MATH 8: ASSIGNMENT 20

MARCH 10, 2018

1. Chinese Remainder Theorem

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

Recall that we have defined congruences mod m, for a positive integer m, to denote a system of addition and multiplication performed on the possible remainders upon division by m (i.e., the integers from 0 to $n-1$). Many of the properties of arithmetic mod m can be derived from representation of m as a product of two smaller integers. Recall also that we have explored the equation $ax \equiv 1 \mod b$ and the notion that, if such a solution x exists for given a, b, then a is said to be invertible mod b. We now note the following fact:

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. 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. □

Indeed a is not the only non-invertible residue mod m: all multiples of a and also all multiples of b are also non-invertible mod m by a similar argument to above. 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. (Note that ba has remainder $0 \mod b$, and thence the sequence repeats, with $(b+1)a \equiv a$, $(b+2)a \equiv 2a$, etc.)*

Proof. We prove by contradiction: suppose that $xa \equiv ya \mod b$ for $x, y < b$. 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 $x, y < b$, so $x - y$ 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 another (possibly the same) residue mod b; such pairs of residues are simply equivalent to choosing a pair of integers (x, y) with $0 \leq x < a$ and $0 \leq y < b$. 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. Is it possible for a multiple of 3 to be congruent to $5 \mod 12$?

2. Given $m = ab$ for $m, a, b > 1$, how many of the residues mod m can be written as multiples of a? Of b?

3. 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 $\gcd(r, m) = 1$.

4. Determine the residue mod 15 which is congruent to ($1 \mod 3$) and ($1 \mod 5$). Then, determine the residue mod 15 which is congruent to ($2 \mod 3$) and ($4 \mod 5$).

5. Determine the residue mod 35 which is congruent to ($1 \mod 5$) and ($6 \mod 7$). Then, determine the residue mod 35 which is congruent to ($4 \mod 5$) and ($1 \mod 7$).

6. (a) Find the remainder upon division of 19^{2019} by 7.
(b) Find the remainder upon division of 19^{2019} by 70. [Hint: use $70 = 7 \cdot 10$ and Chinese Remainder Theorem.]

7. (a) Find the remainder upon division of 24^{46} by 100.
(b) Determine all integers k such that $10^k - 1$ is divisible by $50^2 - 49^2$.

8. How many residues mod 2310 can be expressed as powers of 6?

9. 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 which are congruent both mod a and 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.