# MATH 302 Examination 2 May 29, 2009

Name Key

**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 $\{0, 1, \dots, p-1\}$.

**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.

1



Prove:

$$p \mid (ab) \text{ and } \underbrace{p \nmid b}_{} \Rightarrow p \mid a$$

$$\Downarrow$$

$$\gcd(p, b) = 1$$

$$\Downarrow$$

$\exists x, y \in \mathbb{Z}$ s.t.

$$px + by = 1$$

multiply by $a$

$$apx + aby = a$$

Clearly $p \mid (apx)$

It is assumed that $p \mid (ab)$, so

$$p \mid (aby).$$

Since $a = apx + aby$, we conclude

$$p \mid a.$$

② $p \in \mathbb{P}$, $p > 2$. $\boxed{2}$

Clearly two solutions of the congruence

$$x^2 \equiv 1 \pmod{p}$$

are $x = 1$ and $x = p-1$

$$(p-1)^2 = p^2 - 2p + 1$$

$$(p-1)^2 - 1 = p(p-2)$$

Hence $p \mid ((p-1)^2 - 1)$.

Now assume $x \in \{1, 2, \dots, p-1\}$ and $x^2 \equiv 1 \pmod{p}$. Then $p \mid (x^2 - 1)$.

Then $p \mid ((x-1)(x+1))$. By Th 1.

$$p \mid (x-1) \quad \text{or} \quad p \mid (x+1).$$

Notice $x - 1 \in \{0, 1, 2, \dots, p-2\}$ so $p \mid (x-1)$ implies $x - 1 = 0$, that is $x = 1$

$p \mid (x+1)$. Notice $x+1 \in \{2, 3, \dots, p-1, p\}$. $\boxed{3}$

So $p \mid (x+1)$ implies $x+1 = p$, that

is $x = p-1$.

Hence

$p \mid (x^2-1)$ implies $x = 1$ or $x = p-1$.

Thus 1 and $p-1$ are the only solutions.

3 $d = \gcd(a, n)$

$ax \equiv b \pmod{n}$

is equivalent to

$\exists k \in \mathbb{Z}$ s.t. $b - ax = nk$

or $nk + ax = b$

We know that the equation

$nk + ax = b$

has a solution $k, x$ if and only if

$d \mid b$. Thus $ax \equiv b \pmod{n}$

has a solution iff $d \mid b$

4

④ ⓐ

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 2009 | 302 | 197 | 105 | 92 | 13 | 1 | 0 | |
| | 6 * | 1 * | 1 * | 1 | 7 | 13 | | |
| 153 | 23 | 15 | 8 | 7 | 1 | 0 | | 1 |

$2009 * 23 - 302 * 153 = 1$

7 6

Hence 23 is a multiplicative inverse of 2009 modulo 302

3 5 7 11 13

ⓑ $302 = 2 * 151$

prime prime

All even numbers in $\{1, 2, \ldots, 301\}$ do not have a mult. inv. modulo 302 since they are not rel. prime with 302. Also 151 does not have a mult. inv. ALL ~~other~~ odd numbers $\neq 151$ have mult. inv. modulo 302.

ⓒ You (I) must avoid even years. Also avoid years divisable by 151. But the next one is 2114 no problems here!