MATH 9
ASSIGNMENT 23: CHINESE REMAINDER THEOREM CONTINUED

APRIL 10, 2022

Summary of previous results

Theorem. *If two integers a, b, are relatively prime, then there exist $x, y \in \mathbb{Z}$ such that*

$$ax + by = 1.$$

Corollary: an congruence class $[a] \in \mathbb{Z}_n$ is invertible if and only if a is relatively prime with n.
Chinese Remainder Theorem:

Theorem. *Let m, n be relatively prime. Then for any k, l, the system of congruences*

$$x \equiv k \mod m$$
$$x \equiv l \mod n$$

has a solution, and any two solutions differ by a multiple of mn.

Reformulation of CRT:

Theorem. *Let m, n be relatively prime. Then we have a bijection*

$$f \colon \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n.$$

Moreover, this bijection agrees with addition and multiplication.

Homework

1. You have a pile of identical coins. If you try to divide them between 4 people, one coin will be left over, and same happens when you try dividing it among 5 or 6 people. However, they can be divided equally among 7 people.

What is the smallest possible number of coins for which it is possible?

2. Compute the following remainders, using Chinese Remainder Theorem
(a) $35^9 \mod 48$
(b) $2^{2170} \mod 1001$. (Hint: do you remember the factorization of 1001?)

3. Let m, n be relatively prime.
(a) Show that an integer a is invertible mod mn if and only if a is invertible mod m and is also invertible mod n
(b) For any positive n, define Euler's function $\varphi(n)$ by

$$\begin{aligned}\varphi(n) &= \text{number of remainders modulo } n \text{ which are relatively prime to } n \\ &= \text{number of invertible elements in } \mathbb{Z}_n\end{aligned}$$

Use Chinese remainder theorem to prove that if m, n are relatively prime, then $\varphi(mn) = \varphi(m)\varphi(n)$.

***4.** The following is a famous number theory problem.

Five men and a monkey were shipwrecked on an island. They spent the first night gathering coconuts. During the night, one man woke up and decided to take his share of the coconuts. He divided them into five piles. One coconut was left over so he gave it to the monkey, then hid his share, put the rest back together, and went back to sleep.

Soon a second man woke up and did the same thing. After dividing the coconuts into five piles, one coconut was left over which he gave to the monkey. He then hid his share, put the rest back together, and went back to bed. The third, fourth, and fifth man followed exactly the same procedure.

The next morning, after they all woke up, they divided the remaining coconuts into five equal shares; again, one coconut was left over so they gave it to the monkey.

How many coconuts were there in the original pile?

For those interested, a series of hints helping one to solve this problem is given on the back.

Hints for the last problem:

1. Show that each "operation" (sailor wakes up, divides the pile, throwing a coconut to the monkey, hides his share) changes the number of coconuts by the formula
$$n \mapsto \tfrac{4}{5}(n-1)$$
2. If the original number of coconuts is N, show that we get an equation
$$f(f(f(f(f(N))))) = 5k+1$$
where $f(n) = \frac{4}{5}(n-1)$ and $5k+1$ is the number of coconuts that was left by the morning.
3. Rewrite this equation in the form $aN = bk + c$, for some integer a, b, c.
4. Show that one solution is $N = -4$
5. Find a smallest positive solution.