Number Theory notes

Vatsal Limbachia

September 2019

Contents

1 Divisibility and Primes

1.1 Introduction

Well ordering Principle:
Let $S \neq 0$ be a set of positive integers.
Then there exists $s \in S$ such that for all $a \in S, s \leq a$

Induction:
If a set s of positive integers contains the integer 1
And contains $n+1$ whenever it contains n
Then S consists of all the positive integers

1.2 Divisibility

Definition 1.1: Divisibility
An integer b is divisible by an integer $a \neq 0$ if there is an integer x such that $b = ax$.
We write $a|b$ (a divides b)

Theorem 1.1: Properties of divisibility

1. $a|b \ \rightarrow a|bc \quad c \in \mathbb{Z}$
2. $a|b \ \& \ b|c \rightarrow a|c$
3. $a|b \ \& \ a|c \rightarrow a|(bx+cy) \quad x, y \in \mathbb{Z}$
4. $a|b \ \& \ b|a \rightarrow a = \pm b$
5. $a|b, \ a > 0, \ b > 0 \rightarrow a \leq b$
6. $m \neq 0, \ a|b \ \leftrightarrow ma|mb$

Proof: Theorem 1.1 (3)

$a|b \rightarrow b = ar$ for some $r \in \mathbb{Z}$ and $a|c \rightarrow c = as$ for some $s \in \mathbb{Z}$. Hence $bx + cy = a(rx + sy)$ and this proves that $a|(bx + cy)$

Theorem 1.2: The Division Algorithm
Let $a, b \in \mathbb{Z},\ a > 0$.
Then there exists unique $q, r \in \mathbb{Z}$ such that $b = qa + r,\ 0 \leq r < a$.
If $a \nmid b$ then $0 < r < a$

Proof: Theorem 1.2

Consider the arithmetic progression:

$$..., b - 3a, b - 2a, b - a, b, b + a, b + 2a, b + 3a, ...$$

In the sequence select the smallest non-negative member and denote it by r. Thus by definition r satisfies the inequalities of the Theorem. But also r, being in the sequence, is of the form $b - qa$, and thus q is defined in terms of r.

To prove uniqueness we suppose there is another pair q_1 and r_1 satisfying the same conditions. First we prove that $r = r_1$. If not, we may presume that $r < r_1$ so that $0 < r_1 - r < a$ and then we see that $r_1 - r = a(q - q_1)$ and so $a|(r_1 - r)$, a contradiction to Theorem 1.1 (5). Hence $r = r_1$ and also $q = q_1$.

Note: We stated the Theorem with $a > 0$. However this is not necessary and we may formulate as:

Given $a, b \in \mathbb{Z}$, $a \neq 0$, there exists $q, r \in \mathbb{Z}$ such that $b = qa + r$, $0 \leq r < |a|$.

Definition 1.2:
The integer a is a common divisor of b and c if $a|b$, $a|c$ and at least $b \neq 0$ or $c \neq 0$, the greatest among their common divisors is called the greatest common divisor of b and c and is denoted by $gcd(b, c)$ or (b, c).

Let $b_1, ..., b_n \in \mathbb{Z}$, not all zero. We denote $g = (b_1, ...b_n)$ to be the greatest common divisor.

Theorem 1.3:
If $g = (b, c)$, then there exist $x_0, y_0 \in \mathbb{Z}$ such that $g = (b, c) = bx_0 + cy_0$

Proof: Theorem 1.3
Consider the linear combination $bx + cy$, where x, y range over all the integers. This set of integers $\{bx + cy\}$ includes positive and negative values and also 0. $(x = y = 0)$. Choose x_0 and y_0 so that $bx_0 + cy_0$ is the least positive integer l in the set. Thus $l = bx_0 + cy_0$.

Next we prove that $l|b$ and $l|c$. Assume that $l \nmid b$, then it follows that there exists integers q and r , by Theorem 1.2, such that $b = lq + r$ with $0 < r < l$. Hence we have $r = b - lq = b - q(bx_0 + cy_0) = b(1 - qx_0) + c(-qy_0)$, and thus r is in the set $\{bx + cy\}$. This contradicts the fact that l is the least positive integer in $\{bx + cy\}$. Similar proof for $l|c$. Now since $g = (b, c)$ we may write $b = gB$

, $c = gC$ and $l = bx_0 + cy_0 = g(Bx_0 + Cy_0)$. Thus $g|l$ and so by Theorem 1.1 (5) we conclude that $g \leq l$. We know $g < l$ is impossible since g is the greatest common divisor, so $g = l = bx_0 + cy_0$.

Theorem 1.4:
The greatest common denominator of b and c can be characterised in the following two ways:

1. It is the least positive value of $bx + cy$ where $x,\ y \in \mathbb{Z}$
2. If d is any common divisor of b and c then $d|g$ by Theorem 1.1 (3).

Proof: Theorem 1.4

1. Follows from Theorem 1.3
2. If d is any common divisor of b and c, then $d|g$ by Theorem 1.1 (3). Moreover, there cannot be two distinct integers with property (2), because of Theorem 1.1 (4).

Note: If $d = bx + cy$, then d is not necessary the $gcd(b, c)$. However, it does follow from such equation that (b, c) is a divisor of d. In particular , if $bx+cy = 1$ for some $x, y \in \mathbb{Z}$, then $(b, c) = 1$.

Theorem 1.5:
Given $b_1, ..., b_n \in \mathbb{Z}$ not all zero with greatest common divisor g, there exists integers $x_1, ..., x_n$, such that

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

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

Proof: Theorem 1.5

Exercise for the reader.

Theorem 1.6:
For any $m \in \mathbb{Z}, m > 0$

$$(ma, mb) = m(a, b) \tag{2}$$

Proof: Theorem 1.6

By Theorem 1.4 we have:

(ma, mb) = least positive value of $max + mby = m$ { least positive integer of $ax + by$} $= m(a, b)$

Theorem 1.7:
If $d|a$, $d|b$ and $d > 0$, then

$$\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d}(a, b) \tag{3}$$

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

$$\left(\frac{a}{g}, \frac{b}{g}\right) = 1 \tag{4}$$

Proof: Theorem 1.7

The second assertion is the special case of the first using $d = (a, b) = g$. The first assertion is a direct consequence of Theorem 1.6, obtained by replacing m, a, b in Theorem 1.6 by d, $\frac{a}{d}$, $\frac{b}{d}$ respectively.

Theorem 1.8:
If $(a, m) = (b, m) = 1$ then $(ab, m) = 1$

Proof: Theorem 1.8

Exercise for the reader.

Definition: 1.3

We say that a and b are relatively prime in case $(a, b) = 1$, and that $a_1, a_2, ..., a_n$ are relatively prime in the case $(a_1, a_2, ..., a_n) = 1$. We say that $a_1, a_2, ..., a_n$ are relatively prime in pairs in case $(a_i, a_j) = 1$ for all $i = 1, 2, ..., n$ and $j = 1, 2, ...n$ with $i \neq j$.

Note: $(a, b) = 1$ we also say a and b are coprime.

Theorem 1.9:
For any $x \in \mathbb{Z}$ we have

$$(a, b) = (b, a) = (a, -b) = (a, b + ax) \tag{5}$$

Proof: Theorem 1.9

Exercise for the reader.

Theorem 1.10: Euclid's Lemma
If $c|ab$ and $(b, c) = 1$, then $c|a$.

Proof: Theorem 1.10

By Theorem 1.6 , $(ab, ac) = a(b, c) = a$. By hypothesis $c|ab$ and clearly $c|ac$, so $c|a$ by Theorem 1.4 (2).

Now we observe for $c \neq 0$, we have $(b, c) = (b, -c)$ by Theorem 1.9 and hence we may presume $c > 0$.

Theorem 1.11: The Euclidean Algorithm
Given $b, c \in \mathbb{Z}, c > 0$, we can make a repeated application of the division algorithm, **Theorem 1.2**, to obtain a series of aligns

$$b = cq_1 + r_1 \quad 0 < r_1 < c \tag{6}$$
$$c = r_1q_2 + r_2 \quad 0 < r_2 < r_1 \tag{7}$$
$$r_1 = r_2q_3 + r_3 \quad 0 < r_3 < r_2 \tag{8}$$
$$... \tag{9}$$
$$r_j = r_{j+1}q_j + r_j \quad 0 < r_j < r_{j-1} \tag{10}$$
$$r_{j-1} = r_jq_{j+1}. \tag{11}$$

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: Theorem 1.11

See Theorem 1.11 in the textbook or Theorem 1.13 in the Lecture Notes.

Example 1 $gcd(841, 160)$

$$\begin{aligned} 841 &= 160 \times 5 + 41 \\ 160 &= 41 \times 3 + 37 \\ 41 &= 37 \times 1 + 4 \\ 37 &= 34 \times 9 + 1 \\ 4 &= 1 \times 4 + 0 \end{aligned} \tag{12}$$

Hence (841,160)=1 working backwards gives:

$$1 = 37 \times 1 - 4 \times 9 \tag{13}$$
$$1 = 37 \times 1 - (41 - 37) \times 9 \tag{14}$$
$$1 = 37 \times 10 - 41 \times 9 \tag{15}$$
$$1 = (160 - 3 \times 41) \times 10 - 41 \times 9 \tag{16}$$
$$1 = 160 \times 10 - 41 \times 39 \tag{17}$$
$$1 = 160 \times 10 - (841 - 160 \times 5) \times 39 \tag{18}$$
$$1 = (-39) \times 841 + 205 \times 160 \tag{19}$$

Note the solution is not unique:

$$1 = 121 \times 841 - 636 \times 160 \tag{20}$$

Example 2 Extended Algorithm

$$\begin{aligned} r_i &= r_{i-2} - q_i r_{i-1} \\ x_i &= x_{i-2} - q_i x_{i-1} \\ y_i &= y_{i-2} - q_i y_{i-1} \\ r_1 &= b, r_0 = c \\ x_1 &= 1, x_0 = 0 \\ y_1 &= 0, y_0 = 1 \end{aligned} \tag{21}$$

We want to compute the $gcd(841, 160)$ and express as a linear combination of 841 and 160.

Definition 1.4:
The integers $a_1, ..., a_n$, all different from zero, have a **common multiple** b if $a_i|b$ for $i = 1, ..., n$. The least of the positive common multiples is called the **least common multiple** and it is denoted by $[a_1, ..., a_n]$ or $lcm(a1, ..., a_n)$

Theorem 1.12:
If b is any common multiple of $a_1, ..., a_n$, then $[a_1, ..., a_n] \mid b$. This is the same as saying that if $h = [a_1, ..., a_n]$ then $0, \pm h, \pm 2h, ...$ comprise all the common multiples of $a_1, ..., a_n$.

Proof: Theorem 1.12

Let m be any common multiple and divide m and h. By Theorem 1.2 , $\exists q, r$ such that $m = qh + r$, $0 \leq r < h$. We must probe that $r = 0$. If $r \neq 0$ we argue as follows. For each $i = 1, 2, ..., n$ we know that $a_i|h$ and $a_i|m$, so that $a_i|r$.

Thus r is a positive common multiple of $a_1, a_2, ..., a_n$ contrary to the fact that h is the least of all positive common multiples.

Theorem 1.13:
If $m > 0$

1. $[ma, mb] = m[a, b]$
2. $[a, b](a, b) = |ab|$

Proof: Theorem 1.13

1. Let $H = [ma, mb]$ and $h = [a, b]$. Then mh is a multiple of ma and mb, so that $mh \geq H$. Also, H is a multiple of both ma and mb so H/m is a multiple of a and b. Thus, $H/m \geq h$ from which it allows that $mh = H$.
2. It will suffice to prove this for $a, b \in \mathbb{Z}$ with $a > 0$, $b > 0$, since $[a, -b] = [a, b]$.
   v We begin with the special case where $(a, b) = 1$. Now $[a, b]$ is a multiple of a, say ma. Then $b|ma$ and $(a, b) = 1$, so by Theorem 1.10 we conclude that $b|m$. Hence $b \leq m$, $ba \leq ma$. But ba, being a positive common multiple of b and a , cannot be less than the least common multiple, so $ba = ma = [a, b]$.

   Let $(a, b) = g > 1$. we have $(a/g, b/g) = 1$ by Theorem 1.7. Applying the result of the previous paragraph we have:

$$\left[\frac{a}{g}, \frac{b}{g}\right] \cdot \left(\frac{a}{g}, \frac{b}{g}\right) = \frac{a}{g}\frac{b}{g} \tag{22}$$

   Multiplying by g^2 and using Theorem 1.6 as well as the first part (1.), we get $[a, b] \cdot (a, b) = ab$.

1.3 Primes

Definition 1.5:
An integer $p > 1$ is called a **prime number** if there is no divisor d of p satisfying $1 < d < p$. If an integer $a > 1$ is not a prime, is is called a **composite number**.

Theorem 1.14:
Every integer $n > 1$ can be expressed as a product of primes (with perhaps only one factor).

Proof: Theorem 1.14
If $n = p$ a prime then it is a 'product' with one factor. Otherwise $n = n_1 n_2$,

where $1 < n_1, n$ and $1 < n_2, n$. If n_1 is a prime, let it stand; otherwise it will factor into, $n_1 = n_3 n_4$, with $1 < n_3, n$ and $1 < n_4, n$, similarly for n_2. This process of writing each composite number that arises as a product of factors must terminate because the factors are smaller then the composite number itself, and yet each factor is an integer greater then 1. Thus in the end we have

$$n = p_1^{a_1} p_2^{a_2} ... p_r^{a_r}$$

since the prime factors are not necessarily distinct where $p_1, p_2, ..., p_r$ are distinct primes and $a_1, a_2, ..., a_r > 0$

Theorem 1.15:
If $p|ab$, p prime, then $p|a$ or $p|b$.
More generally if $p|a_1...a_n$, then p divides at least on of the factors a_i

Proof: Theorem 1.15
If $p \nmid a$, then $(a, p) = 1$ and so by **Thm 1,10**, $p|b$. For the general case, we use induction.

Theorem 1.16: Fundamental Theorem of Arithmatic
The factoring of any integer $n > 1$ into primes is unique apart from the order of the prime factors.

Definition 1.6:
We call a a square (or **perfect square**) if it can be written as $a = n^2$. By the **F.T.A.** a is a square if all the exponents $\alpha(p)$ in (1.6) are even. We say that a is **square free** if 1 is the largest square dividing a. Thus a is square free iff the exponents $\alpha(p) = 0$ or 1. If p is prime, then the assertion $p^k || a$ is equivalent to $k = \alpha(p)$.

Theorem 1.17: (Euclid)
The number of primes is infinite.

Definition 1.7:
Let $n \in \mathbb{N}$ and p a prime. Then

$$v_p(n) = max(k \in \mathbb{N}_{\cup 0} : p^k | n) \tag{23}$$

where k is the unique non-negative integer such that $p^k | n$ but $p^{k+1} | n$
Equivalently $V_p(n) = k$ iff $n = p^k n'$ where $n' \in \mathbb{N}$ and $p \nmid n'$

Lemma: Let $n, m \in \mathbb{N}$ and p be a prime. then

$$v_p(mn) = v_p(m) + v_p(n) \tag{24}$$

2 Congruences

2.1 Congruences

Definition 2.1:
If $m \in \mathbb{Z}$, $m \neq 0$ is such that $m|a-b$, we say that a is congruent to b modulo m and we write $a \equiv b \ (mod\ m)$

Since $a-b$ is divisible by $-m$, we can focus our attention to a positive modulus. We will assume in this chapter that $m > 0$.

Theorem 2.1: Properties of Congruences

1. $a \equiv b \ (mod\ m)$ $b \equiv a \ (mod\ m)$, and $a - b \equiv 0 \ (mod\ m)$ are equivalent statements.
2. If $a \equiv b \ (mod\ m)$ and $b \equiv c \ (mod\ m)$, then $a \equiv c \ (mod\ m)$
3. If $a \equiv b \ (mod\ m)$ and $c \equiv d \ (mod\ m)$, then $a + c \equiv b + d \ (mod\ m)$
4. If $a \equiv b \ (mod\ m)$ and $c \equiv d \ (mod\ m)$, then $ac \equiv bd \ (mod\ m)$
5. If $a \equiv b \ (mod\ m)$ and $d|m,\ d > 0$, then $a \equiv b \ (mod\ d)$
6. If $a \equiv b \ (mod\ m)$ then $ac \equiv bc \ (mod\ mc)$ for $c > 0$

Theorem 2.2:
Let f denote a polynomial with integral coefficients. If $a \equiv b \ (mod\ m)$ then $f(a) \equiv f(b) \ (mod\ m)$

Theorem 2.3:

1. If $ax \equiv ay \ (mod\ m)$ iff $x \equiv y \ (mod\ \frac{m}{(a,m)})$
2. $ax \equiv ay \ (mod\ m)$ and $(a, m) = 1$, then $x \equiv y \ (mod\ m)$
3. $x \equiv y \ (mod\ m_i)$ for $i = 1, ..., r$ iff $x \equiv y \ (mod\ [m_1, ..., m_r])$

Theorem 2.4:
If $b \equiv c \ (mod\ m)$, then $(b, m) = (c, m)$.

Proof: Theorem 2.4
We have $b = c + mx$ for some integer x. To see that $(b, m) = (c + ax, m)$, take $a = m$ in Theorem 1.9.

Definition 2.2: Complete Residue System
If $x \equiv y \ (mod\ m)$ then y is called a residue of $x \ (mod\ m)$. A set $y_1, ..., y_m$ is

called a complete residue system modulo m if for every integer x, there is one and only one y_j such that $x \equiv y_j \ (mod\ m)$

Definition 2.3: Reduced Residue System
A reduced residue system modulo m is a set of integers r_i such that
$(r_i, m) = 1$,
$r_i \not\equiv r_j, \ (mod\ m)$ if $i \neq j$,
for every x where $(x, m) = 1$, there is r_i in the set such that $x \equiv r_i \ (mod\ m)$.

- You can obtain a reduced residue system by deleting from a complete residue system modulo m those members that are not relatively prime to m.
- All reduced reside system modulo m have the same number of elements.
- We will denote by $\Phi(m)$ to be the number of elements of a reduced residue system modulo m.
- $\Phi(m)$ is called the Euler's Φ-function or Euler's totient-function

Theorem 2.5:
The number $\Phi(m)$ is the number of positive integers less than or equal to m that are relatively prime to m.

Theorem 2.6:
Let $(a, m) = 1$. Let $r_1, ..., r_n$ be a complete, or a reduced, residue system modulo m. Then $ar_1, ..., ar_n$ is a complete, or a reduced, residue system, respectively, modulo m.

Proof: Theorem 2.6
If $(r_i, m) = 1$, then $(ar_i, m) = 1$ by Theorem 1.8.
There are the same number of $ar_1, ar_2, ..., ar_n$ as of $r_1, r_2, ..., r_n$. Therefore we only need to show that $ar_i \not\equiv ar_j \ (mod\ m)$ if $i \neq j$. But Theorem 2.3 (2) shows that $ar_i \equiv ar_j \ (mod\ m)$ implies $r_i \equiv r_j \ (mod\ m)$ and hence $i = j$.

Theorem 2.7: Fermat's Theorem
Let p denote a prime. If $p \nmid a$ for $a \in \mathbb{Z}$ then
$a^{p-1} \equiv 1 \ (mod\ p)$.
$a^{p} \quad \equiv a \ (mod\ p)$.

Theorem 2.8: Euler's Generalization of Fermat's Theorem
If $(a, m) = 1$, then

$$a^{\Phi(m)} \equiv 1 \ (mod\ m) \tag{25}$$

Proof: Theorem 2.8
Let $r_i, r_2, ..., r_{\Phi(m)}$ be a reduced residue system $(mod\ m)$. Then by Theorem

2.6, $ar_1, ar_2, ..., ar_{\Phi(m)}$ is also a reduced residue system $(mod\ m)$. Hence, corresponding to each r_i there is only one ar_j such that $r_i \equiv ar_j\ (mod\ m)$. Furthermore, different r_i will have different corresponding ar_j. This means that the numbers $ar_1, ar_2, ..., ar_{\Phi(m)}$ are just the residues $(mod\ m)$ of $r_1, r_2, ..., r_{\Phi(m)}$, but not necessarily in the same order. Multiplying and using Theorem 2.1 (4) we obtain

$$\prod_{j=1}^{\Phi(m)} (ar_j) \equiv \prod_{i=1}^{\Phi(m)} r_i\ (mod\ m)$$

$$a^{\Phi(m)} \prod_{j=1}^{\Phi(m)} (r_j) \equiv \prod_{i=1}^{\Phi(m)} r_i\ (mod\ m)$$

Now $(r_j, m) = 1$, so we can use Theorem 2.3 (2), to cancel the r_j and we obtain $a^{\Phi(m)} \equiv 1\ (mod\ m)$.

Proof: Theorem 2.7
To find $\Phi(p)$, we refer to Theorem 2.5. All the integers $1, 2, ..., p-1, p$ with the exception of p are relatively prime to p. This we have $\Phi(p) = p-1$ and the first part of Fermat's Theorem follows.
The second part is obtained from the first, multiplying by a.

Theorem 2.9:
If $(a, m) = 1$ then there is an x such that $ax \equiv 1\ (mod\ m)$. Any two such x are congruent $(mod\ m)$. If $(a, m) > 1$ then there is no such x.

Proof: Theorem 2.9
If $(a, m) = 1$, then there exists $x, y \in \mathbb{Z}$ such that $ax + my = 1$. That is, $ax \equiv 1\ (mod\ m)$. Conversely, if $ax \equiv 1\ (mod\ m)$, then there is a y such that $ax + my = 1$, that that $(a, m) = 1$. Thus if $ax_1 \equiv ax_2 \equiv 1\ (mod\ m)$ then $(a, m) = 1$ and it follows from Theorem 2.3 (2) that $x_1 \equiv x_2\ (mod\ m)$

Lemma 2.10:
Let p be a prime number. Then $x^2 \equiv 1\ (mod\ p)$ iff $x \equiv \pm 1\ (mod\ p)$.

Theorem 2.11: Wilson's Theorem
If p is prime, then $(p-1)! \equiv -1\ (mod\ p)$

Theorem 2.12:
Let p denote a prime. Then $x^2 \equiv -1\ (mod\ p)$ has solutions iff $p = 2$ or $p \equiv 1\ (mod\ 4)$.

Proof: Theorem 2.12

Lemma 2.13:
If p is prime and $p \equiv 1\ (mod\ 4)$, then there exists positive integers a and b such

that $a^2 + b^2 = p$.

Lemma 2.14:
Let q be a prime factor of $a^2 + b^2$. If $q \equiv 3 \ (mod\ 4)$ then $q|a$ and $q|b$.

Theorem 2.15: (Fermat)
Let

$$n = 2^{\alpha} \prod_{p \equiv 1(4)} p^{\beta} \prod_{q \equiv 3(4)} q^{\gamma} \tag{26}$$

Then n can be expressed as a sum of two squares iff all the exponents of γ are even.

2.2 Solutions of Congruences

- Let $f(x)$ denote a polynomial, e.g.

$$f(x) = a_n x^n + ... + a_0 \tag{27}$$

- if $u \in \mathbb{Z}$ such that $f(u) \equiv 0 \ (mod\ m)$ then we say that u is a solution of the congruence $f(x) \equiv 0 \ (mod\ m)$
- If u is a solution of $f(x) \equiv 0 \ (mod\ m)$ and if $v \equiv u \ (mod\ m)$, then Theorem 2.2 shows that v is also a solution.
  - $x \equiv u \ (mod\ m)$ is a solution of $f(x) \equiv 0 \ (mod\ m)$ meaning that every integer congruent to u modulo m satisfied $f(x) \equiv 0 \ (mod\ m)$.

Definition 2.4:
Let $r_1, ..., r_m$ denote a complete residue system modulo m.
The number of solutions of $f(x) \equiv 0 \ (mod\ m)$ is the number of the r_i such that $f(r_i) \equiv 0 \ (mod\ m)$

Definition 2.5:
Let $f(x) = a_n x^n + ... + a_0$. If $a_n \not\equiv 0 \ (mod\ m)$ the degree of the congruence $f(x) \equiv 0 \ (mod\ m)$ is n. If $a_n \equiv 0 \ (mod\ m)$, let j be the largest integer such that $a_j \not\equiv 0 \ (mod\ m)$; then the degree of the congruence is j. If there is no such integer j, then no degree is assigned to the congruence.

Theorem 2.16:
If $d|m$, $d > 0$, and if u is a solution of $f(x) \equiv 0 \ (mod\ m)$, then u is a solution of $f(x) \equiv 0 \ (mod\ d)$

- We say that $f(x) \equiv 0 \ (mod\ m)$ is an identical congruence if it holds for all integers x

– If $f(x)$ is a polynomial whose coefficients are divisible by m, then $f(x) \equiv 0 \ (mod \ m)$ is an identical congruence

– $x^p \equiv x \ (mod \ p)$ is true for all integers x by Fermat's **Theorem :**

Theorem 2.17: Linear Congruences
Let a, b and $m > 0$ be given integers, and put $g = (a, m)$. The congruence $ax \equiv b \ (mod \ m)$ has a solution iff $g|b$. If this condition is met, then the solution forms an arithmetic progression with common difference $\frac{m}{g}$, giving g solutions $(mod \ m)$.

How to solve general linear congruences: Let $a, b \in \mathbb{Z}$ and let $n \in \mathbb{N}$. Suppose we wish to solve the linear congruence

$$ax \equiv b \ (mod \ n) \tag{28}$$

Firstly apply the Extended Euclidean Algorithm to compute $d = gcd(a, n)$ and find $x_0, y_0 \in \mathbb{Z}$ such that

$$ax_0 + ny_0 = d \tag{29}$$

If $d \nmid b$ then there are no solutions by Theorem 2.17. Otherwise, there are exactly d solutions modulo n by Theorem 2.17, which we can find as follows
Write

$$a = da', \quad b = db', \quad n = dn' \tag{30}$$

Dividing by d gives

$$a'x_0 + n'y_0 = 1 \tag{31}$$

Then reducing mod n' gives

$$a'x_0 \equiv 1 \ (mod \ n') \tag{32}$$

and multiplying by b' gives

$$a'(b'x_0) \equiv b' \ (mod \ n')$$

Therefore $t = b'x_0$ is the unique solution to $a'x \equiv b' \ (mod \ n')$. Now by Theorem 2.17 the solutions to (17) are $t, t + n', ..., t + (d - 1)n'$

2.3 The Chinese Remainder Theorem

Solve Simultaneous Congruences

Find x (is there are any) that satisfies

$$\begin{aligned} x &\equiv a_1 \ (mod \ m_1) \\ x &\equiv a_2 \ (mod \ m_2) \\ &... \\ x &\equiv a_r \ (mod \ m_r) \end{aligned} \tag{33}$$

Theorem 2.18: The Chinese Remainder Theorem
Let $m_1, ..., m_r$ denote r positive integers that are relatively prime in pairs, and let $a_1, ..., a_r \in \mathbb{Z}$. Then the congruences (21) have have common solutions. If x_0 is one such solution, then an integer x satisfies the congruences (21) iff $x = x_0 + km$ for some integer k. Here $m = m_1 m_2 ... m_r$

Proof: Theorem 2.18
Let $m = m1m2...mr$, we see that $\frac{m}{m_j} \in Z$ and that $(\frac{m}{m_j}, m_j) = 1$. Hence by theorem 2.9, for each j there is an integer b_j such that $(\frac{m}{m_j}, m_j)b_j \equiv 1 \ (mod \, m_j)$. Clearly $(\frac{m}{m_j}, m_j)b_j \equiv 0 \ (mod \ m_i)$ if $i \not\equiv j$. 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

$$x_0 \equiv \frac{m}{m_i} b_i a_i \equiv a_i \ (mod \ m_i)$$

Thus x_0 is a solution of the system (21). If x_0 and x_1 are two solutions of the system (21), then $x_0 \equiv x_1 \ (mod \, m_i)$ for $i = 1, 2, ..., r$ and hence $x_0 \equiv x_1 \ (mod \, m)$ by theorem 2.3 (3). This completes the proof.

- $m_1, ..., m_r$ positive integers relatively prime in pairs
- $m = m_1 m_2 ... m_r$
- Instead of considering just one set of aligns, we will consider all possible systems of this type
- Let

$$\begin{aligned} a_1 &\in \{1, ..., m_1\} \\ a_2 &\in \{1, ..., m_2\} \\ &... \\ a_r &\in \{1, ..., m_r\} \end{aligned} \tag{34}$$

- The number of such r-tuples $(a_1, ..., a_r)$ is $m = m_1 m_2 ... m_r$.

- By the **C.R.T.** each r-tuple determines precisely one residue class x modulo m.
  - Moreover, distinct r-tuples determine different residue classes. To see this, suppose that $(a_1, ..., a_r) \neq (a'_1, ..., a'_r)$. then $a_i \neq a'_i$ for some i, and we see that no integer x satisfies both the congruences $x \equiv a_i \ (mod\ m_i)$ and $x \equiv a'_i \ (mod\ m_i)$
- Thus we have a one-to-one correspondence between the r-tuples $(a_1, ..., a_r)$ and a complete residue system modulo m, such as the integers $1, ..., m$

Theorem 2.19:
If $m_1,\ m_2 > 0,\ (m_1, m_2) = 1$, then $\Phi(m_1 m_2) = \Phi(m_1)\Phi(m_2)$ moreover, if $m = \Pi p^\alpha$ then

$$\Phi(m) = \prod_{p|m}(p^\alpha - p^{\alpha-1}) = m \prod_{p|m}(1 - \frac{1}{p}) \tag{35}$$

Proof: Theorem 2.19
If $m = 1$, then the products are empty, and by convention an empty product has value 1. Thus $\Phi(1) = 1$ in this case, which is correct.

Put $m = m_1 m_2$, and suppose $(x, m) = 1$. By reducing x modulo m_1, we see that there is a unique $a_1 \in \mathcal{C}(m_1)$ for which $x \equiv a_1 \ (mod\ m_1)$. Similarly there is a unique $a_2 \in \mathcal{C}(m_2)$ for which $x \equiv a_2 \ (mod\ m_2)$. Since $(x_1, m_1) = 1$, it follows by theorem 2.4 that $(a_1, m_1) = 1$. Similarly $(a_2, m_2) = 1$. For any $n \in Z,\ n > 0$, let $\mathcal{R}(n)$ be the system of reduced residues formed of those numbers $a \in \mathcal{C}(n)$ for which $(a, n) = 1$. That is $\mathcal{R}(n) = \{a \in \mathcal{C}(n) : (a, n) = 1\}$. Thus we see that any $x \in \mathcal{R}(m)$ gives rise to a pair (a_1, a_2) with $a_i \in \mathcal{R}(m_i)$ for $i = 1, 2$. Suppose, conversely, that we start with such a pair. By the CRT there exists a unique $x \in \mathcal{C}(m)$ such that $x \equiv a_i \ (mod\ mi)$ for $i = 1, 2$. Since $(a_1, m_1) = 1$ and $x \equiv a_1 \ (mod\ m_1)$, it follows by theorem 2.4 that $(x_1, m_1) = 1$. Similarly we find that $(x, m_2) = 1$ and hence $(x, m) = 1$. That is $x \in \mathcal{R}(m)$. In this way we see that CRT enables us to establish a one to one correspondence between the reduced residue classes modulo m and pairs of reduced residue classes modulo m_1 and m_2, provided that $(m_1, m_2) = 1$. Since $a_1 \in \mathcal{R}(m_1)$ can take any one of $\Phi(m_1)$ values and the same for a_2 taking $\Phi(m_2)$ values, there are $\Phi(m_1)\Phi(m_2)$ pairs, so that $\Phi(m) = \Phi(m_1)\Phi(m_2)$. If $m = \prod p^\alpha$, then by repeated use of the above identity, we see that $\Phi(m) = \prod \Phi(p^\alpha)$. If a is one of the p^α numbers $1, 2, ..., p^\alpha$, then $(a, p^\alpha) = 1$ unless a is one of the $p^{\alpha-1}$ numbers, $p, 2p, ..., p^{\alpha-1}p$. on subtracting, we deduce that the number of reduced residue classes modulo p^α is $p^\alpha - p^{\alpha-1} = p^\alpha(1 - frac1p)$. This gives the stated formula.

Theorem 2.20:
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 $(mod\ m)$. If $m = m_1 m_2$ where $(m_1, m_2) = 1$, then $N(m) = N(m_1)N(m_2)$. If $m = \prod p^\alpha$, then $N(m) = \prod N(p^\alpha)$

2.4 Public-key Cryptography

Lemma 2.22:
Suppose $m \in \mathbb{Z},\ m > 0,\ (a, m) = 1$. If $k, \overline{k} \in \mathbb{Z}$ and $k, \overline{k} > 0$ such that $k, \overline{k} \equiv 1\ (mod\ \Phi(m))$, then $a^{k\overline{k}} \equiv a\ (mod\ m)$.

Proof: Theorem 2.22
Write $k\overline{k} = 1 + r\Phi(m)$ for some $r \in \mathbb{Z}$. Then by Euler's congruence

$$a^{k\overline{k}} = aa^{r\Phi(m)} = a(a^{\Phi(m)})^r \equiv a \cdot 1^r = a\ (mod\ m)$$

- If $(a, m) = 1,\ k > 0$, then $(a^k, m) = 1$. Thus if $n = \Phi(m)$ and $r_1, ..., r_n$ is a system of reduced residues $(mod\ m)$, then the numbers $r_1^k, ..., r_n^k$ are also relatively prime to m. These k^{th} powers may not all be distinct $(mod\ m)$, as we see by considering the case $k = \Phi(m)$. On the other hand, from lemma 2.22, we can deduce that these k^{th} powers are distinct $(mod\ m)$ provided that $(k, \Phi(m)) = 1$.

- Suppose that $r_i^k \equiv r_j^k\ (mod\ m)$ and $(k, \Phi(m)) = 1$. By Theorem 2.9 we may find $\overline{k} > 0$ such that $k\overline{k} \equiv 1\ (mod\ \Phi m)$ and then it follows from the lemma that

$$r_i \equiv r_i^{k\overline{k}} = (r_i^k)^{\overline{k}} \equiv (r_j^k)^{\overline{k}} = r_j^{k\overline{k}} \equiv r_j\ (mod\ m) \tag{36}$$

  This implies that $i = j$. We will show later that the converse also holds: the numbers $r_i^k, ..., r_n^k$ are distinct $(mod\ m)$ only if $(k, \Phi(m)) = 1$. Suppose that $(k, \Phi(m)) = 1$. Since the numbers $r_1, ..., r_n^k$ are distinct $(mod\ m)$, they form a system of reduced residues $(mod\ m)$. That is the map $a \mapsto a^k$ permutates the reduced residues $(mos\ m)$ if $(k, \Phi(m)) = 1$. The significance of the lemma is that the further map $b \mapsto b^{\overline{k}}$ is the inverse permutation.

- To apply these observations to cryptography, we take two distinct large primes, p_1, p_2, say each one with about 100 digits.
  - So $m = p_1 p_2$ has about 200 digits.
  - Since we know the prime factorisation of m, from Theorem 2.19 we have that $\Phi(m) = (p_1 - 1)(p_2 - 1)$
  - So $\Phi(m) < m$
  - we choose now a big number k, $0 < k, \Phi(m)$ and check by the Euclidean algorithm that $(k, \Phi(m)) = 1$. We try until we get such a k.

- We make the numbers m and k publicly available, by keep p_1, p_2 and $\Phi(m)$ secret.
- suppose now thatt some associate of ours wants to send us a message, say *'Gauss was a genuis!'*. The associate first converts the characters to number in some standard way, say by emplying (ASCII). Then $G = 071$, $a = 097$,..., ! = 033. Then concatenate these codes to form a number

  $a = 071097117115115126119097115126097126103101110105117115033$

- if the message were longer, it could be ficided into a number of blocks.
- the associate could send the number a and we could reconstruct the message. But suppose that message has some sensitive information. In that case the associate would use the number k and m that we have provided.
- Our associate quickly finds the unique number b, $0 \leq b < m$ such that $b \equiv a^k \ (mod\ m)$ and sends this b to us.
- We use Euclidean Algorithm to find $\overline{k} > 0$ such that $k\overline{k} \equiv 1 \ (mod\ \Phi(m))$ and then we find the unique c such that $0 \leq c < m$, $c \equiv b^{\overline{k}} \ (mod\ m)$. From lemma 2.22 we deduce that $a = c$.

- In theory it might happen that $(a, m) > 1$ in which case the lemma does not apply, but the chances of this is $\approx \frac{1}{p_i} \approx 10^{-100}$. Suppose that some third party gain access to the numbers m, k and b, and seeks to recover the number a. In principle, all that needs to be done is to factor m, which yields $\Phi(m)$, and hence $\overline{k}$. The problem of locating the factors of m for a big number is not easy.

2.5 Prime Power Moduli

Let $f(x)$ be a polynomial with integer coefficients. Let $N(m)$ denote the number of solutions of $f(x) \equiv 0 \ (mod\ m)$.

Suppose that $m = m_1 m_2$, where $(m_1, m_2) =$. With a "little work", Theorem 2.19 shows that the roots of the congruence $f(x) \equiv 0 \ (mod\ m)$ are in one-to-one correspondence with pairs (a_1, a_2) in which a_1 runs over all roots of the congruence $f(x) \equiv 0 \ (mod\ m_1)$ and
a_2 runs over all roots of the congruence $f(x) \equiv 0 \ (mod\ m_2)$.

- From Theorem 2.16 and Theorem 2.20 we have that the congruence $f(x) \equiv 0 \ (mod\ m)$ has solutions iff it has solutions $(mod\ p^\alpha)$ for each prime power p^α exactly dividing m.

Example: Let $f(x) = x^2 + x + 7$. Find all roots of $f(x) \equiv 0 \ (mod\ 189)$, given that $189 = 3^3 \cdot 7$, that all roots $(mod\ 27)$ are 4, 13, and 22, and that the roots $(mod\ 7)$ are 0 and 6.

Solution: By the Eucliean algorithm and (2.2), we find that $x \equiv a_1 \ (mod\ 27)$ and that $x \equiv a_2 \ (mod\ 7)$ iff $x \equiv 28a_1 - 27a_2 \ (mod\ 189)$. We let $a_1 = 4, 13, 22$ and $a_2 = 0, 6$. Thus we obtain the six solutions $13, 49, 76, 112, 139, 175 \ (mod\ 189)$

- The problem of solving a congruence is now reduced to the case of a prime-power modulus.
- To solve $f(x) \equiv 0 \ (mod\ p^k)$ we start with solutions to $f(x) \equiv 0 \ (mod\ p)$ and then move to $p^2, p^3, ..., p^k$.

Suppose that $x = a$ is a solution of $f(x) \equiv 0 \ (mod\ p^j)$ 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

$$f(a + tp^j) = f(a) + tp^j f'(a) + t^2 p^{2j} \frac{f''(a)}{2!} + ... + t^n p^{nj} \frac{f^{(n)}(a)}{n!} \qquad (37)$$

where $n =$ degree of $f(x)$. All derivatives beyond the n^{th} are identicallly zero. Now with respect to the modulus p^{j+1}, equation (37) gives

$$f(a + tp^j) \equiv f(a) + tp^j f'(a) \ (mod\ p^{j+1}) \qquad (38)$$

as the following argument shows. What we want to establish is that the coefficients of $t^1, t^3, ..., t^n$ in (37) are divisible by p^{j+1} and so can be ommited in (38). This is almost obvious because the powers of p in those terms. The explanation is that $\frac{f^{(k)}(a)}{k!}$ is an integer for each value of k, $2 \leq k \leq n$. To see this, let cx^r be a representative term from $f(x)$. The corresponding term in $f^{(k)}(a)$ is $cr(r-1)(r-2)...(r-k+1)a^{r-k}$.

We now use the fact (without proof), that the product of k consecutive integers is divisible by $k!$, and the argument is complete. Thus, we have proved that the coefficients of $t^2, t^3, ..., t^n$ in (37) are divisible by p^{j+1}. The congruence (38) reveals how t should be chosen if $x = a + tp^j$ is to be a solution of $f(x) \equiv 0 \ (mod\ p^{j+1})$. We want t to be a solution of

$$f(a) + tp^j f'(a) \equiv 0 \ (mod\ p^{j+1}) \qquad (39)$$

Since $f(x) \equiv 0 \ (mod\ p^j)$ have the solutions $x = a$, we see that p^j can be removed as a factor to give

$$tf'(a) \equiv -\frac{f(a)}{p^j} \ (mod\ p) \qquad (40)$$

Which is a linear congruence in t. This congruence may have no solution, one solutions, or p solutions. If $f'(a) \equiv 0 \ (mod\ p)$, then this congruence has exactly one solution, and we obtain

Theorem 2.3: Hansel's Lemma:
Suppose that $f(x)$ is a polynomial with integral coefficients. If $f(a) \equiv 0 \ (mod\, p^j)$ and $f'(a) \not\equiv 0 \ (mod\ p)$ then there is a unique $t \ (mod\ p)$ such that $f(a + tp^j) \equiv 0 \ (mod\ p^{j+1})$

- If $f(a) \equiv 0 \ (mod\ p^j)$, $f(b) \equiv 0 \ (mod\ p^k)$, $j < k$ and $a \equiv b \ (mod\ p^j)$, then we say that b lies above a, or a lifts to b.
- If $a \equiv 0 \ (mod\, p^j)$, then a is called a non-singular root if $f'(a) \not\equiv 0 \ (mod\, p)$; otherwise it is singular.
- By Hensel's lemma we see that a non-singular root $a \ (mod\ p)$ lifts to a unique root $a_2 \ (mod\ p^2)$. Since $a_2 \equiv a \ (mod\ p)$ it follows by Theorem 2.2 that $f'(a_2) \equiv f'(a) \not\equiv 0 \ (mod\ p)$.
  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 non-singular root a modulo p lifts to a unique root a_j modulo p^j for $j = 2, 3, ...$ by (2.5) we see that this sequence is generated by means of the recursion

$$a_{j+1} = a_j - f(a_j)\overline{f'(a)} \tag{41}$$

  where $\overline{f'(a)}$ is an integer chosen so that $f'(a)\overline{f'(a)} \equiv 1 \ (mod\ p)$.

Example: Solve $x^2 + x + 47 \equiv 0 \ (mod\ 7^3)$

Solution: First we note that $x \equiv 1 \ (mod\ 7)$ and $x \equiv 5 \ (mod\ 7)$ are the only solutions of $x^2 + x + 47 \equiv 0 \ (mod\ 7)$. Since $f'(x) = 2x + 1$, we see that

- $f'(1) = 3 \not\equiv 0 \ (mod\ 7)$
- $f'(5) = 11 \not\equiv 0 \ (mod\ 7)$

(So these roots are non singular)

Taking $\overline{f'(1)} = 5$, we see by (40) that the root $a \equiv 1 \ (mod\ 7)$ lifts to $a_2 = 1 - 49 \cdot 5 = -244$. Since a_2 is considered $(mod\ 7^2)$, we may take instead $a_2 = 1$. Then $a_3 = 1 - 49 \cdot 5 \equiv 99 \ (mod\ 7^3)$.
Similarly, we take $\overline{f'(5)} = 2$ and see by (40) that the root $5 \ (mod\ 7)$ lifts to $5 - 77 \cdot 2 = -149 \equiv 47 \ (mod\ 7^2)$ and that $47 \ (mod\ 7^2)$ lifts to $47 - f(47) \cdot 2 = 47 - 2303 \cdot 2 = -4599 \equiv 243 \ (mod\ 7^3)$.
Thus we conclude that 99 and 243 are the desired roots and that there are no others.

2.6 Prime Modulus

$f(x) \equiv 0 \ (mod\ m) \rightarrow f(x) \equiv 0 \ (mod\ p)$ *(reduced)*
(No general method exists to solve such congruences)

Question:
Given a polynomial congruence $f(x) \equiv 0 \ (mod\ m)$ is there an analogue to the result in algebra which says that a polynomial equation of degree n with complex coefficients has exactly n roots?
$\rightarrow$ for congruences the solution is more complicated.

e.g. For any $m > 1$, there are $f(x)$ such that $f(x) \equiv 0 \ (mod\ m)$ has no solutions.

e.g.2 $x^p - x + 1 \equiv 0 \ (mod\ m)$, where p is a prime factor of m has no solutions because $x^p - x + 1 \equiv 0 \ (mod\ p)$ has none, by Fermat's Theorem.

$f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$ and we assume $p \nmid a_n$ so that the congruence $f(x) \equiv 0 \ (mod\ p)$ has degree n.

Theorem 2.25:
If the degree n of $f(x) \equiv 0 \ (mod\, p)$ is greater than or equal to p, then either every integer is a solution of $f(x) \equiv 0 \ (mod\ p)$ or there is a polynomial $g(x)$ having integral coefficients, with leading coefficient 1, such that $g(x) \equiv 0 \ (mod\ p)$ is of degree less than p and the solutions of $g(x) \equiv 0 \ (mod\ p)$ are precisely those of $f(x) \equiv 0 \ (mod\ p)$.

Proof: Theorem 2.25
Dividing $f(x)$ by $x^p - x$ we get a quotient $q(x)$ and a remainder $r(x)$ such that $f(x) = (x^p - x)q(x) + r(x)$. here $q(x)$ and $r(x)$ are polynomials with integral coefficients, and $r(x) = 0$ or degree $r(x) < p$. Since every integer is a solutions of $x^p \equiv x \ (mod\ p)$ are the same as those of $r(x) \equiv 0 \ (mod\ p)$ by Fermat's Theorem, we see that the solutions of $f(x) \equiv 0 \ (mod\ p)$ are the same as those of $r(x) \equiv 0 \ (mod\ p)$. If $r(x) = 0$ or if every coefficient of $r(x)$ is divisible by p, then every integer is a solution of $f(x) \equiv 0 \ (mod\ p)$.

On the other hand, if at least one coefficient of $r(x)$ is not divisible by p, then the congruence $r(x) \equiv 0 \ (mod\ p)$ has a degree, and that degree is less than p. The polynomial $g(x)$ in the Theorem can be obtained from $r(x)$ by getting leading coefficient 1, as follows. We may discard all terms in $r(x)$ whose coefficients are divisible by p, since the congruence properties modulo p are unaltered. Then let bx^m be the term of the highest degree in $r(x)$, with $(b, p) = 1$. Choose $\overline{b}$ so that $b\overline{b} \equiv 1 \ (mod\ p)$, and note that $(\overline{b}, b) = 1$ also. Then the congruence $\overline{b}r(x) \equiv 0 \ (mod\ p)$ has the same solutions as $r(x) \equiv 0 \ (mod\ p)$, and so has the same solutions as $f(x) \equiv 0 \ (mod\ p)$. Define $g(x) = \overline{b}r(x)$ with its leading coefficient $b\overline{b}$ replaced by 1, that is,

$$g(x) = \overline{b}r(x) - (b\overline{b} - 1)x^m \tag{42}$$

Theorem 2.26:
The congruence $f(x) \equiv 0 \ (mod\ p)$ of degree n has at most n solutions.

Proof: Theorem 2.26
The proof is by induction on the degree of $f(x) \equiv 0 \ (mod\ p)$. If $n = 0$, the polynomial $f(x) = a_0$ with $a_0 \not\equiv 0 \ (mod\ p)$ and hence the congruence has no solutions. If $n = 1$, the congruence has exactly one solutions by Theorem 2.17. Assume the truth of the Theorem for all congruences of degree $< n$, supppose that there were more than n solutions of the congruence $f(x) \equiv 0 \ (mod\ p)$ of degree n. Let the leading term of $f(x)$ be $a_n x^n$ and let $u_1, ..., u_{n+1}$ be solutions of the congruence with $u_1 \not\equiv u_j \ (mod\ p)$ for $i \neq j$. We define $g(x)$ by

$$g(x) = f(x) - a_n(x - u_1)...(x - u_n) \tag{43}$$

noting the cancellation of $a_n x^n$ on the right.

Note that $g(x) \equiv 0 \ (mod\ p)$ has at least n solutions, namely $u_1, ..., u_n$. We consider two cases:

i. every coefficient. of $g(x)$ is divisible by p

ii. at least one coefficient is not divisible by p

For (i), every integer is a solution of $g(x) \equiv 0 \ (mod\ p)$, and since $f(u_{n+1}) \equiv 0 \ (mod\ p)$ by assumption, it follows that $x = u_{n+1}$ is a solutions of

$$a_n(x - u_1)...(x - u_n) \equiv 0 \ (mod\ p) \tag{44}$$

This contradicts Theorem 1.15.

For (ii), we note that $g(x) \equiv 0 \ (mod\ p)$ has a degree and that degree is $< n$. By the induction hypothesis, this congruence has fewer than n solutions. This contradicts the earlier observation that this congruence has at least n solutions. Thus the proof is complete.

Corollary 2.27: If $b_n x^n + b_{n-1} x^{n-1} + ... + b_0 \equiv 0 \ (mod\ p)$ has more than n solutions, then all the coefficients b_j are divisible by p.

Theorem 2.28:
If $F(x)$ is a function that maps residue classes $(mod\ p)$ to residue classes $(mod\ p)$, then there is a polynomial $f(x)$ with integral coefficients and degree at most $p - 1$ such that $f(x) \equiv F(x) \ (mod\ p)$ for all residue classes $x \ (mod\ p)$.

Proof: Theorem 2.28
By Fermat's Congruence we see that

$$1 - (x - a)^{p-1} \equiv 1 \ (mod\ p) \text{ if } x \equiv a \ (mod\ p) \tag{45}$$

$$1 - (x - a)^{p-1} \equiv 0 \ (mod\ p) \text{ otherwise.} \tag{46}$$

Hence the polynomial

$$f(x) = \sum_{i=1}^{p} F(i)(1 - (x-i)^{p-1}) \tag{47}$$

had the desired properties.

Theorem 2.29:
The congruencs $f(x) \equiv 0 \ (mod\ p)$ of degree n with leading coefficient $a_n = 1$ has n solutions iff $f(x)$ is a factor of $x^p - x$ modulo p, that is if and only if $x^p - x = f(x)q(x) + ps(x)$, where $q(x)$ and $s(x)$ have integral coefficients, $q(x)$ has degree $p - n$ and leading coefficient 1, and where $s(x)$ is a polynomial of degree less than n or $s(x)$ is zero.

Proof: Theorem 2.29
First we assume that $f(x) \equiv 0 \ (mod\ p)$ has n solutions. Then $n \leq p$ by defintion 2.4. Dividing $x^p - x$ by $f(x)$ we get $x^p - x = f(x)q(x) = r(x)$ where degree $r(x) <$ n or $r(x) < n$ or $r(x) = 0$. This equation implies (using Fermat's Theorem) that every solution of $f(x) \equiv 0 \ (mod\ p)$ is a solution of $r(x) \equiv 0 \ (mod\ p)$. Thus $r(x) \equiv 0 \ (mod\ p)$ has at least n solutions and by Corollary 2.27, it follows that every coefficient in $r(x)$ is divisible by p, so $r(x) = ps(x)$ as in the Theorem.

Conversely, assume that $x^p - x = f(x)q(x) + ps(x)$ as in the Theorem. By Fermat's Theorem, the congruence $f(x)q(x) \equiv 0 \ (mod\ p)$ has p solutions. This congruence has leading term x^p. The leading term of $f(x)$ is x^n by hypothesis, and hence the leading term of $q(x)$ is x^{p-n}. By Theorem 2.26, the congruence $f(x) \equiv 0 \ (mod\ p)$ and $q(x) \equiv 0 \ (mod\ p)$ have at most n solutions and $p - n$ solutions, respectively. But every one of the p solutions of $f(x) \equiv 0 \ (mod\ p)$ has a solution of at least one of the congruences $f(x) \equiv 0 \ (mod\ p)$ and $q(x) \equiv$ $0 \ (mod\ p)$. It follows that the two congruences have exactly n solutions and $p - n$ solutions, respectively.

Corollary 2.30: If $d|(p-1)$, then $x^d \equiv 1 \ (mod\ p)$ has d solutions.

Proof: Corollary 2.30
Choose e so that $de = p-1$. Since $(y-1)(1+y+...+y^{e-1}) = y^e - 1$, on taking $y = x^d$ we see that $x(x^d - 1)(1 + x^d + ... + x^{d(e-1)}) = x^p - x$.

Consider

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

We assume $p > 2$. On expanding, we find that

$$f(x) = x^{p-1} - \sigma_1 x^{p-2} + \sigma_2 x^{p-3} - ... + \sigma_{p-1} \tag{48}$$

where σ_j is the sum of all products of J distinct members of the set $\{1, 2, .., p-1\}$. In the two extreme cases we have $\sigma_1 = 1 + 2 + 3 + ... + (p-1) = \frac{p-1}{2}$, and

$\sigma_{p-1} = 1\dot{2}\dot{3}\vdots\dot{(}p-1) = (p-1)!$. The polynomial f(x) has degree $p-1$ and has the $p-1$ roots $1, 2, ..., p-1$ $(mod\ p)$. consequently, the polynomial $xf(x)$ has degree p and has p roots. By Theorem 2.29 in $xf(x)$, we see that there are polynomials $q(x)$ and $s(x)$ such that $x^p - x = xf(x)q(x) + ps(x)$. Since the degree $q(x) = p - p = 0$ 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 $mod(\ p)$to those of $xf(x)$. On comparing the coefficients of x, we deduce that $\sigma_{p-1} = (p-1)! \equiv -1\ (mod\ p)$, which provides a second proof of Wilson's congruence. On comparing the remaining coefficients, we deduce that $\sigma_p \equiv 0\ (mod\ p)$ for $1 \leq j \leq p-2$. To these useful observations, we may add one further remark: if $p \geq 5$ then

$$\sigma_{p-2} \equiv 0\ (mod\ p^2)$$

This is Wolstenholme's congruence. To prove it, we note that $f(p) = (p-1)(p-1)...(p-p+1) = (p-1)!$ On taking $x = p$ in (47) we have

$$(p-1)! = p^{p-1} - \sigma_1 p^{p-2} + ... + \sigma_{p-3}p^2 - \sigma_{p-2}p + \sigma_{p-1}$$

We already know that $\sigma_{p-1} = (p-1)!$ On subtracting this amount from both sides and dividing through by p, we deduce that

$$p^{p-2} - \sigma_1 p^{p-3} + ... + \sigma_{p-3}p - \sigma_{p-2} = 0$$

All terms except the last two contains visible factors of p^2. Thus $\sigma_{p-3}p \equiv \sigma_{p-2}\ (mod\ p^2)$. This gives the desired result, since $\sigma_{p-3} \equiv 0\ (mod\ p)$

Theorem 3.2: Gauss' Lemma
Let p be an odd prime and $(a, p) = 1$.

$$a, 2a, 3a, ..., \frac{p-1}{2}a \tag{49}$$

and their least positive residues

2.7 Primitive Roots and Power Residues

Definition 2.6: Order of modulus
Let $m > 0, m \in \mathbb{Z}$ and $a \in \mathbb{Z}$ such that $(a, m) = 1$. Let h be the smallest positive integer such that $a^h \equiv 1\ (mod\ m)$. In this case, we say that the order of a modulo m is h, or that a belongs to the exponent h modulo m.

Suppose that a has order $h\ (mod\ m)$. Let $k = qh > 0$, then $a^k = a^{qh} = (a^h)^q \equiv 1^q \equiv 1\ (mod\ m)$. Conversely, $k > 0$ such that $a^k \equiv 1\ (mod\ m)$, then by the division algorithm, we have $k = qh + r, q \geq 0$ and $0 \leq r \leq h$. Thus $1 \equiv a^k \equiv a^{qh+r} \equiv (a^h)^q a^r \equiv 1^q a^r \equiv a^r\ (mod\ m)$. But $0 \leq r < h$ and h is the

least positive power of a that is congruent to 1 $(mod\ m)$, so it follows $r = 0$. Thus $h|k$ and we have proved that following

Lemma 2.31:
If a has order h $(mod\ m)$, then the positive integers k such that $a^k \equiv 1\ (mod\ m)$ are precisely those for which $h|k$.

Corollary 2.32:
If $(a, m) = 1$, then the order of a modulo m divides $\Phi(m)$.

Proof:
Each reduced residue class a modulo m has finite order, for by Euler's congruence $a^{\Phi(m)} \equiv 1\ (mod\ m)$. Moreover, if a has order h then by taking $k = \Phi(m)$ in the lemma, we deduce that $h|\phi(m)$.

Lemma 2.33:
If $a\ (mod\ m)$ has order h, then a^k has order $\frac{h}{(h,k)}\ (mod\ m)$

Note:
Since $\frac{h}{(h,k)} = 1$ iff $h|k$, we see that Lemma 2.33 contains Lemma 2.31 as a special case.

Proof:
Lemma 2.31 says that $(a^k)^J \equiv 1\ (mod\ m)$ iff $h|k_J$. But $h|k_J$ iff $\{\frac{h}{(h,k)}\}|\{\frac{k}{h,k}\}J$. As the divisor is relatively prime to the first factor of the dividend, this relation holds iff $\{\frac{k}{h,k}|J$. Therefore the least positive integer J such that $(a^k)^J \equiv 1\ (mod\ m)$ is $J = \frac{h}{(h,k)}$

Note:
If a has order h $(mod\ m)$ and b has order k $(mod\ m)$ then $(ab)^{hk} = (a^h)^k(b^k)^h \equiv 1\ (mod\ m)$ and using Lemma 2.31 we deduce that the order of ab is a divisor of hk.

Lemma 2.34:
If a has order h $(mod\ m)$ and b has order k $(mod\ m)$ and if $(h, k) = 1$, then ab has order hk $(mod\ m)$.

Proof: Lemma 2.34
Let r =order of ab $(mod\ m)$. We have shown that $r|hk$. We now prove $hk|r$. We note that $b^{rh} \equiv (a^h)^r b^{rh} = (ab)^{rh} \equiv 1\ (mod\ m)$. Thus $k|rh$ by Lemma 2.31. As $(h, k) = 1$, it follows that $k|r$. By a similar argument we see that $h|r$. Using again $(h, k) = 1$, we conclude that $hk|r$.

Definition 2.7: Primative Root
If g belongs to the exponent $\Phi(m)$ $(mod\ m)$, then g is called a Primitive root. $(g, m) = 1$ and $g^{\Phi(m)} \equiv 1\ (mod\ m)$ where $\Phi(m)$ is the smallest positive integer with such property.

In view of Lemma 2.31, the number a is a solution of the congruence $x^k \equiv 1 \ (mod\ m)$ iff the order of $a \ (mod\ m)$ divides k.

In one special case, Corollary 2.30, we have determined the number of solutions of this congruence. That is, if p is prime and $k|(p-1)$ the there are precicely k residue classes $a \ (mod\ p)$ such that the order of a moulo p is a divisor of k. If k happens to be a prime power, we can then determine the exact number of residues $a \ (mod\ p)$ of order k.

Lemma 2.35:
The divisors of q^α are the numbers q^β with $\beta = 0, 1, ..., \alpha$. Of these, q^α is the only one that is not a divisor of $q^{\alpha-1}$. There are q^α residues $(mod\ p)$ of order dividing q^α, and among these there are $q^{\alpha-1}$ residues of order dividing $q^{\alpha-1}$. On subtracting we see that there are precisely $q^\alpha - q^{\alpha-1}$ residues a of order $q^\alpha \ (mod\ p)$

Theorem 2.36:
If p is a prime then there exists $\Phi(p-1)$ primitive roots $(mod\ p)$

Proof: Theorem 2.36
We first establish the existence of at least one primitive root.
Let $p-1 = p_1^{\alpha_1} p_2^{\alpha_2} ... p_J^{\alpha_J}$. By lemma 2.35 we may choose numbers $a_i \ (mod\ p)$ so that a_i has order $p_i^{\alpha_i}$, $i = 1, 2, ..., J$. The numbers $p_i^{\alpha_i}$ are pairwise relatively prime, so by repeated use of lemma 2.34 we see that $g = a_1 a_2 ... a_J$ has order $p_1^{\alpha_1} p_2^{\alpha_2} ... p_J^{\alpha_J} = p-1$.
That is, g is a primitive root $(mod\ p)$.

To complete the proof, we determine the exact number of primitive roots $(mod\ p)$. Let g ne a primitive root $(mod\ p)$. Then the numbers $g, g^2, ..., g^{p-1}$ form a system of reduced residues $(mod\ p)$. By Lemma 2.33 we see that g^k has order $(p-1)/(k, p-1)$. Thus g^k is a primitive root iff $(k, p-1) = 1$. By definition of Euler's phi function, there are exactly $\Phi(p-1)$ such values of k in the interval $1 \leq k \leq p-1$.

Definition 2.8: n^{th} power residue
If $(a, p) = 1$ and $x^n \equiv a \ (mod\ p)$ has a solution,
a is called an $\underline{n^{th} \text{ power residue modulo } p}$

If $(g, m) = 1$ then the sequence $g, g^2, ... \ (mod\ m)$ is periodic.
If g is a primitive root $(mod\ m)$ then the least period of this sequence is $\Phi(n)$ and we see that $g, g^2, ... g^{\Phi(m)}$ form a system of reduced residues $(mod\ m)$. Thus $g^i \equiv g^J \ (mod\ m)$ iff $i \equiv j \ (mod\ \Phi(m))$. By expressing numbers as powers of g, we may convert a multiplicative congruence $(mod\ m)$ to an additive congruence $(mod\ \Phi(m))$.

Theorem 2.37:
If p is a prime and $(a, p) = 1$, then the congruence $x^n \equiv a \ (mod\ p)$ had $(n, p-1)$

solutions or no solutions according as

$$a^{\frac{p-1}{(n,p-1)}} \equiv \ (mod\ p)$$

or not.

Proof: Theorem 2.37
Let g be a Primative root $(mod\ p)$, and choose i such that $g^i \equiv a\ (mod\ p)$. If there is an x such that $x^n \equiv a\ (mod\ p)$ then $(x,p) = 1$, so that $x \equiv g^u\ (mod\ p)$. Thus the proposed congruence is $g^{nu} \equiv g^i\ (mod\ p)$, which is equivalent to $nu \equiv i\ (mod\ p-1)$. Put $k = (m, p-1)$. By Theorem 2.17, this has k solutions if $k|i$, and no solutions if $k \nmid i$.
If $k|i$, then $i(p-1)/k \equiv 0\ (mod\ p-1)$, so that $a^{\frac{(p-1)}{k}} \equiv g^{i\frac{(p-1)}{k}} = g^{p-1\frac{i}{k}} \equiv 1\ (mod\ p)$.
On the other hand, if $k \nmid i$, then $i(p-1/k \not\equiv (\ (mod\ p-1)))$, and hence $a^{\frac{p-1}{k}} \not\equiv 1\ (mod\ p)$.

Example: Show that the congruence $x^5 \equiv \ (mod\ 101)$ has 5 solutions.

Solution: By using Binary Algorithm it suffices to verify that $6^20 \equiv 1\ (mod\ 101)$

Corollary 2.38: Euler's Criterion
If p is an off prime and $(a,p) = 1$, then $x^2 \equiv a\ (mod\ p)$ has two solutions or no solutions according as $a^{\frac{p-1}{z}} \equiv 1\ (mod\ p)$ or $a^{\frac{p-1}{2}} \equiv -1\ (mod\ p)$.

Proof: Corollary 2.38
Put $b = a^{\frac{(p-1)}{2}}$. Thus $b^2 = a^{p-1} \equiv 1\ (mod\ p)$ by Fermat's congruence. From lemma 2.10, it follows that $b \equiv \pm 1\ (mod\ p)$.
If $b \equiv -1\ (mod\ p)$, then $x^2 \equiv a\ (mod\ p)$ has no solutions, by Theorem 2.37. If $b \equiv 1\ (mod\ p)$, then $x^2 \equiv a\ (mod\ p)$ has 2 solutions, by Theorem 2.37.

Primitive roots is a tool for analyzing certain congruences $(mod\ p)$. What can be said about other moduli?

Theorem 2.39:
If p is a prime then there exists $\Phi(\Phi(p^2)) = (p-1)\Phi(p-1)$ primitive roots $(mod\ p^2)$.

Proof: Theorem 2.39
Exercise

Theorem 2.40:
If p is an odd prime and g is a primitive root $(mod\ p^2)$, then g is a primitive root $(mod\ p^\alpha)$ for $\alpha = 3, 4, 5...$

Proof: Theorem 2.40
The prime $p = 2$ must be excluded, for $g = 3$ is a primitive root $(mod\ 4)$,

but not $(mod\ 8)$. Indeed it is easy to verify that $a^2 \equiv 1\ (mod\ 8)$, for any odd number a. As $\Phi(8) = 4$, it follows that there is no primitive root $(mod\ 8)$. Suppose that a is odd. Since $8|(a^2-1)$ and $2|(a^2+1)$, it follows that $16|(a^2-1)(a^2+1) = a^4 - 1$. That is $a^4 \equiv 1\ (mod\ 16)$. On repeating this argument we see that $a^8 \equiv 1\ (mod\ 32)$, and in general that $a^{2\alpha-2} \equiv 1\ (mod\ a^\alpha)$ for $\alpha \geq 3$. Since $\Phi(2^\alpha) = 2^{\alpha-1}$ we conclude that if $\alpha \geq 3$ then

$$a^{\frac{\Phi(2^\alpha)}{2}} \equiv 1\ (mod\ 2^\alpha)$$

for all odd a, and hence that there is no primitive root $(mod\ 2^\alpha)$ for $\alpha = 3, 4, 5...$

Suppose that p is an odd prime and that g is a primitive root $(mod\ p^\alpha)$. We may suppose that g is odd, for if g is even then we have only to replace g by $g + p^\alpha$, which is odd. The numbers $g, g^2, ..., g^{\Phi(p^\alpha)}$ forms a reduced residue system $(mod\ p^\alpha)$. Since these numbers are odd, they also form a reduced residue system $(mod\ 2p^\alpha)$. Thus g is a primitve root $(mod\ 2p^\alpha)$.

We have established that a primitive root exists $(mod\ m)$ when $m = 1, 2, 4, p^\alpha$ or $2p^\alpha$, (p odd prime) but that there is no primitive root $(mod\ 2^\alpha)$ for $\alpha \geq 3$. Suppose now that m is not a prime power or twice a prime power. Then m can be expressed as a product, $m = m_1 m_2$ with $(m_1, m_2) = 1$, $m_1 > 2$, $m_2 > 2$. Let $e = lcm(\Phi(m_1), \Phi(m_2))$. If $(a, m) = 1$ then $(a, m_1) = 1$ so that $a^{\Phi(m_1)} \equiv 1\ (mod\ m_1)$, and hence $a^e \equiv 1\ (mod\ m_1)$. Similarly $a^e \equiv 1\ (mod\ m_2)$, and hence $a^e \equiv 1\ (mod\ m)$. Since $2|\Phi(n)$ for all $n > 2$, we see that $2|(\Phi(m_1), \Phi(m_2))$, so that by Theorem 1.13:

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

Thus there is no primitive root in this case.

So we then have...

Theorem 2.41:
There exists a primitive root $(mod\ m)$ iff $m = 1, 2, 4, p^\alpha$ or $2p^\alpha$, where p is an odd prime.
Theorem 2.37 and its proof generalises to any modulus m possessing a primitive root.

Corollary 2.42:
Suppose that $m = 1, 2, 4, p^\alpha$ or $2p^\alpha$, where p is odd prime. If $(a, m) = 1$ then the congruence $x^n \equiv a\ (mod\ m)$ has $(n, \Phi(m))$ solutions or no solutions, according as

$$a^{\frac{\Phi(m)}{(n,\Phi(m))}} \equiv 1\ (mod\ m)$$

or not.

Example:
Determine the number of solutions of the congruence $x^4 \equiv 61 \ (mod\ 117)$

Solution:
We note that $117 = 3^2 \dot{1}3$ As $\Phi(9)/(4, \Phi(9)) = 6/(4, 6) = 3$ and $61^3 \equiv (-2)^3 \equiv 1 \ (mod\ 9)$ we deduce that the congruence $x^4 \equiv 61 \ (mod\ 9)$ has $(4, \Phi(9)) = 2$ solutions.
Similarly $\Phi(13)/(4, \Phi(13)) == 3$ and $61^3 \equiv (-4)^3 \equiv 1 \ (mod\ 13)$ so the congruence $x^4 \equiv 61 \ (mod\ 13)$ has $(4, \Phi(13)) = 4$ solutions.
Thus by Theorem 2.20, the number of solutions $(mod\ 117)$ is $2\dot{4} = 8$.

This method fails in case the modulus is divisible by 8, as corollary 2.42 does not apply to higher powers of 2.

For this we have...

Theorem 2.43:
Suppose that $\alpha \geq 2$. The order of 5 $(mod\ 2^\alpha)$ is $2^{\alpha-2}$. The numbers $\pm 5, \pm 5^2, ..., \pm 5^{2\alpha-2}$ form a system of reduced residues $(mod\ 2^\alpha)$. If a is odd, then there exists i and J such that $a \equiv (-1)^i 5^J \ (mod\ 2^\alpha)$. The values of i and J are uniquely determined $(mod\ 2)$ and ($(mod\ 2^{\alpha-2})$), respectively.

Corollary 2.44:
Suppose $\alpha \geq 3$ and that a is odd.
If n is odd, then the congruence $x^n \equiv a \ (mod\ 2^\alpha)$ has exactly one solution.
If n is even, then choose β such that $(n, 2^{\alpha-2}) = 2^\beta$. The congruence $x^n \equiv a \ (mod\ 2^\alpha)$ has $2^{\beta+1}$ solutions or no solutions according as $a \equiv 1 \ (mod\ 2^{\beta+2})$ or not.

3 Quadratic Reciprocity and Quadratic Forms

3.1 Quadratic Residues

Definition 3.1: Quadratic Residue
For all a such that $(a, m) = 1$, a is called a quadratic residue modulo m if the congruence $x^2 \equiv a \ (mod\ m)$ has a solution. If it has no solution, then a is called a quadratic non-residue modulo m.

e.g.
The quadratic residues modulo 5 are 1 and 4. The non-residues are 2 and 3.

Definition 3.2: Legendre Symbol
If p denotes an odd prime, then the legrende symbol $\left(\frac{a}{p}\right)$ is defined by

$$\left(\frac{a}{p}\right) = 1 \text{ iff a is a quadratic residue}$$

$$\left(\frac{a}{p}\right) = -1 \text{ iff a is a quadratic nonresidue}$$

$$\left(\frac{a}{p}\right) = 0 \text{ iff } a|p$$

Theorem 3.1:
Let p be an odd prime. Then

- $\left(\frac{a}{p}\right) \equiv a^{\frac{(p-1)}{2}} \ (mod\ p)$
- $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$
- $a \equiv b \ (mod\ p) \leftarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
- If $(a,p) = 1 \leftarrow \left(\frac{a^2}{p}\right) = 1,\ \left(\frac{a^2b}{p}\right) = \left(\frac{b}{p}\right)$
- $\left(\frac{1}{p}\right) = 1,\ \left(\frac{-1}{p}\right) = (-1)^{\frac{(p-1)}{2}}$

Remark:
p odd prime, then for $a \in \mathbb{Z}$ the number of solutions of $x^2 \equiv a \ (mod\ p)$ is $1 + \left(\frac{1}{p}\right)$.

Proof:
If $p|a$, then part(1) is obvious. If $(a,p) = 1$ then part(1) follows from Euler's criterion (Corollary 2.38). The remaining parts are all simple consequences of part(1)

Theorem 3.2: Lemma of Gauss
Let p be an odd prime and $(a,p) = 1$. Consider the integers $a, 2a, 3a, ..., \frac{p-1}{2}a$ and their least positive residues modulo p. If n denotes the number of these residues that exceeds $\frac{p}{2}$, then $\left(\frac{a}{p}\right) = (-1)^n$

Proof: Theorem 3.2
Let $r_1, r_2, ..., r_n$ denote the number of residues that exceeds $\frac{p}{2}$ and let $s_1, s_2, ..., s_k$ denote the remaining ones. The r_i and s_i are all distinct and none are zero. Furthermore, $n + k = \frac{p-1}{2}$. Now $0 < p - r_i < \frac{p}{2}$, i.e. $1, 2, ..., n$ and the numbers $p - r_i$ are distinct. Also, no $p - r_i$ is an s_j for if $p - r_i = s_j$ then $r_i \equiv a$.....

Theorem 3.3:

If p is an odd prime and $(a, 2p) = 1$, then

$$\left(\frac{a}{p}\right) = (-1)^t \text{ where } t = \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right]$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

3.2 Quadratic Reciprocity

Theorem 3.4:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \tag{50}$$

Note: If p and q are distinct odd primes of the form $4k + 3$, then one of the congruences $x^2 \equiv p \ (mod\ q)$ or $x^2 \equiv q \ (mod\ p)$ is a solutions and the other is not. However, if at least one of the primes is of the for $4k + 3$, then both congruences are soluable or both are not.

Proof: Theorem 3.4
Let S be the set of pairs of of integers (x, y) such that $1 \leq x \leq \frac{p-1}{2}$ and $1 \leq y \leq \frac{q-1}{2}$.

The set S has $\frac{(p-1)(q-1)}{4}$ elements. Seperate this set into two mutually exclusive subsets S_1 and S_2 according $qx > py$ or $qx < py$. Note that there are no pairs $(x, y) \in S$ such that $qx = py$.

The set S_1 can be described as the set of all pairs (x, y) such that

$$1 \leq x \leq \frac{p-1}{2}, \quad 1 \leq y \leq \frac{qx}{p} \tag{51}$$

The number of pairs in S_1 is

$$\sum_{x=1}^{\frac{p-1}{2}} [\frac{qx}{p}] \tag{52}$$

Similarly for S_2 the number of pairs in S_2 is

$$\sum_{y=1}^{\frac{p-1}{2}} [\frac{qy}{p}] \tag{53}$$

Thus we have:

$$\sum_{j=1}^{\frac{p-1}{2}}[\frac{qj}{p}]+\sum_{j=1}^{\frac{q-1}{2}}[\frac{pj}{q}] \tag{54}$$

$$=\frac{p-1}{2}\frac{q-1}{2} \tag{55}$$

and hence

$$\frac{p}{q}\frac{q}{p}=(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \tag{56}$$

Example: Compute $(\frac{42}{61})$

...

3.3 The Jacobi Symbol

3.4 Binary Quadratic Forms

3.5 Sums of Two Squares