Multiplicative Inverses in Zn

Reading

- Section 8.3

Practice Problems

8.3 1-5, 7, 17
Challenge (Optional) 9

Notes

Inverses

The question of a multiplicative inverse is straightforward:

> Working modulo n, for which a is there an x such that $\bar{a} \cdot \bar{x} = \bar{1}$?

This has a suprisingly simple answer, if we simply unravel the definitions:

- The question is when the congruence classes $\overline{ax} = \bar{1}$.
- By definition, this means that $ax - 1$ is divisible by n, i.e. $ax - 1 = ny$ for some y.
- In other words, $ax - ny = 1$.
- But this just means that $\gcd(a, n) = 1$.

This leads us to:

> $\bar{a}$ has a multiplicative inverse modulo n if and only if $\gcd(a, n) = 1$.
>
> The Euclidean algorithm is a concrete way to find the inverse.

Cancellation

An important property of our normal number systems is that of cancellation: If $ax = ay$ and $a \neq 0$, then $x = y$. This is called the **cancellation property**.

In modular arithmetic, a weaker version is true, and is a general truth: Elements with multiplicative inverses can be cancelled.

> Working modulo n, if $\gcd(a, n) = 1$ and $\bar{a}\bar{x} = \bar{a}\bar{y}$, then $\bar{x} = \bar{y}$.

This is easy to see:

- Since $\gcd(a, n) = 1$ then there is a b such that $\bar{b}\bar{a} = \bar{1}$.
- If $\bar{a}\bar{x} = \bar{a}\bar{y}$, then $\bar{b}\bar{a}\bar{x} = \bar{b}\bar{a}\bar{y}$.
- This leads to $\bar{x} = \bar{y}$. So $\bar{a}$ is cancellable.

Zp is a field

A very special case is when $n = p$ is prime. Then $\gcd(a, p) = 1$ if and only if p doesn't divide a, if and only if $\bar{a} \neq 0$.

> When p is prime, then every non-zero element in $\mathbb{Z}_p$ has a multiplicative inverse.
>
> This makes $\mathbb{Z}_p$ a **field**.

The converse is also true: If $\mathbb{Z}_n$ has multiplicative inverses, then n must be prime. This follows by the following:

- When n is composite, $\mathbb{Z}_n$ has zero-divisors.
- A field cannot have zero-divisors.

Zero-divisors are two non-zero elements x, y such that $xy = 0$, i.e. they are non-zero elements that multiply to zero.

If n is a composite number, then $n = ab$ for some $0 < a, b < n$. Then $\bar{a} \neq 0$ and $\bar{b} \neq 0$. But $\bar{a}\bar{b} = \bar{n} = \bar{0}$. So $\mathbb{Z}_n$ has zero-divisors.

Now we show that a field cannot have zero-divisors. This is because each non-zero element in a field has an inverse, and so is cancellable. So if $\bar{a}\bar{b} = \bar{0} = \bar{a}\bar{0}$, and $\bar{a} \neq 0$, then we could cancel it and get $\bar{b} = \bar{0}$.

In this case the converse is true also:

> Any finite ring with no zero-divisor is a field: Every non-zero element has a multiplicative inverse.
>
> This is usually phrased as: "Any finite integral domain is a field"

To see this in our specific case, consider a fixed non-zero $\bar{a}$, and consider it as a function that takes $\bar{x}$ to $\bar{a}\bar{x}$. This is a function:

$$\mathbb{Z}_n \to \mathbb{Z}_n$$

Let us see what "no zero-divisors" means for this function: If $\bar{a}\bar{x} = \bar{a}\bar{y}$, then $\bar{a}(\bar{x} - \bar{y}) = \bar{0}$. Since we have no zero-divisors and $\bar{a} \neq 0$, it must be that $\bar{x} = \bar{y}$. In other words:

> No zero-divisors means that the function "multiply by $\bar{a}$" is 1-1.

Because the function is between two sets of the same finite size, a function is 1-1 if and only if it is also an onto function. In particular, there must be a $\bar{x}$ so that $\bar{a}\bar{x} = \bar{1}$, i.e. $\bar{a}$ has a multiplicative inverse.

Let us put all this in order:

- $\bar{a}$ cancellable iff not a zero-divisor.
- $\bar{a}$ invertible iff $\bar{a}\bar{x} = \bar{c}$ solvable for all c.
- Invertible elements cannot be zero-divisors.
- Every field is also an integral domain.
- Not all integral domains are fields (e.g. $\mathbb{Z}$)
- In $\mathbb{Z}_n$, $\bar{a}$ is invertible iff $\gcd(a, n) = 1$.
- If n is prime, all nonzero elements in $\mathbb{Z}_n$ are invertible, so $\mathbb{Z}_n$ is a field.
- If n is composite, it has zero-divisors, so $\mathbb{Z}_n$ is not even an integral domain.
- $\bar{a}$ is not a zero-divisor iff the function "multiply by a" is 1-1.
- $\bar{a}$ is invertible iff the function "multiply by a" is onto.
- any integral domain with finitely many elements must be a field.

Wilson's Theorem

Wilson's Theorem is an interesting observation on the product of elements in $\mathbb{Z}_n$. The question concerns the product of all non-zero elements:

$$\bar{1} \cdot \bar{2} \cdots \overline{n-1}$$

It is clear that if n is composite then this must equal 0, since two of those elements multiply to 0.

We now focus on the case where $n = p$ is prime. Recall that each non-zero element has a multiplicative inverse.

So for each of these elements $\bar{x}$ there is a multiplicative inverse $\bar{y}$. When we think of the product above, we can pair these numbers up this way, and they cancel each other out.

The only numbers that can't be paired up are those that are their own inverses, i.e. those where $\bar{x}\bar{x} = \bar{1}$. We now find those numbers.

> If p is prime and $\bar{x} \in \mathbb{Z}_p$, then $\bar{x}$ is its own multiplicative inverse if and only if $\bar{x} = \bar{1}$ or $\bar{x} = \overline{p-1}$.

- It is obvious that those two numbers are their own inverses ($\overline{p-1}$ is just another way of writing $\overline{-1}$).
- Suppose $\bar{x}^2 = \bar{1}$.
- Then $p divides $x^2 - 1 = (x-1)(x+1)$.
- Since p is prime, it must divide $x - 1$ or $x + 1$.
- So $\bar{x} = \bar{1}$ or $\bar{x} = \overline{-1}$.

> **Wilson's Theorem**
>
> If p is prime, then $\bar{1} \cdot \bar{2} \cdots \overline{p-1} = -\bar{1}$.

This follows from the above observations: All numbers along the way are paired up to multiply to 1, with the exception of $\bar{1}$ and $\overline{p-1}$. And these two multiply to -1.