Math 126, Number Theory

Final Exam

May 2006

For this take-home final exam, you may use class notes, the text, and other books and articles. Do not talk to anyone about the test except me. If you have any questions about the test, ask or email me.

Write the answer to each question on a separate page of paper, then staple the pages together.

Problem 1. [20] Carefully prove the following statement.

> If $x = r/s$ is a rational solution of the equation
>
> $$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$$
>
> where all the coefficients $a_n, a_{n-1}, \ldots, a_1, a_0$ are integers, and if r and s are relatively prime, then r divides the constant term a_0 while s divides the leading coefficient a_n.

The proof is not difficult, and it begins by clearing the denominators to turn it into an equation involving integers only. As you write out the proof, point out each time you use a property of divisibility or relative primality.

Problem 2. [24; 6 points each part] The Euclidean algorithm has been essential for us this semester.

a. Choose two of the following numbers, call them m and n, and show how the Euclidean algorithm is used to find their greatest common divisor $d = (m, n)$.

$$2907, 3128, 4807, 9775$$

b. Use the work you did in part a to show how d is a linear combination of m and n, that is, solve the linear Diophantine equation $mx + ny = d$.

c. Continuing with this example, show how you can use your results in part b to solve the linear congruence $mx \equiv 6d \pmod{n}$.

d. The Euclidean algorithm also is used to find continued fraction expansions. Find the continued fraction expansion of m/n, and show your work.

Problem 3. [18] Consider the system of three congruences

$$\begin{aligned} x &\equiv 4 \pmod{11} \\ x &\equiv 3 \pmod{9} \\ x &\equiv 3 \pmod{10} \end{aligned}$$

Since the moduli are pairwise relatively prime, the Chinese remainder theorem says that there is a unique solution to this system modulo 990, the product of the moduli. Find that solution and show your work.

Problem 4. [18] (page 107, exercise 3) Suppose that $(a, n) = 1$. Prove that

$$a^b \equiv a^c \pmod{n}$$

if and only if

$$b \equiv c \pmod{\operatorname{ord}_n(a)}.$$

(You may use the theorems in the text, of course.)

Problem 5. [20; 10 points each part] Consider the Pell equation

$$x^2 - 30y^2 = 1.$$

a. Find solution to the equation from the continued fraction expansion of $\sqrt{30}$, which is

$$\sqrt{30} = 5 + \frac{1}{2+}\,\frac{1}{10+}\,\frac{1}{2+}\,\frac{1}{10+}\,\frac{1}{2+}\,\frac{1}{10+}\cdots.$$

b. Once one solution to a Pell equation is found, you can find infinitely many more. Using your solution in part a, find two more solutions.