MATH 8: HANDOUT 24
DIVISIBILITY VII: CHINESE REMAINDER THEOREM

We have by now discussed congruences mod m, for positive integer m, and we have defined the notion of invertibility of residues mod m (for reference, a remainder mod m is sometimes called a *residue* mod m). What about *noninvertibility*?

Theorem. *If m is a composite number such that $m = ab$ for integers $a, b > 1$, then there exist non-invertible residues (or remainders) modulo m.*

Proof. We prove that a factor of m is noninvertible mod m. To see this, the equation $ax \equiv 1 \mod m$ has no solution because a is not relatively prime to m; i.e., $\gcd(a, m) = a$, thus $ax = 1 + by$ is equivalent to finding x, y such that $ax - by = 1$, which is impossible. So a is noninvertible mod m. □

It turns out that not only are a and b noninvertible mod m, but all of their multiples as well are noninvertible. The nature of the non-invertibility of multiples of a and b mod m is closely related to the non-invertibility of $(0 \mod a)$ and $(0 \mod b)$.

Theorem. *If $m = ab$ and r is non-invertible mod m, then $(r \mod a)$ or $(r \mod b)$ is non-invertible mod a or b, respectively.*

Proof. We have that r is invertible mod m if and only if it is relatively prime to m. Thus this theorem reduces to the following statement: $\gcd(r, m) = 1$ if and only if $\gcd(r, a) = 1$ and $\gcd(r, b) = 1$.

If $\gcd(r, a) \neq 1$, then $\gcd(r, a) = d$ for $d > 1$, and hence $d|ab$ because $d|a$, thus $d|m$; therefore, d is a common factor of r and m and $\gcd(r, m) > 1$: this implies that $\gcd(r, m)$ can be 1 only if $\gcd(r, a) = \gcd(r, b) = 1$. The converse is left as an exercise. □

These theorems motivate us to consider if there is a more specific relationship between the residues mod m and those mod a, b. The full theorem will be given at the end of this section - before we state it, it's worth it to understand the multiples of a mod b: this is where we make use of the assumption that a, b be relatively prime, i.e. $\gcd(a, b) = 1$.

Theorem. *If $a, b > 1$ are integers such that $\gcd(a, b) = 1$, then the numbers $0, a, 2a, ..., (b-1)a$ have unique remainders mod b. In other words, for any integers $0 \leq x < y < b$, we must have $xa \not\equiv ya \mod b$.*

Proof. We prove by contradiction: suppose that $xa \equiv ya \mod b$ for $0 \leq x < y < b$. Then $(x - y)a \equiv 0$. We know also that a is invertible mod b because $\gcd(a, b) = 1$, thus we may multiply this congruence by the inverse h of a mod b (i.e. $ha \equiv 1 \mod b$) to get:

$(x - y)ah \equiv 0 \cdot h \implies (x - y) \cdot 1 \equiv 0 \implies x - y \equiv 0 \implies x \equiv y.$

But $0 \leq x < y < b$, thus it is a simple fact of numbers that $y - x$ cannot be a multiple of b, which is a contradiction. □

As a result, one can imagine that the multiples of a cycle around the residues mod b; if $a = 1$ for example, then the multiples of a are simply $0, 1, 2, 3, ..., b-1, 0, 1, 2, 3, ...$ etc, and if $a > 1$, then the multiples of a need not be consecutive integers mod b, but they will still go through each of the residues mod b exactly once until they return to 0 with $ab \equiv 0 \mod b$.

It remains to notice that there are $a \cdot b$ ways to choose a residue mod a and a residue mod b. Then we guess that, since there are exactly $a \cdot b$ residues mod $m = ab$, there might be a one-to-one relationship between pairs of residues $(x, y) \mod a, b$ and residues $r \mod m$.

Indeed, this is the case.

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

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

has a unique solution mod ab, i.e. there exists exactly one integer x such that $0 \leq x < ab$ and x satisfies both the above congruences.

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, but if this is the case then x and x' cannot both be positive and less than ab unless they are in fact equal.

□

HOMEWORK

1. Is it possible for a multiple of 3 to be congruent to $5 \mod 12$?

2. (a) Find inverse of 7 mod 11.

(b) Find all solutions of the equation

$$7x \equiv 5 \mod 11$$

3. Solve the following systems of congruences

(a)

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

(b)

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

4. (a) Find the remainder upon division of 23^{2019} by 7.

(b) Find the remainder upon division of 23^{2019} by 70. [Hint: use $70 = 7 \cdot 10$ and Chinese Remainder Theorem.]

5. (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.

6. In a calendar of some ancient race, the year consists of 12 months, each 30 days long. They also use 7 day weeks, same as we do.

If first day of the year was a Monday, will it ever happen that 13th day of some month is a Friday? If so, when will be the first time it happens, and how often will it repeat afterwards?

[Hint: this can be rewritten as a system of congruences: $n \equiv 5 \mod 7$, $n \equiv 13 \mod 30$.]

7. How many remainders mod 2310 can be expressed as powers of 6?