Week 4, lecture 1:
Chinese Remainder Theorem.
Euler Phi function

MA180/185/190 Algebra

Angela Carnevale

Chinese Remainder Theorem

More on prime numbers

Euler's Phi function

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:

Find x such that **all** of the following hold:

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

<u>Note</u> if x_0 solves the three congruences, so does $x_0 + 3 \cdot 5 \cdot 7 \cdot n$ for $n \in \mathbb{Z}$.

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:

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

- 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 $(*)$:

$$x_0 = 5 \cdot 2 \cdot 2 + 3 \cdot 3 \cdot 2 + 15n$$ is

a solution to $(*)$ for any $n \in \mathbb{Z}$

Solution to our challenge

Recall: we're looking for x such that $\begin{cases} x \equiv 2 \mod 3 \\ x \equiv 3 \mod 5 \\ x \equiv 2 \mod 7 \end{cases}$

First want to find a solution to the first congruence that can be "ignored" by the other two (i.e. it's 0 mod 5 and 0 mod 7).

Let's find a solution to $5 \cdot 7 \cdot x \equiv 1 \pmod 3$

that is, $2x \equiv 1 \pmod 3$ (because $35 \equiv 2 \mod 3$)

solution: $x = 2$ is a solution.

So $2 \cdot 5 \cdot 7 \cdot 2 \begin{cases} \equiv 2 \pmod 3 \\ \equiv 0 \pmod 5 \\ \equiv 0 \pmod 7 \end{cases}$ (because $2 \cdot 5 \cdot 7 \equiv 1 \mod 3$)

Solution to our challenge

Recall: we're looking for x such that $\begin{cases} x \equiv 2 & \text{mod } 3 \\ x \equiv 3 & \text{mod } 5 \\ x \equiv 2 & \text{mod } 7 \end{cases}$

Next Look for soln to 2nd that is $\equiv 0$ mod 3 AND mod 7

look for x such that $3 \cdot 7 \cdot x \equiv 1 \pmod 5$

but $21 \equiv 1$ mod 5 so we're looking for x such that $x \equiv 1$ ...

So $1 \cdot 3 \cdot 7 \cdot 3 \begin{cases} \equiv 0 \pmod 3 \\ \equiv 3 \pmod 5 \\ \equiv 0 \pmod 7 \end{cases}$

Solution to our challenge

Finally Look for x such that x solves 3^{rd} congruence and it is 0 mod 3 AND mod 5.

Look for x such that $3 \cdot 5 \cdot x \equiv 1 \pmod 7$

but $3 \cdot 5 = 15 \equiv 1 \bmod 7$ so $x \equiv 1$ solves the congruence above.

So

$$1 \cdot 3 \cdot 5 \cdot 2 \begin{cases} \equiv 0 & \bmod 3 \\ \equiv 0 & \bmod 5 \\ \equiv 2 & \bmod 7 \end{cases}$$

$x = 2 \cdot 5 \cdot 7 \cdot 2 + 1 \cdot 3 \cdot 7 \cdot 3 + 1 \cdot 3 \cdot 5 \cdot 2 + 105n$ is a general solution

So $x = 233 + 105n$, $n \in \mathbb{Z}$ are all solutions.

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.