MATH 324 Summer 2006
Elementary Number Theory
Solutions to Assignment 3
Due: Wednesday August 2, 2006

Department of Mathematical and Statistical Sciences
University of Alberta

Question 1. [p 139. #16]

A piggy bank contains 24 coins, all of which are nickels, dimes, or quarters. If the total value of the coins is two dollars, what combinations of coins are possible?

SOLUTION: Let x be the number of nickels, y be the number of dimes, and z be the number of quarters, since there are 24 coins in the piggy bank, then

$$x + y + z = 24,$$

and since there are two dollars in the piggy bank, then

$$5x + 10y + 25z = 200.$$

From the first equation we have

$$5x + 5y + 5z = 120,$$

and subtracting this from the second equation, we have

$$5y + 20z = 80,$$

that is,

$$y + 4z = 16. \qquad (*)$$

A particular solution to $(*)$ is $y_0 = 16$ and $z_0 = 0$, so the general solution to $(*)$ is

$$\begin{aligned} y &= 16 - 4t \\ z &= t \end{aligned}$$

where t is a nonnegative integer. Since we need $0 \leq t \leq 4$, there are 5 solutions to the original diophantine equation:

(1) For $t = 0$, we have $y = 16$, $z = 0$, and $x = 24 - y - z = 8$.

(2) For $t = 1$, we have $y = 12$, $z = 1$, and $x = 24 - y - z = 11$.

(3) For $t = 2$, we have $y = 8$, $z = 2$, and $x = 24 - y - z = 14$.

(4) For $t = 3$, we have $y = 4$, $z = 3$, and $x = 24 - y - z = 17$.

(5) For $t = 4$, we have $y = 0$, $z = 4$, and $x = 24 - y - z = 20$.

Question 2. [p 139. #19]

Let a and b be relatively prime positive integers, and let n be a positive integer. A solution (x, y) of the linear diophantine equation $ax + by = n$ is *nonnegative* when both x and y are nonnegative.

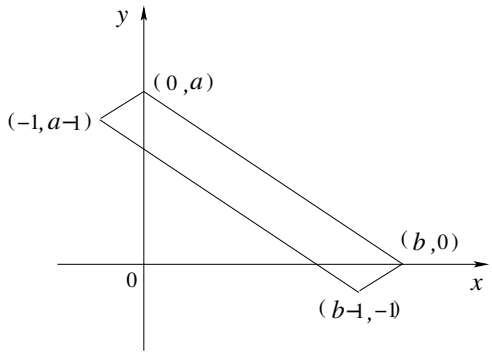
Show that whenever $n \geq (a-1)(b-1)$, there is a nonnegative solution of $ax + by = n$.

SOLUTION: We will show that for $ab - a - b < n < ab$ there is exactly one solution (x, y) to the linear diophantine equation $ax + by = n$ with $x > 0$ and $y > 0$.

We consider the parallelogram with vertices

$$(b, 0),\ (0, a),\ (b-1, -1),\ (-1, a-1)$$

shown below.



The equation of the line joining $(0, a)$ and $(b, 0)$ is

$$ax + by = ab,$$

while the equation of the line joining $(-1, a-1)$ and $(b-1, -1)$ is

$$ax + by = ab - a - b.$$

Let $\mathbf{i}$, $\mathbf{j}$ and $\mathbf{k}$ be the unit vectors in the $x-$, $y-$, and $z-$ directions respectively, and let

$$\mathbf{u} = \mathbf{i} + \mathbf{j} \qquad \text{and} \qquad \mathbf{v} = b\,\mathbf{i} - a\,\mathbf{j},$$

then

$$\mathbf{u} \times \mathbf{v} = -(a+b)\,\mathbf{k},$$

and the area of the parallelogram is given by

$$\text{Area} = \|\mathbf{u} \times \mathbf{v}\| = a + b.$$

Note that the line segment joining $(0, a)$ and $(-1, a-1)$ has no lattice points in its interior, since if it did, the x-component x_0 would satisfy $-1 < x_0 < 0$, which is impossible. Similarly, the line segment joining $(b, 0)$ and $(b-1, -1)$ has no lattice points in its interior.

Next we note that there are no lattice points in the interior of the line segment joining $(0, a)$ and $(b, 0)$. Suppose that (x, y) is a lattice point on $ax + by = ab$, with $x > 0$ and $y > 0$, since $x_0 = 0$ and $y_0 = a$ is a particular solution, the general solution to the diophantine equation gives

$$x = 0 + bt = bt \qquad \text{and} \qquad y = a - at$$

for some $t \in \mathbb{Z}$. Now, $x > 0$ implies that $t > 0$ (since $b > 0$), and $y > 0$ implies that $a(1 - t) > 0$, or $t < 1$ (since $a > 0$). Thus, $0 < t < 1$, which is a contradiction, since t is an integer.

Also we note that there are no lattice points in the interior of the line segment joining $(-1, a - 1)$ and $(b - 1, -1)$. Suppose that (x, y) is a lattice point on the line $ax + by = ab - a - b$, with $x > 0$ and $y > 0$, since $x_0 = -1$ and $y_0 = a - 1$ is a particular solution, the general solution to the diophantine equation gives

$$x = -1 + bt \qquad \text{and} \qquad y = a - 1 - at$$

for some $t \in \mathbb{Z}$. Now, $x > 0$ implies that $t \geq 1$ (since $b \geq 1$), and $y > 0$ implies that $t < (a-1)/a = 1-1/a < 1$, which is a contradiction.

Therefore, the only lattice points on the boundary of the parallelogram are the vertices

$$(b, 0),\ (0, a),\ (b - 1, -1),\ (-1, a - 1).$$

From Pick's theorem, we have

$$\text{Area} = I + \tfrac{1}{2}B - 1,$$

where B is the number of lattice points on the boundary of the parallelogram and I is the number of lattice points in the interior of the parallelogram. Since $B = 4$ and $\text{Area} = a + b$, then the number of lattice points in the interior of the parallelogram is

$$I = a + b - 1.$$

Since the distance between adjacent lattice points on any of the lines

$$ax + by = c$$

is $\sqrt{a^2 + b^2}$, and this is the length of the line segment joining points on the ends of the parallelogram, we see that for each integer c with

$$ab - a - b < c < ab,$$

there can be at most 1 lattice point on the line $ax + by = c$ which is interior to the parallelogram.

Therefore, for each of the $a + b - 1$ integers n with $ab - a - b + 1 \leq n \leq ab - 1$, exactly 1 of the $a + b - 1$ lattice points in the interior of the parallelogram lies on the line $ax + by = n$.

Also, from the general solution to the linear diophantine equation

$$x = x_0 + bt \qquad \text{and} \qquad y = y_o - at,$$

by taking $t = 1$, we see that the distance between adjacent lattice points on the line $ax + by = n$ is

$$D_0 = \sqrt{a^2 + b^2}.$$

Since the length of the line segment joining the intercepts is

$$D = \sqrt{\left(\frac{n}{a}\right)^2 + \left(\frac{n}{b}\right)^2} = \frac{n}{ab}\sqrt{a^2+b^2},$$

we see that if $D \geq D_0$, then the equation has a nonnegative solution, that is, if $n \geq ab$, then the equation has a nonnegative solution.

Combining this with the result above, we see that the linear diophantine equation $ax + by = n$ has a nonnegative solution whenever $n \geq ab - a - b + 1 = (a-1)(b-1)$.

Question 3. [p 139. #20]

Let a and b be relatively prime positive integers, and let n be a positive integer. Show that if $n = ab - a - b$, then there are no nonnegative solutions of $ax + by = n$.

SOLUTION: If we set $x = -1$, then we have

$$-a + by = ab - a - b,$$

so that $y = a - 1$, and a particular solution is $x_0 = -1$, $y_0 = a - 1$, so the general solution is

$$x = -1 + bt \qquad \text{and} \qquad y = a - 1 - at$$

where $t \in \mathbb{Z}$.

Now if $x = -1 + bt \geq 0$, then we have $bt \geq 1$, and since $b \geq 1$ and t is an integer, this implies that $t \geq 1$.

Also, if $y = a - 1 - at \geq 0$, then we have $t \leq \dfrac{a-1}{a} = 1 - \dfrac{1}{a} < 1$, which contradicts the fact that $t \geq 1$.

Therefore, if $n = ab - a - b$, there are no nonnegative solutions to the linear diophantine equation $ax = by = n$.

Question 4. [p 139. #21]

Show that there are exactly $(a-1)(b-1)/2$ nonnegative integers $n < ab - a - b$ such that the equation $ax + by = n$ has a nonnegative solution.

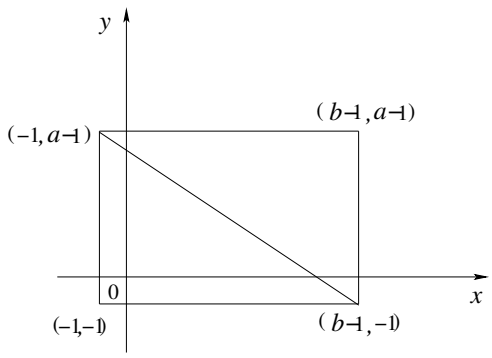
SOLUTION: Here we note that the line

$$ax + by = ab - a - b$$

bisects the rectangle with vertices

$$(-1, a-1),\ (-1, -1),\ (b-1, a-1),\ (b-1, -1),$$

but contains no lattice points.



Therefore, half of the interior points of the rectangle are below the line and half are above the line, and since the number of interior points is

$$(a+1)(b+1) - 2(a+1) - 2(b+1) + 4 = ab - a - b + 1 = (a-1)(b-1),$$

then there are $(a-1)(b-1)/2$ integers $n < ab - a - b$ such that the equation $ax + by = n$ has a nonnegative solution.

Question 5. [p 150. #17]

What can you conclude if $a^2 \equiv b^2 \pmod{p}$, where a and b are integers and p is a prime?

SOLUTION: If $a^2 \equiv b^2 \pmod{p}$, then $p \,|\, (a-b)(a+b)$, and since p is a prime, this implies that

$$p \,|\, a - b \qquad \text{or} \qquad p \,|\, a + b,$$

so that either $a \equiv b \pmod{p}$ or $a \equiv -b \pmod{p}$.

Question 6. [p 150. #19]

Show that if n is an odd positive integer, then

$$1 + 2 + 3 + \cdots + (n-1) \equiv 0 \pmod{n}.$$

Is this statement true if n is even?

SOLUTION: Recall that

$$1 + 2 + 3 + \cdots + (n-1) = \frac{n(n-1)}{2},$$

and if n is odd, then $n-1$ is even, so that $\dfrac{n-1}{2}$ is an integer and $n \,\Big|\, \dfrac{n(n-1)}{2}$, that is,

$$1 + 2 + 3 + \cdots + (n-1) \equiv 0 \pmod{n}$$

in this case.

On the other hand, if n is even, then $n = 2k$ for some integer k and $\dfrac{n(n-1)}{2} = k(n-1)$. However, $\gcd(n, n-1) = 1$, and $1 \le k < n$, so that $n \nmid k$, and therefore $n \nmid k(n-1)$, so

$$1 + 2 + 3 + \cdots + (n-1) \not\equiv 0 \pmod{n}$$

in this case.

Question 7. [p 150. #20]

Show that if n is an odd positive integer or if n is a positive integer divisible by 4, then

$$1^3 + 2^3 + 3^3 + \cdots + (n-1)^3 \equiv 0 \pmod{n}.$$

Is this statement true if n is even but not divisible by 4?

SOLUTION: Recall that

$$1^3 + 2^3 + 3^3 + \cdots + (n-1)^3 = \frac{n^2(n-1)^2}{4},$$

so that if n is an odd positive integer, then $n-1$ is even and $4 \mid (n-1)^2$, so that $n \mid \dfrac{n^2(n-1)^2}{4}$, and

$$1^3 + 2^3 + 3^3 + \cdots + (n-1)^3 \equiv 0 \pmod{n}.$$

If n is a multiple of 4, then $\dfrac{n}{4}$ is an integer, and $n \mid \dfrac{n^2(n-1)^2}{4}$, so that

$$1^3 + 2^3 + 3^3 + \cdots + (n-1)^3 \equiv 0 \pmod{n}.$$

in this case also.

If n is even, but $4 \nmid n$, then $n = 2k$ where k is an odd integer, and $n-1$ is also odd, so that

$$\frac{n^2(n-1)^2}{4} = k^2(2k-1)^2$$

is an odd integer, and since n is even, then

$$1^3 + 2^3 + 3^3 + \cdots + (n-1)^3 \not\equiv 0 \pmod{n}.$$

Question 8. [p 150. #21]

For which positive integers n is it true that

$$1^2 + 2^2 + 3^2 + \cdots + (n-1)^2 \equiv 0 \pmod{n}?$$

SOLUTION: Recall that

$$1^2 + 2^2 + 3^2 + \cdots + (n-1)^2 = \frac{(n-1)n(2n-1)}{6},$$

and since $(n, n-1) = 1$ and $(n, 2n-1) = 1$, then

$$n \left| \frac{(n-1)n(2n-1)}{6} \right. \quad \text{if and only if} \quad 6 \mid (n-1)(2n-1).$$

Also, since $(n-1, 2n-1) = 1$, then $6 \mid (n-1)(2n-1)$ if and only if either (i) $6 \mid n-1$, or (ii) $2 \mid n-1$ and $3 \mid 2n-1$.

(i) $6 \mid n-1$ if and only if $n = 6k+1$, that is, if and only if $n \equiv 1 \pmod{6}$.

(ii) $2 \mid n-1$ and $3 \mid 2n-1$ if and only if $n = 2k+1$ and $2n = 3l+1$. Now, $2n$ is even, so that l is odd, say, $l = 2m+1$. Thus, $2n = 6m+4$, or $n = 3m+2$. But since n is odd, then m must be odd, say, $m = 2q-1$, so that $n = 6q-1$, that is, $n \equiv -1 \pmod{6}$.

Therefore, $1^2 + 2^2 + 3^2 + \cdots + (n-1)^2 \equiv 0 \pmod{n}$ if and only if $n \equiv \pm 1 \pmod{6}$.

Question 9. [p 157. #18]

Show that if p is an odd prime and a is a positive integer which is not divisible by p, then the congruence $x^2 \equiv a \pmod{p}$ has either no solution or exactly two incongruent solutions.

SOLUTION: Note first that if $x_0^2 \equiv a \pmod{p}$, then $(-x_0)^2 \equiv a \pmod{p}$, so that $-x_0$ is also a solution.

Now note that $x_0 \not\equiv -x_0 \pmod{p}$, since this implies that $2x_0 \equiv 0 \pmod{p}$, which is impossible since p is odd and $p \nmid x_0$, since $x_0^2 \equiv a \pmod{p}$ and $p \nmid a$.

To see that there are no more than two incongruent solutions, assume that $x = x_0$ and $x = x_1$ are both solutions to $x^2 \equiv a \pmod{p}$, then $x_0^2 \equiv x_1^2 \equiv a \pmod{p}$, so that

$$x_0^2 - x_1^2 \equiv (x_0 - x_1)(x_0 + x_1) \equiv 0 \pmod{p},$$

so that $p \mid x_0 - x_1$ or $p \mid x_0 + x_1$, that is,

$$x_1 \equiv x_0 \pmod{p} \qquad \text{or} \qquad x_1 \equiv -x_0 \pmod{p}.$$

Thus, if there is a solution to $x^2 \equiv a \pmod{p}$, then there are exactly two incongruent solutions.

Question 10. [p 167. #33]

The three children in a family have feet that are 5 inches, 7 inches, and 9 inches long. When they measure the length of the dining room of their house using their feet, they each find that there are 3 inches left over. How long is the dining room?

SOLUTION: Let n be the length of the dining room (in inches), we solve the following simultaneous congruences using the Chinese remainder theorem:

$$\begin{aligned} n &\equiv 3 \pmod{5} \\ n &\equiv 3 \pmod{7} \\ n &\equiv 3 \pmod{9}. \end{aligned}$$

Here

$$\begin{aligned} a_1 = 3, \qquad a_2 &= 3, \qquad a_3 = 3 \\ m_1 = 5, \qquad m_2 &= 7, \qquad m_3 = 9, \end{aligned}$$

and

$$M_1 = 7 \cdot 9 = 63, \quad M_2 = 5 \cdot 9 = 45, \quad M_3 = 5 \cdot 7 = 35.$$

Also, solving the congrences

$$\begin{aligned} M_1 y_1 &\equiv 1 \pmod{m_1} \\ M_2 y_2 &\equiv 1 \pmod{m_2} \\ M_3 y_3 &\equiv 1 \pmod{m_3} \end{aligned}$$

for the inverses y_1, y_2, and y_3, we have

$$y_1 \equiv 2 \pmod{5}, \qquad y_2 \equiv 5 \pmod{7}, \qquad y_3 \equiv 8 \pmod{9},$$

and the unique solution modulo $5 \cdot 7 \cdot 9$ is given by

$$n = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 = 3 \cdot 63 \cdot 2 + 3 \cdot 45 \cdot 53 \cdot 35 \cdot 9 = 378 + 675 + 945 = 1998 \equiv 3 \pmod{315}.$$

Therefore a reasonable answer would be $n = 3 + 315 = 318$ inches, or 26 feet, 6 inches.