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 $a^k \mid\mid b$, 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 **??**. 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 **??**. Moreover, there cannot be two distinct integers with property 2, because of **??**, 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 $b_1, b_2, \ldots, b_n$. First, we show that g is a common divisor of $b_1, b_2, \ldots, b_n$. 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 $b_1, b_2, \ldots, b_n$. Then $d \mid \sum_{j=1}^{n} b_j x_j$, so $d \mid g$. Therefore, g is the greatest common divisor of $b_1, b_2, \ldots, b_n$.

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 $g = (b_1, b_2, \ldots, b_n) = \sum_{j=1}^{n} b_j x_j$ 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 $b_1, b_2, \ldots, b_n$ that is divisible by every common divisor. □

Theorem 14

For any positive integer$m$ we have

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

Proof. By **??** 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 **??** 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 **??**, 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 **??**, 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 **??**, 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 **??**, 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 **??**, 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, **??**, to obtain a series of equations:

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

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 **??**, 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 **??**, 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 **??** 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 **??**. 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 **??** 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 **??**, 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

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

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 **??**. 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 **??** 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 $\{1, 2, \ldots, n\}$. For each fixed $k, 0 \leqslant k \leqslant n$, we consider the monomial terms obtained from those subsets of $\mathbb{A}$ of $\{1, 2, 3, \ldots, n\}$ 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 $(x+y)^5 = 1x^5 + 5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4 + 1y^5$

1

1 1

1 2 1

1 3 3 1

1 4 6 4 1

1 5 10 10 5 1

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 **??**, part 4, repeatedly to find $a^2 \equiv b^2$, $a^3 \equiv b^3$, $\ldots$, $a^n \equiv b^n \pmod m$, and then $c_i a^j \equiv c_i b^j \pmod m$ 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 **??** and therefore $\frac{m}{(a,m)} \mid (y-x)$ by **??**. 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 **??**, part 6. But (a,m) is a divisor of a, so we can write $ax \equiv ay \pmod{m}$ by **??**, 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 **??**) $[m_1, m_2, \ldots, m_r] \mid (y-x)$. 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 **??** 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 **??** 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 **??**. 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 **??**, $ar_1, ar_2, \ldots, ar_{\varphi(m)}$ 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 **??**, 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 **??**, 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 congurent $pmodm$. 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 **??**, part 2. □

Fact 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 **??**, 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 **??** 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 **??** 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 **??** 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 **??** 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

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

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 $x = \left(\frac{p-1}{2}\right)!$ 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

?? 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 $\iff$ all exponents γ are there.

Fact 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 **??**. 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 **??** 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 **??** 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 **??**, part 5 □

This is a distinction mode in the theorey 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 **??**, the desired congruence holds if and only if $\alpha x \equiv \beta \pmod{\gamma}$. Here $(\alpha, \gamma) = 1$ by **??**, so by **??** 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:

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_r \pmod{m_r}$$

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 **??** holds that means that x is in the form of $x = x_0 + km$ for some integer k. Here, $m = m_1 m_2 \ldots m_r$.

13 February 7, 2025

Proof. Writing $m = m_1 m_2 \ldots m_r$, we see that $\frac{m}{m_j}$ is an integer and that $\left(\frac{m}{m_j}, m_i\right) = 1$. Hence, by **??**, for each j there is an integer b_j such that $\frac{m}{m_j} b_j \equiv 1 \pmod{m_j}$ and $\frac{m}{m_j} b_j \equiv 0 \pmod{m_i}$ if $i \neq j$. Put

$$x_0 = \sum_{j=1}^{r} \frac{m}{m_j} b_j a_j.$$

We consider this number modulo m_i and find that

$$x_0 \equiv a_i \pmod{m_i}.$$

Thus x_0 is a solution of the system. If x_0 and x_1 are two solutions of the system, then $x_0 \equiv x_1 \pmod{m_i}$ for $i = 1, 2, \ldots, r$ and hence $x_0 \equiv x_1 \pmod{m}$. By part 3 of **??**, this completes the proof. □

Example 77
Find the least positive integer such that

$$x \equiv 5 \pmod{7} x \equiv 7 \pmod{11} x \equiv 3 \pmod{13}$$

Solution. *We follow the proof of the theorem, taking* $a_1 \equiv 5 \pmod{7}$, $a_2 \equiv 7 \pmod{11}$, *and* $a_3 \equiv 3 \pmod{13}$. *We follow the proof, let* $m = 7 \cdot 11 \cdot 13 = 1001$. *Now* $(m_1, m_2, m_3) = 1$ *and indeed by* **??**, *part 4, we find that,*

$$(-2)m_2 m_3 + (21)m_1 = 1$$

. So we take $b_1 = 2$. *Similarly,*

$$4m_1 m_3 + (-33)m_2 = 1$$

. *By the Euclidean Algorithm a third time,*

$$(-1)m_1m_2 + 6m_3 = 1$$

. *So we may take* $b_3 = 1$. *Then* **??**, *we see that* $11 \cdot 13 \cdot (-2) \cdot 5 + 7 \cdot 13 \cdot 4 \cdot 7 + 7 \cdot 11 \cdot (-1) \cdot 3 = 887$. *Since the solution is unique* $\pmod{m}$, *there is only a solution among the numbers* $1, 2, \ldots, 1001$. *Thus 887 is the least possible solution.*

In the Chinese Remainder Theorem, the hypthesis that modulo m_j *should be a pairwise is absolutely essential, when this hypothesis fails, a solution* x *of the system is no longer guaranteed, and when such an* x *does exist, we see from part 3 of* **??** *this is unique*

$$m_1, m_2, \ldots, m_3$$

not modulo m. *In this case, there is no solution of the system, and we call the system* **inconsistent**, *The following two examples arise when the* m_j *are allowed to have a common factor. An extension of* **??** *to the case of* m_j *is laid out in the problems 1 9 through 23 in the textbook.*

Example 78

Show that there is no solution x for which $x \equiv 29 \pmod{52}$ and $x \equiv 19 \pmod{72}$

Solution. *Since* $52 = 4 \cdot 13$, *we see by part 4 of* **??** *that the simultaneous congruences* $x \equiv 29 \pmod{4}$, *and* $x \equiv 20 \pmod{13}$ *which reduces to* $x \equiv 1 \pmod{4}$, *and* $x \equiv 3 \pmod{13}$.

Similarly, $72 = 8 \cdot 9$ *and the second congruence is given to be* $x \equiv 19 \pmod{8}$ *and* $x \equiv 19 \pmod{9}$. *These reduces to* $x \equiv 3 \pmod{13}$ *and* $x \equiv 1 \pmod{9}$. *By* **??**, *we know that the constraints* $\pmod{13}$ *and* $\pmod{9}$ *and independent of the congruences* $x \equiv 1 \pmod{4}$ *and* $x \equiv 3 \pmod{8}$.

Once an inconsistency has been identified, a brief proof can be constructed. The first congruence implies that $x \equiv 1 \pmod{4}$ *while the second congruence implies that* $x \equiv 3 \pmod{4}$. *This is a contradiction, so there is no solution.*

Example 79

Determine if whether the system

$$x \equiv 3 \pmod{10},$$
$$x \equiv 5 \pmod{15},$$
$$x \equiv 5 \pmod{84}$$

has a solution and find them all if any exists.

There are two ways of solving this

Solution (First Solution)**.** *We factor each moduli into prime factors by part 3,* **??**, *we see that the first congruence is equivalent to the simultaneous congruences* $x \equiv 3 \pmod{2}$, *and* $x \equiv 3 \pmod{5}$. *Similarly, the system is equivalent to the two conditinos*

$$x \equiv 8 \pmod{3}$$
$$x \equiv 8 \pmod{5}$$

while the third congruence is equivalent to the three congruences $x \equiv 5 \pmod 4$, $x \equiv 5 \pmod 5$, *and* $x \equiv 5 \pmod 3$ *and* $x \equiv 5 \pmod{17}$. *The new congruence of simultaneous is now equivalent to the new ones, but the moduli are prime numbers. So we have,*

$$\begin{aligned} x &\equiv 3 \pmod 2 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 8 \pmod 3 \\ x &\equiv 8 \pmod 5 \\ x &\equiv 5 \pmod 4 \\ x &\equiv 5 \pmod 3 \\ x &\equiv 5 \pmod 3 \\ x &\equiv 3 \pmod 7 \end{aligned}$$

We can consider the first 2 factors. The conditions are

$$x \equiv 3 \pmod 2 \text{ and } x \equiv 1 \pmod 4$$

These two are consistent, but the second one implies the first, so that the first one may be dropped. The The conditions modulo 3 are $x \equiv 8 \pmod 3$ *and* $x \equiv 5 \pmod 3$. *These are equivalent, and may be expressed as* $x \equiv 2 \pmod 3$. *Third, the conditions modulo 5 are* $x \equiv 3 \pmod 5$, $x \equiv 8 \pmod 5$. *These are equivalent, so we drop the second of them. Finally, we have the condition* $x \equiv 5 \pmod 7$.

14 February 10, 2025

We will start using the Chinese Remainder Theorem for this part of the proof. There are multiple things that we need to make sure that they are working want.

15 February 12, 2025

Exhibit for the following one-to-one correspondence expilictly when $m_1 = 7$, $m_2 = 9$, $m = 63$.

Solution. *Consider the following matrix with 7 row and 9 columns at the intersection of* i*th row and* j*th column we place, an entry where* c_{ij} *where* $c_{ij} = i \pmod 7$ *and* $c_{ij} = j \pmod 9$. *According to* **??**, *we can allow the elements* c_{ij} *from a complete residue system* $e = \{1, 2, \ldots, 63\}$. *For example, the element* 40 *is at the intersection of the fifth row and the fourth column because* $40 \equiv 5 \pmod 7$ *and* $40 \equiv 4 \pmod 9$. *Note that the element* 41 *is at the intersection of the sixth row and fifth column, since* $41 \equiv 6 \pmod 7$ *and* $41 \equiv 5 \pmod 9$. *Thus the element* $c + 1$ *in the matrix is just south east from the element* c *allowing for periodicity when* c *is in the last row or column. For example* 42 *is in the last row so* 43 *turns up in in the first row, one column later. This gives an easy way to construct the matrix. Write a* 1 *in the* $c_1 1$ *position*

and proceed downward and so to the right with the $2, 3$, *and so forth.*

1	29	57	**22**	50	15	43	8	36
27	**2**	30	**58**	23	51	16	44	9
10	38	**3**	**31**	59	24	52	17	45
46	11	39	**4**	32	60	25	53	18
19	47	12	**40**	**5**	33	61	26	54
55	**20**	48	**13**	**41**	**6**	34	62	27
28	56	21	49	14	42	**7**	35	63

Here the correspondence between (i) *and* c_{ij} *provide a solution to the problem. In the matrix, the entry* c_{ij} *is entered in boldface if* $(c_{ij}, 63) = 1$. *We note that these entries are precisely those for which* i *is one of the numbers* $\{1, 2, \ldots, 6\}$, *and* j *is one of the numbers* $\{1, 2, 4, 5, 7, 8\}$. *That is,* $(c_{ij}, 63) = 1$ *if and only if* $(i, 7) = 1$ *and* $(j, 9) = 1$. *Since there are exactly 6 such* i, *and for each such* i *there are precisely 6 such* j, *we deduce that* $\varphi(63) = 36 = \varphi(7)\varphi(9)$.

We will show such a formula holds in general and we derive that $\varphi(m)$ in terms of prime factorization of m.

Theorem 80

If m_1 and m_2 denote two positive, relatively prime integers, then $\varphi(m_1 m_2) = \varphi(m_1)\varphi(m_2)$. Moreover, if m has the canonical factorization

$$m = \prod_{i=1}^{k} p_i^{\alpha_i},$$

then

$$\varphi(m) = m \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

Proof. Put $m = m_1 m_2$, and suppose that $(x, m) = 1$. By reducing x modulo m_1 we see that there is a unique $a_1 \in \phi(m_1)$ for which $x \equiv a_1 \pmod{m_1}$. Here, as before, $\phi(m_1)$ is the complete system of residues $\phi(m_1) = \{1, 2, \ldots, m_1\}$. Similarly, there is a unique $a_2 \in \phi(m_2)$ for which $x \equiv a_2 \pmod{m_2}$. Since $(x, m_1) = 1$, it follows by **??** that $(a_1, m_1) = 1$. Similarly $(a_2, m_2) = 1$. For any positive integer n, let $\mathcal{P}(n)$ be the system of reduced residues formed of those numbers $a \in \phi(n)$ for which $(a, n) = 1$. That is, $\mathcal{P}(n) = \{a \in \phi(n) : (a, n) = 1\}$. Thus we see that any $x \in \mathcal{P}(m)$ gives rise to a pair (a_1, a_2) with $a_i \in \mathcal{P}(m_i)$ for $i = 1, 2$. □

16 February 14, 2025

We have now established the first identity of the theorem. If $m = \prod p_i^{\alpha_i}$ is the canonical factorization of m, then by repeated use of this identity we see that $\varphi(m) = \prod \varphi(p_i^{\alpha_i})$. To complete the proof, it remains to determine the value of $\varphi(p_i^{\alpha_i})$. If a is one of the $p_i^{\alpha_i}$ numbers $1, 2, \ldots, p_i^{\alpha_i}$, then $(a, p_i^{\alpha_i}) = 1$ unless a is one

of the $p_i^{\alpha_i-1}$ numbers $p_i, 2p_i, \ldots, p_i^{\alpha_i-1} \cdot p_i$. On subtracting, we deduce that the number of reduced residue classes modulo $p_i^{\alpha_i}$ is $p_i^{\alpha_i} - p_i^{\alpha_i-1} = p_i^{\alpha_i}(1 - \frac{1}{p_i})$. This gives the stated formula.

Let $f(x)$ denote a polynomial with integral coefficients, and let $N(m)$ denote the number of solutions of the congruence $f(x) \equiv 0 \pmod{m}$ as counted in **??**. We suppose that $m = m_1 m_2$, where $(m_1, m_2) = 1$. By employing the same line of reasoning as in the foregoing proof, we show that the roots of the congruence $f(x) \equiv 0 \pmod{m}$ are in one-to-one correspondence with pairs (a_1, a_2) in which a_1 runs over all roots of the congruence $f(x) \equiv 0 \pmod{m_1}$ and a_2 runs over all roots of the congruence $f(x) \equiv 0 \pmod{m_2}$. In this way we are able to relate $N(m)$ to $N(m_1)$ and $N(m_2)$.

Theorem 81

Let $f(x)$ be a fixed polynomial with integral coefficients, and for any positive integer m let $N(m)$ denote the number of solutions of the congruence $f(x) \equiv 0 \pmod{m}$. If $m = m_1 m_2$ where $(m_1, m_2) = 1$, then

$$N(m) = N(m_1)N(m_2).$$

If $m = \prod p_i^{\alpha_i}$ is the canonical factorization of m, then

$$N(m) = \prod N(p_i^{\alpha_i}).$$

Proof. The first part of the theorem is an immediate consequence of **??**. To prove the second part, we note that if $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, then by repeated use of the first part, we have

$$N(m) = N(p_1^{\alpha_1})N(p_2^{\alpha_2}) \cdots N(p_k^{\alpha_k}).$$

Thus it suffices to determine $N(p_i^{\alpha_i})$. If $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$ has a solution $x = a$, then $f(a) \equiv 0 \pmod{p_i}$. By Hensel's lemma, there is a unique solution b of the congruence $f(x) \equiv 0 \pmod{p_i}$ such that $b \equiv a \pmod{p_i^{\alpha_i}}$. Thus if we let $N(p)$ denote the number of solutions of the congruence $f(x) \equiv 0 \pmod{p}$, we see that

$$N(p^k) = pN(p^{k-1}).$$

Since $N(p^1) = 1$, it follows by induction that

$$N(p^k) = p^k.$$

This completes the proof. □

Example 82

Let $f(x) = x^2 + x + 7$. Find all the roots of the congruence $f(x) \equiv 0 \pmod{15}$

Solution. *Trying the values $x = 0, \pm 1, \pm 2$, we find that $f(x) \equiv 0 \pmod{5}$ has no solution. Since $5 \mid 15$, it follows that there is no solution* $\pmod{15}$.

Example 83

Let $f(x) = x^2 + x + 7$. Find all the roots of the congruence $f(x) \equiv 0 \pmod{189}$.

Solution. *We are given that* $189 = 27 \cdot 7$. *By the Chinese Remainder Theorem, we need to find the common solutions of the congruences modulo 27 and modulo 7. The roots modulo 27 are 4, 13, and 22. The roots modulo 7 are 0 and 6. We need to solve the following systems of congruences:*

The roots modulo 27 are 4, 13, and 22. The roots modulo 7 are 0 and 6.

By the Euclidean algorithm and **??**, *we find that* $x = a_1 \pmod{27}$ *and* $x = a_2 \pmod{7}$ *if and only if* $x = 28a_1 - 27a_2 \pmod{189}$. *We let* a_1 *take on the three values 4, 13, and 22, while* a_2 *takes on the values 0 and 6. Thus we obtain the six solutions:*

For $a_1 = 4$ *and* $a_2 = 0$*:*

$$x = 28 \cdot 4 - 27 \cdot 0 = 112 \pmod{189}$$

For $a_1 = 4$ *and* $a_2 = 6$*:*

$$x = 28 \cdot 4 - 27 \cdot 6 = 112 - 162 = -50 \equiv 139 \pmod{189}$$

For $a_1 = 13$ *and* $a_2 = 0$*:*

$$x = 28 \cdot 13 - 27 \cdot 0 = 364 \equiv 175 \pmod{189}$$

For $a_1 = 13$ *and* $a_2 = 6$*:*

$$x = 28 \cdot 13 - 27 \cdot 6 = 364 - 162 = 202 \equiv 13 \pmod{189}$$

For $a_1 = 22$ *and* $a_2 = 0$*:*

$$x = 28 \cdot 22 - 27 \cdot 0 = 616 \equiv 49 \pmod{189}$$

For $a_1 = 22$ *and* $a_2 = 6$*:*

$$x = 28 \cdot 22 - 27 \cdot 6 = 616 - 162 = 454 \equiv 76 \pmod{189}$$

Therefore, the roots of $f(x) \equiv 0 \pmod{189}$ *are* $x \equiv 13, 49, 76, 112, 139, 175 \pmod{189}$.

16.1 Techniques of Numerical Calculation

In here learn how to

Example 84

Determine the value of

Lemma 85

Suppose that $1 \leq k \leq n$, and that the numbers $u_1, u_2, \ldots, u_k$ are independently chosen from the set $\{1, 2, \ldots, n\}$. Then the probability that the numbers $u_1, u_2, \ldots, u_k$ are distinct is

$$\frac{n}{n} \cdot \frac{n-1}{n} \cdot \frac{n-2}{n} \cdots \frac{n-k+1}{n} = \prod_{i=0}^{k-1} \left(1 - \frac{i}{n}\right).$$

Example 86

Use this method to locate a proper divisor of the number $m = 36287$.

16.2 Public Key Cryptography

Lemma 87

Suppose that m is a positive integer and that $(a, m) = 1$. If k and $\hbar k$ are integers, such that $k\hbar k \equiv 1 \pmod{\phi(m)}$, then $a^{k\hbar k} \equiv a \pmod{m}$.

17 February 17, 2025

17.1 Prime Power Moduli

The problem of solving a congruence was reduced in Section **??** to the case of a prime-power modulus. To solve a polynomial congruence $f(x) \equiv 0 \pmod{p^k}$, we start with a solution modulo p, then move on to modulo p^2, then to p^3, and by iteration to p^k. Suppose that $x = a$ is a solution of $f(x) \equiv 0 \pmod{p^j}$ and we want to use it to get a solution modulo p^{j+1}.

The idea is to try to get a solution $x = a + tp^j$, where t is to be determined, by use of Taylor's expansion:

$$f(a + tp^j) = f(a) + tp^j f'(a) + \frac{t^2 p^{2j}}{2!} f''(a) + \cdots + \frac{t^n p^{nj}}{n!} f^{(n)}(a)$$

where n is the presumed degree of the polynomial $f(x)$. All derivatives beyond the n-th are identically zero.

Now with respect to the modulus p^{j+1}, equation (2.3) gives:

$$f(a + tp^j) \equiv f(a) + tp^j f'(a) \pmod{p^{j+1}}$$

as the following argument shows. What we want to establish is that the coefficients of $t^2, t^3, \ldots, t^n$ in equation (2.3) are divisible by p^{j+1} and so can be omitted in (2.4). This is almost obvious because the powers of p in those terms are $p^{2j}, p^{3j}, \ldots, p^{nj}$. But this is not quite immediate because of the denominators $2!, 3!, \ldots, n!$ in these terms. The explanation is that $f^{(k)}(a)\frac{j^k}{k!}$ is an integer for each value of k, $2 \le k \le n$. To see this, let $c_r x^r$ be a representative term from $f(x)$. The corresponding term in $f^{(k)}(a)$ is

$$c_r r(r-1)(r-2)\cdots(r-k+1)a^{r-k}.$$

According to Theorem 1.21, the product of k consecutive integers is divisible by $k!$, and the argument is complete. Thus, we have proved that the coefficients of $t^2, t^3, \ldots$ in (2.3) are divisible by p^{j+1}.

The congruence (2.4) reveals how t should be chosen if $x = a + tp^j$ is to be a solution of $f(x) \equiv 0 \pmod{p^{j+1}}$. We want t to be a solution of

$$f(a) + tp^j f'(a) \equiv 0 \pmod{p^{j+1}}.$$

Since $f(x) \equiv 0 \pmod{p^j}$ is presumed to have the solution $x = a$, we see that p^j can be removed as a factor to give

$$\frac{f(a)}{p} \equiv -tf'(a) \pmod{p},$$

which is a linear congruence in t. This congruence may have no solution, one solution, or p solutions. If $f'(a) \not\equiv 0 \pmod{p}$, then this congruence has exactly one solution, and we obtain a solution $x = a + tp^j$ of $f(x) \equiv 0 \pmod{p^{j+1}}$.

Theorem 88 (Hensel's Lemma)
Suppose $f(x)$ is a polynomial with integer coefficients. If $f(a) \equiv 0 \pmod{p^j}$ and $f'(a) \not\equiv 0 \pmod{p}$, then there is an integer $t \pmod{p}$ such that $f(a + tp^j) \equiv 0 \pmod{p^{j+1}}$.

Proof. If $f(a) \equiv 0 \pmod{p^j}$, $f(b) \equiv 0 \pmod{p^k}$, $j < k$, and $a \equiv b \pmod{p^j}$, then we say that b *lies above* a, or a *lifts to* b. If $f(a) \equiv 0 \pmod{p^j}$, then the root a is called **nonsingular** if $f'(a) \not\equiv 0 \pmod{p}$; otherwise it is **singular**. By Hensel's lemma we see that a nonsingular root $a \pmod{p}$ lifts to a unique root $a_2 \pmod{p^2}$. Since $a_2 \equiv a \pmod{p}$, it follows (by **??**) that $f'(a_2) \equiv f'(a) \not\equiv 0 \pmod{p}$. By a second application of Hensel's lemma we may lift a_2 to form a root a_3 of $f(x)$ modulo p^3, and so on. In general we find that a nonsingular root a modulo p lifts to a unique root a_j modulo p^j for $j = 2, 3, \ldots$. Now, we see that this sequence is generated by means of the recursion

$$a_{j+1} = a_j - \frac{f(a_j)}{f'(a_j)}\overline{f'(a_j)}$$

where $\overline{f'(a_j)}$ is an integer chosen so that $f'(a_j)\overline{f'(a_j)} \equiv 1 \pmod{p}$. This is entirely analogous to Newton's method for locating the root of a differentiable function.

□

Example 89
Solve $x^2 + x + 47 = 0 \pmod{7^3}$

Solution. *First, we note that* $x \equiv 1 \pmod{7}$ *and* $x \equiv 5 \pmod{7}$ *are the only solutions of* $x^2 + x + 47 \equiv 0 \pmod{7}$. *Since* $f'(x) = 2x + 1$, *we see that* $f'(1) \equiv 3 \not\equiv 0 \pmod{7}$ *and* $f'(5) \equiv 11 \not\equiv 0 \pmod{7}$, *so these roots are nonsingular.*

Taking $f'(1) = 3$, *we see by Hensel's Lemma that the root* $a = 1 \pmod{7}$ *lifts to* $a_2 = 1 - \frac{f(1)}{f'(1)} \cdot 7$. *Since* $f(1) = 49 \equiv 0 \pmod{7}$, *we have* $a_2 = 1$. *Then* $a_3 = 1 - \frac{f(1)}{f'(1)} \cdot 7^2 = 1 - 49 \cdot 7 \cdot 3 = 1 - 1029 \equiv 99 \pmod{7^3}$.

Similarly, taking $f'(5) = 11$, *we see by Hensel's Lemma that the root* $a = 5 \pmod{7}$ *lifts to* $a_2 = 5 - \frac{f(5)}{f'(5)} \cdot 7$. *Since* $f(5) = 77 \equiv 0 \pmod{7}$, *we have* $a_2 = 5$. *Then* $a_3 = 5 - \frac{f(5)}{f'(5)} \cdot 7^2 = 5 - 77 \cdot 7 \cdot 11 = 5 - 5929 \equiv 243 \pmod{7^3}$.

Thus, we conclude that 99 *and* 243 *are the desired roots, and that there are no others.*

18 February 19, 2025

Example 90

Solve $x^2 + x + 7 \pmod{81}$

Solution. *Starting with* $x^2 + x + 7 \pmod 3$, *we note that* $x \equiv 1$ *is the only solution. Here,* $f'(1) \equiv 3 \equiv 0 \pmod 3$, *and* $f(1) \equiv 0 \pmod 9$ *is the only solution. Hence, we have the roots* $x \equiv 1, 4, 7 \pmod 9$. *Now* $f(1) \not\equiv 0 \pmod{27}$, *and hence there is no root* $x \pmod{27}$ *for which* $x \equiv 1 \pmod 9$. *As* $f(4) \equiv 0 \pmod{27}$, *we obtain three roots,* $4, 13, 22 \pmod{27}$, *which are* $\equiv 4 \pmod 9$. *On the other hand,* $f(7) \not\equiv 0 \pmod{27}$, *so there is no root* $\pmod{27}$ *that is* $\equiv 7 \pmod 9$. *We are now in a position to determine which, if any, of the roots* $4, 13, 22 \pmod{27}$ *can be lifted to roots* $\pmod{81}$. *We find that* $f(4) \equiv 27 \not\equiv 0 \pmod{81}$, $f(13) \equiv 189 \equiv 27 \not\equiv 0 \pmod{81}$, *and that* $f(22) \equiv 513 \equiv 27 \not\equiv 0 \pmod{81}$, *from which we deduce that the congruence has no solution* $\pmod{81}$. *In this example, we see that singular solution* $a \pmod p$ *may lift a a higher power of* p, *but not necessarily to arbitrarily high powers of* p.

We now show that if the power of p dividing $f(a)$ is sufficiently large compared with the power of p in $f'(a)$, then the solution can be lifted without limit.

Theorem 91

Let $f(x)$ be a polynomial with integral coefficients. Suppose that $f(a) \equiv 0 \pmod{p^j}$ and that $p^\tau \mid\mid f'(a)$, and that $j \geq 2\tau + 1$. If $b \equiv a \pmod{p^{j-\tau}}$ then $f(b) \equiv f(a) \pmod{p^j}$ and $p^\tau \mid\mid f'(b)$. Moreover, there is a unique $t \pmod p$ such that $f(a + tp^{j-\tau}) = 0 \pmod{p^{j+1}}$.

In this situation, a collection of p^τ solutions $\pmod{p^j}$ give rise to p^τ solutions $\pmod{p^{j+1}}$, while the power of p dividing f' dividing remains constant. Since the hypotheses of the theorem apply with a replced by $a + t^{j-\tau}$ and $\pmod{p^j}$ but with τ unchanged, the lifting may be repeated and continues indefinitely

Proof. By Taylor's expansion in **??**, we see that

$$f(b) = f(a + ip^{j-\tau}) \equiv f(a) + ip^{j-\tau} f'(a) \pmod{p^{2j-2\tau}}.$$

Here, the modulus is divisible by p^{j+1}, since $2j - 2\tau = j + (j - 2\tau) \geq j + 1$. Hence,

$$f(a + tp^{j-\tau}) \equiv f(a) + tp^{j-\tau} f'(a) \pmod{p^{j+1}}.$$

Since, both terms, on the R.H.S are divisibly by p^j, the LHS is also. Moreover, on dividing through p^j we find that,

$$\frac{f(a + tp^{j-\tau})}{p^j} \equiv \frac{f(a)p^j}{+} t\frac{f'(a)}{p^\tau} \pmod p$$

and the coefficient of t is relatively prime to p, so that there is a unique $t \pmod p$ for which the right side is divisible by p. This completes final assertion of the theorem. To complete the proof, we note that $f'(x)$ is a unique polynmial with integral coefficients, so that

$$f'(a + tp^{j-\tau}) \equiv f'(a) \pmod{p^{j-\tau}}.$$

for any integer t. But $j-\tau \geq \tau+1$, so this congruence holds, $\pmod{p^{\tau+1}}$. Since p^τ exactly divides $f'(a)$ (in symbols, $p^\tau \mid\mid f'(a)$), we conclude that $p^\tau \mid\mid f'(a+tp^{j-\tau})$. This completes the proof of the theorem. □

19 February 21, 2025

Example 92

Discuss the solutions of $x^2+x+223 \equiv 0 \pmod{3^4 j}$.

Solution. *Since* $223 \equiv 7 \pmod{27}$, *the solutions* $\pmod{27}$ *are the same in example* **??**. *For this polynomial, we find that* $f(4) \equiv 0 \pmod{81}$ *are the same as in example* **??**. *For this new polynomial, we find taht* $f(4) \equiv 0 \pmod{81}$, *and thus we have three solutions* $4, 31, 58 \pmod{81}$. *Similarly,* $f(13) \equiv 0 \pmod{81}$, *giving three solutions* $13, 40, 67 \pmod{81}$. *Moreover,* $f(22) \equiv 0 \pmod{81}$, *yielding the solutoins* $22, 49, 76 \pmod{81}$. *In fact, we note that* $f(4) \equiv 0 \pmod{3^5}$ *and so* $3^4 \mid\mid f(4)$. *So by theorem,* **??**, *we have the solution* $4 \pmod{243}$ *is one of nine solutions of the form* $4+27t \pmod{243}$. *We may further verify that there is precisely one value of* $t \pmod 3$, *namely* $t=2$, *for which* $f(4+27t) = 0 \pmod{3^6}$.

That is since, we have q solutions $\pmod{3^6}$, *one of those solutions must be* $22+81t$. *On the other hand, as* $f'(13) \equiv 0 \pmod{27}$ *so we have solutions for* $13+27t$. *As* $3^4 \mid\mid f(13)$, *we find that none of the three solutions* $13+27t \pmod{81}$ *lifts to a solution* $\pmod{243}$. *In conclusion, we have found that for each* $j \geq 5$ *there are precisely 18 solutions* $\pmod{3^j}$, *of which 12 do not lift to* 3^{j+1}, *while each of the remaining six lifts to three solutions* $\pmod{3^{j+1}}$.

729 729

243

81

27

9

3

Suppose that $f(a) \equiv 0 \pmod p$, and that $f'(a) \equiv 0 \pmod p$. We wish to know whether a can be lifted to solutions modulo arbitrarily high powers of p. The situation is resolved if we can reach a point at which **??** applies, that is, $j \geq 2\tau+1$. However, there is nothing in our discussion thus far to preclude the possibility that the power of p in f' might steadily increase with that in f, so that **??** might never take effect.

19.1 Prime Modulus

We have reduced the problem of solving

$$f(x) \equiv 0 \pmod m$$

to the last state of the solving congruences with prime moduli. Although we have no general method for solving such congruences, there are some interesting facts concerning the solutions. A natural question about polynomial congruences, of the type $f(x) \equiv 0 \pmod{m}$ is whether there is any analogous well-known theorem in algebra that a polynomial equation of degree n whose coefficients are complex numbers has exactly n roots or solutions, allowing for multiple roots. For congruences, the situation is more complicated. In the first place for any number $m > 1$ there are polynomials congruences having no solutions. As an example is written by the following

$$x^p - x + 10 \pmod{m}$$

. There is no solution, because

$$x^p - x + 1 \equiv 0 \pmod{m}$$

has none, by Fermat's Theorem, moreover, we have already more solutions than its degree for example $x^2 - 7x + 2 \equiv 0 \pmod{m}$ has four solutions: $x = 3, 4, 8, 9$. Also, $x^2 + x + 7 \equiv 0 \pmod{27}$ with three solutions: $x = 4, 13, 22$. But if the solution is prime a congruence cannot have more solutions than it's degrees. This is proved in **??**, later in the solution. It is important here to carefully the consider the meaning of the "degree of the polynomial". This is in **??**. Such a polynomial is $5x^3 + x^2 - x$ has degree three, but the congruence $5x^3 + x^2 = x \equiv 0 \pmod{5}$ has degree 2. Consider the congruence

$$5x^2 + 10x + 15 \equiv 0 \pmod{5}$$

having solutions $x = 0, 1, 2, 3$, and at first glance this might appear in **??**. However, by **??**, this congruence is assigned no degree, so that **??** does not apply.

20 February 24, 2025

Theorem 93

The congruence $f(x) \equiv 0 \pmod{p}$ of degree of n has at most n solutions.

21 February 26, 2025

Corollary 94

If $b_n + b_{n-1}x^{n-1} + \cdots + b_0 \equiv 0 \pmod{p}$ has more than n solutions, then all coefficients b_j are divisible by p.

Proof. The reason this is that if some of the coefficients is not divisible by p, then the polynomial has a degree, and that degree is at most n. Therefore, **??** implies that the congruence has at most n solutions and that is a contradiction. □

Theorem 95

If $F(x)$ is a function that maps residue classes $\pmod p$ to residue classes $\pmod p$, then there is a polynomial $f(x)$ with integral coefficients and degree at most $p-1$ such that $F(x) \equiv f(x) \pmod p$ for all residue classes $x \pmod p$

Proof. By Fermat's congruence, we see that

$$1-(x-a)^{p-1} \equiv \begin{cases} 1 \pmod p & \text{if } x \equiv a \pmod p \\ 0 \pmod p & \text{otherwise} \end{cases}$$

Hence the polynomial,

$$f(x) = \sum_{i=1}^{p} F(i)(1-(x-i)^{p-1}$$

has desired properties. □

Theorem 96

The congruence

$$f(x) \equiv 0 \pmod p$$

of degree$n$, with leading coefficients $a_n = 1$ has n solutions iff $f(x)$ is a factor of $x^p - x \pmod p$, that is iff

$$x^p - x = f(x)q(x) + ps(x)$$

where $q(x)$ and $s(x)$ have integral coefficients, $q(x)$ has degree $n-p$ and leading coefficinet 1, and where either $s(x)$ is a polynomial of degree less than n or $s(x)$ is zero.

Proof. First assume that

$$f(x) \equiv 0 \pmod p$$

has n solutions. Then $n \leq p$ by **??** which says (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 $f(r_1) \equiv 0 \pmod m$.) Dividing $x^p - x$ by $f(x)$, we get a quotient $q(x)$ and a remainder $r(x)$ satisfying

$$x^p - x = f(x)q(x) + r(x)$$

where $r(x)$ is either 0 or else a polynomial of degree $< n$. □

This equation implies by an application of Fermat's Theorem to $x^p - x$ that every solution of $f(x) \equiv 0 \pmod p$ is a solution of $r(x) \equiv 0 \pmod p$. Thus $r(x) \equiv 0 \pmod p$. Then $r(x) \equiv 0 \pmod p$ has at least

n solutions, and by **??** it follows that every coefficient is at last divisible by p_1 so $r(x) = ps(x)$ as in the theorem. Conversely, assume that

$$x^p - x = f(x)q(x) + ps(x)$$

as in the statement of the theorem. The congruence

$$f(x)q(x) \equiv 0 \pmod{p}$$

has p solutions. This congruence has least theorem x^p. The leading term coefficient of $f(x)$ is x^n by hypothesis and hence the leading term $q(x)$ is $x^p - x$. By **??** the congruence $f(x) \equiv 0 \pmod{p}$ and $q(x) \equiv 0 \pmod{p}$ has at most n solutions and $p - n$ solutions respectively.

By every one of the p solutions of $f(x)q(x) \equiv 0 \pmod{p}$ is a solution of at least one congruence $f(x) \equiv 0 \pmod{p}$ and $q(x) \equiv 0 \pmod{p}$. It follows that the two congruences have exactly n solutions and $p - n$ solutions, respectively. The restriction $a_n = 1$ in this theorem is needed so that we may divide $x^p - x$ by $f(x)$ and obtain a polynomial $q(x)$ with integral coefficients. However, it is not much of restriction. We can always find an integer $\bar{a_n}$ such that $a_n\bar{a_n} = 1$

as an example, we see that

$$x^5 - 5x^3 + 4x \equiv 0 \pmod{5}$$

has 5 solutions, and

$$x^5 - x = (x^5 - 5x + 4x) + (5x^3 - 5x)$$

as second examples, we

Corollary 97
If $d \mid (p-1)$, then $x^d \equiv 1 \pmod{m}$ has d solutions.

22 February 28, 2025

Proof. Choose e so that $de = p - 1$. Since $(y-1)(1+y+\cdots+y^{e-1}) = y^e - 1$, on taking $y = x^d$, we see that

$$x(x^d - 1)(1 + x^d + \cdots + x^{d(e-1)}) = x^p - x.$$

A further application of **??** arises considering a polynomial

$$f(x) = (x-1)(x-2)\ldots(x-p+1).$$

For convenience, let $p > 2$, and expanding we find that

$$x^{p-1} + \sigma_1 x^{p-2} + \sigma_2 x^{p-3} + \cdots .$$

where σ_j is the sum of all products of j distinct members of the set $\{1, 2, \ldots, p-1\}$. In the two extreme cases we have $\sigma_1 = 1+2+\cdots+(p-1) = \frac{p(p-1)}{2}$, and $\sigma_{p-1} = 1 \cdot 2 \cdot \cdots \cdot (p-1) = (p-1)!$. The polynomial $f(x)$ has degree $p-1$ and has the $p-1$ roots $1, 2, \ldots, p-1 \pmod{p}$. Consequently, the polynomial $xf(x)$ has degree p and has p roots. By applying **??** to this latter polynomial, we see that there are polynomials

$q(x)$ and $s(x)$ such that $x^p - x = xf(x)q(x) + ps(x)$. Since $q(x)$ has degree $p - p = 0$ and leading coefficient 1, we see that $q(x) = 1$. That is, $x^p - x = xf(x) + ps(x)$, which is to say that the coefficients of $x^p - x$ are congruent $\pmod p$ to those of $xf(x)$. On comparing the coefficients of x, we deduce that $\sigma_{p-1} = (p-1)! \equiv -1 \pmod p$, which provides a second proof of Wilson's congruence. On comparing the remaining coefficients, we deduce that

$$\sigma_j \equiv 0 \pmod p \text{ for } 1 \leq j \leq p-2$$

. If $p \geq 5$ □

Theorem 98

Theorem 99

22.1 Primitive Roots and Power Residues

Definition 100

Let m denote a positive integer, and and any integer a such that $(a, m) = 1$. Let m be the smallest positive integer such that

$$a^n \equiv 1 \pmod m$$

We say that the order of $a \pmod m$ in h is such that the exponent of h is modulo m.

The terminology "a belongs to the exponent h" is a classical language of numbers. The language is replaced more and more in the current literature by "the order of a is h" as a usage that is standard in group theory. We shall explore the ideas of number theory and those of group theory. We explore the idea of number theory and those of group theory.

Suppose that a has order $h \pmod m$. If k is a positive multiple of h, say $k = qh$, then

$$ak = a^{qh} = (a^h)^q = 1^q = 1 \pmod m.$$

Conversely, if k is a positive integer such that $a^k = 1 \pmod m$, then we apply the division algorithm to obtain integers q and r such that

$$k = qh + r, \quad q \geq 0, \quad \text{and} \quad 0 \leq r < h.$$

Thus,

$$1 = a^k = a^{qh+r} = (a^h)^q a^r = 1^q a^r = a^r \pmod m.$$

But $0 \leq r < h$ and h is the least positive power of a that is congruent to 1 modulo m, so it follows that $r = 0$. Thus h divides k, and we have proved the following lemma.

Lemma 101

If a has order h modulo m, then the positive integer k satisfies $a^k \equiv 1 \pmod{m}$ if and only if $h \mid k$.

Corollary 102

If a has order h modulo m, and if $a^k \equiv a^j \pmod{m}$, then $k \equiv j \pmod{h}$.

Proof. Since $a^k \equiv a^j \pmod{m}$, we have $a^{k-j} \equiv 1 \pmod{m}$ or $a^{j-k} \equiv 1 \pmod{m}$, depending on whether $k \geq j$ or $k < j$. By **??**, $h \mid (k-j)$ or $h \mid (j-k)$, which means $k \equiv j \pmod{h}$. □

23 March 3, 2025

Proof. Each reduced residue class a m □

Lemma 103

If a has order h modulo m, then a^k has order $h/(h,k)$ modulo m.

Since $h/(h,k) = 1$ if and only if $h \mid k$ **??** contains **??** as a special case.

Proof. According to **??**, $(a^k)^j \equiv 1 \pmod{m}$ □

Lemma 104

If a has order $h \pmod{m}$ and b has order $k \pmod{m}$, and if $\gcd(h,k) = 1$, then ab has order $hk \pmod{m}$.

Proof. □

Definition 105

If g belongs to the exponent $\phi(m)$ modulo m, then g is called a **primitive root modulo m**.

In algebraic language, this definition can be stated. If the order of g modulo m in is $\varphi(m)$, then the multiplicative group of reduced residues modulo m is a cyclic group generated by the element g. In terms of **??**, the number of a is the solution of the congruence

Theorem 106

Ifp is a prime then there exist $\phi(p-1)$ primitive roots modulo p.

Proof. Just write the proof for now and then we can figure out the other things later in the course □

24 March 5, 2025

25 March 7, 2025

Theorem 107

If p is a prime then there exist

$$\varphi(\varphi(p^2)) = (p-1)\varphi(p-1)$$

primitive roots modulo p^2.

Proof. We begin by noting that if g is a primitive root modulo p, then g has order $p-1$ modulo p. We need to show that there exist $\varphi(\varphi(p^2)) = (p-1)\varphi(p-1)$ primitive roots modulo p^2.

First, we observe that if g is a primitive root modulo p, then g has order $p-1$ modulo p. This means that $g^{p-1} \equiv 1 \pmod{p}$ and for any $1 \leq k < p-1$, $g^k \not\equiv 1 \pmod{p}$.

Next, we consider the order of g modulo p^2. We need to show that there exist integers g such that the order of g modulo p^2 is $(p-1)p$. This means that $g^{(p-1)p} \equiv 1 \pmod{p^2}$ and for any $1 \leq k < (p-1)p$, $g^k \not\equiv 1 \pmod{p^2}$.

To do this, we use Hensel's Lemma (**??**). Let g be a primitive root modulo p. Then $g^{p-1} \equiv 1 \pmod{p}$. By Hensel's Lemma, there exists an integer h such that $h \equiv g \pmod{p}$ and $h^{p-1} \equiv 1 \pmod{p^2}$. This h is a lift of g to modulo p^2.

Now, we need to show that h has order $(p-1)p$ modulo p^2. Suppose $h^k \equiv 1 \pmod{p^2}$ for some k. Then $h^k \equiv 1 \pmod{p}$, which implies that $p-1$ divides k. Let $k = (p-1)m$. Then $h^{(p-1)m} \equiv 1 \pmod{p^2}$. Since $h^{p-1} \equiv 1 \pmod{p^2}$, we have $h^{(p-1)m} \equiv 1 \pmod{p^2}$. This implies that m must be a multiple of p, say $m = pn$. Therefore, $k = (p-1)pn = (p-1)p$, which means that the order of h modulo p^2 is $(p-1)p$.

Finally, we need to count the number of such primitive roots modulo p^2. By Lemma **??**, since there are $\varphi(p-1)$ primitive roots modulo p, and each of these can be lifted to p different primitive roots modulo p^2, there are $(p-1)\varphi(p-1)$ primitive roots modulo p^2.

Thus, we have shown that there exist $(p-1)\varphi(p-1)$ primitive roots modulo p^2. □

To show that there are no other primitive roots $\pmod{p^2}$, it signifies to argue as in the preceeding proof. Let g denote a primitive p^2, so that the members $g, g^2, \ldots, g^{p(p-1)}$ form a reduced residues $\pmod{p^2}$. By **??**, we have that g^k is a primitive root if and only if $k, p(p-1) = 1$. By definitino of Euler's $\varphi-$function, there are precisely $\varphi(p(p-1))$ such values of k among the numbers, $1, 2, 3, \ldots, p(p-1)$. Since $p, p-1 = 1$, we deduce from **??**, If m_1, and m_2, are two possible numbers, then $\varphi(m_1, m_2)$ such that $\varphi(p(p-1)) = \varphi(p)\varphi(p-1) = (p-1)\varphi(p-1)$.

Theorem 108

If p is an odd prime, and g is a primitive root $\pmod{p^2}$, then g is a primitive root $\pmod{2p^\alpha}$ for $\alpha = 3, 4, \ldots$.

Proof. Suppose that g is a primitive root of $\pmod{p^2}$ and that h is the order of $g \pmod{p^\alpha}$ where $\alpha > 2$. From the congruence,

$$g^h \equiv 1 \pmod{p^\alpha}$$

, we deduce that $g^h \equiv 1 \pmod{p^2}$ and hence that $\varphi(p^2) \mid h$, by **??**, we also have that $h \mid \varphi(p^\alpha)$. Thus

$$h = p^\beta(p-1)$$

for some $\beta = 1, 2, \ldots, \beta - 1$. To prove that β itself proves that we have the following:

$$g^{p^{\alpha-2}(p-1)} \not\equiv 1 \pmod{p^\alpha}$$

. We use induction to show that this holds for all $\alpha > 2$. By hypothesis, the order of $g \pmod{p^2}$ is $\varphi(p^2) = p(p-1)$. Hence $g^{p(p-1)} \equiv 1 \pmod{p^2}$. By Fermat's congruence, we have the following:

$$g^{p-1} \equiv 1 \pmod{p}$$

. So we can write $g^{p-1} = 1 + kp$ for some integer k. Now consider $g^{p(p-1)}$:

$$g^{p(p-1)} = (1+kp)^p \equiv 1 + pkp \pmod{p^3} \equiv 1 + p^2k \pmod{p^3}.$$

Since g is a primitive root modulo p^2, $g^{p(p-1)} \not\equiv 1 \pmod{p^3}$. Therefore, $g^{p(p-1)} \equiv 1 + p^2k \pmod{p^3}$ and $1 + p^2k \not\equiv 1 \pmod{p^3}$, which implies $k \not\equiv 0 \pmod{p}$. Thus, $g^{p(p-1)} \not\equiv 1 \pmod{p^3}$.

By induction, assume that $g^{p^{\alpha-2}(p-1)} \not\equiv 1 \pmod{p^\alpha}$ for some $\alpha \geq 3$. Then consider $g^{p^{\alpha-1}(p-1)}$:

$$g^{p^{\alpha-1}(p-1)} = (g^{p^{\alpha-2}(p-1)})^p \not\equiv 1^p \pmod{p^{\alpha+1}}.$$

Therefore, $g^{p^{\alpha-1}(p-1)} \not\equiv 1 \pmod{p^{\alpha+1}}$, completing the induction.

Hence, g is a primitive root modulo p^α for all $\alpha \geq 3$. □

26 March 17, 2025

Definition 109

If g belongs to the exponent $\varphi(m)$ modulo m, then g is called a **primitive root modulo *m***.

Theorem 110

If p is a prime, then there exist $\varphi(\varphi(p^2)) = (p-1)\varphi(p-1)$ primitive roots modulo p^2.

Theorem 111

If p is an odd prime, and g is a primitive root $\pmod{p^2}$, then g is a primitive root $\pmod{2p^\alpha}$ for $\alpha = 3, 4, \ldots$.

The prime $p = 2$ must be excluded, for $g = 3$ is a primitive root $\pmod 4$ but not $\pmod 8$. Indeed, it is easy to verify that

$$a^2 \equiv 1 \pmod 8$$

for any odd number a. As $\varphi(8) = 4$, it follows that there is no primitive root $\pmod 8$. Suppose that a is odd. Since

$$8 \mid (a^2 - 1) \text{ and } 2 \mid (a^2 + 1)$$

It follows that

$$16 \mid (a^2 + 1)(a^2 - 1) = a^4 - 1$$

That is

$$a^2 \equiv 1 \pmod{16}$$

If we repeat this argument, we see that

$$a^8 \equiv 1 \pmod{32}$$

and in general that

$$a^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}$$

for $\alpha \geq 3$. Since $\varphi(2^\alpha) = 2^{\alpha-1}$, we conclude that if $\alpha \geq 3$, then

$$a^{\varphi(2^\alpha)} \equiv 1 \pmod{2^\alpha}$$

for all odd a, and hence there is no primitive root $\pmod{2^\alpha}$ for $\alpha \geq 3$. Suppose p is an odd prime and that g is a primitive root $\pmod{p^\alpha}$. We may suppose that g is odd, for if g is even, we have only to replace

$$g + p^\alpha$$

which is odd. The numbers $g, g^2, \ldots, g^{\varphi(p^\alpha)}$ form a reduced residue system $\pmod{p^\alpha}$. Since, these numbers are odd, they also form a reduced residue system $\pmod{2^\alpha}$. The g is a primitive root $\pmod{2p^\alpha}$. We have established that a primitive root exists modulo m when $m = 1, 2, 4, p^\alpha,$ or $2p^\alpha$ (p an odd prime prime) but there no primitive root $\pmod{2^\alpha}$ for $\alpha \geq 3$. Suppose now that m is not a prime power or twiece a prime power it can be expressed as a product as following:

$$m = m_1 m_2$$

with $(m_1, m_2) = 1$, where $m_1 > 2$ and $m_2 > 2$. Let

$$e = \text{lcm}(\varphi(m_1), \varphi(m_2))$$

If $(a, m) = 1$ then we have $(a_1, m_1) = 1$ so that $\alpha^{\varphi(m_1)} = 1 \pmod{m_1}$, and hence we have

$$a^e \equiv 1 \pmod{m_1}$$

Similarly, we have $a^e \equiv 1 \pmod{m_2}$ and hence $a^e \equiv 1 \pmod{m}$. Since $2 \mid \varphi(n)$ for all $n > 2$, we see that

$2 \mid (\varphi(m_1), \varphi(m_2))$, so that

$$e = \frac{\varphi(m_1)\varphi(m_2)}{(\varphi(m_1), \varphi(m_2))} < \varphi(m_1)\varphi(m_2) = \varphi(m)$$

Thus there is no primitive root m in this case. We now have determined which m possess primitive roots.

Theorem 112

There exists a primitive root modulo m if and only if $m = 1, 2, 4, \ldots, p^\alpha$ or $2p^\alpha$

?? and its proof generalizes to any modulo is m possessing a primitive root.

Corollary 113

Suppose that $m = 1, 2, 4, p^\alpha$ or $2p^\alpha$ where p is an odd prime. If $(a, m) = 1$ the congruence

$$x^n \equiv a \pmod{m}$$

has $n, \varphi(m)$ solutions or no solutions according as

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

or not. For general composite m possessing no primitive roots, we factor m and apply the above to the prime powers dividing m.

Example 114

Determine the number of solutions of the congruence

$$x^4 \equiv 61 \pmod{117}$$

Solution. *We note that* $116 = 3^2 \cdot 13$. *As* $\varphi(9) = 6$ *and* $\gcd(4, \varphi(9)) = 2$, *we have:*

$$\frac{\varphi(9)}{\gcd(4, \varphi(9))} = \frac{6}{2} = 3.$$

Since $61^3 \equiv (-2)^3 \equiv -8 \equiv 1 \pmod 9$, *we deduce that the congruence* $x^4 \equiv 61 \pmod 9$ *has 3 solutions.*

Next, consider the congruence $x^4 \equiv 61 \pmod{13}$. *Since* $\varphi(13) = 12$, *and* $61 \equiv 1 \pmod{13}$, *this congruence also has* $\gcd(4, 12) = 4$ *solutions.*

Thus, by **??**, *the number of solutions modulo* 117 *is* $3 \cdot 4 = 12$.

This method fails when the modulus is divisible by 8, *as* **??** *does not apply to higher powers of* 2. *To establish an analogue of* **??** *for higher powers of* 2, *we first show that nearly a primitive root modulo* 2^α *exists.*

Theorem 115

Suppose that $\alpha \geq 3$. The order of 5 $\pmod{2^\alpha}$ is $2^{\alpha-2}$. The numbers $\pm 5, \pm 5^2, \pm 5^3, \ldots, \pm 5^{\alpha-2}$ include a primitive root. Therefore, there exist integers i and j such that:

$$a \equiv (-1)^i 5^j \pmod{2^\alpha}.$$

The values of i and j are determined by the specific congruence conditions.

27 March 21, 2025

27.1 Number Theory from an algebraic viewpoint

We began with a binary operation denoted by $\oplus$ and we presume this binary operation is simply valued. So $a \oplus b$ has a unique value

Definition 116

A group G is a set of elements, $a, b, c, \ldots$ for all element $a, b, c \in G$ wit a binary operation $\oplus$ such that:

- The set is closed under the operation
- The associative law holds $a \oplus (b \oplus c) = (a \oplus b) \oplus c)$ for all element $a, b, c \in G$
- The set has a variance identity element $e/$
- Each element has a unique inverse in G.

Note 117. *Here are some notes about the types of groups:*

- *A group is valled* **abelian** *or* **commutative** *if $a \oplus b = b \oplus a$ for every pair of element a, b in G.*
- *A finite group is one with a finite number of elements, otherwise it is a finite group.*
- *If a group is finite, the number of its elements is called the order of the group.*

Example 118

The set of all integers (written addivitely) in a group under addition

We get the 'additive group named '

Definition 119 (Isomorphic Group)

Two groups G with the operations $\oplus$ and G' with operation $\odot$ are said to be **isomorphic** if there is a one-to-one corespondence between the elemtns of G and those of G', such that if $a \in G$ corresponds to a $a' \in G'$ and $b \in G$ corresponds to $b' \in G'$ then $a \oplus b$ in G corresponds to $a' \oplus b'$ in G'. In symbols, $G \cong G'$.

Another way of thinking this of the additive gorup $\pmod 6$ is in terms of the so-called residue classes.

$$C_0 = \ldots, -18, -12, -6, 0, 6, 12, 18, \ldots$$

$$C_1 = \ldots, -18, -12, -6, 0, 6, 12, 18, \ldots$$

$$C_0 = \ldots, -18, -12, -6, 0, 6, 12, 18, \ldots$$

$$C_0 = \ldots, -18, -12, -6, 0, 6, 12, 18, \ldots$$

$$C_0 = \ldots, -18, -12, -6, 0, 6, 12, 18, \ldots$$

Theorem 120

Any complete residue system modulo m has a gorup under addition modulo m, This completes the residues modulo m consists isomorphic groups under addition, which we speak of the 'the' additive group modulo m.

Proof. Let's begin with the complete residude system $0, 1, 2, 3, \ldots, m-1$ modulo m. This system is closed under addition modulo m, and the corresponding associative property of addition is inherited from the correspoding properties, for all integers

$$a + (b + c) = (a + b) + c$$

implies that $a + (b + c) = (a + b) + c \pmod m$. Finally, the identity is 0 and it implies and the additive inverse of any element a is $m - a$. The inverses are unique. □

Passing from the system, we have $0, 1, \ldots, m-1$ to any complete residue system $r_a, r_b, r_c, \ldots, r_[m-1]$. We observe that the operation of addition modulo m is preserved. For example, if r_a corresponds to a and r_b corresponds to b, then the sum of the two residues is

$$r_a + r_b = r_{a+b}$$

where $a + b$ is taken modulo m. The identity element is r_0 and the inverse of r_a is r_{m-a}. Thus, we have shown that any complete residue system modulo m has a group under addition modulo m.

28 March 31, 2025

Theorem 121 (Lemma of Gauss)

For any odd prime, let $(a, p) = 1$. Consider the integers

$$a, 2a, 3a, \ldots, \left(\frac{p-1}{2}\right) a$$

and their least positive residues modulo p. If n denotes the number of these residues that don't exceed $\frac{p}{2}$, then

$$\frac{a}{p} = (-1)^n$$

Proof. Let

$$r_1, r_2, r_3, \ldots, r_n$$

denote the residues that exceed $\frac{p}{2}$, and let

$$s_1, s_2, \ldots, s_k$$

denote the remaining residues. The r_i and s_i are all distinct and none is zero. Furthermore, $n + k = \frac{(p-1)}{2}$. Now we have $0 < p - r_i < \frac{p}{2}$ where $i = 1, 2, 3, \ldots, n$ and then numbers $p - r_i$ are distinct. Also note that $p - r_i$ is an s_j for if $p - r_i = s_j$ then $r_i = pa \pmod{p}$ and $r_j = p\sigma$ for some $1 \leq p < \frac{(p-1)}{2}$ for if $1 \leq \sigma \leq \frac{(p-1)}{2}$ and $p - pa \equiv \sigma a \pmod{p}$, since, $(a, p) = 1$ this implies that $a(p + \sigma) \equiv 0$ and $(p + \sigma) \equiv 0 \pmod{p}$, which is impossible because $p, \sigma < \frac{p}{2}$. Thus, $p - r_1, p - r_2 \ldots, p - r_n$ and $s_1, s_2, \ldots, s_k$ are all distinct, and are all at least 1 and less than $\frac{p}{2}$, and they are $n + k = \frac{p-1}{2}$ is a number, that is, they are just the integers

$$1, 2, \ldots, \frac{p-1}{2}$$

in some order. Multiply them together and we have

□

Definition 122

For real part x, the symbol $[x]$ denotes the greatest integer less than or equal to x. This is also called the **integral part** of x, and $x - [x]$ is the **fractional part** of x.

Such an integer as $[\frac{1000}{23}]$ is the quotient where 1000 is divided by 23 and is also the number of positive multiples of 23 less than 1000. On the other hand, its value 43, is immediately obtained by dividing 1000 by 23 and taking the integral part of the answer only. Here are further examples

$$\frac{15}{2} = 7; \frac{-15}{2} = -8; [-15] = -15$$

Theorem 123

If p is n odd prime

Proof. We use the same notation as in the proof of **??**. Here r_i and s_i are the least positive remainders of taruned by dividing ja by $p, j = 1, 2, \ldots, \frac{(p-1)}{2}$. The quotient of the divison is easily seen to be

and hence by subtraction we have

□

29 April 2, 2025

30 April 4, 2025

30.1 The Jacobi Symbol

Definition 124

Let Q be a positive odd integer, so that $Q = q_1 q_2 \ldots q_s$, where the q_i are odd primes, not necessarily distinct. Then the Jacobi symbol $\frac{P}{Q}$ is defined as:

$$\frac{P}{Q} = \frac{P}{q_1} \cdot \frac{P}{q_2} \cdot \ldots \cdot \frac{P}{q_s},$$

where $\frac{P}{q_i}$ is the Legendre symbol for each prime q_i. The Jacobi symbol generalizes the Legendre symbol to composite denominators.

If Q is an odd prime, the Jacobi symbol and the legendre symbol are insdistinguishable. However, this can be cause no explanation since there values are the same. If $(P, Q) > 1$, then $\frac{P}{Q} = 0$ whereas if $(P, Q) = 1$ then $(\frac{P}{Q}) = \pm 1$. Moreover, if P is a quadratic residue modulo and odd prime number Q, then q_i is dividing R, so that