WORKSHEET 11

Date: 11/10/2021

Name:

Linear Congruence and Fermat's Little Theorem

THEOREM 1 (Liner Congruence solutions)**.** *The congruence equation*

$$ax \equiv b \pmod{m}$$

has a solution $x \in \mathbb{Z}$ *if and only if* $hcf(a,m)$ *divides* b*.*

1. Solve the following sets of simultaneous congruence's:

$$x \equiv 1 \pmod{3}, \qquad x \equiv 2 \pmod{5} \qquad x \equiv 3 \pmod{7}$$

2. What is $\frac{2}{3}$ modulo 5?

3. What is $\sqrt{3}$ modulo 7?

4. What is $\sqrt{5}$ modulo 11?

THEOREM 2 (Fermat's Little Theorem)**.** *Let p be a prime and a an integer relatively prime to p. Then,*

$$a^{p-1} \equiv 1 \pmod{p}$$

Proof. It is enough to show the following statement holds, $a^p \equiv a \pmod{p}$, with the conditions above. This proof is by induction. If $a = 1$, then the statement is obviously true. Assume our statement holds for some integer a. Recall from the binomial theorem:

$$(a+1)^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-i} 1^i$$

Where the coefficient $\binom{p}{k}$ is given by

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

We first show $\binom{p}{k} \equiv 0 \pmod{p}$ when $1 \leq k \leq p-1$. To see this, note that

$$k!\binom{p}{k} = p(p-1)\cdots(p-k+1) \equiv 0 \pmod{p}.$$

But p is a prime so $p|k!$ or $p|\binom{p}{k}$. But $p|k!$ implies $p|j$ for some j in $1 \leq j \leq p-1$. Which certainly cannot happen. Hence, $p|\binom{p}{k}$ i.e.

$$\binom{p}{k} \equiv 0 \pmod{p}.$$

Hence,

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

where the right-most congruence uses our inductive assumption. □

Remark: The converse of Fermat's Little Theorem is false.

THEOREM 3 (Wilson's Theorem)**.** *Let p be an integer greater than one. Then, p is a prime if and only if $(p-1)! \equiv -1 \pmod{p}$*

Proof. I am not going to have enough time in section to prove this, but the reverse implication is a lot easier. A proof by contradiction should not be to hard.

$\square$

LEMMA 4. *Let p and q be distinct primes and $x \in \mathbb{Z}$. Assume p divides x and q divides x. Then pq divides x.*

Proof. :

$\square$

1. If $(a, 35) = 1$, show that $a^{12} \equiv 1 \pmod{35}$.

2. For the congruence equations below, either find a solution $x \in \mathbb{Z}$ or show that no solutions exists:

$$x^2 + x + 1 \equiv 0 \pmod{5}$$

3. Let p be an odd prime. Then

   (a) $1^{p-1} + 2^{p-1} + \ldots + (p-1)^{p-1} \equiv -1 \pmod{p}$
   [Hint: when coming up with a strategy, it helps to pick particular values and then generalize. For example, take $p = 3$. How can you solve it?]

(b) $1^p + 2^p + \ldots + (p-1)^p \equiv 0 \pmod{p}$
[Hint: when coming up with a strategy, it helps to pick particular values and then generalize. For example, take $p = 3$. How can you solve it?]