Week 4, lecture 2:
Chinese Remainder Theorem.
PPSn: examples

MA180/185/190 Algebra

Angela Carnevale

Chinese Remainder Theorem

More on prime numbers

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?

In the language of modular arithmetic: Find x such that **all** of the following hold:

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

Remark. We noted that if there is a solution, say x_0, then there are infinitely many solutions since $x_0 + 3 \cdot 5 \cdot 7 \cdot n = x_0 + 105n$ would then be a solution for all $n \in \mathbb{Z}$.

A simpler version

We looked at a simpler version by first solving the following two simultaneous congruences: namely, we found x such that, **both of the following** are satisfied:

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

Idea. First find a number that solves the first equation and that is $0 \pmod 5$, then find a number that is $0 \pmod 3$ but solves the second equation. Then add them up to get an x that solves them both at once.

How to achieve this? If, say, we want a number that is $2 \pmod 3$ and $0 \pmod 5$, we take 2 itself, and multiply it by $5 \cdot x$ where x is such that $5x \equiv 1 \pmod 3$. After doing this for both congruences, the solution we found was:

$$x_0 = 5 \cdot 2 \cdot 2 + 3 \cdot 3 \cdot 2 = 20 + 18 = 38$$

And as observed, any number of the form $x_0 + 15n$ $n \in \mathbb{Z}$ will also solve $(*)$

Solution to our challenge

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

Strategy: look for 3 integers:

(1) → one that is $\equiv 2 \pmod 3$ and $\equiv 0 \pmod 5$, and $\pmod 7$

(2) → one " " $\equiv 3 \pmod 5$ and $\equiv 0 \pmod 3$, $\pmod 7$

(3) → one " " $\equiv 2 \pmod 7$ and $\equiv 0 \pmod 3$, $\pmod 5$

(1) Need to solve $5 \cdot 7 \cdot x \equiv 1 \pmod 3$

$35x \equiv 1 \pmod 3$ this is the same as solving

$2x \equiv 1 \pmod 3$ (because $35 \equiv 2 \pmod 3$)

Easy to see: $x = 2$ solves

So $5 \cdot 7 \cdot 2 \cdot 2$ is the first bit of our solution ✓

(2) Need to solve $3 \cdot 7 \cdot x \equiv 1 \pmod 5$ this is equivalent to

solving $21 \cdot x \equiv 1 \pmod 5$ in turn equivalent to

$1 \cdot x \equiv 1 \pmod 5$

So $x = 1$ is a sol to

So $3 \cdot 7 \cdot 1 \cdot 3$ is the second bit of our solution ✓

Solution to our challenge

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

(3) Need x such that $3 \cdot 5 \cdot x \equiv 1 \pmod 7$

$15x \equiv 1 \pmod 7$ since $15 \equiv 1 \pmod 7$

we get that $x \equiv 1$ is a solution here too

So the last bit of our solution is

$3 \cdot 5 \cdot 1 \cdot 2$ ✓

Last step: add them all up, and allow for further multiples of 105 to be added too. The general solution looks as follows:

$$X = 5 \cdot 7 \cdot 2 \cdot 2 + 3 \cdot 7 \cdot 1 \cdot 3 + 3 \cdot 5 \cdot 1 \cdot 2 + 105 \cdot n$$

$$= 140 + 63 + 30 + 105n$$

$$= 233 + 105n$$

Solution to our challenge

Note 3 times we looked for inverses mod some integer n. That tells us that a system of congruences might not always be solvable.

Chinese Remainder Theorem

The formal theorem is as follows

Chinese Remainder Theorem

Let n_1, n_2 and n_3 be positive integers pairwise coprime. Let a_1, a_2 and a_3 be any integers. Then the following system of congruences

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ x \equiv a_3 \pmod{n_3} \end{cases}$$

can be solved.

Chinese Remainder Theorem

To find a solution, we first solve three auxiliary linear congruences:

- $n_2 n_3 x \equiv 1 \pmod{n_1} \rightsquigarrow$ solution: d_1
- $n_1 n_3 x \equiv 1 \pmod{n_2} \rightsquigarrow$ solution: d_2
- $n_1 n_2 x \equiv 1 \pmod{n_3} \rightsquigarrow$ solution: d_3

We then combine them to find a general solution of the form:

$$x = a_1 \cdot d_1 \cdot (n_2 n_3) + a_2 \cdot d_2 \cdot (n_1 n_3) + a_3 \cdot d_3 \cdot (n_1 n_2) + (n_1 n_2 n_3)t$$

where $t \in \mathbb{Z}$.

New challenge! (hard)

Problem. Three comets **A**, **B** and **C** are known to have orbital periods of 3, 8 and 13 years, respectively. They have last been seen in their perihelia (=point on their orbit closest to our Sun) in years 2020, 2021 and 2021, respectively. When will all of them in their perihelia in the same year next?

Hint. The year of the last observation (modulo the orbital period of the corresponding comet) will give you the right-hand sides of the three congruences that should be simultaneously satisfied. From that, just apply the strategy on the previous slide.

Back to PPSn

Example. Find the missing digit in the following PPSn: 12109x4GH.

8	7	6	5	4	3	2	1	9
1	2	1	0	9	x	4	7	8

$7 \equiv 8\cdot 1 + 7\cdot 2 + 6\cdot 1 + 5\cdot 0 + 4\cdot 9 + 3x + 2\cdot 4 + 9\cdot 8 \pmod{23}$

$7 \equiv 8 + 14 + 6 + 36 + 3x + 8 + 72 \pmod{23}$

$7 \equiv 8 + 14 + 6 + 13 + 3x + 8 + 3 \pmod{23}$

note: $36 \equiv 13 \pmod{23}$

$72 \equiv 3 \pmod{23}$

$0 \equiv 45 + 3x \pmod{23}$

want to solve: $3x \equiv -45 \pmod{23}$

note: $-45 \equiv -22 = 1 \pmod{23}$

so want to find $3^{-1} \pmod{23}$

Euclid: $23 = 3\cdot 7 + 2$

$3 = 2\cdot 1 + 1$

$\ldots \quad 0$

$\rightarrow$ backwards: $1 = 3 + 2\cdot(-1)$

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

$= 23\cdot(-1) + 3\cdot 8$

so $3^{-1} \equiv 8 \bmod 23 \Rightarrow x = 8$

Next week

- More on prime/coprime numbers
- Powers modulo a number
- Cryptography!