WRITTEN HW #5 SOLUTIONS

(1) (10 points) Solve the following systems of congruences (5 each):
  (a) $x \equiv 3 \bmod 4, x \equiv 5 \bmod 7, x \equiv 1 \bmod 9$.
  (b) $2x \equiv 3 \bmod 5, 3x \equiv 4 \bmod 7$.

Solution. For the first set of congruences, $4, 7, 9$ are mutually coprime, so the CRT guarantees a unique solution mod $4 \cdot 7 \cdot 9 = 252$. A solution to $x \equiv 5 \bmod 7$ satisfies $x \equiv 5, 12, 19, 26 \bmod 28$, and only $19 \equiv 3 \bmod 4$, so $x \equiv 19 \bmod 28$ is the unique solution to $x \equiv 3 \bmod 4, x \equiv 5 \bmod 7$. Notice that $19 \equiv 1 \bmod 9$ as well, so $x \equiv 19 \bmod 252$ is the solution to the first system.

For the second system, first notice $2x \equiv 3 \bmod 5$ has solution $x \equiv 4 \bmod 5$, and $3x \equiv 4 \bmod 7$ has solution $x \equiv 6 \bmod 7$. The CRT guarantees that simultaneous solutions are unique mod 35, and the above procedure (or inspection; notice that $x \equiv -1 \bmod 5, x \equiv -1 \bmod 7$) shows that $x \equiv -1 \equiv 34 \bmod 35$ is the unique solution to this system. □

(2) (10 points) Solve the following systems of congruences (5 each):
  (a) $x \equiv 4 \bmod 6, x \equiv 7 \bmod 15$.
  (b) $3x \equiv 4 \bmod 10, x \equiv 12 \bmod 14$.

Solution. $x \equiv 4 \bmod 6, x \equiv 7 \bmod 15$ need to satisfy the compatibility relation $4 \equiv 7 \bmod \gcd(6, 15) = 3$, which it does, so there will be a unique solution mod $\operatorname{lcm}(15, 6) = 30$. Since $x \equiv 7 \bmod 15$ implies $x \equiv 7, 22 \bmod 30$, we see by inspection that $x \equiv 22 \bmod 30$ is the unique solution.

For the second system, first notice that $3x \equiv 4 \bmod 10$ has the unique solution $x \equiv 8 \bmod 10$. Again, this is compatible with $x \equiv 12 \bmod 14$, because $12 \equiv 8 \bmod gcd(14, 10) = 2$, and the solution will be unique mod $\operatorname{lcm}(14, 10) = 70$. Inspection (notice $x \equiv -2 \bmod 10, x \equiv -2 \bmod 14$) shows that $x \equiv -2 \equiv 68 \bmod 70$ solves both equations. □

(3) (10 points) Suppose you are given a system of linear congruences

$$x \equiv a_1 \bmod n_1, \ldots, x \equiv a_k \bmod n_k,$$

where the a_i are arbitrary integers and the n_i are positive integers. Show that there are either no solutions to this system, or all the solutions can be described by $x \equiv a \bmod \operatorname{lcm}(n_1, \ldots, n_k)$, for some integer a.

Solution. Factor n_i as $p_1^{e_{i1}} p_2^{e_{i2}} \ldots p_r^{e_{ir}}$, where we let some of the exponents be equal to 0. (The ps are the set of primes which appear in the factorization of some n_i.) Then our original system is equivalent to the system consisting of $x \equiv a_i \bmod p_j^{e_{ij}}$, where the indexing runs over both i, j. Fix attention on the congruences consisting of moduli to powers of p_j, for fixed j. Then either this system has a solution which is unique mod $p_j^{\max_i(e_{ij})}$, or has no solutions at all. (The exponent is the maximum of the exponents of p_j that appear in the factorizations of all the n_i.) If any of these systems have no solutions, then our original system have no solutions, and we are done.

Suppose all of these systems have solutions. Since the $p_j^{\max_i(e_{ij})}$ are all mutually coprime, the CRT implies that the original system has unique solution mod their product. But their product is just the lcm of $n_1, \ldots, n_k$. $\square$

(4) (10 points) Show, using basic methods (in particular, without citing Lemma 4.8 of the text), that 1105 and 1729 are Carmichael numbers.

Solution. First, we factor each of these numbers. For example, $1105 = 5 \cdot 13 \cdot 17$. Then Fermat's Little Theorem tells us that $a^5 \equiv a \bmod 5$, and if $5 \nmid a$, then $a^4 \equiv 1 \bmod 5$. Furthermore, notice that $4 \mid 1104$. Therefore, if $5 \nmid a$, then $a^{1104} \equiv 1 \bmod 5$, or $a^{1105} \equiv a \bmod 5$. However, notice this last congruence is also true if $5 \mid a$, so $a^{1105} \equiv a \bmod 5$ is true for all integers a. Similarly, we show that $a^{1105} \equiv a \bmod 13, a^{1105} \equiv a \bmod 17$ is true for all integers a, because $(13-1) = 12 \mid 1104$, $(17-1) = 16 \mid 1104$. These three congruences imply that $a^{1105} \equiv a \bmod 1105$, so 1105 is Carmichael.

The same procedure works for $1729 = 7 \cdot 13 \cdot 19$. In particular, $6 \mid 1728, 12 \mid 1728, 18 \mid 1728$. $\square$

(5) (10 points) In this problem, we will check that 703 is a strong pseudoprime to base 3.

(a) (5 points) Carry out the fast-exponentiation method by hand to compute 3^{351} and 3^{702} mod 703. You should show work when you calculate the binary expansion of 351 and also the results of computing successive squares of 3 mod 703.

(b) (5 points) Based on your answers to the previous part, explain why 703 is a strong psuedoprime to base 3. Is 703 a strong psuedoprime to base 2? (You should carry out the same calculations as in the previous part, except this time you can just use your computer to calculate $2^{351}, 2^{702}$ mod 703.)

Solution. 351 has binary expansion $256+64+16+8+4+2+1$. We compute:

$$3^1 \equiv 3 \bmod 703, 3^2 \equiv 9 \bmod 703, 3^4 \equiv 81 \bmod 703, 3^8 \equiv 234 \bmod 703, 3^{16} \equiv 625 \bmod 703,$$
$$3^{32} \equiv 460 \bmod 703, 3^{64} \equiv 700 \bmod 703, 3^{128} \equiv 9 \bmod 703, 3^{256} \equiv 81 \bmod 703.$$

We now multiply the appropriate powers of 3 together:

$$3^{351} \equiv 8 \cdot 700 \cdot 625 \cdot 234 \cdot 81 \cdot 9 \cdot 3 \equiv 702 \bmod 703.$$

Computing 3^{702} involves squaring this answer, which is just 1 mod 703.

703 is a strong pseudoprime to base 3, because $3^{351} \equiv -1 \bmod 703$, so the Miller-Rabin test is inconclusive, but 703 is composite, because $703 = 19 \cdot 37$.

On the other hand, $2^{351} \equiv 265 \bmod 703$, so 703 fails the Miller-Rabin test to base 2, and hence is composite. (Alternately, notice $2^{702} \equiv 628 \bmod 703$, so fails the simpler Fermat compositeness test.) $\square$