Inverses in Z_n

Definition: We say that x is *invertible* in $\mathbb{Z}_n$ if $\exists a \in \mathbb{Z}\ (ax \equiv 1 \bmod n)$. If so, we write that $x^{-1} = a$ in $\mathbb{Z}_n$.

Examples:

In $\mathbb{Z}_7$, $3^{-1} = 5$ as $3 \cdot 5 = 15 \equiv 1 \bmod 7$.

In $\mathbb{Z}_{20}$, $9^{-1} = 9$ as $9 \cdot 9 = 81 \equiv 1 \bmod 20$.

Q: Which x are invertible in $\mathbb{Z}_n$?

Theorem: $\forall n \in \mathbb{N}\ \forall x \in [n-1]\ (x$ is invertible in $\mathbb{Z}_n \leftrightarrow \gcd(n,x)=1)$
Moreover, if $\gcd(n,x)=1$, then x^{-1} is unique (modulo n).

Proof: If $\gcd(n,x)=1$, by Bézout's Identity, $\exists a,b \in \mathbb{Z}\ (1 = an+bx)$ so $bx \equiv 1 \bmod n$. If $\gcd(n,x) > 1$ then $\forall a,b \in \mathbb{Z}\ (an+bx \neq 1)$ as $\gcd(n,x) \mid (an+bx)$. Thus, x is not invertible in $\mathbb{Z}_n$.

Uniqueness of x^{-1}: If $ax \equiv 1 \bmod n$ and $bx \equiv 1 \bmod n$ then
$a \equiv a(xb) \equiv (ax)b \equiv b \bmod n$

Finding Inverses in Z_n

Q: If $\gcd(n,x)=1$, how can we find x^{-1} in $\mathbb{Z}_n$?

A: Use extended Euclid's algorithm to find $a,b \in \mathbb{Z}$ such that $1=an+bx$ and then $x^{-1}=b \bmod n$.

Example: What is 10^{-1} in $\mathbb{Z}_{27}$?

$n=27 \quad x=10$

$27 = 2\cdot 10 + 7$

$10 = 1\cdot 7 + 3$

$7 = 2\cdot 3 + 1$

$7 = 27 - 2\cdot 10$

$n - 2x$

$3 = 10 - 1\cdot 7$

$x - (n-2x) = 3x-n$

$1 = 7 - 2\cdot 3$

$(n-2x) - 2\cdot(3x-n) = 3n-8x$

In $\mathbb{Z}_{27}$, $10^{-1} = -8 \bmod 27 = 19$

$19\cdot 10 = 190 = 7\cdot 27 + 1$