4.4 - Linear congruences

- Solving equations in the following format:

  $ax \equiv b \bmod m$, assuming $\gcd(a,m)=1$
- Theorem 1: If a and m are relatively prime integers and $m>1$, then an inverse of a mod m exists. Furthermore, this inverse is unique mod m.

when $\gcd(a,m)=1$, then
- $a \cdot \bar{a} \equiv 1$
- $\bar{a}$ means the inverse of a.

ex: What are the solutions of the linear congruence

$3x \equiv 4 \bmod 7$?

Solution

First find $\gcd(3,7)$ using Euclidean Algorithm Ensure its 1.

$7 = 3 \cdot 2 + 1 \leftarrow \gcd(3,7)$

$3 = 1 \cdot 3 + 0$

second step, you can do either backward pass or Extend Euclidean.

Backward pass:

$1 = 7 - 3 \cdot 2 = 1 \cdot 7 - 2 \cdot 3$

inverse

Bezout's Identity:

$\gcd(a,b) = s \cdot a + t \cdot b$

inverse

I want the final answer to be smallest positive number that's being modded.

inverse:

$7-2=5$

$-2 \bmod 7 = 5 \bmod 7$ this is our inverse that's smallest positive

Third step:

$\cancel{3 \cdot 5}x \equiv 4 \cdot 5 \bmod 7$

1

$x \equiv 20 \bmod 7$

$x = 6 \bmod 7$

<u>ex:</u> Find the solution to $17x \equiv 4 \bmod 36$

<u>Solution:</u>

need to ensure $\gcd(17, 36) = 1$

$36 = 17 \cdot 2 + 2$

$17 = 2 \cdot 8 + 1$ ← gcd is 1

$2 = 1 \cdot 2$

$1 = 17 - 2 \cdot 8$

$2 = 36 - 17 \cdot 2$

$1 = 17 - 2 \cdot 8 = 17 - (36 - 17 \cdot 2) \cdot 8$

$= 17 - 8 \cdot 36 + 16 \cdot 17$

$= 17 \cdot 17 - 8 \cdot 36$

$\gcd(a,b) = s \cdot a + t \cdot b$ → $1 = -8 \cdot 36 + 17 \cdot 17$

INVERSE

Solve:

$\cancel{17 \cdot 17}x \equiv 4 \cdot 17 \bmod 36$

1

$x \equiv 68 \bmod 36$

$\boxed{= 32 \bmod 36}$

Fermat's Little Theorem:

If p is prime and a is an integer not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$

Furthermore, for every integer a we have

$a^p \equiv a \mod p$

ex: $7^{222} \mod 11 = ?$, use Fermat's Little Theorem.

Solution:

$p = 11$

$a = 7$

$11 \nmid 7$

$7^{11-1} \equiv 1 \mod 11$

$7^{10} \equiv 1 \mod 11$

$(7^{10})^k \equiv 1 \mod 11$

$$7^{222} \equiv (7^{10})^{22} \cdot 7^2$$

$$\equiv 1^{22} \cdot 7^2 \mod 11$$

$$\equiv 49 \mod 11 = 5$$