Worksheet 4.4

Max's Lecture
MATH 55

July 8, 2019

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

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

3. How many solutions does $5x \equiv 1 (\mod 6)$? 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 $ax \equiv b (\mod m)$ 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 $\mod m$.

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

Exercise C. Solve the following congruences:

1. $101x \equiv 2 \pmod{4620}$
2. $3x \equiv 4 \pmod{7}$

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

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 2 \pmod 7 \end{aligned}$$

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

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
$$(p-1)! \equiv a^{p-1}(p-1)! \pmod{p}$$
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 $a^{p-1} \equiv 1 \pmod{p}$.
4. Now show that $a^p \equiv a \pmod{p}$ for all integers a.