Problem Set 04 – Section 4.4 Solving Congruences

Due Date: September 27, 2017

All solutions must show all work and be written clearly and legibly. When applicable expand your answer to a short paragraph. Failure to not show work will result in no points awarded.

Exercises – 4.4 Solving Congruences

4. By inspection (as discussed prior to Example 1), find an inverse of 2 modulo 17.
6. Find an inverse of a modulo m for each of these pairs of relatively prime integers using the method followed in Example 2.
a) $a = 2$, $m = 17$
b) $a = 34$, $m = 89$
c) $a = 144$, $m = 233$
~~**d)** $a = 200$, $m = 1001$~~
10. Solve the congruence $2x \equiv 7$ (mod 17) using the inverse of 2 modulo 7 found in part (a) of Exercise 6.
12. Solve each of these congruences using the modular inverses found in parts (b), (c), ~~and (d)~~ of Exercise 6.
a) $34x \equiv 77$ (mod 89)
b) $144x \equiv 4$ (mod 233)
~~**c)** $200x \equiv 13$ (mod 1001)~~
20. Use the construction in the proof of the Chinese remainder theorem to find all solutions to the system of congruences
$x \equiv 2$ (mod 3), $x \equiv 1$ (mod 4), and $x \equiv 3$ (mod 5).
22. Solve the system of congruence $x \equiv 3$ (mod 6) and $x \equiv 4$ (mod 7) using the method of back substitution.
32. Which integers are divisible by 5 but leave a remainder of 1 when divided by 3?
34. Use Fermat's little theorem to find 231002 **mod** 41.
36. Use Exercise 35 to find an inverse of 5 modulo 41.
38. a) Use Fermat's little theorem to compute 3^{302} **mod** 5, 3^{302} **mod** 7, and 3^{302} **mod** 11.
b) Use your results from part (a) and the Chinese remainder theorem to find 3^{302} **mod** 385. (Note that $385 = 5 \cdot 7 \cdot 11$.)
~~**46.** Show that 1729 is a Carmichael number.~~
50. Find the nonnegative integer a less than 28 represented by each of these pairs, where each pair represents (a **mod** 4, a **mod** 7). Show all work.
a) (0, 0) **b)** (1, 0) **c)** (1, 1)
d) (2, 1) **e)** (2, 2) ~~**f)** (0, 3)~~
~~**g)** (2, 0) **h)** (3, 5) **i)** (3, 6)~~
52. Explain how to use the pairs found in Exercise 51 to add 4 and 7.
54. Show that 2 is a primitive root of 19.