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

Reduced Residues

> $\bar{a}$ is a **reduced residue** if $\gcd(a, n) = 1$.
>
> Reduced residues are also called "units". The set of all reduced residues is some times denoted by $\mathbb{Z}_n^*$.
>
> 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 $p_1, p_2, \ldots p_k$ are distinct primes and $a_1, a_2, \ldots a_k$ are nonnegative, then:

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