Week 07 Participation Assignment

Corey Mostero - 2566652

13 October 2023

Contents

1 Week 07 Participation Assignment

1.1

Show that the positive integers less than 11, except 1 and 10, can be split into pairs of integers such that each pair consists of integers that are inverses of each other modulo 11.

$$\begin{aligned}
2 \cdot 6 &\equiv 12 = 1 (\text{mod } 11) \\
3 \cdot 4 &\equiv 12 = 1 (\text{mod } 11) \\
5 \cdot 9 &\equiv 45 = 1 (\text{mod } 11) \\
7 \cdot 8 &\equiv 56 = 1 (\text{mod } 11)
\end{aligned}$$

1.2

Show that if p is a prime, the only solutions of $x^2 \equiv 1(\bmod(p))$ are the integers x such that $x \equiv 1(\text{mod}(p))$ or $x \equiv -1(\text{mod}(p))$.

$$\begin{aligned}
x^2 &\equiv 1(\text{mod}(p)) \\
x^2 - 1 &\equiv 0(\text{mod}(p)) \\
(x-1)(x+1) &\equiv 0(\text{mod}(p)) \\
&\therefore p \mid (x-1)(x+1)
\end{aligned}$$

$$\begin{aligned}
x - 1 &\equiv 0(\text{mod}(p)) \\
x &\equiv 1(\text{mod}(p)) \\
x + 1 &\equiv 0(\text{mod}(p)) \\
x &\equiv -1(\text{mod}(p))
\end{aligned}$$

1.3

Generalize the result in part 1.1; that is, show that if p is a prime, the positive integers less than p, except 1 and $p-1$, can be split into $\frac{p-3}{2}$ pairs of integers such that each pair consists of integers that are inversed of each other.

$$S = \mathbb{Z}_p = \{1, 2, \cdots, p-2, p-1\}$$

From 1.2 we can see that there is x that makes $x \cdot x^{-1} \equiv 1(\bmod (p))$. It can also be observed that the equivalences for x can be written as $x = 1, p-1$. The set S can now be rewritten as

$$S = \{2, 3, \cdots, p-3, p-2\}$$

where we have $p-3$ (cannot be $p-2$ as primes cannot be even, and the result of an odd divided by an even is not an integer) positive integers, $\therefore \frac{p-3}{2}$ pairs.

1.4

From part 1.3, conclude that $(p-1)! \equiv -1(\text{mod}(p))$ whenever p is prime.

$$\begin{aligned}
&(p-1)! \equiv 1 \cdot 2 \cdots (p-2) \cdot (p-1) \\
&(p-1)! \equiv 1 \cdot (2 \cdot 2^{-1}) \cdots \left[(p-2)(p-2)^{-1}\right] \cdot (p-1), \quad \text{using 1.3} \\
&(p-1)! \equiv 1 \cdot (1) \cdots [1] \cdot (p-1) \\
&(p-1)! \equiv 1 \cdot (p-1) \\
&(p-1)! \equiv (p-1) \bmod (p) \\
&(p-1)! \equiv (p \bmod (p)) - (1 \bmod (p)) \\
&(p-1)! \equiv 0 - 1 \bmod (p) \\
&(p-1)! \equiv -1 \bmod (p)
\end{aligned}$$

1.5

Suppose that a is not divisible by the prime p. Show that no two of the integers $1 \cdot a, 2 \cdot a, \cdots, (p-1) \cdot a$ are congruent modulo p.

Let the two integers be x and y, where $1 \leq x < y < p$, giving $p \mid a(y-x)$. As a is not divisible by the prime p, it must conclude that $p \mid (y-x)$. Though as p is prime, and $1 \leq y - x < p$, this cannot be true by the definition of a prime number.

1.6

Conclude from part 1.5 that the product of $1, 2, \cdots, p-1$ is congruent modulo p to the product of $a, 2a, \cdots, (p-1)a$. Use this to show that $(p-1)! \equiv a^{p-1}(p-1)!(\text{mod}(p))$.

1.5 shows that no two integers $1 \cdot a, 2 \cdot a, \cdots, (p-1) \cdot a$ are congruent modulo p.

$$\begin{aligned}
a \cdot 2a \cdots (p-1)a &= (1 \cdot 2 \cdots p-1) \bmod (p) \\
(1 \cdot 2 \cdots (p-1)) \cdot (a^{p-1}) &= (p-1)! \\
(p-1)! \cdot a^{p-1} &= (p-1)!
\end{aligned}$$

1.7

Use Theorem 7 of Section 4.3 to show that from part 1.6 that $a^{p-1} \equiv 1(\bmod p)$ if $p \mid a$.

$$\begin{aligned}(p-1)! &\equiv -1(\bmod(p))\\ (-1)\cdot a^{p-1} &\equiv -1(\bmod(p))\\ -1\cdot(-1)\cdot a^{p-1} &\equiv -1(\bmod(p))\cdot -1\\ a^{p-1} &\equiv 1(\bmod(p))\end{aligned}$$

1.8

Use part 1.3 to show that $a^p \equiv a(\bmod(p))$ for all integers a.

- Case 1: $p \mid a$

$$\forall a \in \mathbb{Z}(a^p \equiv 0 \bmod (p) \iff a(\bmod(p)) \equiv 0 \bmod (p))$$

- Case 2: $p \nmid a$ (Fermat's Little Theorem)

$$\begin{aligned}a^{p-1} &\equiv 1(\bmod(p))\\ a^p &\equiv a(\bmod(p))\end{aligned}$$