Math 126, Number Theory

Second Test

5 Apr 2006

Your name: _____

You may use one sheet of prepared notes and a calculator for the test. Points for each problem are in square brackets. Before writing out any proof, please work on scratch paper until you know how the proof goes, then write the proof in the space provided.

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).]

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?

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

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

_____ **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 untique solution modulo 160?

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.]

Problem 4. [20; 5 points each part] On order and primitive roots.

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

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 $\mathrm{ord}_{19}(2)$?

c. How many primitive roots modulo 19 are there?

d. Name one primitive root modulo 19.

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

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

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?

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.

#1.[18]	
#2.[16]	
#3.[18]	
#4.[20]	
#5.[10]	
#6.[18]	
Total	