Solutions to Attendance Quiz # 13 for Dr. Z.'s Number Theory Course for Oct. 21, 2013

1. Illustrate the proof of Wilson's theorem for $p = 11$.

Sol. 1: $[2^{-1}]_{11} = 6$, $[3^{-1}]_{11} = 4$, $[5^{-1}]_{11} = 9$, $[7^{-1}]_{11} = 8$, so the pairs

$$\{2,6\}, \{3,4\}, \{5,9\}, \{7,8\}$$

are 'inverse pairs', whose product is 1 (modulo 17). So, by commutativity of multiplitcation:

$$2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \; = \; (2 \cdot 6)(3 \cdot 4)(5 \cdot 9)(7 \cdot 8) \equiv 1^4 \pmod{11} \equiv 1 \pmod{11}$$

Multiplying by 1 and $10 \equiv -1 \pmod{11}$ gives

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \; = \; 1 \cdot (2 \cdot 6)(3 \cdot 4)(5 \cdot 9)(7 \cdot 8) \cdot 10 \equiv 1^4(-1) \pmod{11} \equiv -1 \pmod{11} \quad .$$

2. Check, empirically, Fermat's little theorem for $p = 17$, and $a = 4$.

Sol. to 2: We use fast modular exponentiation to evaluate $4^{17} \pmod{17}$.

$$4^2 = 16 \equiv -1 \pmod{17} \quad ,$$

hence $4^{16} \equiv (-1)^8 \pmod{17} \equiv 1 \pmod{17}$. Finally

$$4^{17} \equiv 4 \pmod{17} \quad .$$

Comment: This problem turned out to be easier than I intended. 4^2 is already -1 (modulo 17) so you get right away $4^{16} \equiv 1 \pmod{17}$. For other a it is not so fast.