MATH 324 Summer 2010
Elementary Number Theory
Solutions to Assignment 3
Due: Wednesday July 28, 2010

Question 1. [p 139. #13]

Which combinations of pennies, dimes, and quarters have a total value of 99¢ ?

Solution: Let $x = \#$ of pennies, $y = \#$ of dimes, $z = \#$of quarters, then we want to solve the linear diophantine equation

$$x + 10y + 25z = 99 \qquad (*)$$

in nonnegative integers.
Let $a = 1,\ b = 10,\ c = 25,$ and $d = (a, b, c) = 1$, then $d \mid 99$ so there are solutions to $(*)$. Setting

$$2y + 5z = t \qquad (**)$$

then $1 = 2 \cdot (-2) + 5 \cdot 1$, so that $t = 2 \cdot (-2t) + 5 \cdot t$, and a particular solution to $(**)$ is $y_0 = -2t,\ z_0 = t$, and so the general solution to $(**)$ is

$$\begin{aligned} y &= -2t + 5s \\ z &= \quad\ t - 2s \end{aligned}$$

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

But then $x = 99 - 10y - 25z$ becomes $x = 99 - 5t$, and the general solution to $(*)$ is

$$\begin{aligned} x &= 99 - 5t \\ y &= -2t + 5s \\ z &= \quad\ t - 2s \end{aligned}$$

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

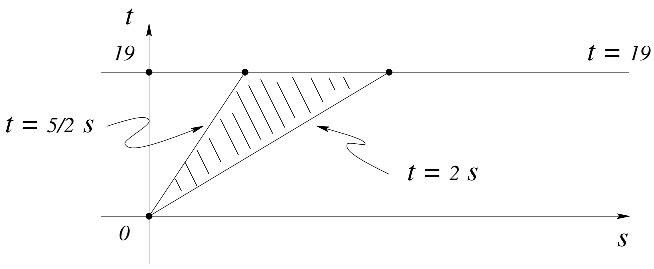
Since x, y, z have to be nonnegative, then (s, t) must lie in the region of the s, t–plane determined by the inequalities:

$$\begin{aligned} 99 - 5t &\geq 0 \\ -2t + 5s &\geq 0 \\ t - 2s &\geq 0. \end{aligned}$$

That is,

$$\begin{aligned} t &\leq 19 \\ 2t &\leq 5s \\ 2s &\leq t \end{aligned}$$

So we need to find the lattice points (i.e. points with integer coordinates) (s, t) which lie inside the region shown.



This is most easily done by starting with $t = 0$, then $t = 1$, ... and finally $t = 19$, and for each t value, determining the values of s so that (s, t) is in the region. For example,

If $t = 0$, then $s = 0$, and this implies that $x = 99$, $y = 0$, $z = 0$.

$$\vdots$$

If $t = 19$, then $s = 8$ or $s = 9$, and this implies that $x = 4$, $y = 2$, $z = 3$ or $x = 4$, $y = 7$, $z = 1$.

Question 2. [p 149. #5]

Show that if a is an odd integer, then $a^2 \equiv 1 \pmod 8$.

SOLUTION:

If $a \equiv 1 \pmod 8$, then $a^2 \equiv 1^2 \equiv 1 \pmod 8$.
If $a \equiv 3 \pmod 8$, then $a^2 \equiv 3^2 \equiv 9 \equiv 1 \pmod 8$.
If $a \equiv 5 \pmod 8$, then $a^2 \equiv 5^2 \equiv 25 \equiv 1 \pmod 8$.
If $a \equiv 7 \pmod 8$, then $a^2 \equiv 7^2 \equiv 49 \equiv 1 \pmod 8$.

Therefore, $a^2 \equiv 1 \pmod 8$ for any odd integer a since every odd integer is congruent to 1, 3, 5, or 7 modulo 8.

Question 3. [p 149. #6]

Find the least nonnegative residue modulo 13 of each of the following integers.

(a) 22
(b) 100
(c) 1001
(d) -1
(e) -100
(f) -1000

SOLUTION:

(a) $22 \equiv 9 \pmod{13}$.

(b) $100 \equiv 9 \pmod{13}$.

(c) $1001 \equiv 0 \pmod{13}$.

(d) $-1 \equiv 12 \pmod{13}$.

(e) $-100 \equiv 4 \pmod{13}$.

(f) $-1000 \equiv 1 \pmod{13}$.

Question 4. [p 149. #7]

Find the least positive residue of $1! + 2! + \cdots + 100!$ modulo each of the following integers.

(a) 2 (c) 12

(b) 7 (d) 25

SOLUTION:

(a) $1! + \underbrace{2! + \cdots + 100!}_{\text{all } \equiv\, 0 \pmod 2} \equiv 1 \pmod 2$

(b) $1! + 2! + 3! + 4! + 5! + 6! + \underbrace{7! + \cdots + 100!}_{\text{all } \equiv\, 0 \pmod 7} \equiv 1 + 2 + 6 + 24 + 120 + 720 \equiv 5 \pmod 7$

(c) $1! + 2! + 3! + \underbrace{4! + \cdots + 100!}_{\text{all } \equiv\, 0 \pmod{12}} \equiv 9 \pmod{12}$

(d) $1! + 2! + \cdots + 9! + \underbrace{10! + \cdots + 100!}_{\text{all } \equiv\, 0 \pmod{25}} \equiv 1! + 2! + \cdots + 9! \pmod{25}$

Now,

$$1! \equiv 1 \pmod{25},\ 2! \equiv 2 \pmod{25},\ 3! \equiv 6 \pmod{25},\ 4! \equiv 24 \equiv -1 \pmod{25},$$
$$5! \equiv -5 \pmod{25},\ 6! \equiv -30 \equiv -5 \pmod{25},\ 7! \equiv -35 \equiv 15 \pmod{25},$$
$$8! \equiv 120 \equiv -5 \pmod{25},\ 9! \equiv -45 \equiv 5 \pmod{25},$$

and therefore $1! + 2! + \cdot + 100! \equiv 1 + 2 + 6 - 1 - 5 - 5 + 15 - 5 + 5 \equiv 13 \pmod{25}$.

Question 5. [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

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

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 6. [p 150. #25]

Show that if $n \equiv 3 \pmod 4$, then n cannot be the sum of the squares of two integers.

SOLUTION:

If $a \equiv 0 \pmod 4$ then $a^2 \equiv 0 \pmod 4$

If $a \equiv 1 \pmod 4$ then $a^2 \equiv 1 \pmod 4$

If $a \equiv 2 \pmod 4$ then $a^2 \equiv 0 \pmod 4$

If $a \equiv 3 \pmod 4$ then $a^2 \equiv 1 \pmod 4$

Therefore, if $n = a^2 + b^2$, then $n \equiv 0,\ 1,\ \text{ or } 2 \pmod 4$, but $n \not\equiv 3 \pmod 4$.

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 $4 \,\big|\, (n-1)^2$, so t hat $n \,\Big|\, \dfrac{n^2(n-1)^2}{4}$, 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 $n \,\Big|\, \dfrac{n^2(n-1)^2}{4}$, 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 int eger, 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 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 $p \,\big|\, x_0 - x_1$ or $p \,\big|\, x_0 + x_1$, 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 9. [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

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

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.

Question 10. [p 221. #12]

Using Fermat's little theorem, find the least positive residue of $2^{1000000}$ modulo 17.

SOLUTION: Since $p = 17$ is prime and $17 \not| \, 2$, then by Fermat's little theorem, $2^{16} \equiv 1 \pmod{17}$.

Now, $1000000 = 2^{19} + 2^{18} + 2^{17} + 2^{16} + 2^{14} + 2^{9} + 2^{6}$, so that

$$2^{1000000} = 2^{2^{19}} \cdot 2^{2^{18}} \cdot 2^{2^{17}} \cdot 2^{2^{16}} \cdot 2^{2^{14}} \cdot 2^{2^{9}} \cdot 2^{2^{6}}$$

and

$$2^{1000000} = \left(2^{2^4}\right)^{2^{15}} \cdot \left(2^{2^4}\right)^{2^{14}} \cdot \left(2^{2^4}\right)^{2^{13}} \cdot \left(2^{2^4}\right)^{2^{12}} \cdot \left(2^{2^4}\right)^{2^{10}} \cdot \left(2^{2^4}\right)^{2^{5}} \cdot \left(2^{2^4}\right)^{2^{2}}$$

so that $2^{1000000} \equiv 1 \pmod{17}$.