Math 126, Number Theory

Second Test, alternate answers

11 Apr 2006

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, y, or z is divisible by 5. [Hint: what are the squares mod 5?]

The squares modulo 5 are 0, 1, and -1 (which is the same as 4). Thus, each of x^2, y^2 and z^2 is one of those three. If any one is congruent to 0 modulo 5, then it's divisible by 5, so one of x, y, or z is divisible by 5. That leaves the case where each of x^2, y^2 and z^2 is congruent to ± 1. But the sum of the first two is the third, and no combination of ± 1 added to ± 1 gives ± 1 modulo 5. Thus, the remaining case never occurs. Therefore, one of x, y, or z is divisible by 5. Q.E.D.

Problem 2. Yes/no. [16; 4 points each part]

a. Note that if $(a, 15) = 1$, then $a^4 \equiv 1 \pmod{15}$. Also note that $\phi(15) = 8$. Does 15 have any primitive roots?

No. Since $\phi(15) = 8$ a primitive root has order 8, but since $a^4 \equiv 1 \pmod{15}$, the highest order any totative can be 4.

b. Fermat's last theorem says that the Diophantine equations $x^n + y^n = z^n$ have no positive solutions for $n > 2$. Did Fermat prove this theorem for any value of $n > 2$ at all?

Yes, and we studied his proof for $n = 4$.

c. If $xy = z^2$ and x and y are relatively prime, then does it follow that each of x and y are perfect squares?

Yes, and we repeatedly used this principle to solve higher order Diophantine equations.

d. If $a^4 \equiv 1 \pmod{n}$, then is the order of a modulo n equal to 4?

No, it could be 1 or 2. For instance $(-1)^4 \equiv 1 \pmod{n}$, but it's order is not 4.

Problem 3. [18] Find at least one positive solution of quadratic Diophantine equation

$$x^2 + xy - 6y^2 = 21.$$

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

The left side factors as $(x+3y)(x-2y)$. We need to find a factoring of 21 so that when we set the first factor to $x+3y$ and the second factor to $x-2y$ we get positive integers for x and y. There are several factorings to consider. One that works is $x+3y = 21$ and $x-2y = 1$. The solution to that pair of equations is $(x, y) = (9, 4)$.

Problem 4. [15; 5 points each part] On order and primitive roots.

a. What is the order of 2 modulo 17?

We need to raise 2 to higher and higher powers modulo 17 until we reach 1.

n	1	2	3	4	5	6	7	8
2^n	2	4	8	16	15	13	9	1

Thus, $\operatorname{ord}_{17} 2 = 8$.

b. Is 2 a primitive root modulo 17?

No, to be a primitive root, it would have to have an order equal to $\phi(17) = 16$.

c. How many primitive roots modulo 17 are there?

There are $\phi(16) = 8$ of them.

Problem 5. [15] On Euler's ϕ function.

a. [5] How many positive integers less than 56 are relatively prime to 56?

$$\phi(56) = \phi(8)\phi(7) = 4 \cdot 6 = 24$$

b. [10] Show that if $n > 2$ then $2|\phi(n)$.

Here's one proof. Let the prime decomposition of n be

$$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}.$$

Then

$$\phi(n) = \phi(p_1^{e_1})\phi(p_2^{e_2}) \dots \phi(p_k^{e_k}).$$

If any one of the primes p_i is odd, then since

$$\phi(p_i) = (p_i - 1)p_i^{e_i -},$$

$\phi(p_i)$ is even, and so $\phi(n)$ is even. Otherwise, there's only one prime $p_1 = 2$, so $n = 2^e$ is a power of 2. Now, since $n > 2$, therefore $e > 1$, and $\phi(n) = \phi(2^e) = 2^{e-1}$ is therefore even. Q.E.D.

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

$$\begin{cases} 4x + 2y \equiv 3 \pmod{11} \\ 2x - 3y \equiv 8 \pmod{11} \end{cases}$$

Show your work.

Here's one computation that finds the solution. Subtract twice the second congruence from the first to get

$$8y \equiv 9 \pmod{11}.$$

Since $8 \cdot 7 = 56$, therefore 7 acts as the inverse of 8 modulo 11. Multiply that last congruence by 7 to get

$$y \equiv 8 \pmod{11}.$$

To find x put 8 in for y in one of the original congruences, say the first. Then $4x + 5 \equiv 3 \pmod{11}$ so

$$4x \equiv 9 \pmod{11}.$$

The inverse modulo 11 of 4 is 3 (since $4 \cdot 3 = 12$, so multiply by 3 to get

$$x \equiv 5 \pmod{11}.$$

Thus, the solution is $x \equiv 5 \pmod{11}$ and $y = \equiv 8 \pmod{11}$.