Math 345 – Monday 9/25/17

Exercise 17. Prove the following.

(a) If $x = x_0$ is a solution to $a + x \equiv b \pmod{n}$, then so is $x = x_0 + kn$ for all $k \in \mathbb{Z}$.
(b) If $x = x_0$ is a solution to $ax \equiv b \pmod{n}$, then so is $x = x_0 + kn$ for all $k \in \mathbb{Z}$.

Exercise 18. For each of the following congruences, decide if there are any solutions. If there are, give a maximal set of distinct (non-congruent) solutions.
[For examples involving numbers larger than 20, use a computer to calculate relevant data to start the problem. For example, in problem (e), you'll use a computer to calculate $\gcd(21, 91)$, as well as one example of $u \in \mathbb{Z}$ such that $21u \equiv \gcd(21, 91) \pmod{91}$. Use functions that allow you to reduce modulo n easily.]

(a) $7x \equiv 3 \pmod{15}$
(b) $6x \equiv 5 \pmod{15}$
(c) $8x \equiv 6 \pmod{14}$
(d) $66x \equiv 100 \pmod{121}$
(e) $21x \equiv 14 \pmod{91}$
(f) $72x \equiv 47 \pmod{200}$
(g) $4183x \equiv 5781 \pmod{15087}$
(h) $1537x \equiv 2863 \pmod{6731}$

Exercise 19. (a) Show that $a \in \mathbb{Z}_{>0}$ is divisible by 4 if and only if its last two digits are divisible by 4. [Hint: consider an equivalence modulo 100.]
(b) The number $a \in \mathbb{Z}_{>0}$ is divisible by 3 if and only if the sum of its digits is divisible by 3. [Hint: Express a number as integral combination of powers of 10, and reduce modulo 3.]
(c) The number $a \in \mathbb{Z}_{>0}$ is divisible by 9 if and only if the sum of its digits is divisible by 9. [Hint: Express a number as integral combination of powers of 10, and reduce modulo 9.]

Exercise 20.

(a) Use a computer to compute a maximal set of (non-congruent) solutions to the following.
  (i) $x^2 \equiv 1 \pmod{8}$
  (ii) $x^2 \equiv 2 \pmod{7}$
  (iii) $x^2 \equiv 3 \pmod{7}$
  (iv) $x^4 + 5x^3 + 4x^2 - 6x = 4 \equiv 0 \pmod{11}$
(b) For $x^2 \equiv 1 \pmod{8}$, you should have gotten more than 2 solutions. Note that these are all solutions to $x^2 - 1 \equiv 0 \pmod{8}$. Why isn't this a contradiction to the Polynomial Roots Mod p Theorem?
(c) Let p and q be distinct primes. What is the maximum number of possible non-congruent solutions to a congruence of the form $x^2 - a \equiv 0 \pmod{pq}$.