MATH 8: HANDOUT 25
NUMBER THEORY 7: CHINESE REMAINDER THEOREM

Chinese Remainder Theorem

The previous result can be stated as follows: if a, b are relatively prime, then

$$x \equiv 0 \mod a$$
$$x \equiv 0 \mod b$$

happens if and only if $x \equiv 0 \mod ab$.

This is a special case of the following famous result.

Theorem (Chinese Remainder Theorem). *Let a, b be relatively prime. Then, for any choice of k, l, the following system of congruences:*

$$x \equiv k \mod a$$
$$x \equiv l \mod b$$

has a unique solution mod ab, i.e. it has solutions and any two solutions differ by a multiple of ab. In particular, there exists exactly one solution x such that $0 \leq x < ab$.

Proof. Let $x = k + ta$ for some integer t. Then x satisfies the first congruence, and our goal will be to find t such that x satisfies the second congruence.

To do this, write $k + ta \equiv l \mod b$, which gives $ta \equiv l - k \mod b$. Notice now that because a, b are relatively prime, a has an inverse $h \mod b$ such that $ah \equiv 1 \mod b$. Therefore $t \equiv h(l-k) \mod b$, and $x = k + ah(l-k)$ is a solution to both the congruences.

To see uniqueness, suppose x and x' are both solutions to both congruences such that $0 \leq x, x' < ab$. Then we have

$$x - x' \equiv k - k \equiv 0 \mod a$$
$$x - x' \equiv l - l \equiv 0 \mod b$$

Thus $x - x'$ is a multiple of both a and b; because a, b are relatively prime, this implies that $x - x'$ is a multiple of ab. Thus, any two solutions differ by a multiple of ab. □

Homework

1. Solve the following systems of congruences

(a)

$$x \equiv 1 \mod 3$$
$$x \equiv 1 \mod 5$$

(b)

$$z \equiv 1 \mod 5$$
$$z \equiv 6 \mod 7$$

2. Daniil has number of toys. If he tries to divide them equally among 4 kids, one toy is left over. Same happens if he tries to divide them equally among 5 or 6 kids; however, the toys can be divided equally among 7 kids. What is the smallest number of toys Daniil can have? [Hint: if number of toys is n, then what can you say about number $n-1$?]

3. (a) Find the remainder upon division of 23^{2021} by 7.

(b) Find the remainder upon division of 23^{2021} by 70. [Hint: use $70 = 7 \cdot 10$ and Chinese Remainder Theorem.]

4. (a) Find the remainder upon division of 24^{46} by 100.

(b) Determine all integers k such that $10^k - 1$ is divisible by 99.