M328K: Homework 3

Katherine Ho

September 24, 2024

Definition. A *complete residue system modulo n* is a set of integers such that every integer is congruent modulo n to exactly one integer in the set. For example, the "canonical" complete residue system modulo n is the set of integers $\{0, 1, 2, \ldots, n-1\}$.

1. (a) Prove that any set of n incongruent integers modulo n forms a complete residue system modulo n.

   Proof. Suppose a set of n integers does not form a complete residue system mod n. Then it contains at least one integer a that is not congreuent to another integer in the set. This means when a is divided by n, then none of the other elements are equal to its remainder. There are at most $n-1$ remainders in the set. By the pigeonhole principle, at least 2 integers in the set have the same remainder $\pmod{n}$. However this contradicts the supposition where a is incongruent with all of the other integers in the set. Hence any set of n incongruent integers modulo n forms a complete residue system modulo n. $\square$

   (b) Suppose $\gcd(a, n) = 1$. Prove that the integers

   $$c, c+a, c+2a, \ldots, c+(n-1)a$$

   form a complete residue system modulo m for any c.[1]

2. Find a complete (up to congruence) set of solutions to the linear congruence $34x \equiv 60 \pmod{98}$.

   Proof. We have that $\gcd(34, 98) = 2$. Also, $2 \mid 60$, so there are 2 solutions $\pmod{98}$. First we can find a solution to

   $$\begin{aligned} 17x &\equiv 30 \pmod{49} \\ 17x - 49y &= 30 \end{aligned}$$

   Then, by the Euclidean Algorithm:

   $$\begin{aligned} 49 &= 17(2) + 15 \\ 49 - 17(2) &= 15 \\ 49(2) - 17(4) &= 30 \\ 17(-4) - 49(-2) &= 30 \end{aligned}$$

[1] Note: With $c = 0$, this is the fundamental fact we used in class to prove Fermat's Little Theorem.

$$x = -4,\ y = -2$$

So, $x = -4 + 49 = 45$ is a solution. The other solution $\pmod{98}$ is

$$x = 45 + 49 = 94$$

$x = 45, 94$ is a complete set of solutions up to congruence $\pmod{98}$. ☐

3. This exercise illustrates a neat inductive proof of Fermat's Little Theorem using the binomial theorem.

   (a) Let p be prime. Show that p divides $\binom{p}{k}$ for $1 \le k \le p-1$, where

   $$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p(p-1)\cdots(p-k+1)}{1 \cdot 2 \cdot 3 \cdots k}.$$

   Hint: First show that p divides $k!\binom{p}{k}$.

   Proof. Let $n = \binom{p}{k}$:

   $$\begin{aligned} n &= \binom{p}{k} \\ n &= \frac{p!}{k!(p-k)!} \\ n \cdot k!(p-k)! &= p! \end{aligned}$$

   p divides $p!$, so the left expression is also divisible by p.
   This means that at least one factor of the expression is divisible by p.

   i. $k!$ is not divisible by p since it is less than p and p is prime.
   ii. $(p-k)!$ is not divisible by p since $p-k$ is less than p and p is prime.

   This leaves n, which must be divisible by p. Therefore, p divides $\binom{p}{k}$. ☐

   (b) Use induction on a together with the binomial theorem[2] to give another proof of Fermat's Little Theorem.

   Proof. We aim to prove $a^{p-1} \equiv 1 \pmod{p}$ for a prime p and $p \nmid a$. It can be rewritten as $a^p \equiv a \pmod{p}$.
   Base case ($a = 1$): $1^p \equiv 1 \pmod{p}$.

   $$1^p - 1 = px \quad \text{for some } x \in \mathbb{Z}$$

   This is true for any prime p and $x = 0$.
   Inductive Hypothesis: Assume $a^p \equiv a \pmod{p}$ for an integer $a \in \mathbb{Z}$ is true.
   Consider $a + 1$:

   $$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{k}a^{p-k} + \cdots + \binom{p}{p-1}a + 1$$

[2]Binomial theorem: $(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{k}a^{p-k} + \cdots + \binom{p}{p-1}a + 1$

By (a), each binomial coefficient $\binom{p}{k}$ is divisible by p since p is prime. So, if we take (mod p) of this sum, we are left with:

$$(a+1)^p \equiv a^p + 1 \pmod{p}$$

$a^p \equiv a \pmod{p}$ is true for $a+1$, thus proving Fermat's Little Theorem. □

4. A composite integer $n > 1$ is called a *Fermat pseudoprime to base a* if $a^{n-1} \equiv 1 \pmod{n}$.

   (a) Prove the following: If $d, n \in \mathbb{N}$ with $d \mid n$, then $2^d - 1 \mid 2^n - 1$.
   Hint: Use the identity

   $$x^k - 1 = (x-1)(x^{k-1} + x^{k-2} + \cdots + x + 1).$$

   Proof. Let $n = db$ for some $b \in \mathbb{Z}$.

   $$2^n - 1 = 2^{db} - 1$$
   $$2^n - 1 = (2^d)^b - 1$$
   $$2^n - 1 = (2^d - 1)((2^d)^{b-1} + (2^d)^{b-2} + \cdots + (2^d)^1 + (2^d)^0)$$

   Thus if $d, n \in \mathbb{N}$ with $d \mid n$, then $2^d - 1 \mid 2^n - 1$. □

   (b) Prove that if n is a Fermat pseudoprime to base 2, then $M_n = 2^n - 1$ is also a Fermat pseudoprime to base 2.

   Proof. If $n \mid 2^{n-1} - 1$, then $2^{n-1} - 1 = nx$ for some $x \in \mathbb{Z}$. □

   (c) Conclude that there are infinitely many Fermat pseudoprimes to base 2.

   Proof. □

5. A *Carmichael* number is an integer $n > 1$ that is a Fermat pseudoprime to base a for all a with $\gcd(a, n) = 1$.

   (a) Prove that if $n = p_1 p_2 \cdots p_r$ is a composite square-free integer such that $p_i - 1 \mid n - 1$ for $i = 1, 2, \ldots, r$, then n is a Carmichael number.

   Proof. □

   (b) Show that 6601 is a Carmichael number.

   Proof. □

6. Prove the converse to Wilson's Theorem: If $(m-1)! \equiv -1 \pmod{m}$, then m is prime.

Proof. Let m be composite. That is, $m = ab$ for some $1 < a < b < m$.
We can then say $a \mid (m-1)!$ since $1 < a < m$. If Wilson's Theorem holds for m, then

$$(m-1)! \equiv -1 \pmod{m}$$
$$(m-1)! = mx - 1 \quad \text{for some x } \in \mathbb{Z}$$

So, $m \mid (m-1)! + 1$. Since $a|m$, then $a \mid (m-1)! + 1$. We can conclude that $a \mid 1$ since we also have $a \mid (m-1)!$. If this is true, then $a = 1$. However, this is a contradiction to $1 < a < m$. Thus m cannot be composite. Therefore if $(m-1)! \equiv -1 \pmod{m}$, then m is prime. □