Assignment 20: Congruence

Declan Murphy Zink

11/2/2020

2 Let p be a prime number and k a positive integer.

2.a Show that if x is an integer such that $x^2 \equiv x$ mod p, then $x \equiv 0$ or 1 mod p.

For some $a \in \mathbb{Z}$:

$$\begin{aligned} x^2 &= x + pa \\ x^2 - x &= pa \\ x(x-1) &= pa \end{aligned}$$

Thus either $p|x$ or $p|(x-1)$. p can only divide a multiple of itself (including 0), so $x \equiv 0$ mod p or $(x-1) \equiv 0$ mod $p \Rightarrow x \equiv 1$ mod p.

2.b Show that if x is an integer such that $x^2 \equiv x$ mod p^k, then $x \equiv 0$ or 1 mod p^k.

For some $a \in \mathbb{Z}$:

$$\begin{aligned} x^2 &= x + p^k a \\ x^2 - x &= p^k a \\ x(x-1) &= p^k a \end{aligned}$$

Since x and $x-1$ are coprime, p cannot divide both. Thus, either $p^k|x$ or $p^k|(x-1)$. p^k can only divide a multiple of itself (including 0), so $x \equiv 0$ mod p^k or $(x-1) \equiv 0$ mod $p^k \Rightarrow x \equiv 1$ mod p^k.

3 For each of the following congruence equations, either find a solution $x \in \mathbb{Z}$ or show that no solution exists:

3.a $99x \equiv 18$ mod 30.

$99x = 18 + 30y, y \in \mathbb{Z}$
$hcf(99, 30) = ?$

$$\begin{aligned} 99 &= 3(30) + 9 \\ 30 &= 3(9) + 3 \\ 9 &= 3(3) + 0 \end{aligned}$$

$hcf(99,30) = 3$
$\Rightarrow \exists\ s,t \in \mathbb{Z}$ such that $99s + 30t = 3$

$$\begin{aligned} 3 &= 30 - 3(9) \\ 3 &= 30 - 3(99 - 3(30)) \\ 3 &= -3(99) + 10(30) \end{aligned}$$

Thus $99(-3) = 3 + 30(-10)$
multiplying by 6: $99(-18) = 18 + 30(-60) \Rightarrow 99(-18) \equiv 18 \bmod 30.$
$x = -18$

3.b $\quad 91x \equiv 84$ **mod** 143**.**

$hcf(91,143) = ?$

$$\begin{aligned} 143 &= 1(91) + 52 \\ 91 &= 1(52) + 39 \\ 51 &= 1(39) + 13 \\ 39 &= 3(13) + 0 \end{aligned}$$

$hcf(91,143) = 13$
13 does not divide 84, so there is no solution.

3.c $\quad x^2 \equiv 2$ **mod** 5**.**

$0^2 \equiv 0 \bmod 5$
$1^2 \equiv 1 \bmod 5$
$2^2 \equiv 4 \bmod 5$
$3^2 \equiv 4 \bmod 5$
$4^2 \equiv 1 \bmod 5$
No solution exists.

3.d $\quad x^2 + x + 1 \equiv 0$ **mod** 5**.**

$0^2 + 0 + 1 \equiv 1 \bmod 5$
$1^2 + 1 + 1 \equiv 3 \bmod 5$
$2^2 + 2 + 1 \equiv 2 \bmod 5$
$3^2 + 3 + 1 \equiv 3 \bmod 5$
$4^2 + 4 + 1 \equiv 1 \bmod 5$
No solution exists.

3.e $\quad x^2 + x + 1 \equiv 0$ **mod** 7**.**

$x^2 + x \equiv -1 \bmod 7$
$x(x+1) \equiv 6 \bmod 7$
$x = 2$ is a solution.

5

5.a Use the fact that 7 divides 1001 to find your own "rule of 7." Use your rule to work out the remainder when 6005004003002001 is divided by 7.

Since $7|1001$:
$10^3 \equiv -1 \bmod 7$
$10^6 \equiv 1 \bmod 7$
$10^9 \equiv -1 \bmod 7$
so $10^{3n} \equiv (-1)^n \bmod 7$

Thus for $a_1...a_k \in \mathbb{Z}$ and $i \in \mathbb{Z}$:
$a_1(10^0) + a_2(10^3) + ... + a_k(10^{3i}) \equiv a_1 - a_2 + a_3 - a_4 + ... \pm a_k \bmod 7.$

So, $6005004003002001 \equiv 1 - 2 + 3 - 4 + 5 - 6 \equiv -3 \equiv 4 \bmod 7.$
Thus the remainder is 4.

5.b 13 also divides 1001. Use this to get a rule of 13 and find the remainder when 6005004003002001 is divided by 13.

This is the same rule as 7, so $6005004003002001 \equiv 1 - 2 + 3 - 4 + 5 - 6 \equiv -3 \equiv 10 \bmod 13.$
Thus the remainder is 10.

5.c Use the observation that $27 \times 37 = 999$ to work out a rule of 37, and find the remainder when 6005004003002001 is divided by 37.

Since $27 \times 37 = 999$, therefore $37|999$, so:
$10^3 \equiv 1 \bmod 37$
$10^6 \equiv 1 \bmod 37$
so $10^{3n} \equiv 1 \bmod 37$

Thus for $a_1...a_k \in \mathbb{Z}$ and $i \in \mathbb{Z}$:
$a_1(10^0) + a_2(10^3) + ... + a_k(10^{3i}) \equiv a_1 + a_2 + ... + a_k \bmod 37.$

So, $6005004003002001 \equiv 1 + 2 + 3 + 4 + 5 + 6 \equiv 21 \bmod 37.$
Thus the remainder is 21.

6 Let p be a prime number, and let a be an integer that is not divisible by p. Prove that the congruence equation $ax \equiv 1 \bmod p$ has a solution $x \in \mathbb{Z}$.

Since p is prime and p doesn't divide a, $hcf(a, p) = 1$. Thus $\exists\ s, t \in \mathbb{Z}$ such that $as + pt = 1$. Therefore $as = 1 - pt$, so $x = s$ is a solution in $\mathbb{Z}$ to $ax \equiv 1 \bmod p$.