MATH 8
NUMBER THEORY 5: CHINESE REMAINDER THEOREM

1. Chinese Remainder Theorem

This week we will explore the nature of what happens inside the product of relatively prime numbers.

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 non-invertible. 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.

□

2. Homework

1. (a) Let x, y be positive integers with $\gcd(x, y) = d$. How many distinct numbers are in the set $\{n \cdot x \mod y \mid n \in \mathbb{Z}\}$? Be sure to prove your answer.

(b) Given $m = ab$ for integers $m, a, b > 1$, and some positive integer r, prove that $\gcd(r, a) = \gcd(r, b) = 1$ implies that $\gcd(r, m) = 1$.

(c) Prove that there are no integer solutions to the following equation:

$$(x + 1)^2 = 2y + x$$

2. Let n be a positive integer greater than 1.

(a) Let $S(n)$ be the sum of all residues mod n, taken mod n. For what values of n is $S(n)$ invertible mod n?

(b) Let $f(x) = x^2 - n$, and let $R(x)$ denote the set $\{x, f(x), f(f(x)), f(f(f(x))), ...\}$. For what values of x does there exist three numbers in $R(x)$ that form an arithmetic progression with common difference 10^n?

3. Let $\mathbb{Z}^2$ be the integer lattice, i.e. the set of all ordered pairs of integers. Let f, g be functions defined on this lattice as follows:

$$f(x, y) = (y^3 + 2x + 1, x^3 + 2y + 1)$$
$$g(x, y) = (x - 3, y - 3)$$

For what starting points (a, b) is it possible to use f and g to navigate to the origin? You may apply each function as many times as you want and in whatever order, but you have to get to the origin in a finite number of steps.

4. Let p be a prime number greater than 3, and a an integer such that $1 < a < p - 1$.

(a) Prove that there exists some integer n such that $a^n \equiv 1 \mod p$.

(b) Let b be any positive integer. Prove that if $b^2 \equiv a^2 \mod p$, then $(b \equiv a \mod p) \vee (b \equiv -a \mod p)$.

(c) Write out several pairs of numbers p, a and find the value of n from part (a). What is the smallest number than n can be? Provide an example of a p, a with such an n, and prove why smaller values of n are impossible for any other pair p, a.

5. This problem poses an alternate proof to the Chinese Remainder Theorem. Let a, b be relatively prime positive integers.

(a) Prove that if x, y are residues mod ab such that $x \equiv y \mod a$ and $x \equiv y \mod b$, then $x \equiv y \mod ab$.

(b) Deduce that any pair of residues $(k, l) \mod a, b$ must correspond to a unique residue mod ab.

(c) Deduce, then, that there are at least $a \cdot b$ residues mod ab which correspond to a pair of residues mod a, b.

(d) Prove thence the statement of the Chinese Remainder Theorem.

6. This problem poses yet another proof to the Chinese Remainder Theorem. Again, let a, b be relatively prime positive integers.

(a) Prove that the residues of multiples of $a \mod ab$ are of the form ak for $0 \leq k < b$.

(b) Using the theorem that the multiples ak of a for $0 \leq k < b$ are unique mod b, prove that the pair of congruences

$$\begin{aligned} y &\equiv 0 \mod a \\ y &\equiv l \mod b \end{aligned}$$

has a unique solution mod ab.

(c) Use the solution to the above system to produce a solution to the system

$$\begin{aligned} x &\equiv k \mod a \\ x &\equiv l \mod b \end{aligned}$$

(d) Prove that this solution is unique.