Solutions to Attendance Quiz # 20 for Dr. Z.'s Number Theory Course for Nov. 14, 2013

1. By 'brute force', Find the set of quadratic residues, and the set of quadratic non-residues of $p = 13$.

Sol. to 1:
$$QR(13) = \{0^2, 1^2, 2^2, 3^2, 4^2, 5^2, 6^2\} \ mod\ 13$$
$$= \{0, 1, 4, 9, 16, 25, 36\} \ mod\ 13$$
$$= \{0, 1, 4, 9, 3, 12, 10\}$$
$$= \{0, 1, 3, 4, 9, 10, 12\} \quad .$$

Ans. to 1: The set of quadratic residues modulo 13 is $\{0, 1, 3, 4, 9, 10, 12\}$.

2. Using the Quadratic Reciprocity Law and Rules 1-3, find (no credit for other methods)
$$\left(\frac{7}{17}\right)$$

Sol. to 2: By Rule 4 **the Quadratic Reciprocity Law**
$$\left(\frac{7}{17}\right)\left(\frac{17}{7}\right) = (-1)^{(7-1)(17-1)/4} = (-1)^{(6)(16)/4} = (-1)^{24} = 1 \quad ,$$
so
$$\left(\frac{7}{17}\right) = \left(\frac{17}{7}\right) = \left(\frac{3}{7}\right) \quad ,$$
since $17\ mod 7 = 3$.

Moving right along, using Rule 4 (QRL) once again
$$\left(\frac{3}{7}\right)\left(\frac{7}{3}\right) = (-1)^{(3-1)(7-1)/4} = (-1)^{(2)(6)/4} = (-1)^3 = -1 \quad .$$
So
$$\left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) \quad .$$
But since $7\ mod\ 3 = 1$,
$$\left(\frac{7}{3}\right) = \left(\frac{1}{3}\right) = 1 \quad .$$

(Of course $\left(\frac{1}{p}\right)$ is **always** 1, since $1^2 = 1$.

Going back we have,
$$\left(\frac{3}{7}\right) = -1 \quad ,$$
and finally,
$$\left(\frac{7}{17}\right) = -1 \quad .$$

Ans. to 2: $\left(\frac{7}{17}\right) = -1$, in other words 7 is a **quadratic NON-residue** of 17.