Introduction to Analytic Number Theory

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 500

1. Congruences
   - Definition and Basic Properties of Congruences
   - Residue Classes and Complete Residue Systems
   - Linear Congruences
   - Reduced Residue Systems and the Euler-Fermat Theorem
   - Polynomial Congruences Modulo p. Lagrange's Theorem
   - Applications of Lagrange's Theorem
   - Simultaneous Linear Congruences. Chinese Remainder Theorem
   - Applications of the Chinese Remainder Theorem
   - Polynomial Congruences with Prime Power Moduli
   - Cross-Classification or Inclusion-Exclusion
   - A Decomposition Property of Reduced Residue Systems

Subsection 1

Definition and Basic Properties of Congruences

Congruence Modulo a Positive Integer

- Unless otherwise indicated, small latin and Greek letters will denote integers (positive, negative or zero).

Definition

Given integers a, b, m, with $m > 0$, we say that a is **congruent to** b **modulo** m, and we write

$$a \equiv b \pmod{m},$$

if m divides the difference $a - b$. The number m is called the **modulus** of the congruence.
In other words, the congruence $a \equiv b \pmod{m}$ is equivalent to the divisibility relation

$$m \mid (a - b).$$

Remarks

- According to the definition,

$$a \equiv 0 \pmod{m} \quad \text{if, and only if,} \quad m \mid a.$$

- Hence,

$$a \equiv b \pmod{m} \quad \text{if, and only if,} \quad a - b \equiv 0 \pmod{m}.$$

- If $m \nmid (a - b)$, we write

$$a \not\equiv b \pmod{m}$$

and say that a and b are **incongruent** mod m.

Examples

1. $19 \equiv 7 \pmod{12}$, $1 \equiv -1 \pmod{2}$, $3^2 \equiv -1 \pmod{5}$.
2. n is even if, and only if, $n \equiv 0 \pmod{2}$.
3. n is odd if, and only if, $n \equiv 1 \pmod{2}$.
4. $a \equiv b \pmod{1}$, for every a and b.
5. If $a \equiv b \pmod{m}$, then $a \equiv b \pmod{d}$, when $d \mid m$, $d > 0$.

Equivalence Property of Congruences

- The symbol $\equiv$ was chosen by Gauss to suggest analogy with $=$.
- Congruences possess many of the formal properties of equations.

Theorem

Congruence is an equivalence relation. That is, we have:

(a) $a \equiv a \pmod{m}$ (**reflexivity**);

(b) $a \equiv b \pmod{m}$ implies $b \equiv a \pmod{m}$ (**symmetry**);

(c) $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ imply $a \equiv c \pmod{m}$ (**transitivity**).

- The proofs follow from the following properties of divisibility:
  (a) $m \mid 0$.
  (b) If $m \mid (a-b)$, then $m \mid (b-a)$.
  (c) If $m \mid (a-b)$ and $m \mid (b-c)$, then $m \mid (a-b)+(b-c)=a-c$.

Algebraic Congruence Property of Congruences

Theorem

If $a \equiv b \pmod{m}$ and $\alpha \equiv \beta \pmod{m}$, then we have:

(a) $ax + \alpha y \equiv bx + \beta y \pmod{m}$, for all integers x and y;

(b) $a\alpha \equiv b\beta \pmod{m}$;

(c) $a^n \equiv b^n \pmod{m}$, for every positive integer n;

(d) $f(a) \equiv f(b) \pmod{m}$, for every polynomial f with integer coefficients.

(a) By hypothesis, $m \mid (a-b)$ and $m \mid (\alpha - \beta)$.
Therefore, $m \mid x(a-b) + y(\alpha-\beta) = (ax+\alpha y) - (bx + \beta y)$.

(b) We have $a\alpha - b\beta = \alpha(a-b) + b(\alpha - \beta) \equiv 0 \pmod{m}$ by Part (a).

(c) Take $\alpha = a$ and $\beta = b$ in Part (b) and use induction on n.

(d) Use the preceding parts and induction on the degree of f.

Example: Test for Divisibility by 9

Claim: An integer $n > 0$ is divisible by 9 if, and only if, the sum of its digits in its decimal expansion is divisible by 9.

This property is easily proved using congruences.

If the digits of n in decimal notation are $a_0, a_1, \ldots, a_k$, then

$$n = a_0 + 10a_1 + 10^2 a_2 + \cdots + 10^k a_k.$$

Using the preceding theorem, we have, modulo 9,

$$10 \equiv 1, \quad 10^2 \equiv 1, \ldots, 10^k \equiv 1 \pmod{9}.$$

So

$$n \equiv a_0 + a_1 + \cdots + a_k \pmod{9}.$$

- Note that all these congruences hold modulo 3 as well. So a number is divisible by 3 if, and only if, the sum of its digits is divisible by 3.

Example: The Fermat Numbers

- The Fermat numbers are $F_n = 2^{2^n} + 1$.

  The first five are primes:

  $$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65,537.$$

  We show that F_5 is divisible by 641 without explicitly calculating F_5.

  We consider the successive powers 2^{2^n} modulo 641. We have

  $$2^2 = 4,\ 2^4 = 16,\ 2^8 = 256,\ 2^{16} = 65,536 \equiv 154 \pmod{641}.$$

  So

  $$2^{32} \equiv (154)^2 = 23,716 \equiv 640 \equiv -1 \pmod{641}.$$

  Therefore, $F_5 = 2^{32} + 1 \equiv 0 \pmod{641}$.

  So F_5 is composite.

Cancelations In General

- Common nonzero factors cannot always be canceled from both members of a congruence as they can in equations.

  Example: Consider the congruence

  $$48 \equiv 18 \pmod{10}.$$

  Both sides are divisible by 6.

  But, if we cancel the common factor 6, we get an incorrect result,

  $$8 \equiv 3 \pmod{10}.$$

Cancelations Given Divisibility of the Modulus

- A common factor can be canceled if the modulus is also divisible by this factor.

Theorem

If $c > 0$, then

$$a \equiv b \pmod{m} \quad \text{if, and only if,} \quad ac \equiv bc \pmod{mc}.$$

- We have

$$m \mid (b-a) \quad \text{if, and only if,} \quad cm \mid c(b-a).$$

Cancelation Law

- The next theorem describes a cancelation law which can be used when the modulus is not divisible by the common factor.

Theorem (Cancelation Law)

If $ac \equiv bc \pmod{m}$ and if $d = (m, c)$, then

$$a \equiv b \pmod{\frac{m}{d}}.$$

In other words, a common factor c can be canceled provided the modulus is divided by $d = (m, c)$. In particular, a common factor which is relatively prime to the modulus can always be canceled.

- Since $ac \equiv bc \pmod{m}$, we have $m \mid c(a - b)$. So $\frac{m}{d} \mid \frac{c}{d}(a - b)$. But $(\frac{m}{d}, \frac{c}{d}) = 1$. Hence $\frac{m}{d} \mid (a - b)$.

Consequences of Congruence

Theorem

Assume $a \equiv b \pmod{m}$. If $d \mid m$ and $d \mid a$, then $d \mid b$.

- It suffices to assume $d > 0$.

  If $d \mid m$, then $a \equiv b \pmod{m}$ implies $a \equiv b \pmod{d}$.

  If $d \mid a$, then $a \equiv 0 \pmod{d}$.

  We conclude that $b \equiv 0 \pmod{d}$.

More Consequences of Congruence

Theorem

If $a \equiv b \pmod{m}$, then $(a, m) = (b, m)$. In other words, numbers which are congruent mod m have the sane gcd with m.

- Let $d = (a, m)$ and $e = (b, m)$.

  Then $d \mid m$ and $d \mid a$. So $d \mid b$. Hence $d \mid e$.

  Similarly, $e \mid m, e \mid b$. So $e \mid a$. Hence $e \mid d$.

  So $d = e$.

Theorem

If $a \equiv b \pmod{m}$ and if $0 \leq |b - a| < m$, then $a = b$.

- Since $m \mid (a - b)$, we have $m \leq |a - b|$ unless $a - b = 0$.

Even More Consequences of Congruence

Theorem

We have $a \equiv b \pmod{m}$ if and only if a and b give the same remainder when divided by m.

- Write $a = mq + r$, $b = mQ + R$, where $0 \leq r < m$ and $0 \leq R < m$.
  Then $a - b \equiv r - R \pmod{m}$ and $0 \leq |r - R| < m$.
  Now use the preceding theorem.

Theorem

If $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$, where $(m, n) = 1$, then $a \equiv b \pmod{mn}$.

- By hypothesis, both m and n divide $a - b$.
  Since $(m, n) = 1$, so does their product.

Subsection 2

Residue Classes and Complete Residue Systems

Residue Classes Modulo m

Definition

Consider a fixed modulus $m > 0$. We denote by $\widehat{a}$ the set of all integers x, such that $x \equiv a \pmod{m}$ and we call $\widehat{a}$ the **residue class** a **modulo** m.

- Thus, $\widehat{a}$ consists of all integers of the form $a + mq$, where $q = 0, \pm 1, \pm 2, \ldots,$

$$\widehat{a} = \{a + mq : q = 0, \pm 1, \pm 2, \ldots\}.$$

Properties of Residue Classes

Theorem

For a given modulus m we have:

(a) $\widehat{a} = \widehat{b}$ if, and only if, $a \equiv b \pmod{m}$.

(b) Two integers x and y are in the same residue class if, and only if, $x \equiv y \pmod{m}$.

(c) The m residue classes $\widehat{1}, \widehat{2}, \ldots, \widehat{m}$ are disjoint and their union is the set of all integers.

- Parts (a) and (b) follow at once from the definition.

(c) Note that the numbers $0, 1, 2, ..., m-1$ are incongruent modulo m.
Hence, by Part (b), the residue classes $\widehat{0}, \widehat{1}, \ldots, \widehat{m-1}$ are disjoint.
Now, for every integer x, $x = qm + r$, where $0 \leq r < m$.
So $x \equiv r \pmod{m}$. Hence, $x \in \widehat{r}$.
Since $\widehat{0} = \widehat{m}$, this proves Part (c).

Complete Residue Systems

Definition

A set of m representatives, one from each of the residue classes $\widehat{1}, \widehat{2}, \ldots, \widehat{m}$, is called a **complete residue system modulo** m.

Example: Any set consisting of m integers, incongruent mod m, is a complete residue system mod m.

For example, the following are complete residue systems mod m:

- $\{1, 2, \ldots, m\}$;
- $\{0, 1, 2, \ldots, m-1\}$;
- $\{1, m+2, 2m+3, 3m+4, \ldots, m^2\}$.

Another Complete Residue System

Theorem

Assume $(k, m) = 1$. If $\{a_1, \ldots, a_m\}$ is a complete residue system modulo m, so is $\{ka_1, \ldots, ka_m\}$.

- Suppose $ka_i \equiv ka_j \pmod{m}$.

  Since $(k, m) = 1$, $a_i \equiv a_j \pmod{m}$

  Thus, no two elements in $\{ka_1, \ldots, ka_m\}$ are congruent modulo m.

  But there are m elements in this set.

  So it forms a complete residue system.

Subsection 3

Linear Congruences

Polynomial Congruences

- Polynomial congruences deal with polynomials $f(x)$ with integer coefficients.
- The values of these polynomials are integers when x is an integer.
- An integer x satisfying a polynomial congruence

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

  is called a **solution** of the congruence.
- If $x \equiv y \pmod{m}$, then $f(x) \equiv f(y) \pmod{m}$.
- So every congruence having one solution has infinitely many.
- For this reason, we adopt the convention that solutions belonging to the same residue class will not be counted as distinct.

Number of Solutions of Polynomial Congruences

- When we speak of the number of solutions of a congruence we shall mean the number of incongruent solutions.
- That is, the number of solutions contained in the set $\{1, 2, \ldots, m\}$ or in any other complete residue system modulo m.
- Therefore, every polynomial congruence modulo m has at most m solutions.

Examples

Example: The linear congruence $2x \equiv 3 \pmod 4$ has no solutions.

Note that $2x - 3$ is odd, for every x.

Therefore it cannot be divisible by 4.

Example: The quadratic congruence

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

has exactly four solutions.

They are given by

$$x \equiv 1, 3, 5, 7 \pmod 8.$$

Linear Congruences: Sufficient Condition

Theorem

Assume $(a, m) = 1$. Then the linear congruence

$$ax \equiv b \pmod{m}$$

has exactly one solution.

- We need only test the numbers $1, 2, \ldots, m$, since they constitute a complete residue system. Form the products $a, 2a, \ldots, ma$.

  Since $(a, m) = 1$, they constitute a complete residue system.

  Hence, exactly one of these products is congruent to b modulo m.

  That is, there is exactly one x satisfying the given congruence.

Comments

- The theorem tells us that the linear congruence
$$ax \equiv b \pmod{m}$$
has a unique solution, if $(a, m) = 1$.
- However, it does not tell us how to determine this solution.
- If $(a, m) = 1$, the unique solution of the congruence
$$ax \equiv 1 \pmod{m}$$
is called the **reciprocal** of a modulo m.
- If $(a, m) = 1$ and a' is the reciprocal of a, then ba' is the unique solution of
$$ax \equiv b \pmod{m}.$$

Linear Congruences: Necessary and Sufficient Condition

Theorem

Assume $(a, m) = d$. Then the linear congruence

$$ax \equiv b \pmod{m}$$

has solutions if, and only if, $d \mid b$.

- Suppose a solution x exists.
  Then, for some k, $b = ax + km$.
  Since $d \mid a$ and $d \mid m$, we get $d \mid b$.
  Conversely, suppose $d \mid b$. Then, $(\frac{a}{d}, \frac{m}{d}) = 1$.
  It follows that the congruence

  $$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$$

  has a solution. This solution is also a solution of $ax \equiv b \pmod{m}$.

Linear Congruences: Number of Solutions

Theorem

Assume $(a, m) = d$ and suppose that $d \mid b$. Then the linear congruence

$$ax \equiv b \pmod{m}$$

has exactly d solutions modulo m. These are given by

$$t, t + \frac{m}{d}, t + 2\frac{m}{d}, \ldots, t + (d-1)\frac{m}{d},$$

where t is the solution, unique modulo $\frac{m}{d}$, of the linear congruence

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}.$$

Linear Congruences: Number of Solutions (Cont'd)

- Every solution of the last equation is also a solution of the first.

  Conversely, every solution of the first satisfies the last.

  Now the d numbers listed are solutions of the last.

  So they are also solutions of the first.

  We show that no two of these are congruent modulo m.

  Suppose
  $$t + r\frac{m}{d} \equiv t + s\frac{m}{d} \pmod{m},$$
  with $0 \leq r < d$, $0 \leq s < d$.

  Then $r\frac{m}{d} \equiv s\frac{m}{d} \pmod{m}$.

  Hence, $r \equiv s \pmod{d}$.

  But $0 \leq |r - s| < d$.

  So $r = s$.

Linear Congruences: Number of Solutions (Cont'd)

- It remains to show that the first equation has no solutions except those listed.

  Suppose y is a solution of $ax \equiv b \pmod{m}$.

  Then $ay \equiv at \pmod{m}$.

  So $y \equiv t \pmod{\frac{m}{d}}$.

  Hence, $y = t + k\frac{m}{d}$, for some k.

  But $k \equiv r \pmod{d}$, for some r satisfying $0 \leq r < d$.

  Thus,
$$k\frac{m}{d} \equiv r\frac{m}{d} \pmod{m}.$$

  So $y \equiv t + r\frac{m}{d} \pmod{m}$.

  Hence, y is congruent modulo m to one of the numbers in the list.

Greatest Common Divisor and Congruences

Theorem

If $(a, b) = d$, there exist integers x and y, such that

$$ax + by = d.$$

- The linear congruence $ax \equiv d \pmod{b}$ has a solution.

  Hence, there is an integer y, such that

  $$d - ax = by.$$

  This gives $ax + by = d$, as required.

  Note: Geometrically, the pairs (x, y) satisfying $ax + by = d$ are lattice points lying on a straight line.

  The x-coordinate of each of these points is a solution of the congruence $ax \equiv d \pmod{b}$.

Subsection 4

Reduced Residue Systems and the Euler-Fermat Theorem

Reduced Residue Systems

Definition

By a **reduced residue system modulo** m we mean any set of $\varphi(m)$ integers, incongruent modulo m, each of which is relatively prime to m.

Theorem

If $\{a_1, a_2, \ldots, a_{\varphi(m)}\}$ is a reduced residue system modulo m and if $(k, m) = 1$, then $\{ka_1, ka_2, \ldots, ka_{\varphi(m)}\}$ is also a reduced residue system modulo m.

- No two of the numbers ka_i are congruent modulo m.

  Also, since $(a_i, m) = (k, m) = 1$, we have $(ka_i, m) = 1$.

  So each ka_i is relatively prime to m.

Euler-Fermat Theorem

Theorem (Euler-Fermat Theorem)

Assume $(a, m) = 1$. Then we have

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

- Let $\{b_1, b_2, \ldots, b_{\varphi(m)}\}$ be a reduced residue system modulo m.

  Then $\{ab_1, ab_2, \ldots, ab_{\varphi(m)}\}$ is also a reduced residue system.

  Hence the product of all the integers in the first set is congruent to the product of those in the second set. Therefore,

  $$b_1 \cdots b_{\varphi(m)} \equiv a^{\varphi(m)} b_1 \cdots b_{\varphi(m)} \pmod{m}.$$

  Each b_i is relatively prime to m.

  So we can cancel each b_i to obtain the theorem.

A Consequence

Theorem

If a prime p does not divide a, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

- For p a prime, $\varphi(p) = p - 1$.

  So , by the theorem,

$$a^{p-1} \equiv 1 \pmod{p}.$$

Little Fermat Theorem

Theorem (Little Fermat Theorem)

For any integer a and any prime p, we have

$$a^p \equiv a \pmod{p}.$$

- If $p \nmid a$, this is the preceding theorem.

  If $p \mid a$, then both a^p and a are congruent to $0 \pmod{p}$.

Linear Congruences

Theorem

If $(a, m) = 1$, the solution (unique mod m) of the linear congruence

$$ax \equiv b \pmod{m}$$

is given by

$$x \equiv ba^{\varphi(m)-1} \pmod{m}.$$

- By the Euler-Fermat Theorem,

$$a \cdot ba^{\varphi(m)-1} = ba^{\varphi(m)} \equiv b \pmod{m}.$$

  So the number x given satisfies the linear congruence.

  The solution is unique mod m, since $(a, m) = 1$.

Example

- Solve the congruence $5x \equiv 3 \pmod{24}$.

  Since $(5, 24) = 1$, there is a unique solution.

  Note that
  $$\varphi(24) = \varphi(3)\varphi(8) = 2 \cdot 4 = 8.$$

  Using the preceding theorem,
  $$x \equiv 3 \cdot 5^{\varphi(24)-1} \equiv 3 \cdot 5^7 \pmod{24}.$$

  Modulo 24 we have $5^2 \equiv 1$, and $5^4 \equiv 5^6 \equiv 1$.

  So, $5^7 \equiv 5$.

  So $x \equiv 15 \pmod{24}$.

Example

- Solve the congruence $25x \equiv 15 \pmod{120}$.

  Note that $d = (25, 120) = 5$ and $d \mid 15$.

  So the congruence has exactly five solutions modulo 120.

  To find them we divide by 5 and solve the congruence

$$5x \equiv 3 \pmod{24}.$$

  Using the preceding example and a previous theorem, we find that the five solutions are given by

$$x \equiv 15 + 24k, \quad k = 0, 1, 2, 3, 4.$$

  These are

$$x \equiv 15, 39, 63, 87, 111 \pmod{120}.$$

Subsection 5

Polynomial Congruences Modulo p. Lagrange's Theorem

Number of Solutions of a Polynomial Congruence

- The fundamental theorem of algebra states that, for every polynomial f of degree $n \geq 1$, the equation $f(x) = 0$ has n solutions among the complex numbers.
- There is no direct analog of this theorem for polynomial congruences.
  - Some linear congruences have no solutions;
  - Some have exactly one solution;
  - Some have more than one.
- Thus, even in this special case, there appears to be no simple relation between the number of solutions and the degree of the polynomial.
- For congruences modulo a prime there exists a theorem of Lagrange on the number of solutions.

Lagrange's Theorem

Theorem (Lagrange)

Given a prime p, let

$$f(x) = c_0 + c_1 x + \cdots + c_n x^n$$

be a polynomial of degree n with integer coefficients, such that $c_n \not\equiv 0 \pmod{p}$. Then the polynomial congruence

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

has at most n solutions.

Note: This result is not true for composite moduli.

Example: Consider the quadratic congruence $x^2 \equiv 1 \pmod{8}$.

It has 4 solutions, $1, 3, 5, 7 \pmod{8}$.

Proof of Lagrange's Theorem

- We use induction on n, the degree of f.

  When $n = 1$ the congruence is linear, $c_1 x + c_0 \equiv 0 \pmod{p}$.

  By hypothesis, $c_1 \not\equiv 0 \pmod{p}$. So $(c_1, p) \equiv 1$.

  We know that, then, there is exactly one solution.

  Assume that the theorem holds for polynomials of degree $n - 1$.

  Suppose, towards a contradiction, that the congruence $f(x) \equiv 0 \pmod{p}$ has $n + 1$ incongruent solutions modulo p.

  Say $x_0, x_1, \ldots, x_n$ are such that, for all $k = 0, 1, \ldots, n$,

$$f(x_k) \equiv 0 \pmod{p}.$$

Proof of Lagrange's Theorem (Cont'd)

- We have the algebraic identity

$$f(x) - f(x_0) = \sum_{r=1}^{n} c_r(x^r - x_0^r) = (x - x_0)g(x),$$

where $g(x)$ is a polynomial of degree $n-1$ with integer coefficients and with leading coefficient c_n.

But $f(x_k) \equiv f(x_0) \equiv 0 \pmod{p}$.

Therefore,

$$f(x_k) - f(x_0) = (x_k - x_0)g(x_k) \equiv 0 \pmod{p}.$$

Now, for $k \neq 0$, $x_k - x_0 \not\equiv 0 \pmod{p}$.

So we must have $g(x_k) \equiv 0 \pmod{p}$, for each $k \neq 0$.

This means that the congruence $g(x) \equiv 0 \pmod{p}$ has n incongruent solutions modulo p, contradicting the induction hypothesis.

Subsection 6

Applications of Lagrange's Theorem

Multitude of Roots

Theorem

If $f(x) = c_0 + c_1x + \cdots + c_nx^n$ is a polynomial of degree n with integer coefficients, and if the congruence

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

has more than n solutions, where p is prime, then every coefficient of f is divisible by p.

- Suppose there is some coefficient not divisible by p.
  Let c_k be the one with largest index.
  Then $k \leq n$ and the congruence

  $$c_0 + c_1x + \cdots + c_kx^k \equiv 0 \pmod{p}$$

  has more than k solutions.
  So, by Lagrange's Theorem, $p \mid c_k$, a contradiction.

A Special Polynomial

Theorem (Special Polynomial Theorem)

For any prime p, all the coefficients of the polynomial

$$f(x) = (x-1)(x-2)\cdots(x-p+1) - x^{p-1} + 1$$

are divisible by p.

- Let $g(x) = (x-1)(x-2)\cdots(x-p+1)$. The roots of g are the numbers $1, 2, \ldots, p-1$. Hence they satisfy the congruence

$$g(x) \equiv 0 \pmod{p}.$$

By the Euler-Fermat Theorem, these numbers also satisfy the congruence $h(x) \equiv 0 \pmod{p}$, where $h(x) = x^{p-1} - 1$.
The difference, $f(x) = g(x) - h(x)$ has degree $p-2$ but the congruence $f(x) \equiv 0 \pmod{p}$ has $p-1$ solutions, $1, 2, \ldots, p-1$.
By the preceding theorem, each coefficient of $f(x)$ is divisible by p.

Wilson's Theorem

Theorem (Wilson's Theorem)

For any prime p we have

$$(p-1)! \equiv -1 \pmod{p}.$$

- The constant term of the polynomial

$$f(x) = (x-1)(x-2)\cdots(x-p+1) - x^{p-1} + 1$$

  in the preceding theorem is $(p-1)! + 1$.

  Note: The converse of Wilson's theorem also holds:

$$\text{If } n > 1 \text{ and } (n-1)! \equiv -1 \pmod{n}, \text{ then } n \text{ is prime.}$$

Wolstenholme's Theorem

Theorem (Wolstenholme's Theorem)

For any prime $p \geq 5$, we have

$$\sum_{k=1}^{p-1} \frac{(p-1)!}{k} \equiv 0 \pmod{p^2}.$$

- The sum $\sum_{k=1}^{p-1} \frac{(p-1)!}{k}$ is the sum of the products of the numbers $1, 2, \ldots, p-1$ taken $p-2$ at a time.

  It is also equal to the coefficient of $-x$ in

  $$g(x) = (x-1)(x-2)\cdots(x-p+1).$$

Wolstenholme's Theorem (Cont'd)

- The polynomial $g(x) = (x-1)(x-2)\cdots(x-p+1)$ can be written in the form

  $$g(x) = x^{p-1} - S_1 x^{p-2} + S_2 x^{p-3} - \cdots + S_{p-3}x^2 - S_{p-2}x + (p-1)!,$$

  where S_k is the k-th elementary symmetric function of the roots.

  That is, S_k is the sum of the products of the numbers $1, 2, \ldots, p-1$, taken k at a time.

  By the Special Polynomial Theorem, each of $S_1, S_2, \ldots, S_{p-2}$ is divisible by p.

Wolstenholme's Theorem (Cont'd)

- We wish to show that S_{p-2} is divisible by p^2.
  The product for $g(x) = (x-1)(x-2)\cdots(x-p+1)$ shows that
  $$g(p) = (p-1)!.$$
  So
  $$(p-1)! = p^{p-1} - S_1 p^{p-2} + \cdots + S_{p-3}p^2 - S_{p-2}p + (p-1)!.$$
  Canceling $(p-1)!$, we get
  $$p^{p-1} - S_1 p^{p-2} + \cdots + S_{p-3}p^2 - S_{p-2}p = 0.$$
  Reducing the equation mod p^3 we get, since $p \geq 5$,
  $$pS_{p-2} \equiv 0 \pmod{p^3}.$$
  Hence $S_{p-2} \equiv 0 \pmod{p^2}$.

Subsection 7

Simultaneous Linear Congruences. Chinese Remainder Theorem

Systems of Linear Congruences

- A system of two or more linear congruences need not have a solution, even though each individual congruence has a solution.

  Example: Consider the system

  $$\begin{array}{rcll} x & \equiv & 1 & \pmod{2} \\ x & \equiv & 0 & \pmod{4} \end{array}$$

  Each of these equations has a solution.

  However, there is no x simultaneously satisfying both.
- Note that the moduli 2 and 4 are not relatively prime.
- We will prove that any system of two or more linear congruences which can be solved separately with unique solutions can also be solved simultaneously, if the moduli are relatively prime in pairs.

The Chinese Remainder Theorem

Theorem (Chinese Remainder Theorem)

Assume $m_1, \ldots, m_r$ are positive integers, relatively prime in pairs, $(m_i, m_k) = 1$, if $i \neq k$. Let $b_1, \ldots, b_r$ be arbitrary integers. Then the system of congruences

$$\begin{array}{rcll} x & \equiv & b_1 & \pmod{m_1} \\ & \vdots & & \\ x & \equiv & b_r & \pmod{m_r} \end{array}$$

has exactly one solution modulo the product $m_1 \cdots m_r$.

- Let $M = m_1 \cdots m_r$ and set $M_k = \frac{M}{m_k}$.
  Since the m_i's are relatively prime in pairs, $(M_k, m_k) = 1$.
  So each M_k has a unique reciprocal M_k' modulo m_k.

The Chinese Remainder Theorem (Cont'd)

- Let
$$x = b_1 M_1 M_1' + b_2 M_2 M_2' + \cdots + b_r M_r M_r'.$$
Consider each term in this sum modulo m_k.
If $i \neq k$, $M_i \equiv 0 \pmod{m_k}$.
So we have
$$x \equiv b_k M_k M_k' \equiv b_k \pmod{m_k}.$$
Hence, x satisfies every congruence in the system.
Claim: The system has only one solution mod M.
Suppose x and y are two solutions of the system.
Then we have $x \equiv y \pmod{m_k}$, for each k.
But the m_k are relatively prime in pairs.
So we also have $x \equiv y \pmod{M}$.

Extension of the Chinese Remainder Theorem

Theorem

Assume $m_1, \ldots, m_r$ are relatively prime in pairs. Let $b_1, \ldots, b_r$ be arbitrary integers and let $a_1, \ldots, a_r$ satisfy $(a_k, m_k) = 1$, for $k = 1, 2, \ldots, r$. Then the linear system of congruences

$$\begin{aligned} a_1 x &\equiv b_1 \pmod{m_1} \\ &\vdots \\ a_r x &\equiv b_r \pmod{m_r} \end{aligned}$$

has exactly one solution modulo $m_1 m_2 \cdots m_r$.

- Since $(a_k, m_k) = 1$, a_k has a reciprocal a'_k modulo m_k.
  Then $a_k x \equiv b_k \pmod{m_k}$ is equivalent to $x \equiv b_k a'_k \pmod{m_k}$.
  Now apply the Chinese Remainder Theorem.

Subsection 8

Applications of the Chinese Remainder Theorem

Polynomial Congruences With Composite Moduli

Theorem

Let f be a polynomial with integer coefficients. Let $m_1, m_2, \ldots, m_r$ be positive integers relatively prime in pairs. Let $m = m_1 m_2 \ldots m_r$. Then the congruence

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

has a solution if, and only if, each of the congruences

$$f(x) \equiv 0 \pmod{m_i}, \quad i = 1, 2, \ldots, r,$$

has a solution. Moreover, if $v(m)$ and $v(m_i)$ denote the number of solutions, respectively, then

$$v(m) = v(m_1) v(m_2) \cdots v(m_r).$$

Polynomial Congruences With Composite Moduli (Cont'd)

- If $f(a) \equiv 0 \pmod{m}$, then $f(a) \equiv 0 \pmod{m_i}$, for each i.

  Hence, every solution of $f(x) \equiv 0 \pmod{m}$ is also a solution of $f(x) \equiv 0 \pmod{m_i}$.

  Conversely, let a_i be a solution of $f(x) \equiv 0 \pmod{m_i}$.

  By the Chinese Remainder Theorem, there exists an integer a, such that

  $$a \equiv a_i \pmod{m_i}, \quad i = 1, 2, \ldots, r.$$

  So $f(a) \equiv f(a_i) \equiv 0 \pmod{m_i}$.

  But the moduli are relatively prime in pairs.

  So we also have $f(a) \equiv 0 \pmod{m}$.

  Therefore, if each of $f(x) \equiv 0 \pmod{m_i}$ has a solution, so does $f(x) \equiv 0 \pmod{m}$.

Polynomial Congruences With Composite Moduli (Cont'd)

- We also know, by a previous theorem, that each r-tuple of solutions $(a_1, \ldots, a_r)$ of the last congruences gives rise to a unique integer a mod m satisfying $a \equiv a_i \pmod{m_i}$, $i = 1, \ldots, r$.

  By hypothesis, each a_i runs through $v(m_i)$ solutions.

  So the number of integers a which satisfy these congruences, and hence the last congruence, is $v(m_1) \cdots v(m_r)$.

  Note: If m has the prime power decomposition at $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, we can take $m_i = p_i^{\alpha_i}$ in the theorem.

  So the problem of solving a polynomial congruence for a composite modulus is reduced to that for prime power moduli.

  Later we will show that the problem can be reduced further to polynomial congruences with prime moduli plus a set of linear congruences.

Lattice Points Visible from the Origin

Theorem

The set of lattice points in the plane visible from the origin contains arbitrarily large square gaps. That is, given any integer $k > 0$ there exists a lattice point (a, b), such that none of the lattice points

$$(a + r, b + s), \quad 0 < r \leq k,\ 0 < s \leq k,$$

is visible from the origin.

- Let $p_1, p_2, \ldots$, be the sequence of primes.
  Given $k > 0$, consider the $k \times k$ matrix whose entries consist of:
  - The first k primes in the first row;
  - The next k primes in the second row; etc.

  Let m_i be the product of the primes in the i-th row;

  Let M_i be the product of the primes in the i-th column.

  Then the numbers m_i are relatively prime in pairs, as are the M_i.

Lattice Points Visible from the Origin (Cont'd)

- Consider the set of congruences

$$\begin{array}{rcll} x & \equiv & -1 & \pmod{m_1} \\ x & \equiv & -2 & \pmod{m_2} \\ & \vdots & & \\ x & \equiv & -k & \pmod{m_k} \end{array}$$

This system has a solution a which is unique mod $m_1 \cdots m_k$. Similarly, the system

$$\begin{array}{rcll} y & \equiv & -1 & \pmod{M_1} \\ & \vdots & & \\ y & \equiv & -k & \pmod{M_k} \end{array}$$

has a solution b which is unique mod $M_1 \cdots M_k = m_1 \cdots m_k$.

Lattice Points Visible from the Origin (Conclusion)

- Consider the square with opposite vertices (a, b), $(a+k, b+k)$.
  Any lattice point inside this square has the form
  $$(a+r, b+s), \quad \text{where } 0 < r < k,\ 0 < s < k.$$
  Those points with $r = k$ or $s = k$ lie on the boundary of the square.
  Claim: No such point is visible from the origin.
  Consider the point $(a+r, b+s)$.
  We have $a \equiv -r \pmod{m_r}$ and $b \equiv -s \pmod{M_s}$.
  So the prime in the intersection of row r and column s divides both $a+r$ and $b+s$.
  Hence, $a+r$ and $b+s$ are not relatively prime.
  Therefore, the lattice point $(a+r, b+s)$ is not visible from the origin.

Subsection 9

Polynomial Congruences with Prime Power Moduli

Congruences Modulo a Prime Power

- We saw that the problem of solving a polynomial congruence

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

can be reduced to that of solving a system of congruences

$$f(x) \equiv 0 \pmod{p_i^{\alpha_i}}, \quad i = 1, 2, \ldots, r,$$

where $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$.
- In this section we show that the problem can be further reduced to congruences with prime moduli plus a set of linear congruences.

Remainders Generated from Solutions

- Let f be a polynomial with integer coefficients.
- Suppose that for some prime p and some $\alpha \geq 2$ the congruence

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

  has a solution, say $x = a$, where a is chosen so that it lies in the interval $0 \leq a < p^\alpha$.
- This solution also satisfies, for each $\beta < \alpha$, the congruences

$$f(x) \equiv 0 \pmod{p^\beta}.$$

- In particular, a satisfies $f(x) \equiv 0 \pmod{p^{\alpha-1}}$.
- Divide a by $p^{\alpha-1}$ and write

$$a = qp^{\alpha-1} + r, \quad 0 \leq r < p^{\alpha-1}.$$

- The remainder r is said to be **generated** by a.

Lifting Generated Remainders

- Since $r \equiv a \pmod{p^{\alpha-1}}$, r is a solution of $f(x) \equiv 0 \pmod{p^{\alpha-1}}$.
- In other words, every solution a of the congruence $f(x) \equiv 0 \mod p^{\alpha}$ in the interval $0 \leq a < p^{\alpha}$ generates a solution r of the congruence $f(x) \equiv 0 \pmod{p^{\alpha-1}}$ in the interval $0 \leq r < p^{\alpha-1}$.
- Suppose we start with a solution r of $f(x) \equiv 0 \pmod{p^{\alpha-1}}$ in the interval $0 \leq r < p^{\alpha-1}$.
- We ask whether there is a solution a of $f(x) \equiv 0 \mod p^{\alpha}$ in the interval $0 \leq a < p^{\alpha}$, which generates r.
- If this happens, we say that r can be **lifted** from $p^{\alpha-1}$ to p^{α}.
- The next theorem shows that the possibility of r being lifted depends on $f(r) \mod p^{\alpha}$ and on the derivative $f'(r) \mod p$.

Lifting of a Solution

Theorem

Assume $\alpha \geq 2$. Let r be a solution of the congruence

$$f(x) \equiv 0 \pmod{p^{\alpha-1}}$$

lying in the interval $0 \leq r < p^{\alpha-1}$.

(a) Assume $f'(r) \not\equiv 0 \pmod{p}$.
Then r can be lifted in a unique way from $p^{\alpha-1}$ to p^{α}.
That is, there is a unique a in the interval $0 \leq a < p^{\alpha}$, which generates r and satisfies the congruence

$$f(x) \equiv 0 \pmod{p^{\alpha}}.$$

Lifting of a Solution (Cont'd)

Theorem (Cont'd)

(b) Assume $f'(r) \equiv 0 \pmod{p}$.

Then we have two possibilities:

- (b_1) If $f(r) \equiv 0 \pmod{p^\alpha}$, r can be lifted from $p^{\alpha-1}$ to p^α in p distinct ways.
- (b_2) If $f(r) \not\equiv 0 \pmod{p^\alpha}$, r cannot be lifted from $p^{\alpha-1}$ to p^α.

- If n is the degree of f we have the identity (Taylor's formula)

$$f(x+h) = f(x) + f'(x)h + \frac{f''(x)}{2!}h^2 + \cdots + \frac{f^{(n)}(x)}{n!}h^n,$$

for every x and h.

We note that each polynomial $\frac{f^{(k)}(x)}{k!}$ has integer coefficients.

Lifting of a Solution (Cont'd)

- Take $x = r$, where r is a solution of $f(x) \equiv 0 \pmod{p^{\alpha-1}}$ in the interval $0 \leq r < p^{\alpha-1}$.

  Let $h = qp^{\alpha-1}$, where q is an integer to be specified.

  Since $\alpha \geq 2$, the terms involving h^2 and higher powers of h are integer multiples of p^α.

  Therefore,

  $$f(r + qp^{\alpha-1}) \equiv f(r) + f'(r)qp^{\alpha-1} \pmod{p^\alpha}.$$

  By hypothesis, $f(r) = kp^{\alpha-1}$, for some integer k.

  So the last congruence becomes

  $$f(r + qp^{\alpha-1}) \equiv \{qf'(r) + k\}p^{\alpha-1} \pmod{p^\alpha}.$$

Lifting of a Solution (Cases)

- We showed $f(r + qp^{\alpha-1}) \equiv \{qf'(r) + k\}p^{\alpha-1} \pmod{p^\alpha}$.
  Let $a = r + qp^{\alpha-1}$.
  Then a satisfies $f(x) \equiv 0 \pmod{p^\alpha}$ if, and only if, q satisfies the linear congruence $qf'(r) + k \equiv 0 \pmod{p}$.
  - Suppose $f'(r) \not\equiv 0 \pmod{p}$.
    Then $qf'(r) + k \equiv 0 \pmod{p}$ has a unique solution $q \mod p$.
    Choose q in the interval $0 \leq q < p$.
    Then $a = r + qp^{\alpha-1}$ satisfies $f(x) \equiv 0 \pmod{p^\alpha}$ and $0 \leq a < p^\alpha$.
  - Suppose $f'(r) \equiv 0 \pmod{p}$.
    Then $qf'(r) + k \equiv 0 \pmod{p}$ has a solution q if, and only if, $p \mid k$.
    Equivalently, if and only if $f(r) \equiv 0 \pmod{p^\alpha}$.
    - If $p \nmid k$, there is no choice of q to make a satisfy $f(x) \equiv 0 \pmod{p^\alpha}$.
    - If $p \mid k$, then the p values $q = 0, 1, \ldots, p-1$ give p solutions a of $f(x) \equiv 0 \pmod{p^\alpha}$ which generate r and lie in the interval $0 \leq a < p^\alpha$.

The Procedure for Determining Solutions

- We have a method for obtaining solutions of congruence $f(x) \equiv 0 \pmod{p^\alpha}$ if solutions of $f(x) \equiv 0 \pmod{p^{\alpha-1}}$ are known.
- We solve the congruence $f(x) \equiv 0 \pmod{p}$.
  - If the latter has no solutions, then the original has no solutions.
  - If the latter has solutions, we choose one, call it r, which lies in the interval $0 \leq r < p$. Corresponding to r, there will be 0, 1, or p solutions of the congruence $f(x) \equiv 0 \pmod{p^2}$, depending on the numbers $f'(r)$ and $k = \frac{f(r)}{p}$.
    - If $p \nmid k$ and $p \mid f'(r)$ then r cannot be lifted to a solution. In this case we begin anew with a different solution r. If no r can be lifted, then $f(x) \equiv 0 \pmod{p^2}$ has no solution.
    - If $p \mid k$ for some r, we examine the linear congruence $qf'(r) + k \equiv 0 \pmod{p}$. This has 1 or p solutions q according as $p \nmid f'(r)$ or $p \mid f'(r)$. For each solution q the number $a = r + qp$ gives a solution of $f(x) \equiv 0 \pmod{p^2}$.

For each such solution a similar procedure can be used to find all solutions of $f(x) \equiv 0 \pmod{p^3}$, and so on.

Subsection 10

Cross-Classification or Inclusion-Exclusion

Notation

- The principle of **cross-classification** or **inclusion-exclusion** is a formula which counts the number of elements of a finite set S which do not belong to certain prescribed subsets $S_1, \ldots, S_n$.
- If T is a subset of S, we write $N(T)$ for the number of elements of T.
- Denote by $S - T$ the set of those elements of S which are not in T.
- Thus, $S - \bigcup_{i=1}^{n} S_i$ consists of those elements of S which are not in any of the subsets $S_1, \ldots, S_n$.
- For brevity we write:
  - $S_i S_j$ for the intersection $S_i \cap S_j$;
  - $S_i S_j S_k$ for the intersection $S_i \cap S_j \cap S_k$;

  $\vdots$

Principle of Cross-Classification

Theorem (Principle of Cross-Classification)

If $S_1, \ldots, S_n$ are given subsets of a finite set S, then

$$N(S - \bigcup_{i=1}^n S_i) = N(S) - \sum_{1 \le i \le n} N(S_i) + \sum_{1 \le i < j \le n} N(S_i S_j) - \sum_{1 \le i < j < k \le n} N(S_i S_j S_k) + \cdots + (-1)^n N(S_1 S_2 \cdots S_n).$$

- If $T \subseteq S$ let $N_r(T)$ denote the number of elements of T which are not in any of the first r subsets $S_1, \ldots, S_r$.
  In this notation, $N_0(T)$ is simply $N(T)$.
  The elements enumerated by $N_{r-1}(T)$ fall into two disjoint sets, those which are not in S_r and those which are in S_r.
  Therefore we have $N_{r-1}(T) = N_r(T) + N_{r-1}(TS_r)$.
  Hence
  $$N_r(T) = N_{r-1}(T) - N_{r-1}(TS_r).$$

Principle of Cross-Classification (Cont'd)

- We obtained $N_r(T) = N_{r-1}(T) - N_{r-1}(TS_r)$.

  Now take $T = S$.

  Use the relation to express each term on the right in terms of N_{r-2}.

  We obtain

$$\begin{aligned} N_r(S) &= \{N_{r-2}(S) - N_{r-2}(SS_{r-1})\} - \{N_{r-2}(S_r) - N_{r-2}(S_r S_{r-1})\} \\ &= N_{r-2}(S) - N_{r-2}(S_{r-1}) - N_{r-2}(S_r) + N_{r-2}(S_r S_{r-1}). \end{aligned}$$

  Applying the previous equation, repeatedly we finally obtain

$$\begin{aligned} N_r(S) &= N_0(S) - \textstyle\sum_{i=1}^r N_0(S_i) + \sum_{1 \le i < j \le r} N_0(S_i S_j) \\ &\qquad - \cdots + (-1)^r N_0(S_1 \cdots S_r). \end{aligned}$$

  When $r = n$, this gives the required formula.

Example: Product Formula for Euler's Totient

- Let $p_1, \ldots, p_r$ denote the distinct prime divisors of n.
- Let $S = \{1, 2, \ldots, n\}$ and let S_k be the subset of S consisting of those integers divisible by p_k.
- The numbers in S relatively prime to n are those in none of the sets $S_1, \ldots, S_r$.
- It follows that

$$\varphi(n) = N(S - \cup_{k=1}^{r} S_k).$$

Example: Product Formula for Euler's Totient (Cont'd)

- If $d \mid n$, there are $\frac{n}{d}$ multiples of d in the set S.
- Hence:
  - $N(S_i) = \frac{n}{p_i}$;
  - $N(S_i S_j) = \frac{n}{p_i p_j}$;

    $\vdots$
  - $N(S_1 \cdots S_r) = \frac{n}{p_1 \cdots p_r}$.
- So the Cross-Classification Principle gives us

$$\begin{aligned} \varphi(n) &= n - \sum_{i=1}^{n} \frac{n}{p_i} + \sum_{1 \le i < j \le r} \frac{n}{p_i p_j} - \cdots + (-1)^r \frac{n}{p_1 \cdots p_r} \\ &= n \sum_{d \mid n} \frac{\mu(d)}{d} \\ &= n \prod_{p \mid n} \left(1 - \frac{1}{p}\right). \end{aligned}$$

Number of Elements in a Reduced Residue System

Theorem

Given integers r, d and k, such that $d \mid k$, $d > 0$, $k \geq 1$ and $(r, d) = 1$. Then the number of elements in the set

$$S = \left\{ r + td : t = 1, 2, \ldots, \frac{k}{d} \right\}$$

which are relatively prime to k is $\frac{\varphi(k)}{\varphi(d)}$.

- Suppose a prime p divides k and $r + td$.

  Then $p \nmid d$. Otherwise $p \mid r$, contradicting $(r, d) = 1$.

  Therefore, the primes which divide k and elements of S are those which divide k but do not divide d.

  Call them $p_1, \ldots, p_m$ and let $k' = p_1 p_2 \cdots p_m$.

Elements in a Reduced Residue System (Cont'd)

- Now the elements of S relatively prime to k are those not divisible by any of $p_1, \ldots, p_m$.

  Let
  $$S_i = \{x : x \in S \text{ and } p_i \mid x\}, \quad i = 1, 2, \ldots, m.$$

  If $x \in S_i$ and $x = r + td$, then $r + td \equiv 0 \pmod{p_i}$.

  Since $p_i \nmid d$, there is a unique t mod p_i with this property.

  Therefore, exactly one t in each of the intervals
  $$[1, p_i], [p_i + 1, 2p_i], \ldots, [(q-1)p_i + 1, qp_i],$$
  where $qp_i = \frac{k}{d}$, satisfies $r + td \equiv 0 \pmod{p_i}$.

  So $N(S_i) = \frac{k/d}{p_i}$.

Elements in a Reduced Residue System (Cont'd)

- Similarly, we obtain:
  - $N(S_iS_j) = \frac{k/d}{p_ip_j}$;

    $\vdots$
  - $N(S_1 \cdots S_m) = \frac{k/d}{p_1 \cdots p_m}$.

  Hence, by the Cross-Classification Principle, the number of integers in S which are relatively prime to k is

$$\begin{aligned} N(S - \bigcup_{i=1}^m S_i) &= \frac{k}{d} \sum_{\delta | k'} \frac{\mu(\delta)}{\delta} \\ &= \frac{k}{d} \prod_{p | k'} (1 - \frac{1}{p}) \\ &= \frac{k \prod_{p|k} (1 - \frac{1}{p})}{d \prod_{p|d} (1 - \frac{1}{p})} \\ &= \frac{\varphi(k)}{\varphi(d)}. \end{aligned}$$

Subsection 11

A Decomposition Property of Reduced Residue Systems

Example

- Let S be a reduced residue system mod 15, say
$$S = \{1, 2, 4, 7, 8, 11, 13, 14\}.$$
- We display the 8 elements of S in a 4×2 matrix as follows:
$$\begin{bmatrix} 1 & 2 \\ 4 & 8 \\ 7 & 11 \\ 13 & 14 \end{bmatrix}.$$
- Each row contains a reduced residue system mod 3.
- The numbers in each column are congruent to each other mod 3.
- Taking rows representing reduced systems modulo 5 and columns with numbers congruent modulo 5, we get
$$\begin{bmatrix} 1 & 2 & 4 & 8 \\ 11 & 7 & 14 & 13 \end{bmatrix}.$$

Decomposition Property of Reduced Residue Systems

Theorem

Let S be a reduced residue system mod k, and let $d > 0$ be a divisor of k. Then we have the following decompositions of S:

(a) S is the union of $\frac{\varphi(k)}{\varphi(d)}$ disjoint sets, each of which is a reduced residue system mod d.

(b) S is the union of $\varphi(d)$ disjoint sets, each of which consists of $\frac{\varphi(k)}{\varphi(d)}$ numbers congruent to each other mod d.

- First we prove that properties (a) and (b) are equivalent.
  - Suppose (b) holds. Display the $\varphi(k)$ elements of S as a matrix, using the $\varphi(d)$ disjoint sets of (b) as columns. This matrix has $\frac{\varphi(k)}{\varphi(d)}$ rows. Each row contains a reduced system mod d. These are the disjoint sets required for part (a).
  - Similarly, it is easy to verify that Property (a) implies Property (b).

Decomposition Property of Reduced Residue Systems (b)

- We now prove Property (b).

  Let S_d be a given reduced residue system mod d.

  Suppose $r \in S_d$.

  There are $\varphi(d)$ values of r in S_d and $\varphi(k)$ integers in S.

  So there cannot be more than $\frac{\varphi(k)}{\varphi(d)}$ integers n in S, distinct mod k, such that

  $$n \equiv r \pmod{d}.$$

  To complete the proof it suffices to prove the following.

  Claim: There are at least $\frac{\varphi(k)}{\varphi(d)}$ integers n in S, distinct mod k, such that

  $$n \equiv r \pmod{d}.$$

Decomposition Property (Claim)

Claim: There are at least $\frac{\varphi(k)}{\varphi(d)}$ integers n in S, distinct mod k, such that $n \equiv r \pmod{d}$.

The required numbers n are selected from the residue classes mod k, represented by the following $\frac{k}{d}$ integers:

$$r,\ r+d,\ r+2d,\ \ldots,\ r+\frac{k}{d}d.$$

These numbers are congruent to each other mod d and they are incongruent mod k.

Since $\in S_d$, $(r,d)=1$.

So the preceding theorem shows that $\frac{\varphi(k)}{\varphi(d)}$ of the numbers in the list are relatively prime to k.