Worksheet 4.4

Max's Lecture
MATH 55

July 8, 2019

Exercise A . 1. How many solutions does $3x \equiv 1 \pmod 6$ have?

2. How many solutions does $3x \equiv 0 \pmod 6$ have? How many solutions does this have with $0 \leq x < 6$?

3. How many solutions does $5x \equiv 1 \pmod 6$? How many solutions does it have with $0 \leq x < 6$?

4. Make a conjection on what conditions you can put on a such that $ax \equiv b \pmod m$ has what we call a unique solution mod m. This means there is is exactly one solution such that $0 \leq x < m$ and all other solutions are congruent to this solution mod m.

1. None! You can check for all $0 \leq x < 6$.

2. ~~$3x \equiv 0 \pmod 6$ has infinitely many solutions~~

$3x \equiv 0 \pmod 6$ has infinitely many solutions. It has 3 solutions with $0 \leq x < 6$. Those solutions are $x = 0, 2, 4$.

3. $5x \equiv 1 \pmod 6$ has infinitely many solutions, but it has exactly 1 solution x with $0 \leq x < 6$.

This solution is $x = 5$

Exercise B. What is the inverse of 101 mod 4620?

~~We first do Euclidian algorithm of 101, 4620~~

~~4620 =~~

This is Example 2 on pages 292-293 in book.

let me know if you have any questions!

The inverse ends up being 1601

Exercise C. Solve the following congruences:

1. $101x \equiv 2(\mod 4620)$
2. $3x \equiv 4(\mod 7)$

1. We multiply both sides by the inverse computed in the last problem.

$1601 \cdot 101\, x \equiv 1601 \cdot 2 \pmod{4620}$

So $x \equiv 3202 \pmod{4620}$

Exercise D (from ancient texts). Solve the system of congruences:

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

This is done in example 5 on page 295 of book. let me know if you have any questions!

Exercise E. Compute $7^{222} \mod 11$

By FLT, we know $7^{10} \equiv 1 \mod 11$.

So $7^{222} \equiv 7^{10 \cdot 22 + 2} \equiv (7^{10})^{22} \cdot 7^2 \equiv 7^2 \equiv 49 \equiv 5 \mod 11$.

Exercise F (4.4.19). This exercise outlines a proof of Fermats little theorem

1. Suppose that a is not divisible by the prime p. Show that no two integers $1a, 2a, \ldots, (p-1)a$ are congruent modululo p.
2. Conclude from part (a) that the product of $1, 2, \ldots p-1$ is congruent modulo p to the product of $1a, \ldots (p-1)a$. Use this to show that

$$(p-1)! \equiv a^{p-1}(p-1)!(\mod p)$$

3. Use theorem 7 from 4.3(the theorem that says you can divide both sides by a product that is relatively prime to the modulus) to show that $a^{p-1} \equiv 1(\mod p)$.
4. Now show that $a^p \equiv a(\mod p)$ for all integers a.

This is more of a challenge problem, so I will not post the solutions right now, but: please let me know if you have any questions!