

# Reduced Residues and Euler's phi

## Reading

- Section 9.2

## Practice Problems

**9.2** 1, 3, 4, 5, 8, 10, 11, 18, 21, 22

## Notes

Before we extend Fermat's theorem to non-primes, we will need some preliminary work.

### Reduced Residues

$\bar{a}$  is a **reduced residue** if  $\gcd(a, n) = 1$ .

The reduced residues are exactly those numbers that have a multiplicative inverse modulo  $n$ .

Reduced residues are also called “units”. The set of all reduced residues is some times denoted by  $\mathbb{Z}_n^*$ .

In simple terms, a number is a reduced residue if it has no common prime factors with the modulus  $n$ .

Euler's phi function is:  $\phi(n)$  = the number of reduced residues modulo  $n$ , i.e. the size of  $\mathbb{Z}_n^*$ .

This is well defined: If  $\bar{a} = \bar{b}$  and  $\gcd(a, n) = 1$ , then it is also the case that  $\gcd(b, n) = 1$ . To see this, note that  $b = a + nk$  for some integer  $k$ . And we already know  $\gcd(a + nk, n) = \gcd(a, n)$ .

What are the reduced residues in  $\mathbb{Z}_{10}$ ,  $\mathbb{Z}_{12}$ ,  $\mathbb{Z}_{15}$ ?

Here is a crucial property of reduced residues:

If  $\bar{a}$  and  $\bar{b}$  are two reduced residues in  $\mathbb{Z}_n$ , then their product  $\bar{a} \cdot \bar{b}$  is also a reduced residue.

In other words the set  $\mathbb{Z}_n^*$  of residues is closed under the operation of multiplication. And as we also know, all elements there also have inverses.

In algebraic systems language, we say that  $\mathbb{Z}_n^*$  is a **group** under multiplication.

Some standard results about Euler's phi function:

- If  $p$  is prime, then  $\phi(p) = p - 1$ .
- If  $p$  is prime and  $a > 0$  then  $\phi(p^a) = (p - 1)p^{a-1}$ .
- If  $p, q$  are distinct primes, then  $\phi(pq) = (p - 1)(q - 1)$ .
- In general if  $m, n$  are relatively prime, then  $\phi(mn) = \phi(m)\phi(n)$ .
- If  $p_1, p_2, \dots, p_k$  are distinct primes and  $a_1, a_2, \dots, a_k$  are nonnegative, then:

$$\phi(p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}) = (p_1 - 1)p_1^{a_1-1} \cdots (p_k - 1)p_k^{a_k-1}$$

Let us discuss the proofs of some of the above, starting with the second one,  $\phi(p^a) = (p - 1)p^{a-1}$ :

- We need to count all the numbers from 1 to  $p^a - 1$  that are relatively prime to  $p^a$ , or simply relatively prime to  $p$ .
- Since  $p$  is prime, we need to exclude all multiples of  $p$ .
- The first such multiple is 0, the last is  $p^a - p = p(p^{a-1} - 1)$ .
- There are exactly  $p^{a-1}$  such numbers.
- There is a total of  $p^a$  numbers.
- So there are  $p^a - p^{a-1}$  numbers that are relatively prime to  $p^a$ .

The next key thing to prove is the fourth case: If  $m, n$  are relatively prime, then  $\phi(mn) = \phi(m) \cdot \phi(n)$ . This will turn out to be related to the Chinese Remainder Theorem. For this we will need the following:

Consider  $m, n$  relatively prime. Then there is a function:

$$I : \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$$

that sends the congruence class  $\bar{x}$  in  $\mathbb{Z}_{mn}$  to the pair  $(\bar{x}, \bar{x}) \in \mathbb{Z}_m \times \mathbb{Z}_n$

This function is 1-1 and onto (this is effectively the Chinese Remainder Theorem).

Further, this function respects addition and multiplication:  $I(x + y) = I(x) + I(y)$  and  $I(xy) = I(x)I(y)$ .

A class  $\bar{x} \in \mathbb{Z}_{mn}$  is a reduced residue if and only if the corresponding  $\bar{x}$  in  $\mathbb{Z}_m$  and  $\mathbb{Z}_n$  are reduced residues.

Let us discuss the 1-1 / onto statement:

- Suppose  $I(\bar{x}) = I(\bar{y})$ .
  - This means that  $x \equiv y \pmod{m}$  and also  $x \equiv y \pmod{n}$ .
  - By the Chinese Remainder Theorem, the common solution to  $x \equiv a \pmod{m}$  and  $x \equiv b \pmod{n}$  is unique modulo  $mn$ .
  - Therefore  $x$  and  $y$  must be equal modulo  $mn$ .

- Suppose  $(\bar{a}, \bar{b})$  is an element in  $\mathbb{Z}_m \times \mathbb{Z}_n$ .
  - The Chinese Remainder Theorem says that there is an  $x$  such that  $x \equiv a \pmod{m}$  and  $x \equiv b \pmod{n}$ .
  - We just showed that  $I(\bar{x}) = (\bar{a}, \bar{b})$ .

Now we consider the last part, about reduced residues.

- If  $\bar{x}$  has an inverse, i.e. there is a  $y$  such that  $\bar{x}\bar{y} = \bar{1}$  in  $\mathbb{Z}_{mn}$ , then the same formula holds in  $\mathbb{Z}_m$  and in  $\mathbb{Z}_n$ .
- So if a number is invertible (hence reduced residue) in  $\mathbb{Z}_{mn}$ , then it is also invertible (reduced residue) in  $\mathbb{Z}_m$  and in  $\mathbb{Z}_n$ .
- Conversely, suppose  $\bar{x}$  is invertible in  $\mathbb{Z}_m$  and in  $\mathbb{Z}_n$ . Then there are  $y_1$  and  $y_2$  such that:

$$xy_1 = 1 \pmod{m}$$

$$xy_2 = 1 \pmod{n}$$

- The Chinese Remainder Theorem (onto property of  $I$ ) essentially says that there is a  $y$  that is both equal to  $y_1 \pmod{m}$  and equal to  $y_2 \pmod{n}$ .  
Then  $I(\bar{x}\bar{y}) = (\bar{1}, \bar{1})$ .
- Again by the Chinese Remainder Theorem (1-1 property of  $I$ ), it follows that  $\bar{x}\bar{y} = \bar{1}$  in  $\mathbb{Z}_{mn}$ . So  $\bar{x}$  is a reduced residue.