Solving Congruences

Solving equations of the form $ax \equiv b \mod m$ for x is a huge necessity in number theory.

This type of equation is called a linear congruence.

One method first requires solving the congruence $ax \equiv 1 \mod m$.

If such an x exists it is called the inverse of a modulo m & is denoted a^{-1} or $\bar{a}$. However a^{-1} does not always exist!

Theorem: If a & m are relatively prime then a^{-1} exists. And $a^{-1} \in \mathbb{Z}_m$ is unique.

Pf: Since $\gcd(a,m) = 1$ we can use the extended Euclidean Alg to find s, t s.t.

$$as + mt = 1 \Rightarrow a \cdot s + tm \equiv 1 \mod m$$

$$tm \equiv 0 \mod m \Rightarrow a \cdot s \equiv 1 \mod m$$ Thus s is the inverse

& $a^{-1} \equiv s \mod m$ is the unique value of $\mathbb{Z}_m$. $\square$

This actually gives an efficient way of finding inverses! The extended Euclidean Alg:

Ex: Find the inverse of 101 mod 4620.

First we do Euclidean alg:

$4620 = 45 \cdot 101 + 75$

$101 = 1 \cdot 75 + 26$

$75 = 2 \cdot 26 + 23$

$26 = 1 \cdot 23 + 3$

$23 = 7 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$ ← gcd.

$2 = 2 \cdot 1 + 0$

Now solve for 1 & work backwards:

$1 = 3 - 1 \cdot 2$

$= 3 - 1 \cdot (23 - 7 \cdot 3)$

$= 8 \cdot 3 - 1 \cdot 23$

$= 8(26 - 23) - 1 \cdot 23$

$= 8 \cdot 26 - 9 \cdot 23$

$= 8 \cdot 26 - 9(75 - 2 \cdot 26)$

$= 26 \cdot 26 - 9 \cdot 75$

$= 26(101 - 75) - 9\cdot 75$

$= 26\cdot 101 - 35\cdot 75$

$= 26\cdot 101 - 35(4620 - 45\cdot 101)$

$= 1601\cdot 101 - 35\cdot 4620$ $\leftarrow$ We can check this holds!

but more importantly: $1 = 1601\cdot 101 - 35\cdot 4620 \Rightarrow 1 \equiv 1601\cdot 101 \mod 4620$

$\Rightarrow 1601 \equiv 101^{-1} \mod 4620.$

<u>Ex</u>: What are solutions to $3x \equiv 4 \mod 7$.

<u>Step 1</u>: $3^{-1} \mod 7 = ?$ 7 is small, lets just check

$3\cdot 1 \equiv 3$
$3\cdot 2 \equiv 6$
$3\cdot 3 \equiv 2$
$3\cdot 4 \equiv 5$
$3\cdot 5 \equiv 1$ ✓

<u>Step 2</u>: multiply both sides by 5

$$x \equiv 4\cdot 5 \mod 7 = 20 \mod 7 \equiv 6$$

$\Rightarrow 3\cdot 6 = 18 \equiv 4 \mod 7.$

<u>Ex</u>: Solve $19x \equiv 4 \mod 141$

<u>Step 1</u>: $19^{-1} \mod 141 = ?$

$141 = 7\cdot 19 + 8$
$19 = 2\cdot 8 + 3$
$8 = 2\cdot 3 + 2$
$3 = 1\cdot 2 + 1$
$2 = 2\cdot 1 + 0$

$1 = 3 - 1\cdot 2$
$= 3 - 1\cdot(8 - 2\cdot 3)$
$= 3\cdot 3 - 1\cdot 8$
$= 3(19 - 2\cdot 8) - 1\cdot 8$
$= 3\cdot 19 - 7\cdot 8$
$= 3\cdot 19 - 7\cdot(141 - 7\cdot 19)$
$= 52\cdot 19 - 7\cdot 141$

$\Rightarrow 52 \equiv 19^{-1} \mod 141$

So $19x \equiv 4 \mod 141$

$\Rightarrow x \equiv 4\cdot 52 \mod 141$
$= 208 \mod 141 \equiv \boxed{67}$