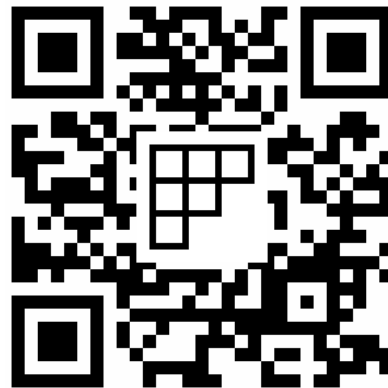


Week 3, lecture 2:
Inverses modulo m .
Chinese Remainder Theorem
MA180/185/190 Algebra

Angela Carnevale



Division modulo m

Chinese Remainder Theorem

Inverses and division modulo m

Combining Bézout's Theorem (see slides from [Lecture 3](#)) and the theory of congruences we get the following result.

Linear congruences and division modulo m

The linear congruence

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

has a solution **if and only if** $\gcd(a, m) = 1$.

In practice:

- ▶ If $\gcd(a, m) = 1$, we can find one solution to the above equation by using Euclid's algorithm backwards.
- ▶ If the result is not one of the numbers in \mathbb{Z}_m , we add/subtract multiples of m until finding an integer in the range $0, 1, \dots, m - 1$.

Example

Example. Find, if it exists, $x \in \mathbb{Z}_{15}$ such that

$$7x \equiv 1 \pmod{15}.$$

- Euclid's algorithm:

$$\boxed{15 = 7 \cdot 2 + 1}$$
$$7 = 1 \cdot 7 + 0$$

- Euclid's algorithm backwards

$$1 = 15 + 7 \cdot (-2)$$

this equation mod 15 becomes: $7 \cdot (-2) \equiv 1 \pmod{15}$

$$\text{So } x \equiv -2 \equiv \underline{\underline{13}} \pmod{15}$$

Inverses and division modulo m

The previous result tells us how to define “**division**” modulo m , and when it is possible to perform it:

Division modulo m

We can make sense of

$$\frac{b}{a} \pmod{m} \quad \text{as} \quad b \cdot a^{-1} \pmod{m}.$$

In turn, an integer $a \in \mathbb{Z}_m$ has an inverse $a^{-1} \pmod{m}$ **if and only if** $\gcd(a, m) = 1$.

Examples.

- Compute, if it exists, $7^{-1} \pmod{9}$

We can proceed as usual with Euclid's algorithm (backwards) to find $7^{-1} \pmod{9}$. Alternatively, since the modulus is quite small, we can look for an inverse among the elements of \mathbb{Z}_9 :

0 1 2 3 4 5 6 7 8

The following observation rules out some of the above candidates:

Note. If $\gcd(a, m) = 1$ then there exists a number $a^{-1} \in \mathbb{Z}_m$ (we knew this....)

Such number a^{-1} is also COPRIME with m !

This restricts our search: ~~0~~ 1 2 ~~3~~ 4 5 ~~6~~ 7 8

We can now easily see that 4 is the number we were looking for:

$$7 \cdot 4 = 28 \equiv 1 \pmod{9}$$

So $7^{-1} = 4$ in \mathbb{Z}_9 .

Inverses and division modulo m

The previous result tells us how to define “**division**” modulo m , and when it is possible to perform it:

Division modulo m

We can make sense of

$$\frac{b}{a} \pmod{m} \quad \text{as} \quad b \cdot a^{-1} \pmod{m}.$$

In turn, an integer $a \in \mathbb{Z}_m$ has an inverse $a^{-1} \pmod{m}$ **if and only if** $\gcd(a, m) = 1$.

Examples.

- Compute, if possible, $3 \cdot 5^{-1} \pmod{9}$

Again, since $\gcd(5, 9) = 1$ we know 5^{-1} exists.

We can easily see that $5^{-1} = 2$ in \mathbb{Z}_9 (since $5 \cdot 2 = 10 \equiv 1 \pmod{9}$)

So:
$$3 \cdot 5^{-1} \equiv 3 \cdot 2 \equiv 6 \pmod{9}.$$

Division modulo m

Chinese Remainder Theorem

Simultaneous congruences

Recall one of our challenges from the first lectures:

There are certain things whose number is unknown. If we count them by threes, we have two left over; by fives, we have three left over; and by sevens, two are left over. How many things are there?

We now know how to reformulate this problem in the language of congruences:
for x such that Call the unknown quantity x . We are looking for x such that ALL of the following hold:

$$\begin{cases} x \equiv 2 & (\text{mod } 3) \\ x \equiv 3 & (\text{mod } 5) \\ x \equiv 2 & (\text{mod } 7) \end{cases}$$

A simpler version

Let's take one step back and consider the following two simultaneous congruences: we'd like to find x such that, **both of the following** are satisfied:

$$x \equiv 2 \pmod{3} \quad \text{and} \quad x \equiv 3 \pmod{5}. \quad (*)$$

- ▶ Consider the following linear congruence: $5x \equiv 1 \pmod{3}$. We can easily see that **2** is a solution to that.
- ▶ Consider the following linear congruence: $3x \equiv 1 \pmod{5}$. Again, **2** is a solution to that.

We can use these facts to construct a number that satisfies both equations in $(*)$:

$$x_0 = 5 \cdot 2 \cdot 2 + 3 \cdot 3 \cdot 2$$