MATH 302 Examination 2 May 29, 2009

102

Name Hill Zahradnik

Theorem 1. Let p be a prime and let a and b be integers. If $p\,|(ab)$, the $p\,|a$ or $p\,|b$.

Problem 2. Let p be a prime such that $p > 2$. Prove that the congruence $x^2 \equiv 1 \pmod{p}$ has exactly two solutions in $\{0, 1, \ldots, p-1\}$.

Proposition 3. Let a and b be integers, and let n be a positive integer. Set $d = \gcd(a, n)$. Prove that the congruence $ax \equiv b \pmod{n}$ has a solution if and only if $d|b$.

Problem 4. (a) Find a multiplicative inverse of 2009 modulo 302. Express your answer as a positive integer smaller than 302.

(b) Which positive integer smaller than 302 do not have a multiplicative inverse modulo 302? There are many such integers. Describe them all.

(c) Based on what you found in (b), tell me a simple rule for which future years can I repeat the question in (a) with the year adjusted.

Theorem 1

Let $a, b \in \mathbb{Z}$ and $p \in \mathbb{P}$. If $p \mid (ab)$ then $p \mid a$ or $p \mid b$

Know

$p \mid ab$, $p \in \mathbb{P} \Rightarrow ab = pk$ $k \in \mathbb{Z}$

Prove

$p \mid a$ or $p \mid b$

1.) let $ab = pk$ $k \in \mathbb{Z}$

2.) Assume $p \nmid a$ (case 1)

3) then a and p are relatively prime because only other divisor of p is 1.

4.) $ax + py = 1$

5.) $bax + bpy = b$

6.) $ab = pk \Rightarrow pkx + bpy = b$

7.) $p(kx + by) = b$, let $kx + by = n$ $n \in \mathbb{Z}$, then $pn = b$

8.) so $p \mid b$

9.) Assume $p \nmid b$ (case 2)

10.) then b and p are relatively prime because only other divisor of p is 1.

11.) $bx + py = 1$

12.) $abx + apy = a$

13.) because $ab = pk \Rightarrow pkx + apy = a$

14.) $p(kx + ay) = a$, let $kx + ay = j \Rightarrow pj = a$

15.) so $p \mid a$

Problem 2

Let $p \in \mathbb{P}$ s.t. $p > 2$. Prove the congruence $x^2 \equiv 1 \pmod{p}$ has exactly two solutions in $\{0, 1, \cdots, p-1\}$

Know
$p \in \mathbb{P}, p > 2 \quad x^2 \equiv 1 \pmod{p}$

Prove
$x^2 \equiv 1 \pmod{p}$ has exactly two solutions for $\{0, 1, \cdots, p-1\}$

1.) $x^2 \equiv 1 \pmod{p} \Rightarrow x^2 - 1 = pn \quad n \in \mathbb{Z}$

2.) $x^2 - 1 = (x-1)(x+1)$

3.) $(x-1)(x+1) = pn$

4.) theorem 1 says that If $p \mid ab$ then $p \mid a$ or $p \mid b$

5.) therefore $p \mid (x-1)$ or $p \mid (x+1)$

6.) Assume $p \mid (x-1)$ (case 1)

7.) $x - 1 = pk \quad k \in \mathbb{Z}$

8.) $x = pk + 1$ (similar to $a = qn + r$) so $r = 1$ $\quad 0 < 1 < p$

9.) Assume $p \mid (x+1)$ (case 2)

10.) $x + 1 = pl \quad l \in \mathbb{Z}$

11.) $x = pl - 1 \Rightarrow r = -1 \Rightarrow r = p - 1 \quad 0 < p-1 < p$

12.) $(p-1)^2 \equiv 1 \pmod{p} \Rightarrow p^2 - 2p + 1 \equiv 1 \pmod{p} \Rightarrow p^2 - 2p = pn$

13.) $1^2 \equiv 1 \pmod{p} \Rightarrow 1 - 1 = pn \Rightarrow 0 = pn$

14.) therefore $x^2 \equiv 1 \pmod{p}$ has exactly 2 solutions, in $\{0, 1, \cdots, p-1\}$, 1 and $p-1$.

Problem 3

Hill Zahradnik

Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}_{>0}$. Set $d = \gcd(a, n)$. Prove that the congruence $ax \equiv b \pmod{n}$ has a solution if and only if $d \mid b$.

Case 1: Know $ax \equiv b \pmod{n}$, $d = \gcd(a, n)$ — Prove $d \mid b \Rightarrow b = dl$, $l \in \mathbb{Z}$

1.) $ax \equiv b \pmod{n} \Rightarrow ax - b = nk$, $k \in \mathbb{Z}$

2.) also $d \mid a$ and $d \mid n \Rightarrow a = dm$ and $n = dq$, $m, q \in \mathbb{Z}$

3.) $(dm)x - b = (dq)k$

4.) $(dmx - dqk) = b$

5.) $d(mx - qk) = b \Rightarrow$ let $mx - qk = l$

6.) then $dl = b$, so $d \mid b$.

Case 2: Know $d \mid b$, $d = \gcd(a, n)$ — Prove $ax \equiv b \pmod{n} \Rightarrow ax - b = nl$, $l \in \mathbb{Z}$

1.) $d \mid b \Rightarrow b = dk$, $k \in \mathbb{Z}$

2.) $b = (ax_0 + ny_0)k$

3.) $b = ax_0k + ny_0k \Rightarrow ax_0k - b = n(-y_0k)$

4.) let $x_0k = x$ and $-y_0k = l$, $x, l \in \mathbb{Z}$

5.) then $ax - b = nl$

6.) so $ax \equiv b \pmod{n}$

Problem 4

a) Find a multiplicative inverse of 2009 modulo 302, express your answer as a positive integer smaller than 302

1.) $2009x \equiv 1 \pmod{302} \Rightarrow 2009x - 1 = 3024$

2.) $2009x - 3024 = 1$

3.)

2009	302	147	105	42	13	1	0
	6	1	1	1	7	13	
153	23	15	8	7	1	0	1

4.) $2009(23) - 302(153) = 1$

5.) $\boxed{x = 23}$

b.)