Mathematics 546 Homework.

We have seen that if a, n, x, y, b are integers and

$$ax + ny = b$$

then is we reduce modulo n and use that $ny \equiv 0 \pmod{n}$ we get that

$$ax \equiv b \pmod{n}.$$

Conversely if

$$ax \equiv b \pmod{n}$$

then $n \mid (ax - b)$ which means there is an integer k with $ax - b = kn$. This can be rewritten as

$$ax + (-k)n = b$$

and this if we set $y = -k$ this is

$$ax + by = b.$$

Therefore solving

$$ax \equiv b \pmod{n}$$

for x is the same as solving

$$ax + ny = b$$

for x and y and then just using the x value.

We are experts as using the Euclidean algorithm to finding a solution to

$$ax + ny = \gcd(a, n).$$

In particular when $\gcd(a, n) = 1$ we can find x and y with

$$ax + ny = 1.$$

Reducing modulo n lets us find a solution to $ax \equiv 1 \pmod{n}$.

Definition 1. It $n \geq 1$ and a are integers with $\gcd(a, n) = 1$ then any solution to

$$ax \equiv 1 \pmod{n}$$

is an ***inverse of*** a ***modulo*** n. We will denote such an inverse by $\widehat{a}$. $\square$

To be explicit $\widehat{a}$ is an integer such that

$$\widehat{a}a \equiv 1 \pmod{n}.$$

Theorem 2. *Let a, b, n be integers with $n \geq 1$ and $\gcd(a, n) = 1$. Then the congruence*

$$ax \equiv b \pmod{n}$$

has a solution. It is given by

$$x \equiv \widehat{a}b.$$

Proof. We just check directly that $x \equiv \widehat{a}b \pmod{n}$ works:

$$\begin{aligned} ax &\equiv a(\widehat{a}b) \pmod{n} \\ &\equiv (a\widehat{a})b \pmod{n} \\ &\equiv 1b \pmod{n} \\ &\equiv b \pmod{n}. \end{aligned}$$

□

The solution given in Theorem 2 is unique modulo n as we now show. The proof is based on the following, which we have used several times before (but here we change the notation a bit to match what we are currently working on).

Theorem 3. *Let a, x, n be integers with $n \geq 1$ and $\gcd(a, n) = 1$. Then $n \mid ax$ implies $n \mid x$.* □

Here is the uniqueness result:

Theorem 4. *If a, n, b are integers with $n \geq 1$ and $\gcd(a, n) = 1$, and x_1 and x_2 satisfy*

$$\begin{aligned} ax_1 &\equiv b \pmod{n} \\ ax_2 &\equiv b \pmod{n} \end{aligned}$$

then

$$x_1 \equiv x_2 \pmod{n}.$$

Problem 1. Prove this. *Hint:* Note

$$\begin{aligned} ax_2 - ax_1 &\equiv b - b \pmod{n} \\ &0 \pmod{n}. \end{aligned}$$

Use this to show $n \mid a(x_2 - x_1) = ax$ where $x = x_2 - x_1$ and then use Theorem 3. □

As an example let us solve

$$17x \equiv 42 \pmod{132}.$$

To start we saw in the Lesson
`http://ralphhoward.github.io/Classes/Fall2020/546/Lesson_2/`
that

$$x \equiv 101 \pmod{132}.$$

is a solution to

$$17x \equiv 1 \pmod{132}.$$

therefore we have that

$$\widehat{17} \equiv 101 \pmod{132}$$

is the inverse of 17 modulo 132. Whence the solution to $17x \equiv 42 \pmod{132}$ is

$$x \equiv \widehat{17} \cdot 42 \equiv 101 \cdot 42 \equiv 4242 \pmod{132}.$$

To get a nicer looking answer use that if 132 is divided into 4242 the remainder is 18 and therefore

$$x \equiv 18 \pmod{132}$$

is a pleasanter looking solution. (And you can check that $17(18) = 306 = 2(132) + (42)$ which implies $17 \cdot 18 \equiv 42 \pmod{132}$.)

Problem 2. Solve the following
(a) $14x \equiv 8 \pmod{51}$
(b) $3x \equiv 59 \pmod{538}$

Now that we know how to solve $ax \equiv b \pmod{n}$ when $\gcd(a, n) = 1$, it is natural to ask what happens when $\gcd(a, n) > 1$. We now work this out (you should compare this with pages 30–33 in the text). As we saw above

$$ax \equiv b \pmod{n}$$

has a solution for x if and only if

$$ax + ny = b$$

has a solution (x, y) with x and y integers.

Proposition 5. *If*

$$ax \equiv b \pmod{n}$$

has a solution, then

$$\gcd(a, n) \mid b.$$

(That is if the congruence has a solution, then $\gcd(a, b)$ *divides* b*.)*

Problem 3. Prove this. *Hint:* If the congruence has a solution, then there are integers x and y with

$$ax + yn = b.$$

Set $d = \gcd(a, n)$. Then d is a divisor of both of a and n therefore there are integers a_1 and n_1 such that $a = a_1 d$ and $n = n_1 d$. Use this in $ax + yn = b$ to show $d \mid b$. □

Proposition 6. *If* a *and* b *are integers, not both zero, and* $d = \gcd(a, b)$*. Then the integers*

$$a_1 = \frac{a}{d} \qquad b_1 = \frac{b}{d}$$

are relatively prime. (That is $\gcd(a_1, b_1) = 1$*.)*

Problem 4. Prove this. *Hint:* By the GCD is a Linear Combination Theorem we have that there are integers x and y with

$$ax + by = d.$$

And we also have $a = a_1 d$ and $b = b_1 d$. Put these facts together to get that

$$a_1 x + b_1 y = 1$$

which implies $\gcd(a_1, b_1) = 1$. □

Proposition 7. *If* a, n, b *are integers with* $n \geq 1$ *and so that* $\gcd(a, n) \mid b$*, then*

$$ax \equiv b \pmod{n}$$

has solutions. These are found by solving

$$a_1 x \equiv b_1 \pmod{n_1}$$

where

$$a_1 = \frac{a}{\gcd(a,n)}, \qquad b_1 = \frac{b}{\gcd(a,n)}, \quad n_1 = \frac{n}{\gcd(a,n)}.$$

Problem 5. Prove this. *Hint:* First a bit of notation. Let $d = \gcd(a, n)$. Then form the definitions of a_1, b_1, and n_1 we have

$$a = a_1 d, \quad b = b_1 d, \quad n = n_1 d.$$

We know that $ax \equiv b \pmod{n}$ has solution if and only if there are integers x and y with

$$ax + ny = b.$$

But this can be rewritten as

$$a_1 dx + n_1 dy = b_1 d.$$

Dividing out the d gives that this is equivalent to solving

$$a_1 x + n_1 y = b_1$$

which in turn has a solution if and only if

$$a_1 x \equiv b_1 \pmod{n_1}.$$

Now use Proposition 6 to see that $\gcd(a_1, n_1) = 1$ and explain why this implies $a_1 x \equiv b_1 \pmod{n_1}$ has solutions. □

Problem 6. In the following congruences either solve them or explain why they have no solutions.

(a) $15x \equiv 33 \pmod{65}$.
(b) $15x \equiv 32 \pmod{65}$.
(c) $38x \equiv 52 \pmod{101}$. □