

12. Congruence Classes.

Earlier, we found it useful to split \mathbf{Z} into the even and odd integers. In our new language of modular arithmetic :

$$\begin{aligned}\text{set of even integers} &= \{ x \in \mathbf{Z} : x \equiv 0 \pmod{2} \} \\ \text{set of odd integers} &= \{ x \in \mathbf{Z} : x \equiv 1 \pmod{2} \}\end{aligned}$$

We call these the congruence classes modulo 2. We can generalize.

Definition Let a, m be integers, with m positive.
The *congruence class of a modulo m* is the set $[a]_m$ defined by

$$[a]_m = \{ x \in \mathbf{Z} : x \equiv a \pmod{m} \}$$

For example $[8]_6 = \{ \dots, -4, 2, 8, 14, \dots \}$

Theorem 1 Suppose that a, b, m are integers, with m positive. Then

$$a \equiv b \pmod{m} \Leftrightarrow [a]_m = [b]_m$$

Proof We prove \Leftarrow first as it is easier.

Suppose that $[a]_m = [b]_m$
As $a \in [a]_m, a \in [b]_m$ so $a \equiv b \pmod{m}$, by the definition of $[b]_m$.
Thus $[a]_m = [b]_m \Rightarrow a \equiv b \pmod{m}$.

Now suppose that $a \equiv b \pmod{m}$. Then $a \in [b]_m$
If $c \in [a]_m$ then $c \equiv a \pmod{m}$
Now we have $c \equiv a \pmod{m}$ and $a \equiv b \pmod{m}$, so $c \equiv b \pmod{m}$.
Then $c \in [b]_m$.
It follows that $[a]_m = [b]_m$.
Thus, $a \equiv b \pmod{m} \Rightarrow [a]_m = [b]_m$

We know that any integer is congruent modulo m to *one* of the integers $0, 1, \dots, m-1$. Thus, the set of all integers splits into m classes, $[0]_m, [1]_m, \dots, [m-1]_m$.
Each integer belongs to *exactly one* of these classes.

Definition Let m be a positive integer. A *complete set of residues modulo m* is a set containing exactly one member from each congruence class modulo m .

This is usually abbreviated as CSR (mod m).

As there are precisely m congruence classes modulo m , a CSR (mod m) must have precisely m members.

Example Which of the following sets are CSR (mod 3)?

(1) {1,2}, (2) {4,5,7}, (3) {3,5,7}.

Solution

Set (1) is *not* a CSR (mod 3) as it has only 2 members (a CSR (mod 3) has 3).

Set (2) is not a CSR (mod 3) as it has *two* members, 4, 7, of the class $[1]_3$. This is enough, but we could equally observe that it has *no* member of $[0]_3$.

Set (3) *is* a CSR (mod 3) as it has representatives of all three classes. It has 3 in $[0]_3$, 7 in $[1]_3$, and 5 in $[2]_3$.

There are few applications of CSRs at this stage.

Definition Let m be a positive integer. Then $\phi(m)$ is the *number of integers in the list* $1, 2, \dots, m$ *which are coprime to* m .

The function ϕ is called the *Euler Function*.

Directly from the definition we have the first few values

m	1	2	3	4	5	6
$\phi(m)$	1	1	2	2	4	2

For example,

- (1) for $m = 5$, we note that 1, 2, 3, 4 are coprime to 5, 5 is not,
- (2) for $m = 6$, we note that 1, 5 are coprime to 6, 2, 3, 4, 6 are not.

Exercise to reader Show that, if p is prime, then $\phi(p) = p-1$.

Hint. Of the integers $1, 2, \dots, p$, only the first and last are *not* coprime to p .

Definitions

For a positive integer m ,

(1) Let $a(1), a(2), \dots, a(\phi(m))$ be the integers in $1, 2, \dots, m$ coprime to m .

For example, we know that $\phi(6) = 2$. We have $a(1) = 1, a(2) = 5$.

(2) A *reduced set of residues modulo* m is a set of integers *exactly one* of which is congruent modulo m to each of the $a(i)$. This abbreviates to an RSR (mod m).

Note that, from its definition, an RSR (mod m) must have *exactly* $\phi(m)$ members.

Theorem 2 Suppose that $a \equiv b \pmod{m}$, then $\gcd(a,m) = 1 \Leftrightarrow \gcd(b,m) = 1$.

Proof As $a \equiv b \pmod{m}$, $a = b + mt$ for some $t \in \mathbb{Z}$.

Suppose that $\gcd(a,m) = 1$. Then there are integers x, y with $ax + my = 1$.
As $a = b + mt$, we can substitute for a to get

$$1 = ax + my = (b + mt)x + my$$

i.e. $1 = bx + m(tx + y)$

As $tx + y$ is an integer, $\gcd(b,m) = 1$.

This proves \Rightarrow , the proof for \Leftarrow is very similar.

Theorem 2 shows that, if $\gcd(a,m) = 1$, then every element of b of $[a]_m$, being is coprime to m . Thus “coprime to m ” is a property of congruence classes rather than of individual elements.

Now, we can say that $\phi(m)$ is the number of congruence classes modulo m which are coprime to m .

Similarly, we can describe an RSR \pmod{m} as a set which contains exactly one member of each congruence class modulo m which is coprime to m .

Example Working from the definition, determine $\phi(8)$.

Solution

We must count the members of $1, 2, \dots, 8$ which are coprime to 8.
We observe that, of these $2, 4, 6, 8$ are *not* coprime – they have common factor 2.
Any integer a with $\gcd(a, 8) > 1$ must have a factor 2, as $8 = 2^3$.
Thus $1, 3, 5, 7$ are coprime to 8, so $\phi(8) = 4$.

Theorem 3 If p is prime and $k \in \mathbb{Z}$, then

$$\phi(p^k) = p^k - p^{k-1} = p^k (1 - 1/p)$$

Proof Any divisor of p^k must be a power of p (think of prime decompositions)

Thus, $\gcd(a, p^k) > 1 \Leftrightarrow p$ is a factor of a , i.e. $p \mid a$.

It follows that the members of $1, 2, \dots, p^k$ not coprime to p^k are the integers with factor p , i.e. integers of the form $x = pt$ with $t \in \mathbb{Z}$.

Since we are only interested in the range $1 \leq x \leq p^k$, we have $1 \leq t \leq p^{k-1}$.

Thus, we have p^{k-1} integers which are *not* coprime to p^k . Subtracting these,

$$\phi(p^k) = p^k - p^{k-1} = p^k (1 - 1/p).$$

Example Use Theorem 3 to determine $\phi(8)$.

Solution Note that $8 = 2^3$. Then $\phi(8) = \phi(2^3) = 2^3 - 2^2 = 4$.

To evaluate $\phi(n)$ for general n , we use the following result.

Theorem 4 If $\gcd(m,n) = 1$, then $\varphi(mn) = \varphi(m)\varphi(n)$.

Proof Let $M = \{a(1), \dots, a(\varphi(m))\}$, and $N = \{b(1), \dots, b(\varphi(m))\}$.

Suppose that c is an integer with $\gcd(c, mn) = 1$ and $1 \leq c \leq mn$.
 Then $\gcd(c, m) = 1$, so that $c \equiv a(i) \pmod{m}$ for some integer i .
 Similarly $\gcd(c, n) = 1$, so that $c \equiv b(j) \pmod{n}$ for some integer j .
 Thus, each such c leads to a pair $\{a(i), b(j)\}$ with $a(i) \in M$, $b(j) \in N$.

Conversely, suppose that we have a pair $\{a(i), b(j)\}$ with $a(i) \in M$, $b(j) \in N$.
 As $\gcd(m, n) = 1$, the Chinese Remainder Theorem guarantees that there is a unique integer c with $c \equiv a(i) \pmod{m}$ and $c \equiv b(j) \pmod{n}$ and $1 \leq c \leq mn$.
 Then $\gcd(c, mn) = 1$ as $\gcd(a(i), m) = \gcd(b(j), m) = 1$.
 Thus, each pair $\{a(i), b(j)\}$ with $a(i) \in M$, $b(j) \in N$ leads to c with $\gcd(c, mn) = 1$.

By definition, there are $\varphi(mn)$ integers with $\gcd(c, mn) = 1$ and $1 \leq c \leq mn$.
 There are $\varphi(m)\varphi(n)$ pairs of the form $\{a(i), b(j)\}$.

Thus $\varphi(mn) = \varphi(m)\varphi(n)$.

Example Determine $\varphi(270)$

Solution

We begin by factorizing 270 as $2 \cdot 3^3 \cdot 5$.
 Applying Theorem 4 twice, we get $\varphi(270) = \varphi\{2\} \cdot \varphi\{3^3\} \cdot \varphi(5)$.
 Now, 2 and 5 are *primes*, so $\varphi\{2\} = 2-1 = 1$, and $\varphi(5) = 5-1 = 4$.
 By Theorem 3, $\varphi\{3^3\} = 3^3 - 3^2 = 18$.
 Thus, $\varphi(270) = 1 \cdot 18 \cdot 4 = 72$.

Notation

$$\prod_{p|n} (1-1/p)$$

means the product of the terms of the form $(1-1/p)$, where p runs through the *distinct prime* factors of n .

For example, if $n = 270$, then the distinct prime factors are 2, 3 and 5 – see the above example. Then the product is $(1-1/2)(1-1/3)(1-1/5) = 4/15$.

Corollary For $n \in \mathbf{N}$,

$$\varphi(n) = n \prod_{p|n} (1-1/p)$$

Proof Suppose that n has the prime decomposition $p(1)^{a(1)} \cdot p(2)^{a(2)} \dots p(r)^{a(r)}$

Then repeated use of Theorem 4 then gives

$$\varphi(n) = \varphi(p(1)^{a(1)}) \varphi(p(2)^{a(2)}) \dots \varphi(p(r)^{a(r)})$$

For each prime factor, we can use the second form of Theorem 3

$$\varphi(n) = p(1)^{a(1)}(1-1/p(1)) p(2)^{a(2)} (1-1/p(2)) \dots p(r)^{a(r)} (1-1/p(r))$$

The terms $p(i)^{a(i)}$ on the right combine to give a factor of n . The remaining factors $(1-1/p(i))$ combine to give the second factor on the right of the statement.

Example Use the Corollary to evaluate $\varphi(270)$.

Solution By the Corollary

$$\varphi(270) = 270 \prod_{p|270} (1-1/p)$$

As noted above, the product evaluates as $4/15$. Hence

$$\varphi(270) = 270 \cdot (4/15) = 72.$$

Example Find all $n \in \mathbb{N}$ such that $\varphi(2n) = 2\varphi(n)$.

Solution From the Corollary

$$\varphi(2n) = 2n \prod_{p|2n} (1-1/p)$$

$$\frac{2\varphi(n)}{2n} = \prod_{p|n} (1-1/p)$$

The products on the respective right-hand sides are equal precisely when they involve the same primes p . This will happen if and only if 2 is a factor of n , since otherwise $2n$ has all the prime factors of n and also 2.