Math 126, Number Theory

Final Answers

May 2006

Scale. 85–100 A. 70-84 B. 55 69 C. Median 86.

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.

Naturally, there are many proofs. Here's a straightforward one.

Proof: Let $x = r/x$ be a solution with r and s relatively prime. Then

$$a_n(r/s)^n + a_{n-1}(r/s)^{n-1} + \cdots + a_1(r/s) + a_0 = 0.$$

Multiplying each side of the equation by s^n, we have

$$a_n r^n + a_{n-1}r^{n-1}s + \cdots + a_1 rs^{n-1} + a_0 s^n = 0.$$

All but one of the terms contains a factor of r, so, moving the remaining term to the other side, we can rewrite this equation as

$$(a_n r^{n-1} + a_{n-1}r^{n-2}s + \cdots + a_1 s^{n-1})r = -a_0 s^n.$$

Since r divides the left hand side of the equation (by the definition of divisibility), therefore r divides the right hand side $-a_0 s^n$. But r is relatively prime to s, therefore r is relatively prime to s^n. But r divides $-a_0 s^n$, hence r divides $-a_0$, and thus r divides a_0.

Likewise, all but one of the terms contains a factor of s, so we can rewrite the equation as

$$(a_{n-1}r^{n-1} + \cdots + a_1 rs^{n-2} + a_0 s^{n-1})s = -a_n r^n.$$

Since s divides the left hand side, it also divides $-a_n r^n$. But s being relatively prime to r, it is also relatively prime to r^n. Hence s divides $-a_n$, and so also divides a_n. Q.E.D.

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 $d = (m, n)$.

$$2907, 3128, 4807, 9775$$

Each choice of m and n leads to different greatest common divisors. Let's take $m = 4807$ and $n = 3128$. Then

$$\begin{aligned}
4807 &= 3128 + 1679 \\
3128 &= 1679 + 1449 \\
1679 &= 1449 + 230 \\
1449 &= 6 \cdot 230 + 69 \\
230 &= 3 \cdot 69 + 23 \\
69 &= 3 \cdot 23
\end{aligned}$$

Therefore, the greatest common divisor d is 23.

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 $mx + ny = d$.

One way to do that is to work the equations in part a backwards.

$$\begin{aligned}
23 &= 230 - 3 \cdot 69 \\
&= 230 - 3 \cdot (1449 - 6 \cdot 230) \\
&= 19 \cdot 230 - 3 \cdot 1449 \\
&= 19 \cdot (1679 - 1449) - 3 \cdot 1449 \\
&= 19 \cdot 1679 - 22 \cdot 1449 \\
&= 19 \cdot 1679 - 22 \cdot (3128 - 1679) \\
&= 41 \cdot 1679 - 22 \cdot 3128 \\
&= 41 \cdot (4807 - 3128) - 22 \cdot 3128 \\
&= 41 \cdot 4807 - 63 \cdot 3128
\end{aligned}$$

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

That linear congruence is equivalent to the linear Diophantine equation

$$mx + ny = 6d.$$

Since $d = 41m - 63n$, therefore $6d = 6 \cdot 41m - 6 \cdot 63n = 246m - 378n$. Thus, $x \equiv 246 \pmod{n}$ is a solution.

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

You can find this as a restatement of part a.

$$\begin{aligned}
\frac{4807}{3128} &= 1 + \frac{1679}{3218} \\
&= 1 + \frac{1}{3218/1679} \\
&= 1 + \frac{1}{1+}\,\frac{1449}{1679} \\
&= 1 + \frac{1}{1+}\,\frac{1}{1679/1449} \\
&= 1 + \frac{1}{1+}\,\frac{1}{1+}\,\frac{230}{1449} \\
&= 1 + \frac{1}{1+}\,\frac{1}{1+}\,\frac{1}{6+}\,\frac{69}{230} \\
&= 1 + \frac{1}{1+}\,\frac{1}{1+}\,\frac{1}{6+}\,\frac{1}{3+}\,\frac{23}{69} \\
&= 1 + \frac{1}{1+}\,\frac{1}{1+}\,\frac{1}{6+}\,\frac{1}{3+}\,\frac{1}{3}
\end{aligned}$$

Alternatively, you can read the coefficients 1, 1, 6, 3, 3 directly from the equations in part a.

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.

There are a couple of ways to do this. One is to take the first two congruences and replace them by a single congruence modulo 99, then take that congruence along with the third to get a single congruence modulo 990.

Here's a different method that uses all three together.

Step 1. For each modulus, find a reciprocal of the product of the remaining moduli modulo the given modulus. For the first modulus, 11, that means we need the reciprocal of 90 modulo 11, that is, we need to solve

$$90y \equiv 1 \pmod{11}.$$

That's the same as $2y \equiv 1 \pmod{11}$, and that can be easily found by searching to be $y \equiv 6 \pmod{11}$. Thus, 6 is the reciprocal we're looking for.

For the second modulus, 9, we need the reciprocal of 110 modulo 9. That's the same as the reciprocal of 2 modulo 9, which is 5.

For the third modulus, 10, we need the reciprocal of 99 modulo 10. That's the same as the reciprocal of 9 modulo 10, which is 9.

Step 2. To get x sum three products abc, one for each congruence, where a is the constant in the congruence, b is the product of the other moduli, and c is the reciprocal found in the previous step. That gives us

$$4 \cdot 90 \cdot 6 + 3 \cdot 110 \cdot 5 + 3 \cdot 99 \cdot 9 = 2160 + 1650 + 2673 = 6483$$

and then reduce this number modulo the product 990 of all three moduli. That gives a final answer of $x \equiv 543 \pmod{990}$.

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.)

Of course, there are many proofs. The key theorem 3.26 is the one that says

$$a^x \equiv a \pmod{n} \quad \text{iff} \quad x \equiv 1 \pmod{\operatorname{ord}_n(a)}.$$

Here's a proof that uses this theorem in both directions.

Proof $\Rightarrow$: Let $a^b \equiv a^c \pmod{n}$. Suppose first that $b \geq c$. Then the congruence $a^b - a^c \equiv 0 \pmod{n}$ can be written as $a^c(a^{b-c} - 1) \equiv 0 \pmod{n}$. Thus, $n | a^c(a^{b-c} - 1)$. But $(a, n) = 1$, so $(a^c, n) = 1$, and therefore $n | (a^{b-c} - 1)$. That says $a^{b-c} \equiv 1 \pmod{n}$. Therefore, by theorem 3.26, $b \equiv c \pmod{\operatorname{ord}_n(a)}$. Thus, we've shown that if $b \geq c$, then $b \equiv c \pmod{\operatorname{ord}_n(a)}$ as required. But if $c \geq b$, the same argument holds with b and c interchanged in the argument. Thus, in all cases $b \equiv c \pmod{\operatorname{ord}_n(a)}$.

Proof $\Leftarrow$: Let $b \equiv c \pmod{\operatorname{ord}_n(a)}$. Again, first take the case that $b \geq c$. Then $b = c + k \operatorname{ord}_n(a)$ for some nonnegative integer k. Therefore, modulo n,

$$\begin{aligned}
a^b &\equiv a^{c+k \operatorname{ord}_n(a)} \\
&\equiv a^c (a^{\operatorname{ord}_n(a)})^k \\
&\equiv a^c 1^k \\
&\equiv a^c
\end{aligned}$$

Likewise, if $c \geq b$, we can also show $a^b \equiv a^c \pmod{n}$. Q.E.D.

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

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

A solution will be found among the rational approximations determined by the first period of the continued fraction expansion. The first rational approximation is just 5, that is, $\frac{5}{1}$, but when you set $x = 5$ and $y = 1$, you find $x^2 - 30y^2 = -5$. The next rational approximation is $5 + \frac{1}{2} = \frac{11}{2}$. Next, when you set $x = 11$ and $y = 2$, you find $x^2 - 30y^2 = 11^2 - 30 \cdot 2^2 = 1$, and so $(x, y) = (11, 2)$ is the desired solution.

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.

We have a recurrence relation for solutions to Pell equations, namely, if (a, b) is one solution to $x^2 - dy^2 = 1$, then more solutions (x_i, y_i) are recursively defined by

$$\begin{aligned}
x_1 &= a \\
y_1 &= b \\
x_{n+1} &= ax_n + dby_n \\
y_{n+1} &= bx_n + ay_n
\end{aligned}$$

In our case, $a = 11$, $b = 2$, and $d = 30$, so the next two solutions are

$$\begin{aligned}
(x_2, y_2) &= (11x_1 + 60y_1, 2x_1 + 11y_1) \\
&= (241, 44) \\
(x_3, y_3) &= (11x_2 + 60y_2, 2x_2 + 11y_2) \\
&= (5291, 966)
\end{aligned}$$

The next solution is $(x_4, y_4) = (116161, 21208)$. Notice how these solutions give very close approximations to $\sqrt{30} = 5.477225570517$.

n	x_n	y_n	x_n/y_n
1	11	2	5.5
2	241	44	5.47727272727
3	5291	966	5.4772256728779
4	116161	21208	5.4772255752546