Solutions to Quiz # 3 for Dr. Z.'s Number Theory Course for Oct. 10, 2013

1. (6 points) Find out whether it is possible to express 1 as a linear combination $1 = 11 \cdot m + 27 \cdot n$ for some integers m and n, and if it is, find them.

Sol. to 1: $gcd(27, 11) = gcd(11, 5) = gcd(5, 1) = gcd(1, 0) = 1$. So $gcd(27, 11) = 1$ and it is possible. Now let's do it.

$$\mathbf{27} = 2 \cdot \mathbf{11} + 5 \quad ,$$

so

$$5 = \mathbf{27} - 2 \cdot \mathbf{11} \quad .$$

$$\mathbf{11} = 2 \cdot 5 + 1 \quad ,$$

so

$$1 = \mathbf{11} - 2 \cdot 5 = \mathbf{11} - 2 \cdot (\mathbf{27} - 2 \cdot \mathbf{11})$$

$$= \mathbf{11} - 2 \cdot \mathbf{27} + 4 \cdot \mathbf{11} = 5 \cdot \mathbf{11} - 2 \cdot \mathbf{27} \quad .$$

So

$$1 = 5 \cdot \mathbf{11} + (-2) \cdot \mathbf{27} \quad .$$

Ans.: $m = 5 \qquad n = -2$.

Comment: Most people got it right. One student wrote $n = 2$. Make sure that the sign is correct.

2.(4 points) Find $11^{16} \pmod{13}$

Sol. to 2

$$11^2 \quad mod \quad 13 = 121 \quad mod \quad 13 = 4$$

(since $121 = 13 \cdot 9 + \mathbf{4}$) .

$$11^4 = 4^2 \quad mod \quad 13 = 16 \quad mod \quad 13 = 3$$

$$11^8 = 3^2 \quad mod \quad 13 = 9$$

$$11^{16} = 9^2 \quad mod \quad 13 = 81 \quad mod \quad 13 = 3 \quad ,$$

(since $81 = 13 \cdot 6 + 3$).

Ans.: $11^{16} \equiv 3 \pmod{13}$.

Comment: A faster way (done by Richard Wong) is to first use the fact that

$$11 \equiv -2 \pmod{13} \quad ,$$

and that $(-1)^{16} = 1$. So we have

$$11^{16} \pmod{13} \equiv (-2)^{16} \pmod{13} \equiv 2^{16} \pmod{13} \quad .$$

Now things are a bit simpler (coputationally)

$$2^2 \ mod \ 13 = 4$$

$$2^4 \ mod \ 13 = 4^2 \ mod \ 13 = 3$$

$$2^8 \ mod \ 13 = 3^2 \ mod \ 13 = 9 = -4 \ mod \ 13$$

$$(-4)^2 \ mod \ 13 = 16 \ mod \ 13 = 3 \quad .$$

The trick is that whenver you encounter an integer i than half the modulo m, replace it by by its 'negative' $-(m-i)$.