Solutiosn to Quiz # 6 for Dr. Z.'s Number Theory

1. (5 points) Illustrate the proof of Wilson's theorem for $p = 19$.

Sol. to 1: We have to "pair up" all the 16 integers in

$$\{2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17\}$$

into pairs that multiply together to 1 modulo 19. Let's find 2 a room-mate

$$[2^{-1}]_{19} = 10 \quad ,$$

So $2 \cdot 10 \equiv 1 \pmod{19}$ so $\{2, 10\}$ are happy roomates. But this implies **immediatedly** that $\{-2, -10\}$, alias $\{17, 9\}$ are roomates too! We cross these four integers out, leaving the 12 integers

$$\{3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16\}$$

Let's find 3 a room-mate

$$[3^{-1}]_{19} = 13 \quad ,$$

So $3 \cdot 13 \equiv 1 \pmod{19}$, so $\{3, 13\}$ are happy roomates. But this implies **immediatedly** that $\{-3, -13\}$, alias $\{16, 6\}$ are also roomates! We cross them out, leaving the 8 integers

$$\{4, 5, 7, 8, 11, 12, 14, 15\}$$

Let's find 4 a room-mate

$$[4^{-1}]_{19} = 5 \quad ,$$

So $4 \cdot 5 \equiv 1 \pmod{19}$, so $\{4, 5\}$ are happy roomates. But this implies **immediatedly** that $\{-4, -5\}$, alias $\{15, 14\}$ are also roomates! We cross these four integers out, leaving the 4 integers

$$\{7, 8, 11, 12\}$$

Let's find 7 a room-mate

$$[7^{-1}]_{19} = 11 \quad ,$$

So $7 \cdot 11 \equiv 1 \pmod{19}$, so $\{7, 11\}$ are happy roomates. But this implies **immediatedly** that $\{-7, -11\}$, alias $\{12, 8\}$ are also roomates! And we are done with the room assignments! Of course $1(18) = -1 \pmod{19}$. So using the **commutativity of multiplication**

$$18! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \cdot 12 \cdot 13 \cdot 14 \cdot 15 \cdot 16 \cdot 17 \cdot 18$$

$$= (1 \cdot 18)(2 \cdot 10)(17 \cdot 9)(3 \cdot 13)(16 \cdot 6)(4 \cdot 5)(15 \cdot 14)(7 \cdot 11)(12 \cdot 8)$$

$$\equiv (-1)(1)^8 \pmod{19} \equiv -1 \pmod{19} \quad .$$

2. (5 points) State (2 points) and prove (3 points) Fermat's little theorem.

Sol. of 2(a): If p is prime and a is an integer then

$$a^p \equiv a \ (mod\ p)$$

Sol. of 2(b): First proof:

Induction on a.

Base case: if $a = 0$ then of course it is true.

Inductive step: If it is true for a then it is true for $a + 1$.

By the binomial theorem

$$(a+1)^p = a^p + pa^{p-1} + \frac{p(p-1)}{2} a^{p-2} + \ldots + pa^p + 1 \quad .$$

All the terms on the right side, except the first (i.e. a^p) and the last (i.e. 1) are divisible by p, hence

$$(a+1)^p \equiv a^p + 1 \ (mod\ p) \quad .$$

By the **inductive hypothesis** $a^p \equiv a \ (mod\ p)$, hence

$$(a+1)^p \equiv a^p + 1 \ (mod\ p) \equiv a + 1 \ (mod\ p) \quad .$$

qed.

Second proof: We prove that if $1 \leq a \leq p-1$ then $a^{p-1} \equiv 1 \ (mod p)$. The $p-1$ numbers

$$a, 2a, \ldots, (p-1)a \quad ,$$

are all **distinct** modulo p , since if $ai \equiv aj \ (mod\ p)$ then $a(i-j)$ is divisible by p, but this means that $i-j$ is divisible p by p is prime and $i-j$ is between 1 and $p-2$ so it can't happen.

So the set of integers $a, 2a, \ldots, (p-1)a$ modulo p is a *rearangement* of the set of integers $\{1, \ldots, p-1\}$ and since multiplication is commutative, the products are the same

$$(a)(2a) \cdots, ((p-1)a) \ = \ (1)(2) \cdots (p-1)$$

So

$$a^{p-1}(p-1)! = (p-1)! \ (mod\ p) \quad .$$

Since $(p-1)!$ is **not** 0 mod p, we can cancel it out and get $a^{p-1} \equiv 1 \ (mod p)$. **qed**,