Computer Science & Engineering Department
IIT Kharagpur
Computational Number Theory: CS60094
Lecture III

Instructor: Goutam Biswas *Spring Semester 2014-2015*

1 Basic Properties of Integers II

We shall start with the definition of one of the most important binary relations in number theory. The notation for this relation was introduced by Carl Friedrich Gauss[1]

1.1 Congruences and Modular Arithmetic

We start with the definition of the binary relation *congruence modulo* n.
Definition 1: Given a positive integer n, we define a binary relation on $\mathbb{Z}$. Two integers a and b are said to be related if $n|(a-b)$. We write $a \equiv b (\text{mod } n)$ and read it as "a is congruent to b modulo n".

In other words, a is congruent to b modulo n, if $a \bmod n = b \bmod n$ i.e. $a = pn + r$ and $b = qn + r$, where $0 \leq r < n$. Both a and b leave same remainder when divided by n. So we get $a - b = n(p - q)$ or $a = b + ns$, for some $s \in \mathbb{Z}$.

It is not difficult to prove that *congruence* is an equivalence relation - for all $a, b, c \in \mathbb{Z}$,

- $a \equiv a (\text{mod } n)$,
- if $a \equiv b (\text{mod } n)$, then $b \equiv a (\text{mod } n)$,
- if $a \equiv b (\text{mod } n)$ and $b \equiv c (\text{mod } n)$, then $a \equiv c (\text{mod } n)$.

We know that an equivalence relation partitions the underlying set into *equivalence classes*. Elements of each class are equivalent to one another. In case of *congruence modulo* n, an equivalence class contains all integers that have same remainders when divided by n. Corresponding to n remainders $0, 1, \cdots, n-1$, there are n equivalence classes, $[0], \cdots, [n-1]$.

Example 1. Let $n = 7$, there are seven possible values of remainders $0, 1, 2, 3, 4, 5, 6$ when any integer is divided by 7. Corresponding equivalence classes are $[0], [1], [2], [3], [4], [5], [6]$. No two of these classes have any common elements and their union is the set of integers. Following is an example of an equivalence class.

$$\cdots = [-17] = [-10] = [-3] = [4] = [11] = \cdots = \{\cdots, -17, -10, -3, 4, 11, \cdots\}.$$

The congruence relation is *consistent* or *compatible* with the arithmetic operations of $\mathbb{Z}$.
Proposition 1. Let $a, b, c, d, n \in \mathbb{Z}$ and $n > 1$. If $a \equiv b (\text{mod } n)$ and $c \equiv d (\text{mod } n)$, then $a + c \equiv b + d (\text{mod } n)$ and $a \times c \equiv b \times d (\text{mod } n)$.
Proof: Let $a = b + ns$ and $c = d + nt$, so $a + c = (b + d) + nu$, where $u = s + t$. Similarly, $a \times c = (b + ns)(d + nt) = bd + nv$, where $v = s(d + nt) + bnt$. QED.

Following are a few properties of congruence where $a, b, c, d \in \mathbb{Z}$ and n, k is a positive integer.

1. If $a \equiv b (\text{mod } n)$, then $a + c \equiv b + c (\text{mod } n)$ and $ac \equiv bc (\text{mod } n)$.
2. If $a \equiv b (\text{mod } n)$, then $a^k \equiv b^k (\text{mod } n)$.
3. If $ac \equiv bc (\text{mod } n)$, then $a \equiv b (\text{mod } \frac{n}{d})$, where $gcd(c, n) = d$.

[1] In his book *Disquisitiones Arithmeticae*, Gauss noted, "*We have adopted this symbol because of the analogy between equality and congruence. For the same reason Legendre, in the treatise which we shall often have occasion to cite, used the same sign for equality and congruence. To avoid ambiguity we have made a distinction.*"

Proof: We shall give the proof of (3) only. Let $c = dc'$ and $n = dn'$. We know that $gcd(c', n') = 1$ and $(a-b)c = nk$ for some integer k. Dividing both sides by d we get $(a-b)c' = n'k$. As $gcd(c', n') = 1$, $n'|(a-b)$. So, $a \equiv b (\text{mod } n')$ i.e. $a \equiv b (\text{mod } \frac{n}{d})$. QED.
There are two important corollaries: (i) If $ac \equiv bc (\text{mod } n)$ and $gcd(c, n) = 1$, then c can be cancelled from both sides i.e. $a \equiv b (\text{mod } n)$. (ii) If n is a prime and $n \not| c$, then $gcd(c, n) = 1$, and again $a \equiv b (\text{mod } n)$. Note that in general we cannot do this cancellation, $3 \times 5 \equiv 3 \times 2 (\text{mod } 9)$, but $5 \not\equiv 2 (\text{mod } 9)$.

The structure $(\mathbb{Z}, +, \times, 0, 1)$ is a *commutative ring with identity*, and the congruence relation is consistent with both the operations. This implies that the *quotient set*, $\mathbb{Z}/\equiv (\text{mod } n)$, denoted by $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}_n = \{[0], [1], \cdots, [n-1]\}$ (we assume $n > 1$), also forms a *commutative ring with identity* under modulo-n addition and multiplication operations.

We often denote the equivalence class $[m]$ by the least non-negative element of $[m]$. It is the usual remainder when any element of $[m]$ is divided by n. In this notation $\mathbb{Z}_n = \{0, 1, \cdots, n-1\}$. But it is perfectly acceptable to take a set of n integers $a_1, a_2, \cdots, a_n$, taken one from each equivalence class, to represent $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}_n$. Such a set of integers is called a *complete system of residues*.
Definition 2: We define $+_m$ and $\times_n$ (or $\cdot_n$) on $\mathbb{Z}_n$ as follows:

$$a +_n b = (a + b) \mod n, \quad a \times_n b = (a \times b) \times_n n.$$

Both operations are well-defined due to compatibility of '+' and '×' with congruence. As we claimed earlier, the structure $(\mathbb{Z}_n, +_n, \times_n, 0, 1)$ is a commutative ring with identity.
Proposition 2. Let $[a]$ be a congruence class of $\mathbb{Z}$ modulo positive integer n, and $b \in [a]$. If $gcd(a, n) = 1$, then $gcd(b, n) = 1$.
Proof: So we have $ax + ny = 1$ and $a = b + nk$, for some $x, y, k \in \mathbb{Z}$. So we have $(b+nk)x + ny = 1$ i.e. $bx + n(kx + y) = 1$. So b is also relatively prime to n QED.

We define an interesting subset of $\mathbb{Z}_n$ in the following way.
Definition 3: $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n : gcd(a, n) = 1\}$. the size of $\mathbb{Z}_n^*$, is given by the *Euler's totient* function $\phi(n)$, the count of integers within 0 to n that are relatively prime to n.
Proposition 3. Prove that $(\mathbb{Z}_n^*, \times_n)$ is an abelian group, where $n > 1$.
Proof: We shall show that $\mathbb{Z}_n^*$ is closed under $\times_n$, $1 \in \mathbb{Z}_n^*$ and if $a \in \mathbb{Z}_n^*$, then there is $b \in \mathbb{Z}_n^*$, so that $a \times_n b = 1$. The associativity comes free of cost.

$gcd(n, 1) = 1$, so $1 \in \mathbb{Z}_n^*$.
Let $a, b \in \mathbb{Z}_n^*$, so we have by the Bezout's identity, $ax_a + ny_a = 1$ and $bx_b + ny_b = 1$, where $x_a, y_a, x_b, y_b \in \mathbb{Z}$. Multiplying the identity we get $ab(x_a x_b) + n(x_a y_b + y_a x_b + n y_a y_b) = 1$. So we have $gcd(ab, n) = gcd(ab \bmod n, n) = 1$ i.e. $a \times_n b \in \mathbb{Z}_n^*$.
Let $a \in \mathbb{Z}_n^*$, so by the Bezout's identity we have $ax + ny = 1$, where $x, y \in \mathbb{Z}$. It is clear that $gcd(x, n) = 1$. Let $x = nq + b$, where $0 \le b < n$. So $gcd(x, n) = gcd(b, n) = 1$ i.e. $b \in \mathbb{Z}_n^*$. Again, $a(nq+b) + ny = 1$ implies that $ab \equiv 1 (\text{mod } n)$ i.e. $a \times_m b = 1$. So b is the inverse of a. QED.

A *commutative ring with identity* is called a *field* if every non-zero element has a multiplicative inverse. It is clear from our previous discussion that $\mathbb{Z}_p^* = \{1, \cdots, p-1\}$ if p is a prime ($gcd(p, q) = 1$, $1 \le q < p$). We have already proved that $\mathbb{Z}_p^*$ is an *abelian group*. So for every prime p, $(\mathbb{Z}_p, +_p, 0, \times_p, 1)$ is a *field*.

1.1.1 Linear Congruence

We are now ready to solve linear congruence. We start with the following example.

Example 2. Consider the congruence $5x + 4 \equiv 3 (\text{mod } 7)$. Subtracting 4 from both sides we get, $5x \equiv -1 (\text{mod } 7)$. We know $5 \times 3 \equiv 1 (\text{mod } 7)$ so we multiply our congruence by 3 and get $x \equiv -3 (\text{mod } 7)$. So the solutions of x are those integers that belongs to the equivalence class of $[4] = [-3] = \{\cdots, -17, -10, -3, 4, 11, \cdots\}$.

It is easy to verify that these are solutions of the original equation. Take $x = -10$, $-10 \times 5 + 4 = -46 \equiv 3 (\mathrm{mod}\ 7)$.

The congruence $5x \equiv -1 (\mathrm{mod}\ 7)$ is equivalent to $5x \equiv 6 (\mathrm{mod}\ 7)$. As $gcd(5, 7) = 1$, $5 \in \mathbb{Z}_7^*$. So there is the inverse of 5 in $\mathbb{Z}_7^*$, which is 3. We can multiply the congruence by 3 and get $(3 \times 5)x \equiv (3 \times 6) (\mathrm{mod}\ 7)$ i.e. $x \equiv 4 (\mathrm{mod}\ 7)$.

Example 3. Now consider the congruence $3x \equiv 2 (\mathrm{mod}\ 6)$. There is no x satisfying the congruence. From the algebraic point of view $3 \notin \mathbb{Z}_6^*$, so there is no multiplicative inverse of it. So 3 cannot be cancelled from the left side. Another view is that the subgroup $\{0, 3\}$ of $(\mathbb{Z}_6, +)$ does not contain 2.

It is clear that all linear congruence cannot be solved. Following theorem characterises it.

Theorem 4. Let $a, n \in \mathbb{Z}$, $n > 0$, and $gcd(a, n) = d$. For each $b \in \mathbb{Z}$, the congruence $ax \equiv b (\mathrm{mod}\ n)$ has a solution, if and only if $d|b$.

Proof: Let $a = da', n = dn'$, where $gcd(a', n') = 1$. Let $b \in \mathbb{Z}$ such that the congruence has a solution:

$$\begin{aligned} & ax \equiv b (\mathrm{mod}\ n) \\ \Rightarrow\ & ax = b + qn, \text{ for some } q \in \mathbb{Z} \\ \Rightarrow\ & ax - qn = b \\ \Rightarrow\ & d(a'x - qn') = b \\ \Rightarrow\ & d|b. \end{aligned}$$

We know that there are integers α, β so that $d = a\alpha + n\beta$. If $d|b$, then $b = kd = k \cdot (a\alpha + n\beta) = a\alpha + n\beta$. So α is a solution of $ax \equiv b (\mathrm{mod}\ n)$. QED.

We know under which condition a linear congruence has a solution. Our next propositions show a few properties of the solutions.

Proposition 5.

1. If the linear congruence $ax \equiv b (\mathrm{mod}\ n)$ has a solution, then there is a solution in $\mathbb{Z}_n$.

2. If x is a solution of the linear congruence $ax \equiv b (\mathrm{mod}\ n)$, then every integer of the form $x + ni/d$, where $d = gcd(a, n)$ and $i \in \mathbb{Z}$, is also a solution; and every solution is of this form.

3. If x is a solution of the linear congruence $ax \equiv b (\mathrm{mod}\ n)$ and $d = gcd(a, n)$, then $x + ni/d$, where $i \in \{0, \cdots, d - 1\}$ are incongruent solutions.

4. Let $d = gcd(a, n)$, then every solution of $ax \equiv b (\mathrm{mod}\ n)$ is congruent to a solution of the form $x + ni/d$, where $i \in \{0, \cdots, d - 1\}$.

Proof:

1. Let x be a solution. By the division algorithm $x = nq + x_0$, $0 \leq x_0 < n$. We have $nk = ax - b = a(nq + x_0) - b$. So $n(k - aq) = ax_0 - b$, implies $n|(ax_0 - b)$ and x_0 is a solution of the congruence.

2. $a(x + ni/d) \equiv ax + ani/d \equiv ax + a'ni \equiv ax \equiv b (\mathrm{mod}\ n)$, where $a = a'd$. So $(x + ni/d)$ is a solution of the congruence.
   Let y be any solution of the congruence. We have $ax \equiv ay (\mathrm{mod}\ n)$. Let $a = a'd$, so $gcd(a', n) = 1$, and we can cancel a' from both sides. We have $dx \equiv dy (\mathrm{mod} n) \Rightarrow dy = dx + ni \Rightarrow y = x + ni/d$, where $i \in \mathbb{Z}$.

3. Let $n = n'd$. If $x + ni/d \equiv x + nj/d (\mathrm{mod}\ n)$, where $i, j \in \{0, \cdots, d - 1\}$, then $n(i - j)/d = n'(i - j)$ is divisible by n. But that is not possible unless $i = j$ as $0 < |i - j| < d$.

4. Let $x + nj/d$ be a solution. We can write $j = dq + i$, where $0 \leq i < d$. So $x + nj/d \equiv x + n(dq + i)/d \equiv x + nq + ni/d \equiv x + ni/d (\mathrm{mod}\ n)$.

QED.

Our final conclusion is that $ax \equiv b(\text{mod } n)$ has exactly d incongruent solutions when $gcd(a, n) = d$ divides b. The solution is *unique* (up to congruence) if a and n are relatively prime i.e. $a \in \mathbb{Z}_n^*$. The congruence $ax \equiv b(\text{mod } n)$ has a solution when $b \text{ mod } n$ is an element of the subgroup of $\mathbb{Z}_n$ generated[2] by $a \text{ mod } n$. In fact $ax \equiv b(\text{mod } n)$ has a solution if and only if $a'x \equiv b'(\text{mod } n')$ has a solution, where $a = a'd, b = b'd$ and $n = n'd$, such that $gcd(a, n) = d$.

If $gcd(a, n) = 1$, the congruence $ax \equiv b(\text{mod } n)$ may be viewed as an equation $ax = b$ in $\mathbb{Z}_n^*$. The solution is $x = a^{-1} \times_n b$. This also explains the cancellation law when $gcd(a, n) = 1$. $ax \equiv ay(\text{mod } n) \Rightarrow x \equiv y(\text{mod } n)$ is equivalent to $ax = ay \Rightarrow x = y$ in $\mathbb{Z}_n^*$.

Example 4. The congruence $6x \equiv 15(\text{mod } 21)$ has a three solutions 6, 13 and 20 in $\mathbb{Z}_{21}$ as $gcd(6, 21) = 3$ and $3|15$.
The congruence can be reduced to $2x \equiv 5(\text{mod } 7)$ which has unique solution 6 in $\mathbb{Z}_7$.

The equation $6x \equiv b(\text{mod } 21)$ has a solution if b is an element of the subgroup $\{0, 3, 6, 9, 12, 15, 18\}$ of $\mathbb{Z}_{21}$ generated by 6.
We define a homomorphism $f : \mathbb{Z}_{21} \to \mathbb{Z}_7,\ x \mapsto x \text{ mod } 7$. The Kernel of f is $\{0, 7, 14\}$ (elements of $\mathbb{Z}_{21}$ mapped to 0 of $\mathbb{Z}_7$). $Kerf$ is a subgroup of $\mathbb{Z}_{21}$, which defines the following equivalence relation on $\mathbb{Z}_{21}$: $a \equiv b(\text{mod } Kerf)$ if $a +_{21} (-b) \in Kerf$. Each equivalence class has three elements. There is an isomorphism $\phi : Imf \to \mathbb{Z}_{21}/Kerf$. The solution of $2x \equiv 5(\text{mod } 7)$ is 6. $\phi(6) = \{6, 13, 20\}$, three solutions of $6x \equiv 15(\text{mod } 21)$.

Algorithmically the solution of $ax \equiv b(\text{mod } n)$ is simple.

1. Compute $gcd(a, n) = d$ and the Bezout's coefficients x, y so that $ax+ny = d$.
2. If $d|b$, then there is a solution.
3. If $b = db'$, then $a(xb') + nyb' = b$. So $xb' \text{ mod } n = x_0$ is a solution in $\mathbb{Z}_n$.
4. We can find all other solutions as $(x_0+ni/d) \text{ mod } n$, where $i = 1, \cdots, d-1$.

1.1.2 Linear Diophantine Equation of Two Variables

We consider the equation $ax + by = c$, where $a, b, c \in \mathbb{Z}$ and a, b are non-zero. We wish to get solutions of x, y in integers. Without any loss of generality we may take $b > 0$. If $b < 0$ we take $b' = -b$ and solve the equation $ax + b'y = c$. Any solution of $ax + b'y = c$ gives a solution of the original equation.
Proposition 6. The two variable Diophantine equation $ax+by = c$ has a solution if and only if the linear congruence $ax \equiv c(\text{ mod } b)$ has a solution, where $b > 0$.
Proof: If x_0, y_0 is a solution of $ax + by = c$, then x_0 is a solution of $ax \equiv c(\text{mod } b)$.

If x_0 is a solution of $ax \equiv c(\text{mod } b)$, then there is a some $y_0 \in \mathbb{Z}$ such that $ax_0 - c = by_0$ i.e. $ax_0 + b(-y_0) = c$. So, $(x_0, -y_0)$ is a solution of $ax + by = c$. QED.

So we conclude that $ax+by = c$ has a solution if and only if $gcd(a, b)$ divides c. If (x_0, y_0) is a solution of $ax+by = c$, and $gcd(a, b) = d$, then $(x_0 - \frac{bi}{d}, y_0 + \frac{ai}{d})$ is a solution of $ax + by = c$, where $i \in \mathbb{Z}$.

1.1.3 The Chinese Remainder Theorem

Let $\{n_1, \cdots, n_k\}$ be a set of pairwise relatively prime positive integers. Our main claim is that there is a bijection between $\mathbb{Z}_N$ and $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$, where $N = \prod_{i=1}^{k} n_i$. We start with the following example.

Example 5. Let $k = 2$ and $n_1 = 3$ and $n_2 = 4$. Following is a sequence of

[2] Afterward we shall talk about a subgroup generated by an element of a group.

remainders.

m mod 12	0	1	2	3	4	5	6	7	8	9	10	11
m mod 3	0	1	2	0	1	2	0	1	2	0	1	2
m mod 4	0	1	2	3	0	1	2	3	0	1	2	3

The mapping is from $\mathbb{Z}_{12} \to \mathbb{Z}_3 \times \mathbb{Z}_4$ is $a \mapsto (a \bmod 3, a \bmod 4)$. We may view a as $[b]_{12}$, $a \bmod 3 = [b]_3$, $a \bmod 4 = [b]_4$, where $b \in \mathbb{Z}$.

Modulo-12 arithmetic on $\mathbb{Z}_{12}$ is equivalent to modulo-3 and modulo-4 arithmetic on $\mathbb{Z}_3$ and $\mathbb{Z}_4$ respectively. $5 +_{12} 9 = [5+9]_{12} = 2$ in the domain, and in the codomain $(2 +_3 0, 1 +_4 1) = (2, 2)$. Similarly, $5 \times_{12} 9 = 9$ in the domain, and in the codomain $(2 \times_3 0, 1 \times_4 1) = (0, 1)$.

Theorem 7. Let $\{n_i\}_{i=1}^k$ be a set of pairwise coprime natural numbers. The map

$$f : \mathbb{Z}_N \to \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k},\ a \mapsto (a \bmod n_1, \cdots, a \bmod n_k),$$

is a *bijection*, where $N = n_1 \times \cdots \times n_k$.

Proof: The size of $\mathbb{Z}_N$ is same as the size of $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$. So it is sufficient to show that the map is an injection.

Let $a, b \in \mathbb{Z}_N$ and $f(a) = f(b)$ i.e.

$$(a \bmod n_1, \cdots, a \bmod n_k) = (b \bmod n_1, \cdots, b \bmod n_k).$$

So we have $a \equiv b (\bmod n_i)$, where $i = 1, \cdots, k$ i.e. $n_i | (a-b)$ for all $i = 1, \cdots, k$. But all n_i's are relatively prime so their product N divides $(a-b)$[3]. But that is impossible if a and b are distinct, as $0 \leq |a-b| < N$. So, $a = b$ and the map is an injection. QED.

This is the *Chinese Remainder Theorem* which states that given a set $\{n_i\}_{i=1}^k$ of relatively prime positive integers and k congruence, $x \equiv a_i (\bmod n_i)$, where $a_i \in \mathbb{Z}_{n_i}$, there is a unique $a \in \mathbb{Z}_N$ that satisfies all the congruence.

Example 6. This map is not a bijection if n_i's are not relatively prime. Let $n_1 = 4$ and $n_2 = 6$. So $N = 24$. In this case $f(a) = (a \bmod 4, a \bmod 6)$ is not an injection. $f(0) = f(12) = (0, 0)$, $f(1) = f(13) = (1, 1)$ and so on.

Following proposition gives a construction of a.

Proposition 8. Let $\{n_i\}_{i=1}^k$ be a set of pairwise coprime positive integers and $\{a_i\}_{i=1}^k$ be a set of integers. Then the set of k linear congruence $x \equiv a_i \pmod{n_i}$, $i = 1, \cdots, k$ has a unique solution i.e. there is an integer a so that

$$a \equiv a_i (\bmod n_i), \text{ for all } i = 1, 2, \cdots, k.$$

Proof: The proof is a consequence of the previous theorem. We give a construction of a solution.

Let $N = \prod_{i=1}^k n_i$. We define the sequence $\{N_i\}_{i=1}^k$, where $N_i = N/n_i$. So, $gcd(N_i, n_i) = 1$ and the linear congruence $N_i x \equiv 1 (\bmod n_i)$ has a unique (up to congruence) solution. The reason is $N_i \bmod n_i \in \mathbb{Z}_{n_i}^*$ and it has an inverse. Let $(N_i \bmod n_i)^{-1} = m_i$ and $e_i = N_i m_i$. It is clear that

$$e_i \bmod n_j = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

This is so because $n_j | N_i$ if $i \neq j$. Our solution is

$$a = a_1 e_1 + a_2 e_2 + \cdots + a_k e_k \equiv a_i (\bmod n_i).$$

QED.

Example 7. Let $k = 3, n_1 = 4, n_2 = 9, n_3 = 25$ and let the congruence be $x \equiv 2 (\bmod 4)$, $x \equiv 6 (\bmod 9)$ and $x \equiv 11 (\bmod 25)$. So $N = 900$ and $N_1 = 225, N_2 = 100, N_3 = 36$.

[3] Let m, n be relatively prime integers and both of them divides a i.e. $a = ma_1$, $a = na_2$. We know there are $x, y \in \mathbb{Z}$ so that $mx + ny = 1$. We have $a = a \times 1 = a(mx + ny) = amx + any = na_2 mx + ma_1 ny = mn(a_2 x + a_1 y)$, implies that $mn | a$.

We solve $225x \equiv 1(\text{mod } 4)$ and get $x \equiv 1(\text{mod } 4)$ as $225 \bmod 4 = 1$, $100x \equiv 1(\text{mod } 9)$ and get $x \equiv 1(\text{mod } 9)$, as $100 \bmod 9 = 1$ and $36x \equiv 1(\text{mod } 25)$ and get $x \equiv 16(\text{mod } 25)$, as $1 = 36 \times (-9) + 25 \times 13$ i.e. $36 \times (-9) \equiv 1(\text{mod } 25$. But then $-9 \equiv 16(\text{mod } 25)$, so 16 is the inverse of 36 mod 25. So $e_1 = 225 \times 1 = 225$, $e_2 = 100 \times 1 = 100$, and $e_3 = 36 \times 16 = 576$. So the value of

$$a = 2 \times 225 + 6 \times 100 + 11 \times 576 \equiv 186(\text{mod} 900).$$

The map f not only gives a bijection from $\mathbb{Z}_N \to \prod_{i=1}^{k} \mathbb{Z}_{n_i}$. Following proposition shows that there is another bijection.

Proposition 9. Restriction of f to $\mathbb{Z}_N^*$ is a bijection from $\mathbb{Z}_N^* \to \mathbb{Z}_{n_1}^* \times \cdots \times \mathbb{Z}_{n_k}^*$.

Proof: It is enough to show that $a \in \mathbb{Z}_N^*$ if and only if $(a \bmod n_1, \cdots, a \bmod n_k) \in \mathbb{Z}_{n_1}^* \times \cdots \times \mathbb{Z}_{n_k}^*$.

Let $a \in \mathbb{Z}_N^*$. By the Bezout's identity, $au + Nv = 1$, where $u, v \in \mathbb{Z}$. Using the division algorithm we write $a = q_i n_i + a_i$, $0 \leq a_i < n_i$ i.e $a_i = a \bmod n_i$ for $i = 1, \cdots, k$. Substituting the value of a we get $(q_i n_i + a_i)u + n_i N_i v = 1$ i.e. $a_i u + n_i(q_i u + N_i v) = 1$. So $gcd(a_i, n_i) = 1$. i.e. $a_i \in \mathbb{Z}_{n_i}^*$.

Let $f(a) = (a_1, \cdots, a_k) \in \mathbb{Z}_{n_1}^* \times \cdots \times \mathbb{Z}_{n_k}^*$, where $a \in \mathbb{Z}_N$. By the Bezout's identity we have $a_i u_i + n_i v_i = 1$, for $i = 1, \cdots, k$. In other words, $a_i u_i \equiv 1(\text{mod } n_i)$, for $i = 1, \cdots, k$.

From the *Chinese Remainder theorem* we know that the system of congruence $x \equiv u_i(\text{mod } n_i)$, for $i = 1, \cdots, k$, has a solution u in $\mathbb{Z}_N$, such that $u \equiv u_i(\text{mod } n_i)$, for $i = 1, \cdots, k$. We also have $a \equiv a_i(\text{mod } n_i)$. Multiplying we get $au \equiv a_i u_i \equiv 1(\text{mod } n_i)$, for $i = 1, \cdots, k$. So $au \equiv 1(\text{mod } N)$[4] implies that $gcd(a, N) = 1$, so $a \in \mathbb{Z}_N^*$. QED.

1.1.4 Euler's Totient Function

Euler's *totient function* $\phi : \mathbb{N} \to \mathbb{N}$. The value of $\phi(n)$ is the number of integers in the range 1 to $n-1$ that are relatively prime to n. The value of $\phi(1)$ is defined to be 1. We also know that $\phi(n) = |\mathbb{Z}_n^*|$.

Proposition 10. Let $\{n_1, \cdots, n_k\}$ be a set of pairwise relatively prime integers. $\phi(\prod_{i=1}^{k} n_i) = \prod_{i=1}^{k} \phi(n_i)$.

Proof: Let $N = \prod_{i=1}^{k} n_i$. The proof is a direct consequence of the bijection between $\mathbb{Z}_N^*$ and $\mathbb{Z}_{n_1}^* \times \cdots \times \mathbb{Z}_{n_k}^*$.

$$\begin{aligned}
\phi(\prod_{i=1}^{k} n_i) &= \phi(N) \\
&= |\mathbb{Z}_N^*| \\
&= |\mathbb{Z}_{n_1}^* \times \cdots \times \mathbb{Z}_{n_k}^*| \\
&= |\mathbb{Z}_{n_1}^*| \times \cdots \times |\mathbb{Z}_{n_k}^*| \\
&= \phi(n_1) \times \cdots \times \phi(n_k).
\end{aligned}$$

QED.

If p is a prime, then $\phi(p) = p - 1$. It is not difficult to find the the value of $\phi(p^k)$. There are p^{k-1} multiples of p in the range of $0 \cdots (p^k - 1)$. They are $1 \cdot p, 2 \cdot p, \cdots, (p^{k-1} - 1) \cdot p$. So the integers that are relatively prime to p in that range are, $(p^k - 1) - (p^{k-1} - 1) = p^k - p^{k-1} = p^{k-1}(p-1) = p^k(1 - 1/p)$.

Proposition 11. $\phi(n) = n \prod_{i=1}^{k}(1 - 1/p_k)$, where the prime factorisation of n is $p_1^{e_1} \cdot \cdots \cdot p_k^{e_k}$.

[4] If $a \equiv b(\text{mod } m)$, $a \equiv b(\text{mod } n)$ and $gcd(m, n) = 1$, then $m|(a-b)$ and $n|(a-b)$. We have already argued that $mn|(a-b)$, so $a \equiv b(\text{mod } mn)$.

Solution:

$$\begin{aligned}\phi(n) &= \phi(p_1^{e_1} \cdot \cdots \cdot p_k^{e_k}) \\ &= \phi(p_1^{e_1}) \times \cdots \times \phi(p_k^{e_k}) \\ &= \prod_{i=1}^{k} p_i^{e_i}(1 - 1/p_i) \\ &= n \prod_{i=1}^{k}(1 - 1/p_i).\end{aligned}$$

QED.

1.1.5 Cyclic Group, Euler's and Fermat's Theorem

Let $(G, \cdot, e)$ be a group and $a \in G$. We define an integer powers of a as follows.

$$\begin{aligned}a^0 &= e \\ a^n &= a \cdot a^{n-1},\ n \geq 1.\end{aligned}$$

We further define $a^{-n} = (a^{-1})^n$. Informally, for $n \geq 1$

$$a^n = \overbrace{a \circ \cdots \circ a}^{n\text{-times}},\ \text{and}\ a^{-n} = \overbrace{a^{-1} \circ \cdots \circ a^{-1}}^{n\text{-times}}.$$

Proposition 12. Let $(G, \cdot, e)$ be a group and $a \in G$. The set

$$< a >= \{a^n :\ n \in \mathbb{Z}\}$$

is a *commutative* or *abelian* subgroup of G generated by a.

We leave the proof as an exercise where we have to show that (i) $< a >$ is closed, (ii) $e \in < a >$, (iii) for every $b \in < a >$, $b^{-1} \in < a >$, and finally (iv) for all $b, c \in < a >$, $b \cdot c = c \cdot b$. The associativity law is inherited from G.

Example 8. Consider $(\mathbb{Z}_{20}^*, \times_{20}, 1)$, $\mathbb{Z}_{20}^* = \{1, 3, 7, 9, 11, 13, 17, 19\}$. Let the generator $a = 3$. The cyclic subgroup of $\mathbb{Z}_{20}^*$ is $< 3 >= \{3, 9, 7, 1\}$.
Definition 4: A group $(G, \cdot, e)$ called *cyclic* if $G =< a >$ for some $a \in G$. In this case a is called a *generator* of the group.

Example 9. Consider the group $(\mathbb{Z}_{13}^*, \times_{13}, 1)$. If we take 4 as the generator, we get

$$< 4 >= \{4^1 = 4, 4^2 = 3, 4^3 = 12, 4^4 = 9, 4^5 = 10, 4^6 = 1\},$$

a proper subgroup of $\mathbb{Z}_{13}^*$. But if we take 2 as the generator, we get $< 2 >= \mathbb{Z}_{13}^*$.

A few other cyclic groups are as follows:

1. $(\mathbb{Z}, +, 0)$ is a cyclic group with 1 and -1 as generators.
2. $(\mathbb{Z}_n, +_n, 0)$ is cyclic with $m \in \mathbb{Z}_n$ as a generator, where $gcd(n, m) = 1$.
3. $(\mathbb{Z}_7^*, \times_7, 1)$ is cyclic with 3 and 5 as generators.
4. $(\mathbb{Z}_{25}^*, \times_{25}, 1)$ is cyclic with 2 as a generator.

Definition 5: An integer a is called a *primitive root* of a positive integer n, if $gcd(a, n) = 1$ and $a \bmod n$ is a generator of $\mathbb{Z}_n^*$. The order of a is $\phi(n)$.

$\mathbb{Z}_n^*$ is not cyclic for every $n \in \mathbb{Z}^+$ (does not have *primitive root*). They are cyclic when $n = 1, 2, 4, p^k$ and $2p^k$, where p is an odd prime and k is a positive integer.

Let $(G, \cdot, e)$ be a group and $a \in G$. The size of $< a >$ may be finite or infinite. If it is finite then $| < a > |$ is called the order of the subgroup generated by a; otherwise the order is infinite.

If the order of $< a >$ is finite, then all powers of a cannot be distinct and we have $a^k = a^l$, where $k > l$. By cancellation, we have $a^{k-l} = e$. So there is a *least positive integer* n so that we have

$$a^0 = e, a^1, \cdots, a^{n-1}, a^n = e,$$

The order of $< a >$ is the least positive integer N such that $a^n = e$. It is clear that $a^i \neq a^j$ when $0 \leq i < j < n$. Otherwise $a^{j-i} = e$, $j - i < n$, that contradicts our assumption that n is the least positive integer such that $a^n = e$.

We leave it as an exercise to prove that $a^l = e$ implies that $n|l$ and $a^k = a^l$ implies that $k \equiv l(\text{mod } n)$.

Proposition 13. Let $(G, \cdot, e)$ be a group and $a \in G$ so that the order of a is n. The order of a^m is $n/gcd(m, n)$.

Proof: Let l be the order of a^m i.e. $(a^m)^l = a^{ml} = e$. We know that $n|ml$. Let the $gcd(m, n) = d$ and $m = m'd$ and $n = n'd$. So $n'|m'l$ implies $n'|l$ as n' and m' are relatively prime. The smallest l is $n' = n/gcd(m, n)$.
Again $(a^m)^{n'} = (a^{dm'})^{n'} = (a^n)^{m'} = e^{m'} = e$. QED.

Example 10. Consider $\mathbb{Z}_{13}^*$. The order of 2 is 12. $2^4 \bmod 13 = 3$. $gcd(4, 12) = 4$. So the order of 3 is $12/4 = 3$. $3^1 = 3, 3^2 = 9, 3^3 \bmod 13 = 1$.

Proposition 14. Let $(G, \cdot, e)$ be a group and $a \in G$ so that the order of a is n (finite). The map $f : \mathbb{Z}_n \to < a >,\ k \mapsto a^k$ is an isomorphism.

Proof: We know that $|\mathbb{Z}_n| = | < a > |$. So we prove that (i) the map is a homomorphism, and (ii) it is injective.
Let $i, j \in \mathbb{Z}_n$, (i) $f(i) \cdot f(j) = a^i \cdot a^j = a^{i+j} = a^{n+k} = a^n \cdot a^k = e \cdot a^k = a^{(i+j) \bmod n} = f((i + j) \bmod n)$.
(ii) If $f(i) = f(j)$ and $0 \leq i < j < n$, then $a^j = a^i$, implies that $a^{j-i} = e$. But that is impossible as n is the smallest positive integer such that $a^n = e$ and $j - i < n$. So $i = j$. QED.
So every *cyclic group* of finite order n is isomorphic to $\mathbb{Z}_n$ or $\mathbb{Z}/n\mathbb{Z}$. In fact every *cyclic group* group of infinite order is isomorphic to $(\mathbb{Z}, +)$.

Proposition 15. If $(G, \cdot, e)$ is a finite group and $a \in G$, then $a^{|G|} = e$.

Proof: Let the order of a be n. By Lagrange's theorem, in a finite group, the order of a subgroup divides the order of the group. So n divides the $|G|$, say $|G| = nk$. We also know that $a^n = e$, so $a^{|G|} = (a^n)^k = e^k = e$. QED.

Proposition 16. (*Euler's Theorem*)
If $n \geq 2$ and $a \in \mathbb{Z}_n^*$, then $a^{\phi(n)} = 1$. In terms of congruence, for any positive integer a relatively prime to n $a^{\phi(n)} \equiv 1(\text{mod } n)$.

Proof: We know that $|\mathbb{Z}_n^*| = \phi(n)$, so from the previous proposition the result follows.
Another proof:
Define a map $f : \mathbb{Z}_n^* \to \mathbb{Z}_n^*,\ b \mapsto a \times_n b$ for some a. We claim that this map is bijective. It is enough to show that it is injective. If $a \times_n b = a \times_n c$, then by left cancellation we have $b = c$. So,

$$\prod_{b \in \mathbb{Z}_n^*} b = \prod_{b \in \mathbb{Z}_n^*} a \times_n b = a^{\phi(n)} \prod_{b \in \mathbb{Z}_n^*} b.$$

Cancelling the common factor we have $a^{\phi(n)} = 1$. QED.

If a be any integer relatively prime to n, then $a = nq + b$ such that $b \in \mathbb{Z}_n^*$. And we have $a^{\phi(n)} = (nq + b)^{phi(n)} \equiv b^{\phi(n)} \equiv 1(\text{mod } n)$.

Proposition 17. (*Fermat's Theorem*) If p is prime and $a \in \mathbb{Z}_p^*$, then $a^{p-1} = 1$. If $a \in \mathbb{Z}_p$, then $a^p = a$. In terms of congruence, if $gcd(a, p) = 1$, then $a^{p-1} \equiv 1(\text{mod } p)$. And for any integer a, $a^p \equiv a(\text{mod } p)$

Proof: The first part follows from the Euler's theorem, as for a prime p, $\phi(p) = p - 1$. If we multiply both sides by a we get $a^p = a$. If $a = 0$, then it is true. QED.

Proof: A direct proof of Fermat's theorem is as follows.
Consider $a, 2a, \cdots, (p-1)a$, where $p \not| a$. We claim that no two of these numbers are congruent modulo p. Otherwise $ia \equiv ja(\text{mod } p)$ implies that $p|(i - j)$ which is impossible. So the remainders of these numbers are a permutation of $\{1, 2, \cdots, p - 1\}$. We write

$$a \cdot 2a \cdot \cdots \cdot (p-1)a \equiv 1 \cdot 2 \cdot \cdots \cdot (p-1)(\text{mod } p),$$

implies that $a^{p-1}(p-1)! \equiv (p-1)!(\text{mod } p)$. We can cancel $(p-1)!$ from both sides as it is relatively prime to p. So we have $a^{p-1} \equiv 1(\text{mod } p)$. QED.

For any integer a, we have $a^p \equiv a(\text{mod } p)$. There are two case, (i) $p|a$, $a^p \equiv 0 \equiv a(\text{mod } p)$, (ii) follows from the Fermat's theorem by multiplying it with a.

1.1.6 A Few Properties of ϕ-function

Gauss observed the following fact about Euler's ϕ-function.

Example 11. We know that $24 = 2^3 \times 3^1$ has $(3+1)(1+1) = 8$ factors, $\{1, 24, 2, 12, 3, 8, 4, 6\}$.
$\phi(1)+\phi(24)+\phi(2)+\phi(12)+\phi(3)+\phi(8)+\phi(4)+\phi(6) = 1+8+1+4+2+4+2+2 = 24$.

This fact is formalised in the following theorem.
Theorem 18. (Gauss) For each natural number n,

$$n = \sum_{d|n} \phi(d) = \sum_{d|n} |\mathbb{Z}_d^*|.$$

Proof: We define a binary relation E on $\mathbb{Z}_n^+ = \{1, 2, \cdots, n\}$, such that $(a, b) \in E$ if $gcd(a, n) = gcd(b, n)$. This clearly is an equivalence relation and for every divisor d of n, there is a partition S_d defined as

$$S_d = \{m \in \mathbb{Z}_n^+ : gcd(m, n) = d\}.$$

So $\bigcup_{d|n} S_d = \mathbb{Z}_n^+$ or in other words $\sum_{d|n} |S_d| = |\mathbb{Z}_n^+| = n$.

We claim that the size of S_d is $\phi(n/d)$, and then we have

$$n = \sum_{d|n} |S_d| = \sum_{d|n} \phi(n/d) = \sum_{d|n} |\mathbb{Z}_{\frac{n}{d}}^*| = \sum_{d|n} |\mathbb{Z}_d^*|.$$

We know that $gcd(m, n) = d$ if and only if $gcd(m/d, n/d) = 1$. It means that $m \in S_d$ if and only if $\frac{m}{d} \in \mathbb{Z}_{n/d}^*$ i.e. $1 \leq \frac{m}{d} < \frac{n}{d}$ and $gcd(\frac{m}{d}, \frac{n}{d}) = 1$. But then the number of such $\frac{m}{d}$'s is $\phi(\frac{n}{d})$. So $|S_d| = \phi(\frac{n}{d})$.

We observe that $\mathbb{Z}_n^+ = \bigcup_{d|n} d\mathbb{Z}_{n/d}^*$. Note that $\mathbb{Z}_1^* = \{1\}$. QED.

Example 12. Considering our previous example with $n = 24$, we have $S_1, S_{24}, S_2, S_{12}, S_3, S_8, S_4, S_6$, where

$$\begin{aligned}
S_1 &= \mathbb{Z}_{24}^*,\ |S_1| = \phi(24),\\
S_{24} &= \{24\},\ |S_{24}| = \phi\left(\frac{24}{24}\right) = \phi(1),\\
S_2 &= \{2, 10, 14, 22\},\ |S_2| = \phi\left(\frac{24}{2}\right) = \phi(12),\\
S_{12} &= \{12\},\ |S_{12}| = \phi\left(\frac{24}{12}\right) = \phi(2),\\
S_3 &= \{3, 9, 15, 21\},\ |S_3| = \phi\left(\frac{24}{3}\right) = \phi(8),\\
S_8 &= \{8, 16\},\ |S_8| = \phi\left(\frac{24}{8}\right) = \phi(3),\\
S_4 &= \{4, 20\},\ |S_4| = \phi\left(\frac{24}{4}\right) = \phi(6),\\
S_6 &= \{6, 18\},\ |S_6| = \phi\left(\frac{24}{6}\right) = \phi(4).
\end{aligned}$$

So we have

$$\begin{aligned}
\mathbb{Z}_{24}^+ &= 1\mathbb{Z}_{24}^* \cup 24\mathbb{Z}_1^* \cup 2\mathbb{Z}_{12}^* \cup 12\mathbb{Z}_2^* \cup 3\mathbb{Z}_8^* \cup 8\mathbb{Z}_3^* \cup 4\mathbb{Z}_6^* \cup 6\mathbb{Z}_4^*\\
&= \{1, 5, 7, 11, 13, 17, 19, 23\} \cup \{24\} \cup \{2, 10, 14, 22\} \cup \{12\} \cup \{3, 9, 15, 21\} \cup \{8, 16\} \cup\\
&\quad \{4, 20\} \cup \{6, 18\}.
\end{aligned}$$

Definition 6: A function whose *domain of definition* is the set of natural numbers is called a *number-theoretic function.*

A number theoretic function f is said to be *multiplicative* if $f(mn) = f(m)f(n)$ whenever m, n are relatively prime.

Example 13. Euler's totient function $\phi(n)$ is an example of a multiplicative function.

Proposition 19. Let f be a *multiplicative* function and we define the function g as follows:

$$g(n) = \sum_{d|n} f(d),$$

then g is multiplicative.

Proof: Let m, n be a pair of coprime natural numbers.

$$\begin{aligned} g(mn) &= \sum_{d|mn} f(d) \\ &= \sum_{\substack{d_1|m, d_2|n \\ gcd(d_1,d_2)=1}} f(d_1 d_2) \\ &= \sum_{\substack{d_1|m, d_2|n \\ gcd(d_1,d_2)=1}} f(d_1)f(d_2) \\ &= \left(\sum_{d_1|m} f(d_1)\right)\left(\sum_{d_2|n} f(d_2)\right) \\ &= g(m)g(n). \end{aligned}$$

Any divisor d of mn can be written uniquely as a product of a divisor d_1 of m and a divisor d_2 of n, where $gcd(d_1, d_2) = 1$. QED.

Proof: *(Another proof of Gauss's Theorem)* We know that $\phi(n)$ is *multiplicative* and we define

$$g(n) = \sum_{d|n} \phi(d).$$

By our previous proposition, $g(n)$ is also *multiplicative.*
Let $n = p_1^{e_1} \cdot \cdots \cdot p_k^{e_k}$. So,

$$g(n) = g(p_1^{e_1} \cdot \cdots \cdot p_k^{e_k}) = g(p_1^{e_1}) \cdot \cdots \cdot g(p_k^{e_k}).$$

It is easier to calculate $g(p_i^{e_i})$

$$\begin{aligned} g(p_i^{e_i}) &= \sum_{j=0}^{e_i} \phi(p_i^j), \\ &= 1 + (p_i - 1) + (p_i^2 - p_i) + \cdots + (p_i^{e_i} - p_i^{e_i - 1}), \\ &= p_i^{e_i}. \end{aligned}$$

So $g(n) = p_1^{e_1} \cdot \cdots \cdot p_k^{e_k} = n$. QED.

Proposition 20. Let n be a natural number greater than 1. The sum of the natural numbers less than n, and relatively prime to n is $\frac{1}{2}n\phi(n)$.

Proof: We know that there are $\phi(n)$ many natural numbers $a_1, a_2, \cdots, a_{\phi(n)}$, that are less than and relatively prime to n.
If $gcd(a, n) = 1$, then $gcd(n - a, n) = 1$. So, $n - a_1, n - a_2, \cdots, n - a_{\phi(n)}$ is a permutation of $a_1, a_2, \cdots, a_{\phi(n)}$. So we have

$$a_1 + a_2 + \cdots + a_{\phi(n)} = n - a_1 + n - a_2 + \cdots + n - a_{\phi(n)},$$

Hence,

$$a_1 + a_2 + \cdots + a_{\phi(n)} = \frac{1}{2}n\phi(n).$$

QED.

Ex 1.

1. Let $(G, \cdot)$ be a group, $a \in G$ and let the order of a be n. If $a^k = e = a^l$, then prove that $n|k$ and $k \equiv l (\text{mod } n)$.

References

[AD] *Computational Number Theory* by Abhijit Das, Pub. CRC Press, 2013, ISBN 978-1-4398-6615-3.

[DMB] *Elementary Number Theory* by David M Burton, 6th ed., Pub. TMH, 2007, ISBN 978-0-07-061607-3.

[VS] *A Computational Introduction to Number Theory and Algebra* by Victor Shoup, 2nd ed., Pub. Cambridge University Press, 2009, ISBN 978-0-521-51644-0.