Module-5: Wilson's and Chinese Remainder Theorem

Objectives

- Wilson's Theorem.
- Linear congruence equations.
- Chinese Remainder Theorem.

Theorem 1 (Wilson)**.** *If p is prime, then* $(p-1)! \equiv -1 \pmod{p}$.

Proof. It is easy to see the result when $p=2$ or $p=3$. So, assume that $p>3$. Let $a \in \{1,2,3,\ldots,p-1\}$. Then, $ax \equiv 1 \pmod{p}$ has a unique solution $x = a' \in \{1,2,3,\ldots,p-1\}$. Further, verify $a' = a$ holds only when $a=1$ or $a=p-1$. Thus, the $p-3$ elements in the set $\{2,3,\ldots,p-2\}$ can be paired into (a,a') with $a \neq a'$. Hence, if we multiply these $\frac{p-3}{2}$ congruences, we get

$$2\cdot 3\cdot 4\cdots(p-3)(p-2) \equiv 1 \pmod{p}.$$

Or equivalently,

$$(p-2)! \equiv 1 \pmod{p}.$$

Now multiply above equation both sides by $p-1$, to get

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

Alternate proof

By Fermat's little theorem every element in the set $\{1,2,3,\ldots,p-1\}$ satisfies $x^{p-1} \equiv 1 \pmod{p}$. In other words

$$x^{p-1} - 1 \equiv (x-1)(x-2)\cdots(x-(p-1)) \pmod{p}.$$

By substituting $x=0$ in the above equation and the fact that p is an odd prime, we get the required result.

□

The converse of Wilson's theorem is also true. That is, if $(n-1)! \equiv -1 \pmod{n}$, then n is prime. So, suppose that n is not prime. Then n has a divisor, say d, with $1 < d < n$. As $1 < d < n$, $d|(n-1)!$. Also, $n|(n-1)!+1$ and hence $d|1 = [(n-1)!+1]-(n-1)!$, a contradiction. Thus, if $(n-1)! \equiv -1 \pmod{n}$, then n is prime.

Wilson's theorem and its converse provides a necessary and sufficient condition for determining primality. That is, an integer $n > 1$ is prime if and only if $(n-1)! \equiv -1 \pmod{n}$. But this test is of more theoretical than practical interest because as n increases, $(n-1)!$ becomes very large.

An equation of the form $ax \equiv b \pmod{n}$ is called a *linear congruence*, and by a solution to such an equation we mean an integer x_0 such that $ax_0 \equiv b \pmod{n}$. Thus, finding all integers that satisfy $ax \equiv b \pmod{n}$ is identical with that of obtaining all solutions of the linear Diophantine equation $ax - ny = b$.

It is convenient to treat two solutions of $ax \equiv b \pmod{n}$ that are congruent modulo n as being "equal " even though they are not equal in the usual sense. For example, for $3x \equiv 9 \pmod{12}$, the solutions $x = 3$ and $x = -9$ are considered same as $3 \equiv -9 \pmod{12}$. In short: when we refer to the number of solutions of $ax \equiv b \pmod{n}$, we mean the number of incongruent integers that satisfy the required congruence.

Theorem 2. *The Linear congruence $ax \equiv b \pmod{n}$ has a solution if and only if $d|b$, where $d = \gcd(a,n)$. If $d|b$, then it has d mutually incongruent solutions modulo n.*

Corollary 3. *If $\gcd(a,n) = 1$, then the linear congruence $ax \equiv b \pmod{n}$ has a unique solution modulo n.*

Thus, we observe that whenever $\gcd(a,n) = 1$, the study of the linear congruence $ax \equiv b \pmod{n}$ reduces to finding the value of $a^{-1} \pmod{n}$ as $x_0 = ba^{-1} \pmod{n}$ is the solution of $ax \equiv b \pmod{n}$.

Theorem 4 (Chinese Remainder Theorem)**.** *Let $n_1, n_2, \ldots, n_r$ be positive integers such that $\gcd(n_i, n_j) =$*

1 *for* $i \neq j$. *Then, the system of linear congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_r \pmod{n_r} \end{aligned}$$

has a simultaneous solution, which is unique modulo the integer $M = n_1 n_2 \cdots n_r$.

Proof.

1. Let $N_i = \frac{M}{n_i}$ for $1 \leq i \leq r$. Then, $N_1 = n_2 n_3 \cdots n_r, N_2 = n_1 n_3 \cdots n_r, \ldots, N_r = n_1 n_2 \cdots n_{r-1}$.
2. Observe that for $1 \leq k \leq r$, $\gcd(N_k, n_k) = 1$. Hence, for each k, there exists x_k with $1 \leq x_k \leq n_k - 1$ such that $N_k x_k \equiv 1 \pmod{n_k}$.
3. Now verify that $\bar{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 + \cdots + a_r N_r x_r$ is the required solution.
4. Uniqueness: Let x' be another solution. Then $\bar{x} \equiv a_k \pmod{n_k}$ and $x' \equiv a_k \pmod{n_k}$ holds for $1 \leq k \leq r$. Hence, $n_k | \bar{x} - x'$, for $1 \leq k \leq r$. But, $n_1, n_2, \ldots, n_r$ are relatively prime and hence $M = n_1 n_2 \cdots n_k$ divides $\bar{x} - x'$.

□

Note that if x_0 is a solution then so is $x_0 + Mt$ for all $t \in \mathbb{Z}$. When $n_1, n_2, \ldots, n_r$ are pair wise co-prime then the solutions form a single congruence class modulo M, namely $[x_0]_M$. Otherwise, they are the union of several congruence classes or none.

Example 5. *Show that there is no* x *for which both* $x \equiv 29 \pmod{52}$ *and* $x \equiv 19 \pmod{72}$ *holds.*
Solution:Note that the congruence $x \equiv 29 \pmod{52}$ *is equivalent to the simultaneous congruences*

$$x \equiv 1 \pmod{4} \text{ and } x \equiv 3 \pmod{13}.$$

Similarly, the congruence $x \equiv 19 \pmod{72}$ *is equivalent to* $x \equiv 1 \pmod{9}$ *and* $x \equiv 3 \pmod{8}$. *Now, it is easy to check that the congruences* $x \equiv 1 \pmod{4}$ *and* $x \equiv 3 \pmod{8}$ *can't happen simultaneously.*

Example 6. *Solve* $x \equiv 1 \pmod 9$ *and* $x \equiv 1 \pmod 6$.

Solution:Clearly $x = 1, 19$ *and* 37 *satisfy the equations. So, is* $1 + 54t, 19 + 54t$ *and* $37 + 54t$ *for all* $t \in \mathbb{Z}$. *In other words the solution set is* $[1]_{54} \cup [19]_{54} \cup [37]_{54}$.

Example 7. *Solve*

$$\begin{aligned} x &\equiv 1 \pmod 5 \\ x &\equiv 2 \pmod 6 \\ x &\equiv 3 \pmod 7 \end{aligned}$$

Solution:Note that $M = 5 \times 6 \times 7 = 210$ *and* x_i *is chosen so that* $N_i x_i \equiv 1 \pmod{n_i}$. *Now, we fill the following table to get the required answer:*

Sl. No.	a_i	n_i	N_i	x_i	$N_i x_i \equiv 1 \pmod{n_i}$	$a_1 N_1 x_1$
1	*1*	*5*	$n_2 \cdot n_3 = 42$	*3*	$42 \times 3 \equiv 1 \pmod 5$	*126*
2	*2*	*6*	$n_1 \cdot n_3 = 35$	*5*	$35 \times 5 \equiv 1 \pmod 6$	*350*
3	*3*	*7*	$n_1 \cdot n_2 = 30$	*4*	$30 \times 4 \equiv 1 \pmod 7$	*360*
Sum						*836*

Thus, the required solution is $x \equiv 836 \pmod{210}$. *Or equivalently,* $x = 206$ *is the required solution. In other words, 206 is the smallest solution. The general solution is* $206 + 210t$ *or the solution set corresponds to the unique congruence class* $[206]_{210}$.

Example 8. *Solve*

$$\begin{aligned} x &\equiv 3 \pmod 5 \\ x &\equiv 6 \pmod 7 \\ x &\equiv 4 \pmod{11} \end{aligned}$$

Solution:We fill the following table:

Sl. No.	a_i	n_i	N_i	x_i	$N_i x_i \equiv 1 \pmod{n_i}$	$a_1 N_1 x_1$
1	*3*	*5*	$n_2 \cdot n_3 = 77$	*3*	$77 \times 3 \equiv 1 \pmod{5}$	*693*
2	*6*	*7*	$n_1 \cdot n_3 = 55$	*6*	$55 \times 6 \equiv 1 \pmod{7}$	*1980*
3	*4*	*11*	$n_1 \cdot n_2 = 35$	*6*	$35 \times 6 \equiv 1 \pmod{7}$	*840*
Sum						*3513*

Since

$$3513 \equiv 48 \pmod{385},$$

hence 48 is the smallest solution. Every other solution belongs to the congruence class $[48]_{385}$.

Few Comments on Chinese Remainder Theorem:

1. Let us take a fixed set of positive integers $n_1, n_2, \ldots, n_r$ that are relatively prime in pairs, with product M.

2. Note that we have chosen $a_i \in \mathbb{Z}_i$, for $1 \le i \le r$. In general, a_i may be any integer in a complete residue system modulo n_i, for $1 \le i \le r$.

3. Now, we defined a map $f : \mathbb{Z}_M \to \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_r}$ by
$$f(x) = (x \pmod{n_1}, x \pmod{n_2}, \ldots, x \pmod{n_r}).$$

4. Then, we see that $f(x+y) = f(x) + f(y)$ as $x + y \pmod{n_i} \equiv x \pmod{n_i} + y \pmod{n_i}$, for $1 \le i \le r$.

5. Moreover, for any r-tuples $(a_1, a_2, \ldots, a_r) \in \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \mathbb{Z}_{n_r}$, by Chinese Remainder Theorem, we can find a unique $x \in \mathbb{Z}_M$ such that
$$f(x) = (x \pmod{n_1}, x \pmod{n_2}, \ldots, x \pmod{n_r}) = (a_1, a_2, \ldots, a_r).$$

6. Also, we see that the number of elements in $\mathbb{Z}_M$ and $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \mathbb{Z}_{n_r}$ are same. So, f is an onto function implies that f is one-one as well. Thus, we have a one-to-one correspondence

between the r-tuples $(a_1, a_2, \ldots, a_r) \in \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \mathbb{Z}_{n_r}$ and the complete residue system modulo M.

7. Symbolically , the above argument can be expressed by writing

$$\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_r} \cong \mathbb{Z}_M.$$

The following example illustrates this correspondence:

Example 9. *Let* $n_1 = 5, n_2 = 7$ *and* $M = 35$ *and let* c_{ij} *denote the entry in the i-th row and* j*-th column of the following table of size* $5 \times 7 = n_1 \times n_2$*. Then,* $c_{ij} \equiv i \pmod 5$ *and* $c_{ij} \equiv j \pmod 7$*. For example,* $c_{34} = 18$ *as* $18 = 3 \pmod 5$ *and* $18 = 4 \pmod 7)$*, as well. So, by the Chinese Remainder Theorem* 18 *corresponds to the tuple* $(3,4)$ *as shown in the table.*

$1 \leftrightarrow (1,1)$	*16↔(1,2)*	$31 \leftrightarrow (1,3)$	*11↔(1,4)*	*26↔(1,5)*	*6↔ (1,6)*	*21↔(1,7) or (1,0)*
$22 \leftrightarrow (2,1)$	*2↔(2,2)*	$17 \leftrightarrow (2,3)$	*32↔(2,4)*	*12↔(2,5)*	*27↔(2, 6)*	*7↔(2,7)*
8↔(3,1)	$23 \leftrightarrow (3,2)$	$3 \leftrightarrow (3,3)$	$18 \leftrightarrow (3,4)$	*33↔(3,5)*	*13↔(3,6)*	$28 \leftrightarrow (3,7)$ *or (3,0)*
29↔(4,1)	$9 \leftrightarrow (4,2)$	*24↔(4,3)*	*4↔(4,4)*	*19↔(4, 5)*	*34↔(4,6)*	$14 \leftrightarrow (4,7)$
15↔(5,1)	*30↔(5,2)*	*10↔(5,3)*	*25↔(5,4)*	$5 \leftrightarrow (5,5)$	*20↔(5,6)*	*35↔(5,7) or (0,0)*