to exist we must have $g \mid b$. Suppose that this condition is met, and write $a = g\alpha$, $b = g\beta$, $m = g\gamma$. Then by the first part of Theorem 48, the desired congruence holds if and only if $\alpha x \equiv \beta \pmod \gamma$. Here $(\alpha, \gamma) = 1$ by Theorem 15, so by Theorem 58 there is a unique number $\bar{\alpha} \pmod \gamma$ such that $\alpha\bar{\alpha} \equiv 1 \pmod \gamma$. On multiplying through by $\bar{\alpha}$, we find that $x = \bar{\alpha}\beta \pmod \gamma$. Thus the set of integers x for which $ax \equiv b \pmod m$ is precisely the arithmetic progression of numbers of the form $\bar{\alpha}\beta + k\gamma$. If we allow k to take on the values $0, 1, \ldots, g-1$, we obtain g values of x that are distinct $\pmod m$. All other values of x are congruent $\pmod m$ to one of these, so we have precisely g solutions. □

Fact 75

Since $\bar{\alpha}$ can be found by application of the Euclidean algorithm, we have a method for finding all solutions of $ax \equiv b \pmod m$ when $g \mid b$.

12.1 Chinese Remainder Theorem

We now consider the important problem of solving simultaneous congruences. The simplest case of this is to see if there is any x that satisfies the simultaneous congruences:

$$\begin{aligned}
x &\equiv a_1 \pmod{m_1}\\
x &\equiv a_2 \pmod{m_2}\\
&\vdots\\
x &\equiv a_r \pmod{m_r}
\end{aligned}$$

This is the subject of the Chinese Remainder Theorem because it was known in China in the first century AD.

Theorem 76 (Chinese Remainder Theorem)
Let $m_1, m_2, \ldots, m_r$ denote r positive integers that are relatively prime in pairs. Let $a_1, a_2, \ldots, a_r$ denote any r integers. If the congruence 12.1 holds that means that x is in the form of $x = x_0 + km$ for some integer k. Here, $m = m_1 m_2 \ldots m_r$.