MATH-3420 - Assignment 3 - Jonathon Meney

Jonathon Meney

October 2023

1. Find all solutions modulo 693 of the system:

$$\begin{aligned} 4x &\equiv 5 \pmod 7 \\ 6x &\equiv 3 \pmod 9 \\ 5x &\equiv 1 \pmod{11} \end{aligned}$$

Simplify.

$$\begin{aligned} x &\equiv 3 \pmod 7 \\ x &\equiv 2 \pmod 3 \iff x \equiv 2, 5, 8 \pmod 9 \\ x &\equiv 9 \pmod{11} \end{aligned}$$

Find c_1, c_2, c_3.

$$\begin{aligned} c_1 &= 9(11) = 99 \\ c_2 &= 7(11) = 77 \\ c_3 &= 7(9) = 63 \end{aligned}$$

Find d_1, d_2, d_3.

$$\begin{array}{rrr} 99d_1 \equiv 1 \pmod 7 & 77d_2 \equiv 1 \pmod 9 & 63d_3 \equiv 1 \pmod{11} \\ d_1 \equiv 1 \pmod 7 & 5d_1 \equiv 1 \pmod 9 & 8d_1 \equiv 1 \pmod{11} \\ d_1 \equiv 1 & d_2 \equiv 2 & d_3 \equiv 7 \end{array}$$

There will be 3 solutions since $x \equiv 2, 5, 8 \pmod 9$. For $a_2 = 2$:

$$\begin{aligned} x &= a_1c_1d_1 + a_2c_2d_2 + a_3c_3d_3 \\ x &= 3(99)(1) + 2(77)(2) + 9(63)(7) = 4574 \\ x &\equiv 416 \pmod{693} \end{aligned}$$

For $a_2 = 5$:

$$\begin{aligned} x &= a_1c_1d_1 + a_2c_2d_2 + a_3c_3d_3 \\ x &= 3(99)(1) + 5(77)(2) + 9(63)(7) = 5036 \\ x &\equiv 185 \pmod{693} \end{aligned}$$

For $a_2 = 8$:

$$\begin{aligned} x &= a_1c_1d_1 + a_2c_2d_2 + a_3c_3d_3 \\ x &= 3(99)(1) + 8(77)(2) + 9(63)(7) = 5498 \\ x &\equiv 647 \pmod{693} \end{aligned}$$

Thus the solutions to the system modulo 693 are $x \equiv 185, 416, 647 \pmod{693}$.

2. Show that if p is a prime and $p = n^3 - 1$ for some integer n, then $p = 7$. (Hint: Factor $n^3 - 1$.)

Proof. Assume p is prime and $p = n^3 - 1$ for some integer n. Also note $n \geq 2$. We can first factor $p = n^3 - 1$ to find:

$$\begin{aligned} p &= n^3 - 1 \\ p &= (n-1)(n^2 + n + 1) \end{aligned}$$

Since p is prime we know its factors will be 1 and p. Thus:

$$n - 1 = 1 \quad \text{and} \quad n^2 + n + 1 = p$$

So:

$$\begin{aligned} n - 1 &= 1 \\ n &= 2 \end{aligned}$$

and:

$$\begin{aligned} p &= n^2 + n + 1 \\ p &= 2^2 + 2 + 1 \\ p &= 7 \end{aligned}$$

Therefore, if p is a prime and $p = n^3 - 1$ for some integer n, then p must be 7. $\square$

3. Find the least non-negative integer x such that

$$x \equiv 205^{157} \times 26! \pmod{29}$$

Firstly, using Fermat's Theorem:

$$\begin{aligned}
205^{157} &\equiv 2^{157} \pmod{29} \\
&\equiv (2^{28})^5 + 2^{17} \pmod{29} \\
&\equiv (1)^5 + 2^{14} + 2^3 \pmod{29} \\
&\equiv 1 - 1 + 2^3 \pmod{29} \\
&\equiv 8 \pmod{29}
\end{aligned}$$

Secondly, using Wilson's Theorem:

$$\begin{aligned}
28! &\equiv -1 \pmod{29} \\
(-1)27! &\equiv -1 \pmod{29} \\
27! &\equiv 1 \pmod{29} \\
(-2)26! &\equiv 1 \pmod{29} \\
(-2)26! &\equiv 30 \pmod{29} \\
26! &\equiv -15 \pmod{29} \\
26! &\equiv 14 \pmod{29}
\end{aligned}$$

Therefore:

$$\begin{aligned}
x &\equiv 205^{157} \times 26! \pmod{29} \\
x &\equiv 8 \times 14 \pmod{29} \\
x &\equiv 112 \pmod{29} \\
x &\equiv 25 \pmod{29}
\end{aligned}$$

4. Show that for any integer a and prime p, p divides $a^p + a(p-1)!$.

Proof. Suppose we have some prime p and some integer a. By Wilson's Theorem we know:

$$(p-1)! \quad \equiv \quad -1 \text{ (mod p)}$$

Thus:

$$\begin{aligned} a^p + a(p-1)! \\ a^p + a(-1) \\ a^p - a \end{aligned}$$

By Fermat's Theorem we know:

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

Multiplying both sides of Fermat's Theorem by a we get:

$$a^p \quad \equiv \quad a \text{ (mod p)}$$

Therefore:

$$a^p - a = a - a = 0$$

Thus:

$$a^p + a(p-1)! \quad \equiv \quad 0 \text{ (mod p)}$$

Therefore we have proven that p divides $a^p + a(p-1)!$. □

5. Use Wilson's Theorem to show that

$$1^2 \times 3^2 \times 5^2 \times 7^2 \times \ldots \times 809^2 \equiv 1 \pmod{811}$$

(Hint: $k \equiv k - 811 \pmod{811}$.)

Proof. First we can simplify:

$$\begin{aligned} 1^2 \times 3^2 \times 5^2 \times 7^2 \times \ldots \times 809^2 &\equiv 1 \pmod{811} \\ \sqrt{1^2 \times 3^2 \times 5^2 \times 7^2 \times \ldots \times 809^2} &\equiv \sqrt{1} \pmod{811} \\ 1 \times 3 \times 5 \times 7 \times \ldots \times 809 &\equiv 1 \pmod{811} \end{aligned}$$

Then we can use the fact that $k \equiv k - 811 \pmod{811}$:

$$\begin{aligned} 1 \times 3 \times 5 \times 7 \times \ldots \times 807 \times 809 &\equiv 1 \pmod{811} \\ 1 \times 3 \times 5 \times -804 \times \ldots \times -4 \times -2 &\equiv 1 \pmod{811} \\ 1 \times (3 \times -270) \times (5 \times -162) \times (-804 \times 695) \times \ldots & \\ \ldots \times (-4 \times 203) \times (-2 \times -406) &\equiv 1 \pmod{811} \\ 1 \times 1 \times 1 \times 1 \times \ldots \times 1 \times 1 &\equiv 1 \pmod{811} \end{aligned}$$

Therefore we have shown that:

$$1^2 \times 3^2 \times 5^2 \times 7^2 \times \ldots \times 809^2 \equiv 1 \pmod{811}$$

□