

CSCI 124/224

Discrete Structures II: Existence of Units in \mathbb{Z}_m

Poorvi L. Vora

In this module, we show that an element in a finite ring has a multiplicative inverse if and only if it is not a zero divisor, that an element $x \in \mathbb{Z}_m$ is a zero divisor if and only if $\gcd(x, m) \neq 1$, and hence that an element $x \in \mathbb{Z}_m$ is a unit if and only if $\gcd(x, m) = 1$.

Recall that

$$(A \Leftrightarrow B) \Leftrightarrow (B \Leftrightarrow A) \Leftrightarrow (\bar{A} \Leftrightarrow \bar{B}) \Leftrightarrow (\bar{B} \Leftrightarrow \bar{A})$$

where \bar{X} denotes the negation of X .

Hence, to show that an element in a finite ring has a multiplicative inverse if and only if it is not a zero divisor, we show the converse, which is equivalent:

Theorem: An element $x \in \mathcal{R}$, where \mathcal{R} is a finite ring, is a zero divisor if and only if it is not a unit.

Proof:

\Rightarrow

Suppose x is a zero divisor. $\exists y \in \mathcal{R}, y \neq z$ (where z is the additive identity in \mathcal{R}) such that $xy = z$. If x is a unit, $\exists \bar{x} \in \mathcal{R}$ such that $\bar{x}x = u$ where $u \in \mathcal{R}$ is the multiplicative identity. Hence,

$$xy = z \Rightarrow \bar{x}xy = \bar{x}z \Rightarrow y = z$$

as $rz = z \forall r \in \mathcal{R}$ (this has been done in class previously and is shown in the text.) This is a contradiction, hence x is not a zero divisor.

\Leftarrow

Suppose x is not a unit. This implies that there is no $y \in \mathcal{R}$ such that $xy = u$. Now consider the value of xr for all values of $r \in \mathcal{R}$, such that $r \neq z$. Let the size of the finite ring \mathcal{R} be n . Then there are $n - 1$ values of xr . If these values are all distinct, then one of these values has to be u (because there are exactly $n - 1$ possibilities in \mathcal{R} if z is not included, and one of these is u). If $xr' = u$, then r' is the multiplicative inverse of x . But x is not a unit, hence we cannot assume that all values of xr are distinct. Suppose $xr_1 = xr_2$ for $r_1 \neq r_2$. Then $xr_1 - xr_2 = z$ and $x(r_1 - r_2) = z$ as $r_1 \neq r_2$, x is a zero divisor.

Theorem: An element $x \in \mathbb{Z}_m$ is a zero divisor if and only if $\gcd(x, m) \neq 1$.

Proof:

\Rightarrow

Suppose x is a zero divisor. $\exists y \in \mathbb{Z}_m$ such that $xy = 0 \pmod{m}$, and $y \neq 0 \pmod{m}$. That is, $m \mid (xy)$ and m does not divide y . Hence some factor of m divides x and another divides y . That is $\gcd(x, m) \neq 1$.

←

Suppose $\gcd(x, m) = g \neq 1$. Then $x = n_1g$ and $m = n_2g$, where $1 < n_1, n_2 < m$, and $n_2x = n_2n_1g = n_2g = 0 \pmod{m}$. Hence $\exists y = n_2 \neq 0 \pmod{m}$ such that $xy = 0 \pmod{m}$ and x is a zero divisor.

And the final result simply puts the two results above together to get:

Theorem: An element $x \in \mathbb{Z}_m$ is a unit if and only if $\gcd(x, m) = 1$.

Proof: By the first theorem, $x \in \mathbb{Z}_m$ is a unit if and only if it is not a zero divisor. By the second theorem, it is not a zero divisor if and only if $\gcd(x, m) = 1$. Hence the result.