CSE 311: Foundations of Computing I

Solving Modular Equivalences

Solving a Normal Equation

First, we discuss an analogous type of question when using normal arithmetic.

Question: Solve the equation $27y = 12$.

Solution: We divide both sides by 27 to get $y = \frac{12}{27}$.

Solution: We multiply both sides by 1/27 to get $y = \frac{12}{27}$.

These solutions are two ways of saying the same thing.

Solving a Modular Congruence

Now, we consider a congruence instead:

Question: Solve the congruence $27y \equiv 10 \pmod{4}$.

Note: We can't just divide both sides. For example, consider $5 \equiv 10 \pmod{5}$. If we were to divide both sides by 5, we would get $1 \equiv 2 \pmod{5}$ which is definitely false.

Another way of looking at this would be to ask the question What is $\frac{1}{5}$ mod 5? It really doesn't make any sense, because remainders should always be integers.

So, instead, we need to create machinery to multiply by whatever the *correct* inverse is mod a number.

Inverses

If $xy = 1$, we say that y is the "multiplicative inverse of x".
We have a similar idea mod m: If $xy \equiv 1 \pmod{m}$, we say y is the "multiplicative inverse of x modulo m".

How do we compute the multiplicative inverse of x modulo m?

By definition, $xy \equiv 1 \pmod{m}$ iff $xy + tm = 1$ for some $t \in \mathbb{Z}$. We know by Bezout's Theorem that we can find y and t such that $xy + tm = \gcd(x, m)$. Said another way: If $\gcd(x, m) = 1$, then we can find a multiplicative inverse!

To actually compute the multiplicative inverse, we use the Extended Euclidean Algorithm. For example, consider the equation we were trying to solve above: $27y \equiv 10 \pmod{4}$.

First, we find the multiplicative inverse of 27 modulo 4. That is, we find a y such that $27y \equiv 1 \pmod{4}$. To do this, we first note that the $\gcd(27, 4) = \gcd(4, 3) = \gcd(3, 1) = \gcd(1, 0) = 1$, which means an inverse does exist!

Now, we write out the equations:

$$27 = 6 \bullet 4 + 3$$
$$4 = 1 \bullet 3 + 1$$

Solving each equation for the remainder:

$$3 = 27 - 6 \bullet 4$$
$$1 = 4 - 1 \bullet 3$$

Backward substituting, we get:

$$\begin{aligned} 1 &= 4 - 1 \bullet 3 \\ &= 4 - 1 \bullet (27 - 6 \bullet 4) \\ &= 7 \bullet 4 + (-1) \bullet 27 \end{aligned}$$

So, we have found that -1 mod $4 = 3$ mod 4 is the multiplicative inverse of 27 modulo 4. We can verify this by taking $(27 \bullet 3)$ mod $4 = 81$ mod $4 = 1$.

Solving the original equation

Now, we need to solve the original equation: $27y \equiv 10 \pmod 4$.

We know from above that $27 \bullet 3 \equiv 1 \pmod 4$. So, multiplying both sides by 10 (which works, because of a theorem from lecture; note that this is different than the theorem from the homework!), we get:

$$27 \bullet 30 \equiv 10 \pmod 4$$

Since 30 mod $4 = 2$, we have $27 \bullet 2 \equiv 10 \pmod 4$. It follows that $x = 2$ solves the original equation.

Other Solutions?

We've shown that $x = 2$ is one possible solution. The obvious follow-up question is "are there any others?" There are! Since $2 + 4k \equiv 2 \pmod 4$ for all $k \in \mathbb{Z}$, those are all solutions as well.