Factorization and Primality Testing Chapter 3 Congruences and Residue Classes

Robert C. Vaughan

September 30, 2024

Residue Classes

- The next topic was first developed by Gauss.

Definition 1

Let $m \in \mathbb{N}$ and define *the residue class* $\overline{r}$ modulo m by

$$\overline{r} = \{x \in \mathbb{Z} : m|(x - r)\}.$$

By the division algorithm every integer is in one

$$\overline{0}, \overline{1}, \ldots, \overline{m-1}.$$

This is often called a *complete* system of residues modulo m.

Residue Classes

- The next topic was first developed by Gauss.

Definition 1

Let $m \in \mathbb{N}$ and define *the residue class* $\overline{r}$ modulo m by

$$\overline{r} = \{x \in \mathbb{Z} : m|(x-r)\}.$$

By the division algorithm every integer is in one

$$\overline{0}, \overline{1}, \ldots, \overline{m-1}.$$

This is often called a *complete* system of residues modulo m.

- The remarkable thing is that we can perform arithmetic on the residue classes just as if they were numbers.

Residue Classes

- The next topic was first developed by Gauss.

Definition 1

Let $m \in \mathbb{N}$ and define *the residue class* $\overline{r}$ modulo m by

$$\overline{r} = \{x \in \mathbb{Z} : m|(x - r)\}.$$

By the division algorithm every integer is in one

$$\overline{0}, \overline{1}, \ldots, \overline{m-1}.$$

This is often called a *complete* system of residues modulo m.

- The remarkable thing is that we can perform arithmetic on the residue classes just as if they were numbers.
- The residue class $\overline{0}$ behaves like the number 0,

Residue Classes

- The next topic was first developed by Gauss.

Definition 1

Let $m \in \mathbb{N}$ and define *the residue class* $\overline{r}$ modulo m by

$$\overline{r} = \{x \in \mathbb{Z} : m|(x - r)\}.$$

By the division algorithm every integer is in one

$$\overline{0}, \overline{1}, \ldots, \overline{m-1}.$$

This is often called a *complete* system of residues modulo m.

- The remarkable thing is that we can perform arithmetic on the residue classes just as if they were numbers.
- The residue class $\overline{0}$ behaves like the number 0,
- because $\overline{0}$ is the set of multiples of m and adding any one of them to an element of $\overline{r}$ does not change the remainder.

- Thus for any r

$$\overline{0}+\overline{r}=\overline{r}=\overline{r}+\overline{0}.$$

- Thus for any r
$$\overline{0}+\overline{r}=\overline{r}=\overline{r}+\overline{0}.$$
- Suppose that we are given any two residue classes $\overline{r}$ and $\overline{s}$ modulo m. Let t be the remainder of $r+s$ on division by m. Then the elements of $\overline{r}$ and $\overline{s}$ are of the form $r+mx$ and $s+my$ and we know that $r+s=t+mz$ for some z.

- Thus for any r
$$\overline{0}+\overline{r}=\overline{r}=\overline{r}+\overline{0}.$$
- Suppose that we are given any two residue classes $\overline{r}$ and $\overline{s}$ modulo m. Let t be the remainder of $r+s$ on division by m. Then the elements of $\overline{r}$ and $\overline{s}$ are of the form $r+mx$ and $s+my$ and we know that $r+s=t+mz$ for some z.
- Thus $r+mx+s+my=t+m(z+x+y)$ is in $\overline{t}$, and it is readily seen that the converse is true.

- Thus for any r
$$\overline{0}+\overline{r}=\overline{r}=\overline{r}+\overline{0}.$$
- Suppose that we are given any two residue classes $\overline{r}$ and $\overline{s}$ modulo m. Let t be the remainder of $r+s$ on division by m. Then the elements of $\overline{r}$ and $\overline{s}$ are of the form $r+mx$ and $s+my$ and we know that $r+s=t+mz$ for some z.
- Thus $r+mx+s+my=t+m(z+x+y)$ is in $\overline{t}$, and it is readily seen that the converse is true.
- Thus it makes sense to write $\overline{r}+\overline{s}=\overline{t}$, and then we have $\overline{r}+\overline{s}=\overline{s}+\overline{r}$.

- Thus for any r
$$\overline{0}+\overline{r}=\overline{r}=\overline{r}+\overline{0}.$$
- Suppose that we are given any two residue classes $\overline{r}$ and $\overline{s}$ modulo m. Let t be the remainder of $r+s$ on division by m. Then the elements of $\overline{r}$ and $\overline{s}$ are of the form $r+mx$ and $s+my$ and we know that $r+s=t+mz$ for some z.
- Thus $r+mx+s+my=t+m(z+x+y)$ is in $\overline{t}$, and it is readily seen that the converse is true.
- Thus it makes sense to write $\overline{r}+\overline{s}=\overline{t}$, and then we have $\overline{r}+\overline{s}=\overline{s}+\overline{r}$.
- One can also check that
$$\overline{r}+\overline{-r}=\overline{0}.$$

- In connection with this Gauss introduced a notation.

Definition 2

Let $m \in \mathbb{N}$. If two integers x and y satisfy $m|x-y$, then we write
$$x \equiv y \pmod{m}$$
and we say that x is *congruent to* y modulo m.

- In connection with this Gauss introduced a notation.

Definition 2

Let $m \in \mathbb{N}$. If two integers x and y satisfy $m|x-y$, then we write
$$x \equiv y \pmod{m}$$
and we say that x is *congruent to* y modulo m.

- Here are some of the properties of congruences.

$$x \equiv x \pmod{m},$$

$$x \equiv y \pmod{m} \text{ iff } y \equiv x \pmod{m},$$

$$x \equiv y \pmod{m}, y \equiv z \pmod{m} \text{ implies } x \equiv z \pmod{m}.$$

- In connection with this Gauss introduced a notation.

Definition 2

Let $m \in \mathbb{N}$. If two integers x and y satisfy $m|x-y$, then we write

$$x \equiv y \pmod{m}$$

and we say that x is *congruent to* y modulo m.

- Here are some of the properties of congruences.

$$x \equiv x \pmod{m},$$

$$x \equiv y \pmod{m} \text{ iff } y \equiv x \pmod{m},$$

$$x \equiv y \pmod{m}, y \equiv z \pmod{m} \text{ implies } x \equiv z \pmod{m}.$$

- These say that the relationship $\equiv$ is reflexive, symmetric and transitive.

- In connection with this Gauss introduced a notation.

Definition 2

Let $m \in \mathbb{N}$. If two integers x and y satisfy $m|x-y$, then we write

$$x \equiv y \pmod{m}$$

and we say that x is *congruent to* y modulo m.

- Here are some of the properties of congruences.

$$x \equiv x \pmod{m},$$

$$x \equiv y \pmod{m} \text{ iff } y \equiv x \pmod{m},$$

$$x \equiv y \pmod{m}, y \equiv z \pmod{m} \text{ implies } x \equiv z \pmod{m}.$$

- These say that the relationship $\equiv$ is reflexive, symmetric and transitive.
- I leave their proofs as an exercise.

- In connection with this Gauss introduced a notation.

Definition 2

Let $m \in \mathbb{N}$. If two integers x and y satisfy $m|x-y$, then we write

$$x \equiv y \pmod{m}$$

and we say that x is *congruent to* y modulo m.

- Here are some of the properties of congruences.

$$x \equiv x \pmod{m},$$

$$x \equiv y \pmod{m} \text{ iff } y \equiv x \pmod{m},$$

$$x \equiv y \pmod{m}, y \equiv z \pmod{m} \text{ implies } x \equiv z \pmod{m}.$$

- These say that the relationship $\equiv$ is reflexive, symmetric and transitive.
- I leave their proofs as an exercise.
- It follows that congruences modulo m partition the integers into equivalence classes.

- One can also check the following

- One can also check the following
- If $x \equiv y \pmod{m}$ and $z \equiv t \pmod{m}$, then $x + z \equiv y + t \pmod{m}$ and $xz \equiv yt \pmod{m}$.

- One can also check the following
- If $x \equiv y \pmod{m}$ and $z \equiv t \pmod{m}$, then $x + z \equiv y + t \pmod{m}$ and $xz \equiv yt \pmod{m}$.
- If $x \equiv y \pmod{m}$, then for any $n \in \mathbb{N}$, $x^n \equiv y^n \pmod{m}$ (use induction on n).

- One can also check the following
- If $x \equiv y \pmod{m}$ and $z \equiv t \pmod{m}$, then $x + z \equiv y + t \pmod{m}$ and $xz \equiv yt \pmod{m}$.
- If $x \equiv y \pmod{m}$, then for any $n \in \mathbb{N}$, $x^n \equiv y^n \pmod{m}$ (use induction on n).
- If f is a polynomial with integer coefficients, and $x \equiv y \pmod{m}$, then $f(x) \equiv f(y) \pmod{m}$.

- One can also check the following
- If $x \equiv y \pmod{m}$ and $z \equiv t \pmod{m}$, then $x + z \equiv y + t \pmod{m}$ and $xz \equiv yt \pmod{m}$.
- If $x \equiv y \pmod{m}$, then for any $n \in \mathbb{N}$, $x^n \equiv y^n \pmod{m}$ (use induction on n).
- If f is a polynomial with integer coefficients, and $x \equiv y \pmod{m}$, then $f(x) \equiv f(y) \pmod{m}$.
- Wait a minute, this means that one can use congruences just like doing arithmetic on the integers!

- The following tells us something about this structure.

Theorem 3

Suppose that $m \in \mathbb{N}$, $k \in \mathbb{Z}$, $(k, m) = 1$ *and*

$$\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_m$$

forms a complete set of residues modulo m. *Then so does*

$$\overline{ka_1}, \overline{ka_2}, \ldots, \overline{ka_m}.$$

- The following tells us something about this structure.

Theorem 3

Suppose that $m \in \mathbb{N}$, $k \in \mathbb{Z}$, $(k, m) = 1$ *and*

$$\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_m$$

forms a complete set of residues modulo m*. Then so does*

$$\overline{ka_1}, \overline{ka_2}, \ldots, \overline{ka_m}.$$

- **Proof.** Since we have m residue classes, we need only check that they are disjoint.

- The following tells us something about this structure.

Theorem 3

Suppose that $m \in \mathbb{N}$, $k \in \mathbb{Z}$, $(k, m) = 1$ *and*

$$\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_m$$

forms a complete set of residues modulo m. *Then so does*

$$\overline{ka_1}, \overline{ka_2}, \ldots, \overline{ka_m}.$$

- **Proof.** Since we have m residue classes, we need only check that they are disjoint.
- Consider any two of them, $\overline{ka_i}$ and $\overline{ka_j}$.

- The following tells us something about this structure.

Theorem 3

Suppose that $m \in \mathbb{N}$, $k \in \mathbb{Z}$, $(k, m) = 1$ and

$$\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_m$$

forms a complete set of residues modulo m. Then so does

$$\overline{ka_1}, \overline{ka_2}, \ldots, \overline{ka_m}.$$

- **Proof.** Since we have m residue classes, we need only check that they are disjoint.
- Consider any two of them, $\overline{ka_i}$ and $\overline{ka_j}$.
- Let $ka_i + mx$ and $ka_j + my$ be typical members of each.

- The following tells us something about this structure.

Theorem 3

Suppose that $m \in \mathbb{N}$, $k \in \mathbb{Z}$, $(k, m) = 1$ and

$$\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_m$$

forms a complete set of residues modulo m. Then so does

$$\overline{ka_1}, \overline{ka_2}, \ldots, \overline{ka_m}.$$

- **Proof.** Since we have m residue classes, we need only check that they are disjoint.
- Consider any two of them, $\overline{ka_i}$ and $\overline{ka_j}$.
- Let $ka_i + mx$ and $ka_j + my$ be typical members of each.
- If they were the same integer, than $ka_i + mx = ka_j + my$, so that $k(a_i - a_j) = m(y - x)$.

- The following tells us something about this structure.

Theorem 3

Suppose that $m \in \mathbb{N}$, $k \in \mathbb{Z}$, $(k, m) = 1$ *and*

$$\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_m$$

forms a complete set of residues modulo m. *Then so does*

$$\overline{ka_1}, \overline{ka_2}, \ldots, \overline{ka_m}.$$

- **Proof.** Since we have m residue classes, we need only check that they are disjoint.
- Consider any two of them, $\overline{ka_i}$ and $\overline{ka_j}$.
- Let $ka_i + mx$ and $ka_j + my$ be typical members of each.
- If they were the same integer, than $ka_i + mx = ka_j + my$, so that $k(a_i - a_j) = m(y - x)$.
- But then $m|k(a_i - a_j)$ and since $(k, m) = 1$ we would have $m|a_i - a_j$ so $\overline{a}_i$ and $\overline{a}_j$ would be identical residue classes, so $i = j$.

- An important rôle is played by the residue classes r modulo m with $(r, m) = 1$.

- An important rôle is played by the residue classes r modulo m with $(r, m) = 1$.
- In connection with this we introduce Euler's function.

Definition 4

A function defined on $\mathbb{N}$ is called an arithmetical function.

Definition 5

Euler's function $\phi(n)$ is the number of $x \in \mathbb{N}$ with $1 \le x \le n$ and $(x, n) = 1$.

Definition 6

A set of $\phi(m)$ distinct residue classes $\overline{r}$ modulo m with $(r, m) = 1$ is called a set of *reduced* residues modulo m.

- An important rôle is played by the residue classes r modulo m with $(r, m) = 1$.
- In connection with this we introduce Euler's function.

Definition 4

A function defined on $\mathbb{N}$ is called an arithmetical function.

Definition 5

Euler's function $\phi(n)$ is the number of $x \in \mathbb{N}$ with $1 \le x \le n$ and $(x, n) = 1$.

Definition 6

A set of $\phi(m)$ distinct residue classes $\bar{r}$ modulo m with $(r, m) = 1$ is called a set of *reduced* residues modulo m.

- Since $(1, 1) = 1$ we have $\phi(1) = 1$.

- An important rôle is played by the residue classes r modulo m with $(r, m) = 1$.
- In connection with this we introduce Euler's function.

Definition 4

A function defined on $\mathbb{N}$ is called an arithmetical function.

Definition 5

Euler's function $\phi(n)$ is the number of $x \in \mathbb{N}$ with $1 \le x \le n$ and $(x, n) = 1$.

Definition 6

A set of $\phi(m)$ distinct residue classes $\overline{r}$ modulo m with $(r, m) = 1$ is called a set of *reduced* residues modulo m.

- Since $(1, 1) = 1$ we have $\phi(1) = 1$.
- If p is prime, then the x with $1 \le x \le p - 1$ satisfy $(x, p) = 1$, but $(p, p) = p \ne 1$. Hence $\phi(p) = p - 1$.

- An important rôle is played by the residue classes r modulo m with $(r, m) = 1$.
- In connection with this we introduce Euler's function.

Definition 4

A function defined on $\mathbb{N}$ is called an arithmetical function.

Definition 5

Euler's function $\phi(n)$ is the number of $x \in \mathbb{N}$ with $1 \le x \le n$ and $(x, n) = 1$.

Definition 6

A set of $\phi(m)$ distinct residue classes $\overline{r}$ modulo m with $(r, m) = 1$ is called a set of *reduced* residues modulo m.

- Since $(1, 1) = 1$ we have $\phi(1) = 1$.
- If p is prime, then the x with $1 \le x \le p - 1$ satisfy $(x, p) = 1$, but $(p, p) = p \ne 1$. Hence $\phi(p) = p - 1$.
- The numbers x with $1 \le x \le 30$ and $(x, 30) = 1$ are $1, 7, 11, 13, 17, 19, 23, 29$, so $\phi(30) = 8$.

- One way of thinking about reduced sets of residues is to start from a complete set of fractions with denominator m in the interval $(0,1]$

$$\frac{1}{m}, \frac{2}{m}, \ldots, \frac{m}{m}.$$

- One way of thinking about reduced sets of residues is to start from a complete set of fractions with denominator m in the interval $(0, 1]$

$$\frac{1}{m}, \frac{2}{m}, \ldots, \frac{m}{m}.$$

- Now remove just the ones whose numerator has a common factor $d > 1$ with m.

- One way of thinking about reduced sets of residues is to start from a complete set of fractions with denominator m in the interval $(0, 1]$

$$\frac{1}{m}, \frac{2}{m}, \ldots, \frac{m}{m}.$$

- Now remove just the ones whose numerator has a common factor $d > 1$ with m.
- What is left are the $\phi(m)$ *reduced* fractions with denominator m.

- One way of thinking about reduced sets of residues is to start from a complete set of fractions with denominator m in the interval $(0, 1]$

$$\frac{1}{m}, \frac{2}{m}, \ldots, \frac{m}{m}.$$

- Now remove just the ones whose numerator has a common factor $d > 1$ with m.
- What is left are the $\phi(m)$ *reduced* fractions with denominator m.
- Suppose instead of removing the non-reduced ones we just write them in their lowest form.

- One way of thinking about reduced sets of residues is to start from a complete set of fractions with denominator m in the interval $(0,1]$

$$\frac{1}{m}, \frac{2}{m}, \ldots, \frac{m}{m}.$$

- Now remove just the ones whose numerator has a common factor $d > 1$ with m.
- What is left are the $\phi(m)$ *reduced* fractions with denominator m.
- Suppose instead of removing the non-reduced ones we just write them in their lowest form.
- Then for each divisor k of m we obtain all the reduced fractions with denominator k.

- In fact we just proved the following.

Theorem 7

For each $m \in \mathbb{N}$ we have

$$\sum_{k|m} \phi(k) = m.$$

- In fact we just proved the following.

Theorem 7

For each $m \in \mathbb{N}$ we have

$$\sum_{k|m} \phi(k) = m.$$

- We just saw that $\phi(1) = 1$, $\phi(p) = p - 1$, $\phi(30) = 8$

Example 8

The divisors of 30 are $1, 2, 3, 5, 6, 10, 15, 30$ and

$$\phi(6) = 2,\ \phi(10) = 4, \phi(15) = 8$$

so

$$\sum_{k|30} \phi(k) = 1 + 1 + 2 + 4 + 2 + 4 + 8 + 8 = 30.$$

- Now we can prove a companion theorem to Theorem 3 for reduced residue classes.

Theorem 9

Suppose that $(k, m) = 1$ *and that*

$$a_1, a_2, \ldots, a_{\phi(m)}$$

forms a set of reduced residue classes modulo m. Then

$$ka_1, ka_2, \ldots, ka_{\phi(m)}$$

also forms a set of reduced residues modulo m.

- Now we can prove a companion theorem to Theorem 3 for reduced residue classes.

Theorem 9

Suppose that $(k, m) = 1$ *and that*

$$a_1, a_2, \dots, a_{\phi(m)}$$

forms a set of reduced residue classes modulo m. *Then*

$$ka_1, ka_2, \dots, ka_{\phi(m)}$$

also forms a set of reduced residues modulo m.

- **Proof.** In view of the earlier theorem the residue classes ka_j are distinct, and since $(a_j, m) = 1$ we have $(ka_j, m) = 1$ so they give $\phi(m)$ distinct reduced residue classes, so they are all of them in some order.

- We now examine the structure of residue systems.

Theorem 10

Suppose m, $n \in \mathbb{N}$ *and* $(m, n) = 1$, *and consider the* $xn + ym$ *with* $1 \le x \le m$ *and* $1 \le y \le n$. *Then they form a complete set of residues modulo* mn. *If in addition* x *and* y *satisfy* $(x, m) = 1$ *and* $(y, n) = 1$, *then they form a reduced set.*

- We now examine the structure of residue systems.

Theorem 10

Suppose m, $n \in \mathbb{N}$ and $(m, n) = 1$, and consider the $xn + ym$ with $1 \le x \le m$ and $1 \le y \le n$. Then they form a complete set of residues modulo mn. If in addition x and y satisfy $(x, m) = 1$ and $(y, n) = 1$, then they form a reduced set.

- **Proof.** If $xn + ym \equiv x'n + y'm \pmod{mn}$, then $xn \equiv x'n \pmod{m}$, so $x \equiv x' \pmod{m}$, $x = x'$. Likewise $y = y'$.

- We now examine the structure of residue systems.

Theorem 10

Suppose m, $n \in \mathbb{N}$ and $(m, n) = 1$, and consider the $xn + ym$ with $1 \le x \le m$ and $1 \le y \le n$. Then they form a complete set of residues modulo mn. If in addition x and y satisfy $(x, m) = 1$ and $(y, n) = 1$, then they form a reduced set.

- **Proof.** If $xn + ym \equiv x'n + y'm \pmod{mn}$, then $xn \equiv x'n \pmod{m}$, so $x \equiv x' \pmod{m}$, $x = x'$. Likewise $y = y'$.
- Hence in either case the $xn + ym$ are distinct modulo mn.

- We now examine the structure of residue systems.

Theorem 10

Suppose $m, n \in \mathbb{N}$ and $(m, n) = 1$, and consider the $xn + ym$ with $1 \le x \le m$ and $1 \le y \le n$. Then they form a complete set of residues modulo mn. If in addition x and y satisfy $(x, m) = 1$ and $(y, n) = 1$, then they form a reduced set.

- **Proof.** If $xn + ym \equiv x'n + y'm \pmod{mn}$, then $xn \equiv x'n \pmod{m}$, so $x \equiv x' \pmod{m}$, $x = x'$. Likewise $y = y'$.
- Hence in either case the $xn + ym$ are distinct modulo mn.
- In the unrestricted case we have mn objects, so they form a complete set.

- We now examine the structure of residue systems.

Theorem 10

Suppose m, $n \in \mathbb{N}$ and $(m,n)=1$, and consider the $xn+ym$ with $1 \le x \le m$ and $1 \le y \le n$. Then they form a complete set of residues modulo mn. If in addition x and y satisfy $(x,m)=1$ and $(y,n)=1$, then they form a reduced set.

- **Proof.** If $xn+ym \equiv x'n+y'm \pmod{mn}$, then $xn \equiv x'n \pmod{m}$, so $x \equiv x' \pmod{m}$, $x = x'$. Likewise $y = y'$.
- Hence in either case the $xn+ym$ are distinct modulo mn.
- In the unrestricted case we have mn objects, so they form a complete set.
- In the restricted case $(xn+ym, m) = (xn, m) = (x, m) = 1$ and likewise $(xn+ym, n) = 1$, so $(xn+ym, mn) = 1$ and the $xn+ym$ all belong to reduced residue classes.

- We now examine the structure of residue systems.

Theorem 10

Suppose m, $n \in \mathbb{N}$ and $(m, n) = 1$, and consider the $xn + ym$ with $1 \le x \le m$ and $1 \le y \le n$. Then they form a complete set of residues modulo mn. If in addition x and y satisfy $(x, m) = 1$ and $(y, n) = 1$, then they form a reduced set.

- **Proof.** If $xn + ym \equiv x'n + y'm \pmod{mn}$, then $xn \equiv x'n \pmod{m}$, so $x \equiv x' \pmod{m}$, $x = x'$. Likewise $y = y'$.
- Hence in either case the $xn + ym$ are distinct modulo mn.
- In the unrestricted case we have mn objects, so they form a complete set.
- In the restricted case $(xn + ym, m) = (xn, m) = (x, m) = 1$ and likewise $(xn + ym, n) = 1$, so $(xn + ym, mn) = 1$ and the $xn + ym$ all belong to reduced residue classes.
- Now let $(z, mn) = 1$. Choose x', y', x, y so that $x'n + y'm = 1$, $x \equiv x'z \pmod{m}$ and $y \equiv y'z \pmod{n}$.

- We now examine the structure of residue systems.

Theorem 10

Suppose $m,\ n \in \mathbb{N}$ and $(m, n) = 1$, and consider the $xn + ym$ with $1 \le x \le m$ and $1 \le y \le n$. Then they form a complete set of residues modulo mn. If in addition x and y satisfy $(x, m) = 1$ and $(y, n) = 1$, then they form a reduced set.

- **Proof.** If $xn + ym \equiv x'n + y'm \pmod{mn}$, then $xn \equiv x'n \pmod{m}$, so $x \equiv x' \pmod{m}$, $x = x'$. Likewise $y = y'$.
- Hence in either case the $xn + ym$ are distinct modulo mn.
- In the unrestricted case we have mn objects, so they form a complete set.
- In the restricted case $(xn + ym, m) = (xn, m) = (x, m) = 1$ and likewise $(xn + ym, n) = 1$, so $(xn + ym, mn) = 1$ and the $xn + ym$ all belong to reduced residue classes.
- Now let $(z, mn) = 1$. Choose x', y', x, y so that $x'n + y'm = 1$, $x \equiv x'z \pmod{m}$ and $y \equiv y'z \pmod{n}$.
- Then $xn + ym \equiv x'zn + y'zm = z \pmod{mn}$ and hence every reduced residue is included.

- Here is a table of $xn + ym \pmod{mn}$ when $m = 5$, $n = 6$.

Example 11

x / y	1	2	3	4	5
1	11	17	23	29	5
2	16	22	28	4	10
3	21	27	3	9	15
4	26	2	8	14	20
5	1	7	13	19	25
6	6	12	18	24	30

The 30 numbers 1 through 30 appear exactly once each. The 8 reduced residue classes occur precisely in the intersection of rows 1 and 5 and columns 1 through 4.

- Immediate from Theorem 10 we have

Corollary 12

If $(m, n) = 1$, *then* $\phi(mn) = \phi(m)\phi(n)$.

- Immediate from Theorem 10 we have

Corollary 12

If $(m, n) = 1$, *then* $\phi(mn) = \phi(m)\phi(n)$.

- Thus ϕ is an example of a multiplicative function.

Definition 13

If an arithmetical function f which is not identically 0 satisfies

$$f(mn) = f(m)f(n)$$

whenever $(m, n) = 1$ we say that f is *multiplicative*.

- Immediate from Theorem 10 we have

Corollary 12

If $(m, n) = 1$, *then* $\phi(mn) = \phi(m)\phi(n)$.

- Thus ϕ is an example of a multiplicative function.

Definition 13

If an arithmetical function f which is not identically 0 satisfies

$$f(mn) = f(m)f(n)$$

whenever $(m, n) = 1$ we say that f is *multiplicative*.

- Thus we have another

Corollary 14

Euler's function is multiplicative.

This enables a full evaluation of $\phi(n)$.

- If $n = p^k$, then the number of reduced residue classes modulo p^k is the number of x with $1 \le x \le p^k$ and $p \nmid x$.

- If $n = p^k$, then the number of reduced residue classes modulo p^k is the number of x with $1 \le x \le p^k$ and $p \nmid x$.
- This is $p^k - N$ where N is the number of x with $1 \le x \le p^k$ and $p|x$, and $N = p^{k-1}$.

- If $n = p^k$, then the number of reduced residue classes modulo p^k is the number of x with $1 \le x \le p^k$ and $p \nmid x$.
- This is $p^k - N$ where N is the number of x with $1 \le x \le p^k$ and $p|x$, and $N = p^{k-1}$.
- Thus $\phi(p^k) = p^k - p^{k-1} = p^k(1 - 1/p)$.

- If $n = p^k$, then the number of reduced residue classes modulo p^k is the number of x with $1 \le x \le p^k$ and $p \nmid x$.
- This is $p^k - N$ where N is the number of x with $1 \le x \le p^k$ and $p|x$, and $N = p^{k-1}$.
- Thus $\phi(p^k) = p^k - p^{k-1} = p^k(1 - 1/p)$.
- Putting this all together gives

Theorem 15

Let $n \in \mathbb{N}$. Then $\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$ where when $n = 1$ we interpret the product as an "empty" product 1.

- If $n = p^k$, then the number of reduced residue classes modulo p^k is the number of x with $1 \le x \le p^k$ and $p \nmid x$.
- This is $p^k - N$ where N is the number of x with $1 \le x \le p^k$ and $p|x$, and $N = p^{k-1}$.
- Thus $\phi(p^k) = p^k - p^{k-1} = p^k(1 - 1/p)$.
- Putting this all together gives

Theorem 15

Let $n \in \mathbb{N}$. Then $\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$ *where when $n = 1$ we interpret the product as an "empty" product* 1.

- Some special cases.

Example 16

We have $\phi(9) = 6$, $\phi(5) = 4$, $\phi(45) = 24$. Note that $\phi(3) = 2$ and $\phi(9) \neq \phi(3)^2$.

- Here is a beautiful and useful theorem.

Theorem 17 (Euler)

Suppose that $m \in \mathbb{N}$ and $a \in \mathbb{Z}$ with $(a, m) = 1$. Then

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

- Here is a beautiful and useful theorem.

Theorem 17 (Euler)

Suppose that $m \in \mathbb{N}$ and $a \in \mathbb{Z}$ with $(a, m) = 1$. Then

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

- **Proof.** Let $a_1, a_2, \ldots, a_{\phi(m)}$ be a reduced set modulo m.

- Here is a beautiful and useful theorem.

Theorem 17 (Euler)

Suppose that $m \in \mathbb{N}$ and $a \in \mathbb{Z}$ with $(a, m) = 1$. Then

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

- **Proof.** Let $a_1, a_2, \ldots, a_{\phi(m)}$ be a reduced set modulo m.
- Then $aa_1, aa_2, \ldots, aa_{\phi(m)}$ is another. Hence

$$\begin{aligned} a_1 a_2 \ldots a_{\phi(m)} &\equiv aa_1 aa_2 \ldots aa_{\phi(m)} \pmod{m} \\ &\equiv a_1 a_2 \ldots a_{\phi(m)} a^{\phi(m)} \pmod{m}. \end{aligned}$$

- Here is a beautiful and useful theorem.

Theorem 17 (Euler)

Suppose that $m \in \mathbb{N}$ and $a \in \mathbb{Z}$ with $(a, m) = 1$. Then

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

- **Proof.** Let $a_1, a_2, \ldots, a_{\phi(m)}$ be a reduced set modulo m.
- Then $aa_1, aa_2, \ldots, aa_{\phi(m)}$ is another. Hence

$$\begin{aligned} a_1 a_2 \ldots a_{\phi(m)} &\equiv aa_1 aa_2 \ldots aa_{\phi(m)} \pmod{m} \\ &\equiv a_1 a_2 \ldots a_{\phi(m)} a^{\phi(m)} \pmod{m}. \end{aligned}$$

- As $(a_1 a_2 \ldots a_{\phi(m)}, m) = 1$ we may cancel $a_1 a_2 \ldots a_{\phi(m)}$.

- Here is a beautiful and useful theorem.

Theorem 17 (Euler)

Suppose that $m \in \mathbb{N}$ and $a \in \mathbb{Z}$ with $(a, m) = 1$. Then

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

- **Proof.** Let $a_1, a_2, \ldots, a_{\phi(m)}$ be a reduced set modulo m.
- Then $aa_1, aa_2, \ldots, aa_{\phi(m)}$ is another. Hence

$$\begin{aligned} a_1 a_2 \ldots a_{\phi(m)} &\equiv aa_1 aa_2 \ldots aa_{\phi(m)} \pmod{m} \\ &\equiv a_1 a_2 \ldots a_{\phi(m)} a^{\phi(m)} \pmod{m}. \end{aligned}$$

- As $(a_1 a_2 \ldots a_{\phi(m)}, m) = 1$ we may cancel $a_1 a_2 \ldots a_{\phi(m)}$.
- Thus

Corollary 18 (Fermat)

Let p be a prime and $a \in \mathbb{Z}$. Then $a^p \equiv a \pmod{p}$. If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

- Could Fermat's theorem give a primality test?

- Could Fermat's theorem give a primality test?
- Unfortunately it is possible that $a^{n-1} \equiv 1 \pmod{n}$ when n is not prime, although this is rare.

- Could Fermat's theorem give a primality test?
- Unfortunately it is possible that $a^{n-1} \equiv 1 \pmod{n}$ when n is not prime, although this is rare.
- For example, when are $n = 341, 561, 645$

$$2^{n-1} \equiv 1 \pmod{n}$$

- Could Fermat's theorem give a primality test?
- Unfortunately it is possible that $a^{n-1} \equiv 1 \pmod{n}$ when n is not prime, although this is rare.
- For example, when are $n = 341, 561, 645$

$$2^{n-1} \equiv 1 \pmod{n}$$

- Such n are called *pseudoprimes*.

- Could Fermat's theorem give a primality test?
- Unfortunately it is possible that $a^{n-1} \equiv 1 \pmod{n}$ when n is not prime, although this is rare.
- For example, when are $n = 341, 561, 645$

$$2^{n-1} \equiv 1 \pmod{n}$$

- Such n are called *pseudoprimes*.
- There are 245 less than 10^6, compared with 78498 primes.

- Could Fermat's theorem give a primality test?
- Unfortunately it is possible that $a^{n-1} \equiv 1 \pmod{n}$ when n is not prime, although this is rare.
- For example, when are $n = 341, 561, 645$

$$2^{n-1} \equiv 1 \pmod{n}$$

- Such n are called *pseudoprimes*.
- There are 245 less than 10^6, compared with 78498 primes.
- Moreover

$$3^{341-1} \equiv 56 \neq 1 \pmod{341}$$

suggests a possible primality test.

- Could Fermat's theorem give a primality test?
- Unfortunately it is possible that $a^{n-1} \equiv 1 \pmod{n}$ when n is not prime, although this is rare.
- For example, when are $n = 341, 561, 645$

$$2^{n-1} \equiv 1 \pmod{n}$$

- Such n are called *pseudoprimes*.
- There are 245 less than 10^6, compared with 78498 primes.
- Moreover

$$3^{341-1} \equiv 56 \not\equiv 1 \pmod{341}$$

suggests a possible primality test.
- Given n try trial division a few times, say for $d = 2, 3, 5, 7$ and then check successively for $a = 2, 3, 5, 7$

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

- Could Fermat's theorem give a primality test?
- Unfortunately it is possible that $a^{n-1} \equiv 1 \pmod{n}$ when n is not prime, although this is rare.
- For example, when are $n = 341, 561, 645$

$$2^{n-1} \equiv 1 \pmod{n}$$

- Such n are called *pseudoprimes*.
- There are 245 less than 10^6, compared with 78498 primes.
- Moreover

$$3^{341-1} \equiv 56 \not\equiv 1 \pmod{341}$$

suggests a possible primality test.
- Given n try trial division a few times, say for $d = 2, 3, 5, 7$ and then check successively for $a = 2, 3, 5, 7$

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

- Unfortunately one can still have false positives.

- Could Fermat's theorem give a primality test?
- Unfortunately it is possible that $a^{n-1} \equiv 1 \pmod{n}$ when n is not prime, although this is rare.
- For example, when are $n = 341, 561, 645$

$$2^{n-1} \equiv 1 \pmod{n}$$

- Such n are called *pseudoprimes*.
- There are 245 less than 10^6, compared with 78498 primes.
- Moreover

$$3^{341-1} \equiv 56 \not\equiv 1 \pmod{341}$$

suggests a possible primality test.

- Given n try trial division a few times, say for $d = 2, 3, 5, 7$ and then check successively for $a = 2, 3, 5, 7$

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

- Unfortunately one can still have false positives.
- Thus $561 = 3.11.17$ satisfies

$$a^{560} \equiv 1 \pmod{561}$$

for *all* a with $(a, 561) = 1$.

- Such numbers are interesting

Definition 19

A composite n which satisfies $a^{n-1} \equiv 1 \pmod{n}$ for all a with $(a, n) = 1$ is called a Carmichael number.

- Such numbers are interesting

Definition 19

A composite n which satisfies $a^{n-1} \equiv 1 \pmod{n}$ for all a with $(a, n) = 1$ is called a Carmichael number.

- There are infinitely Carmichael number. The smallest is 561 and there are 2163 of them below 25×10^9.

- Such numbers are interesting

Definition 19

A composite n which satisfies $a^{n-1} \equiv 1 \pmod{n}$ for all a with $(a, n) = 1$ is called a Carmichael number.

- There are infinitely Carmichael number. The smallest is 561 and there are 2163 of them below 25×10^9.
- Also of interest.

Definition 20

Define $M(n) = 2^n - 1$. If it is prime it is a Mersenne prime.

- Such numbers are interesting

Definition 19

A composite n which satisfies $a^{n-1} \equiv 1 \pmod{n}$ for all a with $(a, n) = 1$ is called a Carmichael number.

- There are infinitely Carmichael number. The smallest is 561 and there are 2163 of them below 25×10^9.
- Also of interest.

Definition 20

Define $M(n) = 2^n - 1$. If it is prime it is a Mersenne prime.

- If $n = ab$, then $M(ab) = (2^a - 1)(2^{a(b-1)} + \cdots + 2^a + 1)$.

- Such numbers are interesting

Definition 19

A composite n which satisfies $a^{n-1} \equiv 1 \pmod{n}$ for all a with $(a, n) = 1$ is called a Carmichael number.

- There are infinitely Carmichael number. The smallest is 561 and there are 2163 of them below 25×10^9.
- Also of interest.

Definition 20

Define $M(n) = 2^n - 1$. If it is prime it is a Mersenne prime.

- If $n = ab$, then $M(ab) = (2^a - 1)(2^{a(b-1)} + \cdots + 2^a + 1)$.
- Thus for $M(n)$ to be prime it is necessary that n be prime.

Example 21

We have $3 = 2^2 - 1$, $7 = 2^3 - 1$, $31 = 2^5 - 1\,127 = 2^7 - 1$. However that is not sufficient. $2^{11} - 1 = 2047 = 23 \times 89$.

- As with linear equations, linear congruences are easiest.

- As with linear equations, linear congruences are easiest.
- We have already solved $ax \equiv b \pmod{m}$ in principle since it is equivalent to $ax + my = b$.

Theorem 22

The congruence $ax \equiv b \pmod{m}$ is soluble iff $(a, m)|b$, and the general solution is given by a residue class x_0 modulo $m/(a, m)$. x_0 can be found by applying Euclid's algorithm.

- As with linear equations, linear congruences are easiest.
- We have already solved $ax \equiv b \pmod{m}$ in principle since it is equivalent to $ax + my = b$.

Theorem 22

The congruence $ax \equiv b \pmod{m}$ is soluble iff $(a, m)|b$, and the general solution is given by a residue class x_0 modulo $m/(a, m)$. x_0 can be found by applying Euclid's algorithm.

- **Proof.** The congruence is equivalent to the equation $ax + my = b$ and there can be no solution if $(a, m) \nmid b$.

- As with linear equations, linear congruences are easiest.
- We have already solved $ax \equiv b \pmod{m}$ in principle since it is equivalent to $ax + my = b$.

Theorem 22

The congruence $ax \equiv b \pmod{m}$ is soluble iff $(a, m)|b$, and the general solution is given by a residue class x_0 modulo $m/(a, m)$. x_0 can be found by applying Euclid's algorithm.

- **Proof.** The congruence is equivalent to the equation $ax + my = b$ and there can be no solution if $(a, m) \nmid b$.
- If $(a, m)|b$, then Euclid's algorithm solves

$$\frac{a}{(a, m)}x + \frac{m}{(a, m)}y = \frac{b}{(a, m)}.$$

- As with linear equations, linear congruences are easiest.
- We have already solved $ax \equiv b \pmod{m}$ in principle since it is equivalent to $ax + my = b$.

Theorem 22

The congruence $ax \equiv b \pmod{m}$ is soluble iff $(a, m)|b$, and the general solution is given by a residue class x_0 modulo $m/(a, m)$. x_0 can be found by applying Euclid's algorithm.

- **Proof.** The congruence is equivalent to the equation $ax + my = b$ and there can be no solution if $(a, m) \nmid b$.
- If $(a, m)|b$, then Euclid's algorithm solves

$$\frac{a}{(a, m)}x + \frac{m}{(a, m)}y = \frac{b}{(a, m)}.$$

- Let x_0, y_0 be such a solution and let x, y be any solution. Then $a/(a, m)(x - x_0) \equiv 0 \pmod{m/(a, m)}$ and since $(a/(a, m), m/(a, m)) = 1$ it follows that x is in the residue class $x_0 \pmod{m/(a, m)}$.

- A curious result which uses somewhat similar ideas.

Theorem 23 (Wilson)

Let p be a prime number, then $(p-1)! \equiv -1 \pmod{p}$.

- A curious result which uses somewhat similar ideas.

Theorem 23 (Wilson)

Let p be a prime number, then $(p-1)! \equiv -1 \pmod{p}$.

- **Proof.** The cases $p = 2$ and $p = 3$ are $(2-1)! = 1 \equiv -1 \pmod{2}$ and $(3-1)! = 2 \equiv -1 \pmod{3}$.

- A curious result which uses somewhat similar ideas.

Theorem 23 (Wilson)

Let p be a prime number, then $(p-1)! \equiv -1 \pmod{p}$.

- **Proof.** The cases $p = 2$ and $p = 3$ are $(2-1)! = 1 \equiv -1 \pmod{2}$ and $(3-1)! = 2 \equiv -1 \pmod{3}$.
- Thus we may suppose $p \geq 5$. Observe now that $x^2 \equiv 1 \pmod{p}$ implies $x \equiv \pm 1 \pmod{p}$

- A curious result which uses somewhat similar ideas.

Theorem 23 (Wilson)

Let p be a prime number, then $(p-1)! \equiv -1 \pmod{p}$.

- **Proof.** The cases $p=2$ and $p=3$ are $(2-1)! = 1 \equiv -1 \pmod{2}$ and $(3-1)! = 2 \equiv -1 \pmod{3}$.
- Thus we may suppose $p \geq 5$. Observe now that $x^2 \equiv 1 \pmod{p}$ implies $x \equiv \pm 1 \pmod{p}$
- Thus the numbers $2, 3, \ldots, p-2$ can be paired off into $\frac{p-3}{2}$ mutually exclusive pairs a, b such that $ab \equiv 1 \pmod{p}$.

- A curious result which uses somewhat similar ideas.

Theorem 23 (Wilson)

Let p be a prime number, then $(p-1)! \equiv -1 \pmod{p}$.

- **Proof.** The cases $p=2$ and $p=3$ are $(2-1)! = 1 \equiv -1 \pmod{2}$ and $(3-1)! = 2 \equiv -1 \pmod{3}$.
- Thus we may suppose $p \geq 5$. Observe now that $x^2 \equiv 1 \pmod{p}$ implies $x \equiv \pm 1 \pmod{p}$
- Thus the numbers $2, 3, \dots, p-2$ can be paired off into $\frac{p-3}{2}$ mutually exclusive pairs a, b such that $ab \equiv 1 \pmod{p}$.
- Thus $(p-1)! \equiv p-1 \equiv -1 \pmod{p}$.

- A curious result which uses somewhat similar ideas.

Theorem 23 (Wilson)

Let p be a prime number, then $(p-1)! \equiv -1 \pmod{p}$.

- **Proof.** The cases $p = 2$ and $p = 3$ are $(2-1)! = 1 \equiv -1 \pmod{2}$ and $(3-1)! = 2 \equiv -1 \pmod{3}$.
- Thus we may suppose $p \geq 5$. Observe now that $x^2 \equiv 1 \pmod{p}$ implies $x \equiv \pm 1 \pmod{p}$
- Thus the numbers $2, 3, \ldots, p-2$ can be paired off into $\frac{p-3}{2}$ mutually exclusive pairs a, b such that $ab \equiv 1 \pmod{p}$.
- Thus $(p-1)! \equiv p-1 \equiv -1 \pmod{p}$.
- This theorem actually gives a necessary and sufficient condition for p to be a prime, since if p were to be composite, then we would have $((p-1)!, p) > 1$.

- A curious result which uses somewhat similar ideas.

Theorem 23 (Wilson)

Let p be a prime number, then $(p-1)! \equiv -1 \pmod{p}$.

- **Proof.** The cases $p = 2$ and $p = 3$ are $(2-1)! = 1 \equiv -1 \pmod{2}$ and $(3-1)! = 2 \equiv -1 \pmod{3}$.
- Thus we may suppose $p \geq 5$. Observe now that $x^2 \equiv 1 \pmod{p}$ implies $x \equiv \pm 1 \pmod{p}$
- Thus the numbers $2, 3, \ldots, p-2$ can be paired off into $\frac{p-3}{2}$ mutually exclusive pairs a, b such that $ab \equiv 1 \pmod{p}$.
- Thus $(p-1)! \equiv p - 1 \equiv -1 \pmod{p}$.
- This theorem actually gives a necessary and sufficient condition for p to be a prime, since if p were to be composite, then we would have $((p-1)!, p) > 1$.
- However this is useless since $(p-1)!$ grows very rapidly.

- What about simultaneous linear congruences?

$$\begin{cases} a_1 x & \equiv b_1 \pmod{q_1}, \\ \dots & \dots \\ a_r x & \equiv b_r \pmod{q_r}. \end{cases} \tag{2.1}$$

- What about simultaneous linear congruences?

$$\begin{cases} a_1 x & \equiv b_1 \pmod{q_1}, \\ \dots & \dots \\ a_r x & \equiv b_r \pmod{q_r}. \end{cases} \tag{2.1}$$

- There can only be a solution when each individual equation is soluble, so we require $(a_j, q_j) | b_j$ for every j.

- What about simultaneous linear congruences?

$$\begin{cases} a_1x & \equiv b_1 \pmod{q_1}, \\ \dots & \dots \\ a_rx & \equiv b_r \pmod{q_r}. \end{cases} \tag{2.1}$$

- There can only be a solution when each individual equation is soluble, so we require $(a_j, q_j)|b_j$ for every j.
- Then we know that each individual equation is soluble by some residue class modulo $q_j/(a_j, q_j)$. Thus for some values of c_j and m_j this reduces to

$$\begin{cases} x & \equiv c_1 \pmod{m_1}, \\ \dots & \dots \\ x & \equiv c_r \pmod{m_r} \end{cases} \tag{2.2}$$

- What about simultaneous linear congruences?

$$\begin{cases} a_1x & \equiv b_1 \pmod{q_1}, \\ \dots & \dots \\ a_rx & \equiv b_r \pmod{q_r}. \end{cases} \tag{2.1}$$

- There can only be a solution when each individual equation is soluble, so we require $(a_j, q_j)|b_j$ for every j.
- Then we know that each individual equation is soluble by some residue class modulo $q_j/(a_j, q_j)$. Thus for some values of c_j and m_j this reduces to

$$\begin{cases} x & \equiv c_1 \pmod{m_1}, \\ \dots & \dots \\ x & \equiv c_r \pmod{m_r} \end{cases} \tag{2.2}$$

- Suppose for some i and $j \neq i$ we have $(m_i, m_j) = d > 1$.

- What about simultaneous linear congruences?

$$\begin{cases} a_1x & \equiv b_1 \pmod{q_1}, \\ \dots & \dots \\ a_rx & \equiv b_r \pmod{q_r}. \end{cases} \tag{2.1}$$

- There can only be a solution when each individual equation is soluble, so we require $(a_j, q_j)|b_j$ for every j.
- Then we know that each individual equation is soluble by some residue class modulo $q_j/(a_j, q_j)$. Thus for some values of c_j and m_j this reduces to

$$\begin{cases} x & \equiv c_1 \pmod{m_1}, \\ \dots & \dots \\ x & \equiv c_r \pmod{m_r} \end{cases} \tag{2.2}$$

- Suppose for some i and $j \neq i$ we have $(m_i, m_j) = d > 1$.
- Then x has to satisfy $c_i \equiv x \equiv c_j \pmod{d}$.

- What about simultaneous linear congruences?

$$\begin{cases} a_1x & \equiv b_1 \pmod{q_1}, \\ \dots & \dots \\ a_rx & \equiv b_r \pmod{q_r}. \end{cases} \tag{2.1}$$

- There can only be a solution when each individual equation is soluble, so we require $(a_j, q_j)|b_j$ for every j.
- Then we know that each individual equation is soluble by some residue class modulo $q_j/(a_j, q_j)$. Thus for some values of c_j and m_j this reduces to

$$\begin{cases} x & \equiv c_1 \pmod{m_1}, \\ \dots & \dots \\ x & \equiv c_r \pmod{m_r} \end{cases} \tag{2.2}$$

- Suppose for some i and $j \neq i$ we have $(m_i, m_j) = d > 1$.
- Then x has to satisfy $c_i \equiv x \equiv c_j \pmod{d}$.
- This imposes conditions on c_j which can get complicated.

- What about simultaneous linear congruences?

$$\begin{cases} a_1x & \equiv b_1 \pmod{q_1}, \\ \dots & \dots \\ a_rx & \equiv b_r \pmod{q_r}. \end{cases} \tag{2.1}$$

- There can only be a solution when each individual equation is soluble, so we require $(a_j, q_j)|b_j$ for every j.
- Then we know that each individual equation is soluble by some residue class modulo $q_j/(a_j, q_j)$. Thus for some values of c_j and m_j this reduces to

$$\begin{cases} x & \equiv c_1 \pmod{m_1}, \\ \dots & \dots \\ x & \equiv c_r \pmod{m_r} \end{cases} \tag{2.2}$$

- Suppose for some i and $j \neq i$ we have $(m_i, m_j) = d > 1$.
- Then x has to satisfy $c_i \equiv x \equiv c_j \pmod{d}$.
- This imposes conditions on c_j which can get complicated.
- Thus it is convenient to assume $(m_i, m_j) = 1$ when $i \neq j$.

- The following is known as the Chinese Remainder Theorem

Theorem 24

Suppose that $(m_i, m_j) = 1$ for every $i \neq j$. Then the system (2.2) has as its complete solution precisely the members of a unique residue class modulo $m_1 m_2 \dots m_r$.

- The following is known as the Chinese Remainder Theorem

Theorem 24

Suppose that $(m_i, m_j) = 1$ for every $i \neq j$. Then the system (2.2) has as its complete solution precisely the members of a unique residue class modulo $m_1 m_2 \dots m_r$.

- **Proof.** We first show that there is a solution.

- The following is known as the Chinese Remainder Theorem

Theorem 24

Suppose that $(m_i, m_j) = 1$ *for every* $i \neq j$. *Then the system (2.2) has as its complete solution precisely the members of a unique residue class modulo* $m_1 m_2 \dots m_r$.

- **Proof.** We first show that there is a solution.
- Let $M = m_1 m_2 \dots m_r$ and $M_j = M/m_j$, so that $(M_j, m_j) = 1$.

- The following is known as the Chinese Remainder Theorem

Theorem 24

Suppose that $(m_i, m_j) = 1$ for every $i \neq j$. Then the system (2.2) has as its complete solution precisely the members of a unique residue class modulo $m_1 m_2 \dots m_r$.

- **Proof.** We first show that there is a solution.
- Let $M = m_1 m_2 \dots m_r$ and $M_j = M/m_j$, so that $(M_j, m_j) = 1$.
- We know that there is an N_j so that $M_j N_j \equiv c_j \pmod{m_j}$ (solve $yM_j \equiv c_j \pmod{m_j}$ in y).

- The following is known as the Chinese Remainder Theorem

Theorem 24

Suppose that $(m_i, m_j) = 1$ for every $i \neq j$. Then the system (2.2) has as its complete solution precisely the members of a unique residue class modulo $m_1 m_2 \dots m_r$.

- **Proof.** We first show that there is a solution.
- Let $M = m_1 m_2 \dots m_r$ and $M_j = M/m_j$, so that $(M_j, m_j) = 1$.
- We know that there is an N_j so that $M_j N_j \equiv c_j \pmod{m_j}$ (solve $yM_j \equiv c_j \pmod{m_j}$ in y).
- Let x be any member of the residue class

$$N_1 M_1 + \dots + N_r M_r \pmod{M}.$$

- The following is known as the Chinese Remainder Theorem

Theorem 24

Suppose that $(m_i, m_j) = 1$ for every $i \neq j$. Then the system (2.2) has as its complete solution precisely the members of a unique residue class modulo $m_1 m_2 \ldots m_r$.

- **Proof.** We first show that there is a solution.
- Let $M = m_1 m_2 \ldots m_r$ and $M_j = M/m_j$, so that $(M_j, m_j) = 1$.
- We know that there is an N_j so that $M_j N_j \equiv c_j \pmod{m_j}$ (solve $yM_j \equiv c_j \pmod{m_j}$ in y).
- Let x be any member of the residue class

$$N_1 M_1 + \cdots + N_r M_r \pmod{M}.$$

- Then for every j, since $m_j | M_i$ when $i \neq j$ we have

$$\begin{aligned} x &\equiv N_j M_j \pmod{m_j} \\ &\equiv c_j \pmod{m_j} \end{aligned}$$

so the residue class $x \pmod{M}$ gives a solution.

- $$\begin{cases} x & \equiv c_1 \pmod{m_1}, \\ \dots & \dots \\ x & \equiv c_r \pmod{m_r} \end{cases}$$

- $$\begin{cases} x & \equiv c_1 \pmod{m_1}, \\ \dots & \dots \\ x & \equiv c_r \pmod{m_r} \end{cases}$$
- Now we have to show that the solution modulo M is unique.

- $$\begin{cases} x & \equiv c_1 \pmod{m_1}, \\ \dots & \dots \\ x & \equiv c_r \pmod{m_r} \end{cases}$$
- Now we have to show that the solution modulo M is unique.
- Suppose y is also a solution of the system.

- $$\begin{cases} x & \equiv c_1 \pmod{m_1}, \\ \dots & \dots \\ x & \equiv c_r \pmod{m_r} \end{cases}$$
- Now we have to show that the solution modulo M is unique.
- Suppose y is also a solution of the system.
- Then for every j we have

$$\begin{aligned} y &\equiv c_j \pmod{m_j} \\ &\equiv x \pmod{m_j} \end{aligned}$$

and so $m_j | y - x$.

- $$\begin{cases} x & \equiv c_1 \pmod{m_1}, \\ \dots & \dots \\ x & \equiv c_r \pmod{m_r} \end{cases}$$
- Now we have to show that the solution modulo M is unique.
- Suppose y is also a solution of the system.
- Then for every j we have

$$\begin{aligned} y &\equiv c_j \pmod{m_j} \\ &\equiv x \pmod{m_j} \end{aligned}$$

  and so $m_j | y - x$.
- Since the m_j are pairwise co-prime we have $M | y - x$, so y is in the residue class x modulo M.

- Consider

Example 25

$$\begin{aligned} x &\equiv 3 \pmod{4}, \\ x &\equiv 5 \pmod{21}, \\ x &\equiv 7 \pmod{25}. \end{aligned}$$

- Consider

Example 25

$$x \equiv 3 \pmod 4,$$
$$x \equiv 5 \pmod{21},$$
$$x \equiv 7 \pmod{25}.$$

- $m_1 = 4,\ m_2 = 21,\ m_3 = 25,\ M = 2100,\ M_1 = 525,\ M_2 = 100,\ M_3 = 84.$ Thus first we have to solve

$$525N_1 \equiv 3 \pmod 4,$$
$$100N_2 \equiv 5 \pmod{21},$$
$$84N_3 \equiv 7 \pmod{25}.$$

- $$\begin{aligned} 525 N_1 &\equiv 3 \pmod{4}, \\ 100 N_2 &\equiv 5 \pmod{21}, \\ 84 N_3 &\equiv 7 \pmod{25}. \end{aligned}$$

- $$\begin{aligned} 525N_1 &\equiv 3 \pmod 4, \\ 100N_2 &\equiv 5 \pmod{21}, \\ 84N_3 &\equiv 7 \pmod{25}. \end{aligned}$$

- Reducing the constants gives

$$\begin{aligned} N_1 &\equiv 3 \pmod 4, \\ (-5)N_2 &\equiv 5 \pmod{21}, \\ 9N_3 &\equiv 7 \pmod{25}. \end{aligned}$$

- $$\begin{aligned} 525N_1 &\equiv 3 \pmod 4, \\ 100N_2 &\equiv 5 \pmod{21}, \\ 84N_3 &\equiv 7 \pmod{25}. \end{aligned}$$
- Reducing the constants gives
$$\begin{aligned} N_1 &\equiv 3 \pmod 4, \\ (-5)N_2 &\equiv 5 \pmod{21}, \\ 9N_3 &\equiv 7 \pmod{25}. \end{aligned}$$
- Thus we can take $N_1 = 3$, $N_2 = 20$, $7 \equiv -18 \pmod{25}$ so $N_3 \equiv -2 \equiv 23 \pmod{25}$. Then the complete solution is
$$\begin{aligned} x &\equiv N_1M_1 + N_2M_2 + N_3M_3 \\ &= 3 \times 525 + 20 \times 100 + 23 \times 84 \\ &= 5507 \\ &\equiv 1307 \pmod{2100}. \end{aligned}$$

- The solution of a general polynomial congruence can be quite tricky, even for a polynomial with a single variable

$$f(x) := a_0 + a_1 x + \cdots + a_j x^j + \cdots a_J x^J \equiv 0 \pmod{m} \quad (3.3)$$

where the a_j are integers.

- The solution of a general polynomial congruence can be quite tricky, even for a polynomial with a single variable

$$f(x) := a_0 + a_1 x + \cdots + a_j x^j + \cdots a_J x^J \equiv 0 \pmod{m} \quad (3.3)$$

where the a_j are integers.

- The largest k such that $a_k \not\equiv 0 \pmod{m}$ is the degree of f modulo m.

- The solution of a general polynomial congruence can be quite tricky, even for a polynomial with a single variable

$$f(x) := a_0 + a_1 x + \cdots + a_j x^j + \cdots a_J x^J \equiv 0 \pmod{m} \quad (3.3)$$

where the a_j are integers.

- The largest k such that $a_k \not\equiv 0 \pmod{m}$ is the degree of f modulo m.
- If $a_j \equiv 0 \pmod{m}$ for every j, then the degree of f modulo m is not defined.

- The solution of a general polynomial congruence can be quite tricky, even for a polynomial with a single variable

$$f(x) := a_0 + a_1 x + \cdots + a_j x^j + \cdots a_J x^J \equiv 0 \pmod{m} \quad (3.3)$$

where the a_j are integers.

- The largest k such that $a_k \not\equiv 0 \pmod{m}$ is the degree of f modulo m.
- If $a_j \equiv 0 \pmod{m}$ for every j, then the degree of f modulo m is not defined.
- We have already seen that

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

is solved by any odd x, so that it has four solutions modulo 8, $x \equiv 1, 3, 5, 7 \pmod{8}$.

- The solution of a general polynomial congruence can be quite tricky, even for a polynomial with a single variable

$$f(x) := a_0+a_1x+\cdots+a_jx^j+\cdots a_Jx^J \equiv 0 \pmod{m} \quad (3.3)$$

where the a_j are integers.

- The largest k such that $a_k \not\equiv 0 \pmod{m}$ is the degree of f modulo m.
- If $a_j \equiv 0 \pmod{m}$ for every j, then the degree of f modulo m is not defined.
- We have already seen that

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

is solved by any odd x, so that it has four solutions modulo 8, $x \equiv 1, 3, 5, 7 \pmod{8}$.

- That is, more than the degree 2. However, when the modulus is prime we have a more familiar conclusion.

- When we have a solution x to a polynomial congruence such as (3.3) we may sometimes refer to such values as a *root* of the polynomial modulo m.

Theorem 26 (Lagrange)

Suppose that p is prime, and $f(x) = a_0 + a_1x + \cdots + a_jx^j + \cdots$ is a polynomial with integer coefficients a_j and it has degree k modulo p. Then the number of incongruent solutions of

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

is at most k.

- When we have a solution x to a polynomial congruence such as (3.3) we may sometimes refer to such values as a *root* of the polynomial modulo m.

Theorem 26 (Lagrange)

Suppose that p is prime, and $f(x) = a_0 + a_1x + \cdots + a_jx^j + \cdots$ is a polynomial with integer coefficients a_j and it has degree k modulo p. Then the number of incongruent solutions of

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

is at most k.

- **Proof.** Degree 0 is obvious so we suppose $k \geq 1$.

- When we have a solution x to a polynomial congruence such as (3.3) we may sometimes refer to such values as a *root* of the polynomial modulo m.

Theorem 26 (Lagrange)

Suppose that p is prime, and $f(x) = a_0 + a_1 x + \cdots + a_j x^j + \cdots$ is a polynomial with integer coefficients a_j and it has degree k modulo p. Then the number of incongruent solutions of

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

is at most k.

- **Proof.** Degree 0 is obvious so we suppose $k \geq 1$.
- We use induction on the degree k.

- When we have a solution x to a polynomial congruence such as (3.3) we may sometimes refer to such values as a *root* of the polynomial modulo m.

Theorem 26 (Lagrange)

Suppose that p is prime, and $f(x) = a_0 + a_1x + \cdots + a_jx^j + \cdots$ is a polynomial with integer coefficients a_j and it has degree k modulo p. Then the number of incongruent solutions of

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

is at most k.

- **Proof.** Degree 0 is obvious so we suppose $k \geq 1$.
- We use induction on the degree k.
- If a polynomial f has degree 1 modulo p, so that $f(x) = a_0 + a_1x$ with $p \nmid a_1$, then the congruence becomes $a_1x \equiv -a_0 \pmod{p}$ and since $a_1 \not\equiv 0 \pmod{p}$ (because f has degree 1) we know that this is soluble by precisely the members of a unique residue class modulo p.

- Now suppose that the conclusion holds for all polynomials of a given degree k and suppose that $f = a_0 + \cdots + a_{k+1}x^{k+1}$ has degree $k+1$.

- Now suppose that the conclusion holds for all polynomials of a given degree k and suppose that $f = a_0 + \cdots + a_{k+1}x^{k+1}$ has degree $k+1$.
- If $f(x) \equiv 0 \pmod{p}$ has no solutions, then we are done.

- Now suppose that the conclusion holds for all polynomials of a given degree k and suppose that $f = a_0 + \cdots + a_{k+1}x^{k+1}$ has degree $k+1$.
- If $f(x) \equiv 0 \pmod{p}$ has no solutions, then we are done.
- Hence we may assume at least one, say $x \equiv x_0 \pmod{p}$.

- Now suppose that the conclusion holds for all polynomials of a given degree k and suppose that $f = a_0 + \cdots + a_{k+1}x^{k+1}$ has degree $k+1$.
- If $f(x) \equiv 0 \pmod{p}$ has no solutions, then we are done.
- Hence we may assume at least one, say $x \equiv x_0 \pmod{p}$.
- By the division algorithm for polynomials we have

$$f(x) = (x - x_0)q(x) + f(x_0)$$

where $q(x)$ is a polynomial of degree k.

- Now suppose that the conclusion holds for all polynomials of a given degree k and suppose that $f = a_0 + \cdots + a_{k+1}x^{k+1}$ has degree $k+1$.
- If $f(x) \equiv 0 \pmod{p}$ has no solutions, then we are done.
- Hence we may assume at least one, say $x \equiv x_0 \pmod{p}$.
- By the division algorithm for polynomials we have

$$f(x) = (x - x_0)q(x) + f(x_0)$$

where $q(x)$ is a polynomial of degree k.
- Moreover the leading coefficient of $q(x)$ is $a_{k+1} \not\equiv 0 \pmod{p}$.

- Now suppose that the conclusion holds for all polynomials of a given degree k and suppose that $f = a_0 + \cdots + a_{k+1}x^{k+1}$ has degree $k+1$.
- If $f(x) \equiv 0 \pmod{p}$ has no solutions, then we are done.
- Hence we may assume at least one, say $x \equiv x_0 \pmod{p}$.
- By the division algorithm for polynomials we have

$$f(x) = (x - x_0)q(x) + f(x_0)$$

  where $q(x)$ is a polynomial of degree k.
- Moreover the leading coefficient of $q(x)$ is $a_{k+1} \not\equiv 0 \pmod{p}$.
- But $f(x_0) \equiv 0 \pmod{p}$, so that $f(x) \equiv (x - x_0)q(x) \pmod{p}$.

- Now suppose that the conclusion holds for all polynomials of a given degree k and suppose that $f = a_0 + \cdots + a_{k+1}x^{k+1}$ has degree $k+1$.
- If $f(x) \equiv 0 \pmod{p}$ has no solutions, then we are done.
- Hence we may assume at least one, say $x \equiv x_0 \pmod{p}$.
- By the division algorithm for polynomials we have

$$f(x) = (x - x_0)q(x) + f(x_0)$$

where $q(x)$ is a polynomial of degree k.
- Moreover the leading coefficient of $q(x)$ is $a_{k+1} \not\equiv 0 \pmod{p}$.
- But $f(x_0) \equiv 0 \pmod{p}$, so that $f(x) \equiv (x - x_0)q(x) \pmod{p}$.
- If $f(x_1) \equiv 0 \pmod{p}$, with $x_1 \not\equiv x_0 \pmod{p}$, then $p \nmid x_1 - x_0$ so that $p | q(x_1)$.

- Now suppose that the conclusion holds for all polynomials of a given degree k and suppose that $f = a_0 + \cdots + a_{k+1}x^{k+1}$ has degree $k+1$.
- If $f(x) \equiv 0 \pmod{p}$ has no solutions, then we are done.
- Hence we may assume at least one, say $x \equiv x_0 \pmod{p}$.
- By the division algorithm for polynomials we have

$$f(x) = (x - x_0)q(x) + f(x_0)$$

  where $q(x)$ is a polynomial of degree k.
- Moreover the leading coefficient of $q(x)$ is $a_{k+1} \not\equiv 0 \pmod{p}$.
- But $f(x_0) \equiv 0 \pmod{p}$, so that $f(x) \equiv (x - x_0)q(x) \pmod{p}$.
- If $f(x_1) \equiv 0 \pmod{p}$, with $x_1 \not\equiv x_0 \pmod{p}$, then $p \nmid x_1 - x_0$ so that $p | q(x_1)$.
- By the inductive hypothesis there are at most k possibilities for x_1, so at most $k+1$ in all.

- Non-linear polynomials in one variable are complicated.

- Non-linear polynomials in one variable are complicated.
- The general modulus can be reduced to a prime power modulus, and that case can be reduced to the prime modulus. I will include the theory in the class text for those interested. In general the prime case leads to algebraic number theory.

- Non-linear polynomials in one variable are complicated.
- The general modulus can be reduced to a prime power modulus, and that case can be reduced to the prime modulus. I will include the theory in the class text for those interested. In general the prime case leads to algebraic number theory.
- The quadratic case we will need and will look at later.