Math 126, Number Theory

Second Test Answers

April 2006

Scale. 85–100 A, 70–84 B, 50–69 C. Median 70.

Problem 1. On Pythagorean triples. [18] Recall that a Pythagorean triple (x, y, z) consists of three positive integers such that $x^2+y^2 = z^2$. Show that for any Pythagorean triple at least one of x and y is divisible by 3. [Hint: (mod 3).]

The proof revolves around the fact that the only squares modulo 3 are 0 and 1. Here's one version of it.

Suppose that (x, y, z) is a Pythagorean triple such that neither x nor y is divisible by 3. Since $x^2+y^2 = z^2$, therefore

$$x^2 + y^2 \equiv z^2 \pmod 3$$

but neither x nor y is congruent to 0 (mod 3). Then both x and y are congruent to ± 1 (mod 3), hence their squares x^2 and y^2 are congruent to 1 (mod 3), and so their sum $x^2 + y^2 \equiv 2$ (mod 3). But 2 is not a square modulo 3, so $2 \not\equiv z^2$ (mod 3), a contradiction. Thus, no Pythagorean triple (x, y, z) has neither x nor y divisible by 3. Q.E.D.

Problem 2. Yes/no. [16; 4 points each part] For each of the following just write "yes" or "no". No explanation is needed unless it's not clear which is correct.

a. Fermat's theorem implies that for prime p, $2^p \equiv 2 \pmod p$. Does the converse hold, that is, if $2^p \equiv 2 \pmod p$, then is p prime?

No, pseudoprimes also have this property.

b. If function f is multiplicative, then does that imply that $f(80) = f(8)f(10)$?

No, 8 and 10 are not relatively prime. In fact, Euler's phi function is multiplicative, but $\phi(80) = \phi(16)\phi(5) = 8{\cdot}4 = 32$ while $\phi(8) = 4$ and $\phi(10) = 4$.

c. Is the number 4926834923 is the sum of two squares?

No. It's congruent to 3 modulo 4, but sums of two squares modulo 4 can only be congruent to 0, 1, or 2 modulo 4.

d. Does the Chinese remainder theorem imply that the pair of linear congruences

$$\begin{cases} x \equiv 7 \pmod{16} \\ x \equiv 13 \pmod{10} \end{cases}$$

has a unique solution modulo 160?

No. 16 and 10 are not relatively prime.

Problem 3. [18] Find at least two positive solutions of quadratic Diophantine equation

$$2x^2 + xy - y^2 = 35.$$

[Hint: factor the left side of the equation.]

Factoring the left side, we get

$$(2x - y)(x + y) = 35.$$

We need to find factorings of 35 so that x and y turn out to be positive integers.

$2x-y$	$x+y$	x	y
1	35	12	23
5	7	4	3
7	5	4	1
35	1	12	−11

The three positive solutions for (x, y) are $(4, 3)$, $(4, 1)$, and $(12, 23)$.

Problem 4. [20] On order and primitive roots.

a. Compute $\mathrm{ord}_{19}(7)$, the order of 7 modulo 19. [It's small.]

$$7^2 = 49 \equiv 11 \pmod{19}$$

$$7^3 \equiv 11 \cdot 7 = 77 \equiv 1 \pmod{19}$$

Therefore, $\mathrm{ord}_{19}(7) = 3$.

b. Note that $8^2 \equiv 7 \pmod{19}$, and $2^3 \equiv 8 \pmod{19}$. What does that say about $\mathrm{ord}_{19}(8)$ and $\mathrm{ord}_{19}(2)$?

Since $8^2 \equiv 7$ and $7^3 \equiv 1$, therefore $8^6 \equiv 1$. Hence $\mathrm{ord}_{19}(8)$ divides 6.

In fact, you can quickly rule out the possibilities of $\mathrm{ord}_{19}(8)$ being 1, 2, or 3, so $\mathrm{ord}_{19}(8) = 6$.

Likewise $2^3 \equiv 8$ and $8^6 \equiv 1$ so $2^{18} \equiv 1$, so $\mathrm{ord}_{19}(2)$ divides 18.

It's a little more work to show that $\mathrm{ord}_{19}(2)$ actually equals 18.

c. How many primitive roots modulo 19 are there?

For any prime p the number of primitive roots is $\phi(p-1)$. So the number of primitive roots modulo 19 is

$$\phi(18) = \phi(2)\phi(9) = 1 \cdot 6 = 6.$$

d. Name one primitive root modulo 19.

There are 6 primitive roots; 2 is one of them, but so are 3, 6, 10, 14, and 15.

Problem 5. [10; 2 points each part] On Euler's ϕ function.

a. The ϕ function counts just what? That is, $\phi(n)$ is the number of what?

It's the number of totatives modulo n. A totative is a positive relatively prime number less than or equal to n. Another way of saying that is that it's the number of elements in a reduced residue system.

b. Although Euler did not use the symbol ϕ for this function, and he never called it the totient function, he did invent it, but he didn't use it just to count things, but for something else. What was that?

Euler generalized Fermat's theorem for prime numbers to all numbers by inventing $\phi(n)$. So he used to show that

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

for a relatively prime to n.

Problem 6. [18] Solve the pair of linear congruences

$$\begin{cases} 3x + 2y \equiv 5 \pmod 7 \\ 2x + 3y \equiv 6 \pmod 7 \end{cases}$$

Show your work.

There are many ways to solve this pair of linear congruences just as there are many ways to solve a pair of linear equations. Here's one

Let's eliminate x. Double the first congruence and triple the second, then subtract the first from the second.

$$\begin{cases} 6x + 4y \equiv 10 \pmod 7 \\ 6x + 9y \equiv 18 \pmod 7 \end{cases}$$

Therefore, $5y \equiv 8 \pmod 7$, that is $5y \equiv 1 \pmod 7$. This single congruence can be solved in many ways, including just searching for the answer, $y \equiv 3 \pmod 7$.

We can substitute that back in the first equation to get

$$3x + 6 \equiv 5 \pmod 7$$

which simplifies to $3x \equiv 6 \pmod 7$, so $x \equiv 2 \pmod 7$.

All the processes are invertible modulo 7. We used addition, subtraction, doubling, tripling, and halving, and all those are invertible, the last because 2 and 3 are relatively prime to 7. Therefore, the answer is

$$x \equiv 2 \pmod 7, \text{ and } y \equiv 3 \pmod 7,$$

but it's best to check.