The Chinese Remainder Theorem

Reading

- Section 7.4

Practice Problems

7.4 TODO
Challenge 7.4 (Optional)

Notes

The Chinese remainder theorem concerns itself with the simultaneous solution of two congruence equations:

> For $a, b \in \mathbb{N}$ and $\ell, k \in \mathbb{Z}$, the equations
>
> $$x \equiv \ell \bmod a$$
> $$x \equiv k \bmod b$$
>
> have a common solution if and only if $\gcd(a, b) \mid (\ell - k)$.
>
> Furthermore the solution is unique modulo $lcm(a, b)$.

A special version of this theorem, and usually the one refered to as the Chinese Remainder Theorem, is when a, b are relatively prime:

> If a, b are relatively prime, then the equations
>
> $$x \equiv \ell \bmod a$$
> $$x \equiv k \bmod b$$
>
> have a common solution.
>
> Furthermore the solution is unique modulo ab.

Let us describe the proof of the first theorem:

- First we prove that the condition is necessary and sufficient.
  - The two equations amount to looking for an x that is equal to $\ell + ay$ for some y and at the same time equal to $k + bz$ for some z.
  - This can obviously be done exactly when those two can equal each other.

- So we turned out problem into finding y, z such that $ax - bz = k - \ell$.
- This is a diophantine equation with unknowns x, z. So it has a solution if and only if $\gcd(a, b)$ divides $k - \ell$.
- This proves the necessary and sufficient condition for there to be a solution.
- It also tells us how to *find* a solution: By solving the diophantine equation.

- Now we prove that the solution is unique modulo $lcm(a, b)$, if a solution exists.
  - Suppose we have two solutions, x_1 and x_2 to both equations.
  - Then $x_1 - x_2 \equiv 0 \bmod a$ and also $\equiv 0 \bmod b$.
  - In other words, $x_1 - x_2$ is a common multiple of a, b.
  - Therefore it must be divisible by the lcm.
  - So $x_1 - x_2 \equiv 0 \bmod lcm(a, b)$.
  - This means $x_1 = x_2 \equiv lcm(a, b)$.

In class: Do a specific example.

This allows us to find solutions to moduli problems with complex moduli, by instead solving it for their factors.

For example, say we want to compute 1452365 modulo 36. Since $36 = 4 \times 9$, and those two are relatively prime to each other, we can start with solving those systems:

$$x \equiv 1452365 \bmod 4$$

$$x \equiv 1452365 \bmod 9$$

Both of these are much easier: Since 4 divides into 100, only the last two digits matter, and since $65 \equiv 1 \bmod 4$ we can say that the first equation is simply: $x \equiv 1 \bmod 4$.

For the second equation, we can instead work with the sum of the digits, which is 26, which is 8 modulo 9. So now our system becomes:

$$x \equiv 1 \bmod 4$$

$$x \equiv 8 \bmod 9$$

At this point one way to proceed is to write down all the numbers that are equal to 8 modulo 9, that do not exceed 36. One of those must be a solution to the other equation as well. These numbers are: 8, 17, 26 and 35. From them only one will be equal to 1 mod 4, and it is 17. So this means that:

$$1452365 \equiv 17 \bmod 36$$

Indeed:

$$1452365 = 40343 \times 36 + 17$$