Divisibility II

Los Angeles Math Circle

28 February 2021

Recalling the Chinese Remainder Theorem

The Chinese Remainder Theorem says that given a system of k equations:

$$\begin{cases} x & \equiv r_1 \mod n_1 \\ x & \equiv r_2 \mod n_2 \\ & \vdots \\ x & \equiv r_k \mod n_k \end{cases}$$

Then the solution x has the following form

$$x = c_1 r_1 + c_2 r_2 + \cdots + c_k r_k \mod n_1 \cdot n_2 \cdot \ldots \cdot n_k$$

where

$$\begin{aligned} c_i &\equiv 1 \mod n_i \\ c_i &\equiv 0 \mod n_j \ (\text{if } i \neq j) \end{aligned}$$

The next few problems look at some applications of the Chinese Remainder Theorem (continued from the following week).

Problems

Problem 1

A band of 7 pirates stole a sack of gold coins. When they tried to divide the fortune into equal portions, 2 coins remained. In the ensuing brawl over who should get the extra coins, two pirates were killed. The wealth was redistribution, but this time an equal division left 3 coins. Again, an argument ensued in which two more pirates were killed. But now, the total fortune was evenly distributed among the survivors. What was the least number of coins that could have been stolen?

Problem 2

Solve the following system (for x):

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

Problem 3

Explain why our algorithm for finding solutions to the Chinese Remainder Theorem works: if x has the form

$$x = c_1 r_1 + c_2 r_2 + \ldots + c_k r_k \mod n_1 \cdot n_2 \cdot \ldots \cdot n_k$$

why must

$$c_i \equiv 1 \mod n_i$$

and

$$c_i \equiv \mod n_j \text{ (if } i \neq j)?$$

Two numbers are coprime if their greatest common denominator is 1. So far, we have shown that the Chinese Remainder Theorem applied to a system of equations moduli prime numbers. However, the theorem can be extended to moduli numbers that are coprime to each other.

Problem 4

Solve the following system (for x):

$$\begin{cases} x & \equiv 1 \mod 4 \\ x & \equiv 3 \mod 5 \\ x & \equiv 2 \mod 7 \end{cases}$$

Problem 5

Based on your understanding of the Chinese Remainder Theorem, explain why the Chinese Remainder Theorem can be extended to moduli which are coprime to each other.

Problem 6

Comets 2P/Encke, 4P/Faye and 8P/Tuttle have orbital periods of 3 years, 8 years and 13 years, respectively. The last *perihelions* (the pooint in the orbit which is closest to the sun) of each of these comets were in 2017, 2014 and 2008, respectively. What is the next year in which all three of these comets will achieve perihelions in the same year?

Problem 7

What are the last two digits of 49^{19}? Hint: we are looking for x such that $x \equiv 49^{19} \mod 100$. Furthermore, note that $100 = 25 \cdot 4$ and $\gcd(25, 4) = 1$.

More Problems on Divisibility and Modular Arithmetic

Problem 8

(a) Show that a number is divisible by 2 if and only if its last digit is even.

(b) Show that a number is divisible by 4 if and only if its last two digits make a number divisible by 4

(c) Can you generalize these principles to make a divisibility criterion for any 2^n?

Problem 9

(a) A positive integer n has remainder 7 when divided by 9. Can it have remainder 2 when divided by 3?

(b) A positive integer n has remainder 23 when divided by 144. Can it have remainder 29 when divided by 90?

Problem 10

(a) How many zeros does the number 10! end with? Reminder: $n!$ reads as "n factorial" and

$$n! = 1 \cdot 2 \cdot \ldots \cdot n$$

(b) How many zeros for (100!)?