Lecture 4

Fermat, Euler, Wilson, Linear Congruences

(Definition) Complete Residue System: A complete residue system mod \( m \) is a collection of integers \( a_1 \ldots a_m \) such that \( a_i \neq a_j \mod m \) if \( i \neq j \) and any integer \( n \) is congruent to some \( a_i \mod m \)

(Definition) Reduced Residue System: A reduced residue system mod \( m \) is a collection of integers \( a_1 \ldots a_k \) such that \( a_i \neq a_j \mod m \) if \( i \neq j \) and \( (a_i, m) = 1 \) for all \( i \), and any integer \( n \) coprime to \( m \) must be congruent to some \( a_i \mod m \). Eg., take any complete residue system mod \( m \) and take the subset consisting of all the integers in it which are coprime to \( m \) - these will form a reduced residue system.

Eg. For \( m = 12 \)
complete = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}
reduced = \{1, 5, 7, 11\}

(Definition) Euler’s Totient Function: The number of elements in a reduced residue system mod \( m \) is called Euler’s totient function: \( \phi(m) \) (ie., the number of positive integers \( \leq m \) and coprime to \( m \))

Theorem 15 (Euler’s Theorem).

\[
\text{If } (a, m) = 1, \text{ then } a^{\phi(m)} \equiv 1 \mod m
\]

Proof.

Lemma 16. If \( (a, m) = 1 \) and \( r_1 \ldots r_k \) is a reduced residue system mod \( m \), \( k = \phi(m) \), then \( ar_1 \ldots ar_k \) is also a reduced residue system mod \( m \).

Proof. All we need to show is that \( ar_i \) are all coprime to \( m \) and distinct mod \( m \), since there are \( k \) of these \( ar_i \) and \( k \) is the number of elements in any residue system mod \( m \). We know that if \( (r, m) = 1 \) and \( (a, m) = 1 \) then \( (ar, m) = 1 \). Also, if we had \( ar_i \equiv ar_j \mod m \), then \( m|ar_i - ar_j = a(r_i - r_j) \). If \( (a, m) = 1 \) then \( m|r_i - r_j \Rightarrow r_i \equiv r_j \mod m \), which cannot happen unless \( i = j \).

Choose a reduced residue system \( r_1 \ldots r_k \mod m \) with \( k = \phi(m) \). By lemma, \( ar_1 \ldots ar_k \) is also a reduced residue system. These two must be permutations of
each other mod m (ie., \(ar_i \equiv r_j \pmod{m}\)).

\[
\begin{align*}
    r_1r_2\ldots r_k & \equiv ar_1ar_2\ldots ar_k \pmod{m} \\
    r_1r_2\ldots r_k & \equiv a^{\phi(m)}r_1r_2\ldots r_k \pmod{m} \\
    (r_1r_2\ldots r_k, m) = 1 & \Rightarrow \text{can cancel} \\
    a^{\phi(m)} & \equiv 1 \pmod{m}
\end{align*}
\]

\textbf{Corollary 17 (Fermat’s Little Theorem).}

\[
a^p \equiv a \pmod{p} \quad \text{for prime } p \text{ and integer } a
\]

\textit{Proof.} If \(p \nmid a\) (ie., \((a, p) = 1\)) then \(a^\phi(p) \equiv 1 \pmod{p}\) by Euler’s Theorem. \(\phi(p) = p - 1 \Rightarrow a^{p-1} \equiv 1 \pmod{p} \Rightarrow a^p \equiv a \pmod{p}\). If \(p|a\), then \(a \equiv 0 \pmod{p}\) so both sides are \(0 \equiv 0 \pmod{p}\). \(\blacksquare\)

\textit{Proof by induction.}

\textbf{Lemma 18 (Freshman’s Dream).}

\[
(x + y)^p \equiv x^p + y^p \pmod{p} \quad x, y \in \mathbb{Z}, \text{ prime } p
\]

\textit{Use the Binomial Theorem.}

\[
(x + y)^p = x^p + y^p + \sum_{k=1}^{p-1} \binom{p}{k} x^k y^{p-k} \equiv 0 \pmod{p}
\]

We saw that \(\binom{p}{k}\) is divisible by \(p\) for \(1 \leq k \leq p - 1\), so

\[
(x + y)^p \equiv x^p + y^p \pmod{p}
\]

\(\blacksquare\)

Induction base case of \(a = 0\) is obvious. Check to see if it holds for \(a + 1\) assuming it holds for \(a\)

\[
(a + 1)^p - (a + 1) \equiv a^p + 1 - (a + 1) \pmod{p} \\
\equiv a^p - a \pmod{p} \\
\equiv 0 \pmod{p} \\
(a + 1)^p \equiv (a + 1) \pmod{p}
\]

This is reversible (if holds for \(a\), then also for \(a - 1\), and so holds for all integers by stepping up or down) \(\blacksquare\)
**Proposition 19** (Inverses of elements mod $m$). If $(a, m) = 1$, then there is a unique integer $b \mod m$ such that $ab \equiv 1 \mod m$. This $b$ is denoted by $\frac{1}{a}$ or $a^{-1} \mod m$.

**Proof of Existence.** Since $(a, m) = 1$ we know that $ax + my = 1$ for some integers $x, y$, and so $ax \equiv 1 \mod m$. Set $b = x$.

**Proof of Uniqueness.** If $ab_1 \equiv 1 \mod m$ and $ab_2 \equiv 1 \mod m$, then $ab_1 \equiv ab_2 \mod m$ implies $m | a(b_1 - b_2)$. Since $(m, a) = 1$, $m | b_1 - b_2 \Rightarrow b_1 \equiv b_2 \mod m$.

**Theorem 20** (Wilson’s Theorem). If $p$ is a prime then $(p - 1)! \equiv -1 \mod p$.

**Proof.** Assume that $p$ is odd (trivial for $p = 2$).

**Lemma 21.** The congruence $x^2 \equiv 1 \mod p$ has only the solutions $x \equiv \pm 1 \mod p$.

**Proof.**

\[
x^2 \equiv 1 \mod p
\]

\[
\Rightarrow p | x^2 - 1
\]

\[
\Rightarrow p | (x - 1)(x + 1)
\]

\[
\Rightarrow p | x \pm 1
\]

\[
\Rightarrow x \equiv \pm 1 \mod p
\]

Note that $x^2 \equiv 1 \mod p \Rightarrow (x, p) = 1$ and $x$ has inverse and $x \equiv x^{-1} \mod p$ \{1\ldots p − 1\} is a reduced residue system mod $p$. Pair up elements $a$ with inverse $a^{-1} \mod p$. Only singletons will be 1 and −1.

\[
(p - 1)! \equiv (a_1 \cdot a_1^{-1})(a_2 \cdot a_2^{-1})\ldots(a_k \cdot a_k^{-1})(1)(-1) \mod p
\]

\[
\equiv -1 \mod p
\]

Wilson’s Theorem lets us solve congruence $x^2 \equiv -1 \mod p$.

**Theorem 22.** The congruence $x^2 \equiv -1 \mod p$ is solvable if and only if $p = 2$ or $p \equiv 1 \mod 4$. 
Proof. $p = 2$ is easy. We’ll show that there is no solution for $p \equiv 3 \mod 4$ by contradiction. Assume $x^2 \equiv -1 \mod p$ for some $x$ coprime to $p$ ($p = 4k + 3$). Note that

$$p - 1 = 4k + 2 = 2(2k + 1)$$

so $(x^2)^{2k+1} \equiv (-1)^{2k+1} \equiv -1 \mod p$. But also,

$$(x^2)^{2k+1} \equiv x^{4k+2} \equiv x^{p-1} \equiv 1 \mod p$$

So $1 \equiv -1 \mod p \Rightarrow p | 2$, which is impossible since $p$ is an odd prime.

If $p \equiv 1 \mod 4$:

$$(p - 1)! \equiv -1 \mod p \text{ by Wilson’s Theorem}$$

$$1(2) \ldots (p - 1) \equiv -1 \mod p$$

show that second factor equals the first

$$p - 1 \equiv (-1)1 \mod p$$

$$p - 2 \equiv (-1)2 \mod p$$

$$\vdots$$

$$\frac{p + 1}{2} \equiv (-1)\frac{p - 1}{2} \mod p$$

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

$\frac{p-1}{2}$ is even since $p \equiv 1 \mod 4$, and so second factor equals the first factor, so $x = \left(\frac{p-1}{2}\right)!$ solves $x^2 \equiv -1 \mod p$ if $p \equiv 1 \mod 4$. $\blacksquare$

**Theorem 23.** There are infinitely many primes of form $4k + 1$

Proof. As in Euclid’s proof, assume finitely many such primes $p_1 \ldots p_n$. Consider the positive integer

$$N = (2p_1p_2 \ldots p_n)^2 + 1$$

$N$ is an odd integer $> 1$, so it has an odd prime factor $q \neq p_i$, since each $p_i$ divides $N - 1$. $q | N \Rightarrow (2p_1 \ldots p_n)^2 \equiv -1 \mod q$, so $x^2 \equiv -1 \mod q$ has a solution and so by theorem $q \equiv 1 \mod 4$, which contradicts $q \neq p_i$. $\blacksquare$
**Definition** Congruence: A *congruence* (equation) is of the form \(a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \equiv 0 \mod m\) where \(a_n \ldots a_0\) are integers. Solution of the congruence are integers or residue classes \(\mod m\) that satisfy the equation.

**Eg.** \(x^p - x \equiv 0 \mod p\). How many solutions? \(p\).

**Eg.** \(x^2 \equiv -1 \mod 5\). Answers = 2, 3.

**Eg.** \(x^2 \equiv -1 \mod 43\). No solutions since \(43 \equiv 3 \mod 4\).

**Eg.** \(x^2 \equiv 1 \mod 15\). Answers = \(\pm 1\), \(\pm 4\) mod 15.

**Note:** The number of solutions to a non-prime modulus can be larger than the degree.

**Definition** Linear Congruence: a congruence of degree 1 (\(ax \equiv b \mod m\))

**Theorem 24.** Let \(g = (a, m)\). Then there is a solution to \(ax \equiv b \mod m\) if and only if \(g | b\). If it has solutions, then it has exactly \(g\) solutions \(\mod m\).

**Proof.** Suppose \(g \nmid b\). We want to show that the congruence doesn’t have a solution. Suppose \(x_0\) is a solution \(\Rightarrow ax_0 = b + mk\) for some integer \(k\). Since \(g | a, g | m\), \(g\) divides \(ax_0 - mk = b\), which is a contradiction. Conversely, if \(g | b\), we want to show that solutions exist. We know \(g = ax_0 + my_0\) for integer \(x_0, y_0\).

If \(b = b'g\), multiply by \(b'\) to get

\[
\begin{align*}
  b &= b'g = b'|ax_0 + my_0 \\
  &= a(b'x_0) + m(b'y_0) \\
  \Rightarrow a(b'x_0) &\equiv b \mod m
\end{align*}
\]

and so \(x = b'x_0\) is a solution.

We need to show that there are exactly \(g\) solutions. We know that there is one solution \(x_1\), and the congruence says \(ax \equiv b \equiv ax_1 \mod m\).

\[
\begin{align*}
  a(x - x_1) &\equiv 0 \mod m \\
  a(x - x_1) &\equiv mk \text{ for some integer } k \\
  g = (a, m) &\Rightarrow a = a'g, \ m = m'g
\end{align*}
\]

So \((a, m') = 1\), so \(a'g(x-x_1) = m'gk \Rightarrow a(x-x_1) = m'k\) for some \(k\). So \(m' | x-x_1\), so \(x \equiv x_1 \mod m'\), so any solution of the congruence must be congruent to \(x\).
mod $m' = m$. So all the solutions are $x_1, x_1 + m', x_1 + 2m', \ldots, x_1 + (g - 1)m'$. They are all distinct, so they are all the solutions mod $m$. ■