Math 345 – Monday 10/2/17

Exercise 23.

(a) Solve the following congruences:
  (i) $x^{101} \equiv 7 \pmod{12}$
  (ii) $10^x \equiv 1 \pmod{27}$

(b) The number 3750 satisfies $\phi(3750) = 1000$. Find an integer $1 \le a \le 5000$ that is not a multiple of 7, that satisfies $a \equiv 7^{3003} \pmod{3750}$ [This integer need not be reduced modulo 3750].

(c) Show that if $m = 561 = 3 \cdot 11 \cdot 17$, then $a^{m-1} \equiv 1 \pmod{m}$ for all a relatively prime to m. [Hint: There may be 320 values of a between 1 and m that are relatively prime to m, but it is not necessary (nor called for) to actually compute $a^{m-1} \equiv 1 \pmod{m}$ for all those values. Instead, use Fermats Little Theorem to check that $a^{m-1} \equiv 1 \pmod{p}$ for each prime p dividing m, and then explain why this implies that $a^{m-1} \equiv 1 \pmod{m}$.]

Exercise 24. Let $b_1 < b_2 < \cdots < b_{\phi(n)}$ be the integers $1 \le b_i < n$ that are relatively prime to n, and let $B = b_1 b_2 b_3 \cdots b_{\phi(n)}$ be their product. [This number came up during the proof of Euler's formula.]

(a) Compute B for $n = 4, 5, 6,$ and 8, modulo n. Note that in each case, $B \equiv 1 \pmod{n}$ or $B \equiv n - 1 \pmod{n}$, which, together, is the same as $B \equiv \pm 1 \pmod{n}$.

(b) Prove that $B \equiv \pm 1 \pmod{n}$ in general. [Hint: Think about multiplicative inverses – when does an integer a have an inverse? How many are there modulo n?]

(c) Try to find a pattern for when B is equivalent to $+1 \pmod{n}$ and when it is equivalent to $+1 \pmod{n}$. Can you prove your conjecture?