# MATH 302

Examination Final
June 8, 2009

Name Key

Do 8 out of the following 9 problems.

**Problem 1.** (a) Give a definition of a prime.

(b) Let $a$ be a positive integer greater than 1. Prove that there exists a prime $p$ such that $p \mid a$. (Give all details of the proof.)

**Problem 2.** (a) Let $a$ and $b$ be positive integers. Prove $ab = \gcd(a,b)\,\mathrm{lcm}(a,b)$.

(b) Calculate $\mathrm{lcm}(9009, 6279)$.

**Problem 3.** Prove that there exist infinitely many primes.

**Problem 4.** By definition ~~the~~ primes $p$ and $q$ are called *twin primes* if $q = p+2$. Examples: 5,7; 11,13; 17,19; 29,31; 41,43; 59,61; 71,73; 101,103; 107,109; 137,139; 149,151; 179,181.

(a) If $p$ and $q$ are twin primes with $3 < p < q$, then $p+1$ is divisible by 6.

(b) If $p$ and $q$ are twin primes, then $pq+1$ is a perfect square.

(c) If $p$ and $q$ are twin primes with $3 < p < q$, then $pq+1$ is divisible by 36.

**Problem 5.** Let $a$ and $b$ be integers, not both zero. Prove that there exist integers $x$ and $y$ such that $ax + by = \gcd(a,b)$.

**Problem 6.** (a) State and prove Fermat's Little Theorem.

(b) State the main proposition that you used in the proof of Fermat's Little Theorem.

**Problem 7.** Solve the linear congruence $2076\,x \equiv 3076 \pmod{1076}$. Express your solution as $x \equiv c \pmod{n}$ where $0 < c < m$.

**Problem 8.** (a) Let $a$ and $b$ be any integers. Let $m$ and $n$ be positive relatively prime integers. ~~Prove that there exists an integer $c$ such that~~ If

$$x \equiv a \pmod{m} \quad \text{and} \quad x \equiv b \pmod{n},$$ then $\exists c \in \mathbb{Z}$

~~if and only if~~

$$x \equiv c \pmod{mn}.$$

(b) Solve the system of congruences

$$x \equiv 3 \pmod{7}, \quad x \equiv 2 \pmod{8}, \quad x \equiv 1 \pmod{9}.$$

**Problem 9.** Let $p$ and $q$ be distinct primes. Prove that

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$

(1) (a) An integer $p > 1$ is a prime if $x \mid p$, $x \in \mathbb{N} \Rightarrow x = 1$ or $x = p$.

(b) Set $S = \{y \in \mathbb{Z} : y > 1, y \mid a\}$

(1) $S \subseteq \mathbb{Z}$
(2) $S$ is bdd below by 1.
(3) $S \neq \emptyset$ since $a \in S$.

By WOA there exists $\min S = q$.
I claim $q$ is a prime. Here is a proof. Let $x > 1$ and $x \mid q$. Then $x \mid a$ since $q \mid a$. Hence $x \in S$. Therefore $q \geq x$. But also $x \mid q$ and $x > 1$ imply $x \leq q$. Thus $x = q$. So we proved $x > 1$ and $x \mid q \Rightarrow x = q$.
This is equivalent to
$x \mid q, x \in \mathbb{N} \Rightarrow x = 1$ or $x = q$.
This proves that $q \in \mathbb{P}$.

(2) (a) $a, b \in \mathbb{N}$.

Set $g = \gcd(a,b)$, $\ell = \operatorname{lcm}(a,b)$.

Then $a = gs$, $b = gt$. Set $z = gst$.

Then $a \mid z$ and $b \mid z$. That is $z$ is a common multiple of $a$ and $b$ and $z \geq 1$. Therefore $\ell \leq z$. Hence $g\ell \leq gz = gsgt = ab$.

Thus we proved $\boxed{g\ell \leq ab}$. By a proposition proved in class $s$ and $t$ are relatively prime, so $\exists x, y \in \mathbb{Z}$ s.t.

$$sx + ty = 1.$$

thus $g\ell sx + g\ell ty = g\ell$.

Since $a = gs$ and $b \mid \ell$, and $b = gt$ and $a \mid \ell$ we conclude that $ab \mid gls$ and $ab \mid glt$. therefore $ab \mid g\ell$. Since $ab \geq 1$ and $g\ell \geq 1$ we conclude $\boxed{ab \leq g\ell}$. Thus $\underline{ab = g\ell}$.

(b) calculate $\gcd(9009, 6279) = 273$

9009 6279 2730 819 273 0

1 2 3 3

$$\operatorname{lcm}(9009, 6279) = \frac{9009 * 6279}{273} =$$

$$= 9009 * 23 = 207207.$$

(3) Let $F$ be a finite set of primes. We will prove that $\exists\, q \in \mathbb{P}$ s.t. $q \notin F$. 3

Let $F = \{p_1, \dots, p_n\}$. Let $a = p_1 \cdots p_n + 1$. Then $\gcd(a, p_j) = 1$ for all $j = 1, \dots, n$. By Pr. 1. there exist $q \in \mathbb{P}$ s.t. $q \mid a$. Since $\gcd(a, p_j) = 1$ we have $\gcd(q, p_j) = 1$. Hence $q \neq p_j$ for all $j = 1, \dots, n$. thus $q \notin F$. Hence $F \subsetneq \mathbb{P}$ for each finite set $F$. Hence $\mathbb{P}$ is infinite.

(4) (a) Let $p = 6k + r$ where $r \in \{0, 1, 2, 3, 4, 5\}$. Since $p$ is an odd prime $r \in \{1, 3, 5\}$ Since $p \neq 3$ and $3 \nmid p$ we have $r \neq 3$. Hence $r \in \{1, 5\}$. Since $3 \mid (p+3)$ we get $r \neq 1$. Hence $r = 5$. Therefore $p + 1$ is divisable by 6.

(4)(b) $pq+1 = p(p+2)+1$

$= p^2+2p+1$

$= (p+1)^2$

This proves that $pq+1$ is a perfect square.

(c) By (a) $6 \mid (p+1)$ thus $36 \mid (p+1)^2$.

But $(p+1)^2 = pq+1$. Hence $36 \mid (pq+1)$.

(5) Set $S = \{z \in \mathbb{Z} : z \mid a, z \mid b\}$

We proved that $S$ has a maximum.

$g = \gcd(a,b) = \max S$.

Set $T = \{v \in \mathbb{Z} : v = ax+by \text{ with } x,y \in \mathbb{Z}, v \geq 1\}$

(1) $T \subseteq \mathbb{Z}$

(2) $T$ bounded below by 1.

(3) $T \neq \emptyset$ since $a^2+b^2 \in T$.

By WOA $\min T$ exists. Set $d = \min T$.

$d = ax_0+by_0 = gsx_0+gty_0 = g(sx_0+ty_0)$

so $g \mid d$. Hence $\boxed{g \leq d}$. Now I prove that $d \mid a$ and $d \mid b$. By a theorem from notes $\exists\, q, r \in \mathbb{Z}$ s.t.

$a = dq + r$ and $0 \le r < d$. 

Hence $r \notin T$. (since $r < \min T$)

But $r = a - dq = a - (ax_0 + by_0)q$

$= a(1 - x_0) + b(-y_0 q)$

Since $r \notin T$ $r < 1$. Hence $r = 0$.

Thus $d \mid a$. Similarly $d \mid b$.

Since ~~$d \mid g$~~ ~~and~~ $g$ is the greatest common divisor of $a$ and $b$ we have $\boxed{d \le g}$. This prove $\underline{\underline{d = g}}$.

(6) @ If $a$ is an integer and $p$ is a prime s.t. $p \nmid a$, then $a^{p-1} \equiv 1 \pmod p$.

By Proposition in (6b) the numbers $1a, 2a, \dots, pa$ have distinct remainders when divided by $p$: Set

$ka = r_k \pmod p$ $\quad r_k \in \{0, 1, \dots, p-1\}$

then $\{r_1, \dots, r_{p-1}\} = \{1, \dots, p-1\}$. Hence

$(1a)(2a) \dots ((p-1)a) \equiv (p-1)! \pmod p$

$(p-1)!\, a^{p-1} \equiv (p-1)! \pmod p$

Since $(p-1)!$ and $p$ are relatively prime we conclude that

$$a^{p-1} \equiv 1 \pmod{p}.$$

(6)(b) Proposition. The numbers $a \in \mathbb{Z}$, $p \in \mathbb{P}$, $p \nmid a$

$$1a, 2a, \ldots, pa$$

have distinct remainders when divided by $p$.

---

(7) $2076x \equiv 3076 \pmod{1076}$

$\gcd(2076, 1076) = 4$

| 2076 | 1076 | 1000 | 76 | 12 | 4 | 0 |
|---|---|---|---|---|---|---|
| | 1 | 1 | 13 | 6 | 3 | |

$$519x \equiv 769 \pmod{269}$$

$$250x \equiv 231 \pmod{269}$$

| 269 | 250 | 19 | 3 | 1 | 0 |
|---|---|---|---|---|---|
| | 1 | 13 | 6 | 3 | |

| 85 | 79 | 6 | 1 | 0 | 1 |
|---|---|---|---|---|---|

$269 * 79 + 250(-85) = 1$

inv. 184

$X \equiv 231 * 184 \pmod{269}$

$X \equiv 2 \pmod{269}$

(8) (a) Assume

$x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$

Since $m$ and $n$ are relatively prime ~~we have~~ there exists

~~$\gcd(m, n) = 1$~~ such that

$b_1$ and $b_2$

$$nb_1 \equiv 1 \pmod{m}$$

and $mb_2 \equiv 1 \pmod{n}$.

Set

$$c = ab_1 n + bb_2 m$$

then $x \equiv ab_1 n \pmod{m}$

$0 \equiv bb_2 m \pmod{m}$

so $x \equiv c \pmod{m}$

Similarly $x \equiv c \pmod{n}$

Since $\gcd(m, n) = 1$ we have

$x \equiv c \pmod{mn}$.

8б

$X \equiv 3 \pmod 7$

$X \equiv 2 \pmod 8$

$X \equiv 1 \pmod 9$

8

$m = 7 \cdot 8 \cdot 9$ $\quad m_1 = 8 \cdot 9$ $\quad m_2 = 7 \cdot 9$, $m_3 = 7 \cdot 8$

$n_1 = 7$ $\quad n_2 = 8$ $\quad n_3 = 9$

$72x \equiv 1 \pmod 7$

$2x \equiv 1 \pmod 7$

$\boxed{b_1 = 4}$

$56x \equiv 1 \pmod 9$

$2x \equiv 1 \pmod 9$

$\boxed{b_3 = 5}$

$63x \equiv 1 \pmod 8$

$7x \equiv 1 \pmod 8$

$\boxed{b_2 = 7}$

$c = 3*72*4 + 2*63*7 + 1*56*5$

$= 2026$

$X \equiv 2026 \pmod{504}$

$\boxed{X \equiv 10 \pmod{504}}$

(9) By FLT



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

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

Hence $2 \mid (p^{2-1} - 1)$,

$p \mid (2^{p-1} - 1)$.

Hence $p2 \mid ((p^{2-1} - 1)(2^{p-1} - 1))$

Hence $p2 \mid (p^{2-1}2^{p-1} - (p^{2-1} + 2^{p-1} - 1))$

Since $p2 \mid p^{2-1}2^{p-1}$ we conclude

$p2 \mid (p^{2-1} + 2^{p-1} - 1)$. Thus

$$p^{2-1} + 2^{p-1} \equiv 1 \pmod{p2}$$