

Math 453 - Final Exam - December 12, 2008

Name: _____

Question Number	Possible Points	Score
1	20	
2	20	
3	20	
4	20	
5	20	
6	20	
7	20	
8	20	
9	20	
10	20	
EC	20	
Total	200	

Instructions:

- Write your name on the exam now.
- You may begin when the bell rings.
- You may not use the book, notes, or a calculator.
- Show your reasoning unless otherwise specified.
- You do not need to simplify your answers.

2

1. (20 points). Compute $2^{999999} \pmod{125}$. You do not need to show your reasoning on this problem.

We have $\phi(125) = 100$, and so by Euler's theorem,

$$2^{\phi(125)} = 2^{100} \equiv 1 \pmod{125}.$$

Thus, we may reduce the exponent modulo 100. This gives us

$$2^{999999} \equiv 2^{99} \pmod{125}.$$

Now, $2 \cdot 2^{99} \equiv 1 \pmod{125}$, and so 2^{99} is $\pmod{125}$ the multiplicative inverse of 2. Using the Euclidean algorithm, we get

$$125 - 2 \cdot 62 = 1,$$

and so $2^{99} \equiv -62 \equiv 63 \pmod{125}$.

2. (20 points). You do not need to show your reasoning on this problem.

(a) (10 points). Compute the number of divisors of $8!$.

We have $8! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 = 2^7 \cdot 3^2 \cdot 5 \cdot 7$. Thus, the number of divisors is

$$v(8!) = 8 \cdot 3 \cdot 2 \cdot 2 = 96.$$

(b) (10 points). Compute $\phi(900)$.

We have $900 = 2^2 \cdot 3^2 \cdot 5^2$. Thus, we have

$$\phi(900) = 2^1(2-1)3^1(3-1)5^1(5-1) = 2 \cdot 3 \cdot 2 \cdot 5 \cdot 4 = 16 \cdot 15 = 240.$$

3. (20 points). How many solutions are there to

$$x^2 + 8x - 3 \equiv 0 \pmod{47}$$

that are incongruent mod 47?

We have $b^2 - 4ac = 8^2 - 4(1)(-3) = 64 + 12 = 76$. There are no solutions if 76 is not a square mod 47, there is one solution if $76 \equiv 0 \pmod{47}$ (which it is not), and there are two solutions if 76 is a square mod 47. We have

$$\begin{aligned} \left(\frac{76}{47}\right) &= \left(\frac{76 - 2 \cdot 47}{47}\right) = \left(\frac{-18}{47}\right) \\ &= \left(\frac{-2}{47}\right) \left(\frac{9}{47}\right) = \left(\frac{-2}{47}\right) \\ &= \left(\frac{-1}{47}\right) \left(\frac{2}{47}\right) = (-1) \cdot 1 = -1. \end{aligned}$$

Thus, there are no solutions.

4. (20 points). List all positive integers that are not of the form $4x + 7y$ with $x, y \in \mathbb{Z}$ and $x, y \geq 0$. You do not need to show your reasoning on this problem.

If we make a table of values of $4x + 7y$,

x	$y = 0$	$y = 1$	$y = 2$	$y = 3$
0	0	7	14	21
1	4	11	18	25
2	8	15	22	26
\vdots	\vdots	\vdots	\vdots	\vdots

all the numbers congruent to 0 mod 4 fall in the first column, all the numbers congruent to 3 mod 4 except 3 fall in the second column, all the numbers congruent to 2 mod 4 except 2, 6 and 10 fall in the third column, and all the numbers congruent to 1 mod 4 except 1, 5, 9, 13 and 17 fall in the fourth column. (There is no reason to add more columns, as the residue classes mod 4 will repeat with larger numbers). Thus, the positive integers not of the form $4x + 7y$ are

1, 2, 3, 5, 6, 9, 10, 13, and 17.

5. (20 points). State each of the theorems listed below.

(a) (10 points). The Fundamental Theorem of Arithmetic.

Every integer $n > 1$ can be written uniquely as a product of powers of prime numbers.

(b) (10 points). Wilson's Theorem.

If p is prime, then $(p - 1)! \equiv -1 \pmod{p}$.

6. (20 points). Let $a, m \in \mathbb{Z}$ with $m > 0$ and $(a, m) = 1$. Prove that $a^n \equiv 1 \pmod{m}$ for some positive integer n if and only if $\text{ord}_m(a) | n$.

Let $k = \text{ord}_m(a)$. If $k | n$, then $n = kq$ for some integer q . Then,

$$2^n \equiv (2^k)^q \equiv 1^q \equiv 1 \pmod{m}.$$

Conversely, suppose that $2^n \equiv 1 \pmod{m}$. If we write $n = qk + r$ where $0 \leq r \leq k - 1$, then we have

$$1 \equiv 2^n \equiv (2^k)^q \cdot 2^r \equiv 2^r \pmod{m}.$$

Thus, $2^r \equiv 1 \pmod{m}$. By definition, k is the smallest positive integer so that $2^k \equiv 1 \pmod{m}$. Since $r < k$ and $2^r \equiv 1 \pmod{m}$, it follows that r is not positive. This means $r = 0$, $n = qk$ and so $k | n$.

7. (20 points). Suppose that a and b are positive integers. Show that $(a, b) = 1$ if and only if there is no prime number p that divides both a and b .

Suppose that $(a, b) = 1$. If there is a prime p that divides both a and b , then $(a, b) \geq p$, a contradiction. Hence, there is no prime p that divides both a and b .

Conversely, suppose that there is no prime p that divides both a and b . If $(a, b) = d > 1$ then d has a prime divisor p . Then since $p|d$, and d divides both a and b , p divides both a and b , a contradiction. Hence, $(a, b) = 1$.

8. (20 points). Let $F(n) = \sum_{d|n} d\mu(d)$ and let $G(n) = \mu(n)\phi(n)$.

(a) (7 points). Show that $F(n)$ and $G(n)$ are multiplicative functions.

Since $\mu(n)$ and n are both multiplicative functions, their product $n\mu(n)$ is multiplicative. By Theorem 3.1, it follows that $F(n) = \sum_{d|n} d\mu(d)$ is multiplicative. Similarly, $G(n) = \mu(n)\phi(n)$ is a product of two multiplicative functions, and so $G(n)$ is multiplicative.

(b) (6 points). Show that if p is prime, then $F(p) = G(p)$.

We have $F(p) = \sum_{d|p} d\mu(d) = 1\mu(1) + p\mu(p) = 1 - p$. Also, $G(p) = \mu(p)\phi(p) = (-1)(p-1) = 1 - p$.

(c) (7 points). Use parts (a) and (b) to show that $F(n) = G(n)$ for all squarefree integers n .

If n is squarefree, then $n = \prod_{i=1}^k p_i$, where the p_i are distinct primes. Then,

$$F(n) = \prod_{i=1}^k F(p_i) = \prod_{i=1}^k G(p_i) = G(n).$$

9. (20 points). Let $p \geq 5$ be prime. Show that -6 is a quadratic residue mod p if and only if
- $$p \equiv 1, 5, 7, \text{ or } 11 \pmod{24}.$$

We have

$$\left(\frac{-6}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{2}{p}\right) \left(\frac{3}{p}\right).$$

If $p \equiv 1 \pmod{4}$, then $\left(\frac{-1}{p}\right) = 1$ and $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$. If $p \equiv 3 \pmod{4}$, then $\left(\frac{-1}{p}\right) = -1$ and $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right)$. Thus, in any case

$$\left(\frac{-1}{p}\right) \left(\frac{3}{p}\right) = \left(\frac{p}{3}\right).$$

We have $\left(\frac{2}{p}\right) = 1$ if $p \equiv 1, 7 \pmod{8}$ and $\left(\frac{2}{p}\right) = -1$ if $p \equiv 3, 5 \pmod{8}$. We have $\left(\frac{p}{3}\right) = 1$ if $p \equiv 1 \pmod{3}$ and $\left(\frac{p}{3}\right) = -1$ if $p \equiv 2 \pmod{3}$. In order to have $\left(\frac{-6}{p}\right) = 1$ we must have either both of $\left(\frac{2}{p}\right)$ and $\left(\frac{p}{3}\right)$ equal 1, or both equal -1 .

We have that $p \equiv 1 \pmod{8}$ and $p \equiv 1 \pmod{3}$ if and only if $p \equiv 1 \pmod{24}$.

We have that $p \equiv 3 \pmod{8}$ and $p \equiv 2 \pmod{3}$ if and only if $p \equiv 11 \pmod{24}$.

We have that $p \equiv 5 \pmod{8}$ and $p \equiv 2 \pmod{3}$ if and only if $p \equiv 5 \pmod{24}$.

We have that $p \equiv 7 \pmod{8}$ and $p \equiv 1 \pmod{3}$ if and only if $p \equiv 7 \pmod{24}$.

10. (20 points). Suppose that p is an odd prime. Prove that there is an integer x so that $p|x^8 + 1$ if and only if $p \equiv 1 \pmod{16}$.

Suppose that $p|x^8 + 1$. Then, $x^8 \equiv -1 \pmod{p}$. Squaring this, we get $x^{16} \equiv 1 \pmod{p}$ and by Proposition 5.1, we have that $\text{ord}_p(x)|16$. Moreover, since $x^8 \equiv -1 \pmod{p}$, $\text{ord}_p(x) \nmid 8$. Thus, $\text{ord}_p(x) = 16$. By the last part of Proposition 5.1, we have $\text{ord}_p(x)|\phi(p) = p - 1$ and so $16|p - 1$ and $p \equiv 1 \pmod{16}$.

Conversely, suppose that p is a prime with $p \equiv 1 \pmod{16}$. Let g be a primitive root mod p and

$$x = g^{\frac{p-1}{16}}.$$

By Proposition 5.4,

$$\text{ord}_p(x) = \frac{\text{ord}_p(g)}{(\text{ord}_p(g), \frac{p-1}{16})} = \frac{p-1}{(p-1, \frac{p-1}{16})} = \frac{p-1}{\frac{p-1}{16}} = 16.$$

This implies that $x^{16} \equiv 1 \pmod{p}$, but $x^8 \not\equiv 1 \pmod{p}$. Thus,

$$p|(x^{16} - 1) = (x^8 - 1)(x^8 + 1).$$

However, since $p \nmid x^8 - 1$, it follows that $p|x^8 + 1$, as desired.

EC. (20 points). Find all positive integer solutions to $x^2 + y^2 = z^4$ with x , y , and z pairwise coprime.

By the classification of primitive Pythagorean triples, we have (after possibly switching x and y) that $x = m^2 - n^2$, $y = 2mn$ and $z^2 = m^2 + n^2$ with $m > n > 0$, $(m, n) = 1$ and exactly one of m and n even.

Now, $(m, n) = 1$ and if p is a prime that divides z and one of m or n , then it must divide the other. Thus, m , n , and z are pairwise coprime, and we apply the classification of primitive Pythagorean triples again!

Thus, $m = s^2 - t^2$, $n = 2st$ and $z = s^2 + t^2$ or $m = 2st$, $n = s^2 - t^2$ and $z = s^2 + t^2$ with $s > t > 0$, $(s, t) = 1$ and exactly one of s and t even. We choose the formulas for m and n so that $m > n$. This gives us

$$\begin{aligned}x &= \pm((s^2 - t^2) - (2st)^2) = |s^4 - 6s^2t^2 + t^4| \\y &= 2mn = 4s^3t - st^3 \\z &= s^2 + t^2.\end{aligned}$$