UBC MATH 312 QUIZ 2 SOLUTIONS — 5 Nov 2012

1) $1! + 2! + \cdots + 100! \equiv 1! + 2! + \cdots + 6! \pmod 7$ since $7 \mid k!$ for $k \geq 7$.

$\equiv 1 + 2! + \cdots + 5! + (-1) \pmod 7$ by Wilson's Theorem as 7 is prime.

$\equiv 2! + 3! + 4! + 5! \pmod 7$

$\equiv 2 + 6 + 3 + 1 \pmod 7$

$\equiv 5 \pmod 7$.

---

2) For $n = 1$, the statement is trivially true. ($0 \equiv 0 \pmod 1$)

For $n \geq 2$, we notice that $1^2 + 2^2 + \cdots + (n-1)^2 = \frac{1}{6}(n-1)(n)(2n-1)$.

{This can be proven directly using induction, or an adaptation of the well-known formula $1^2 + 2^2 + \cdots + (n-1)^2 + n^2 = \frac{1}{6} n(n+1)(2n+1)$.

↑ notice the additional term

But in a 2-mark Question on a short Quiz, just state it.}

So now

$1^2 + 2^2 + \cdots + (n-1)^2 \equiv 0 \pmod n$

$\iff \frac{1}{6}(n-1)(n)(2n-1) \equiv 0 \pmod n$

$\iff n \mid \frac{1}{6}(n-1)n(2n-1)$

$\iff \frac{1}{6}(n-1)(2n-1)$ is an integer.

$\iff 6 \mid (n-1)(2n-1)$

$\iff 2 \mid (n-1)(2n-1)$ and $3 \mid (n-1)(2n-1)$. by the Chinese Remainder Thm

Focusing first on $2 \mid (n-1)(2n-1)$, we see that $2 \mid (n-1)$ since $(2n-1)$ is odd.

This means that <u>n must be odd</u>. (equivalently, $n \equiv 1 \pmod 2$)

Now turning to $3 \mid (n-1)(2n-1)$, either $3 \mid (n-1)$ or $3 \mid (2n-1)$.

But if you do the working, you see that this implies that <u>$n \equiv 1$ or $2 \pmod 3$</u>

So by the Chinese Remainder Theorem,

$$\left.\begin{array}{l} n \equiv 1 \pmod 2 \\ n \equiv 1 \text{ or } 2 \pmod 3 \end{array}\right\} n \equiv 1 \text{ or } 5 \pmod 6$$

$\therefore$ The statement is true for $n = 6k+1$ and $n = 6k+5$, $k \in \mathbb{Z}^{\geq 0}$.

3) $5(7) = 35 \equiv 1 \pmod{17}$. So 7 is an inverse of 5 $\pmod{17}$.

4) Chinese Remainder Theorem

Let $m_1, m_2, \ldots, m_k \in \mathbb{Z} \setminus \{0\}$ be pairwise relatively prime.
Let $a_1, a_2, \ldots, a_k \in \mathbb{Z}$.
Then the system of congruences:

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

has a unique solution modulo $\prod_{i=1}^{k} m_i = m_1 m_2 \cdots m_k$

$$\left.\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 1 \pmod 3 \end{aligned}\right\} x \equiv 1 \pmod 6 \qquad \{\text{as in Question 2}\}$$
$$\Longrightarrow x = 6k + 1 \text{ for any } k \in \mathbb{Z}.$$

5) As 19 is a prime, by Wilson's Theorem we have

$$(19-1)! = 18! \equiv -1 \pmod{19}$$
$$(16!)(17)(18) \equiv -1 \pmod{19}$$

But $(17)(18) = 306 \equiv 2 \pmod{19}$
and $2(10) = 20 \equiv 1 \pmod{19}$. Thus,

$$(16!)(2) \equiv -1 \pmod{19}$$
$$(16!)(2)(10) \equiv -10 \pmod{19}$$
$$(16!) \equiv -10 \equiv 9 \pmod{19}$$

IMPORTANT NOTE: In the Euclidean Division Algorithm for integers (i.e. elementary school division), the remainder (in this case) must be an int
r such that $0 \leq r < 19$.
Thus, when the question is worded this way, the correct answer is 9, and not -10 (or any other integer in the same residue class mo

6) Let $a, n \in \mathbb{Z}$ with $n \geq 4$, composite

Then n is a pseudoprime (base a) (Fermat) if $a^n \equiv a \pmod{n}$

Example: 341 (base 2)

Let $n \geq 4$ be a composite integer.

n is a Carmichael number if for every $a \in \mathbb{Z}$ s.t. $\gcd(a, n) = 1$ we have $a^{n-1} \equiv 1 \pmod{n}$

Example: 561

---

7) $a \equiv a^p \equiv b^p \equiv b \pmod{p}$ by Fermat's Little Theorem, since $p \nmid a$, $p \nmid$

So $a = b + pk$ for some $k \in \mathbb{Z}$.

But then $a^p = (b + pk)^p$

Binomial expansion $= b^p + \underbrace{\binom{p}{1} b^{p-1}(pk)}_{\text{divisible by } p^2} + \underbrace{\binom{p}{2} b^{p-2}(pk)^2}_{\text{divisible by } p^2} + \cdots + \underbrace{\binom{p}{p-1} b(pk)^{p-1}}_{\text{divisible by } p^2} + \underbrace{(pk)^p}_{\text{divisible by } p^2}$

$\equiv b^p \pmod{p^2}$