Solutiosn to Quiz # 6 for Dr. Z.'s Number Theory Course for Oct. 31,, 2013

Version of Nov. 1, 2013 (a quicker way to do #1)

1. (4 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. (3 points) How many (circular) necklaces are there of length p, with a colors? Explain!

Sol. to 2: The number of circular necklaces is

$$\frac{a^p - a}{p} + a \quad .$$

Let's look at all the *linear* necklaces of length p with a colors. Obviously, there are a^p of them. But a of them are 'boring' (only using one color). So there are $a^p - a$ interesting linear necklaces. But for each of them, once you make them circular, they can be arranged into families of p each, where each of them yields the same circular necklace (because the only periods can be of length 1 and p since p is a prime). So there are $(a^p - a)/p$ circular necklaces that are non-monochromatic. Adding back the a monochromatic necklaces gives the answer.

3. (3 points) Use the Miller-Rabin primality test to investigage whether the integer 15 is prime or composite, by picking **one** random a's between 2 and 13.

Sol. to 3:

$$14 = 2^1 \cdot 7 \quad ,$$

so $s = 1$ and $d = 7$.

We pick $a = 2$ (the easiest), and do

$$2^7 \textit{ modulo } 15 \quad ,$$

the usual way.

$$2^1 = 2 \textit{ modulo } 15 \ = 2$$

$$2^2 = 2^2 \textit{ modulo } 15 \ = 4$$

$$2^4 = 4^2 \textit{ modulo } 15 \ = 1$$

So

$$2^7 = 2^{4+2+1} = 2^4 \cdot 2^2 \cdot 2 = 1 \cdot 4 \cdot 2 = 8 \textit{ modulo } 15.$$

Some people stopped here. WRONG! If you get ± -1, then you stop and output 'probably prime', but if it is not, you keep going.

$$2^{14} = 8^2 \textit{ modulo } 15 = 4 \quad ,$$

since this is not ± 1, we output **definitely composite**.

Ans. to 3: According to the Miller-Rabin test, 15 is definitely **not** prime.