HOMEWORK ASSIGNMENT #4 SOLUTIONS

(1) (a) Find all simultaneous solutions to the system $x \equiv 7 \mod 20, x \equiv 2 \mod 3$.
(b) Find all simultaneous solutions to the system $x \equiv 3 \mod 7, x \equiv 2 \mod 8, x \equiv 1 \mod 5$.

Solution.

(a) The CRT tells us there is a unique solution mod 60, because $20, 3$ are coprime. $x \equiv 7 \mod 20$ implies $x \equiv 7, 27, 47 \mod 60$, and of these three numbers, only $47 \equiv 2 \mod 3$, so $x \equiv 47 \mod 60$ is the only solution to the original system.
(b) First, there is one simultaneous solution to $x \equiv 3 \mod 7, x \equiv 2 \mod 8$ mod 56, by the CRT, and inspection shows that it is $x \equiv 10 \mod 56$. Next, the system $x \equiv 10 \mod 56, x \equiv 1 \mod 5$ has exactly one solution mod $56 \cdot 5 = 280$, again by the CRT, and inspection shows that it is $x \equiv 66 \mod 280$. So this is the only solution to the original system. □

(2) (a) Find all simultaneous solutions to the system $x^2 + 3x + 1 \equiv 0 \mod 5, 3x \equiv 2 \mod 7$.
(b) Find all simultaneous solutions to the system $x^2 \equiv 1 \mod 8, 5x \equiv 15 \mod 20, 5x \equiv 1 \mod 6$.

Solution.

(a) The equation $x^2 + 3x + 1 \equiv 0 \mod 5$ has solution $x \equiv 1 \mod 5$, as trial and error shows, while $3x \equiv 2 \mod 7$ has unique solution $x \equiv 3 \mod 7$. The CRT tells us there is a unique solution to the original system mod 35, and one finds that $x \equiv 31 \mod 35$ is that solution.
(b) The congruence $5x \equiv 15 \mod 20$ is equivalent to $x \equiv 3 \mod 4$. The congruence $5x \equiv 1 \mod 6$ is equivalent to $x \equiv 5 \mod 6$. Finally, the congruence $x^2 \equiv 1 \mod 8$ has solutions $x \equiv 1, 3, 5, 7 \mod 8$.
Notice that if $x \equiv 1, 5 \mod 8$, then $x \equiv 3 \mod 4$ is impossible. Therefore the simultaneous solutions to $x^2 \equiv 1 \mod 8$ and $5x \equiv 15 \mod 20$ are given by $x \equiv 3 \mod 4$. The congruence $x \equiv 5 \mod 6$ is equivalent to $x \equiv 1 \mod 2$ and $x \equiv 2 \mod 3$; the former is always satisfied if $x \equiv 3 \mod 4$, so the original system of three congruences is equivalent to $x \equiv 3 \mod 4, x \equiv 2 \mod 3$, which has unique solution (by the CRT) $x \equiv 11 \mod 12$. □

(3) Consider the simultaneous system $x \equiv a_1 \mod n_1, x \equiv a_2 \mod n_2$. Prove the following special case of Theorem 3.12 in the textbook: this system has a solution if and only if $\gcd(n_1, n_2) \mid (a_1 - a_2)$, and if there is a solution, it is unique mod $\operatorname{lcm}(n_1, n_2)$. (Obviously, you should not be just citing Theorem 3.12. However it might be worthwhile to look at the proof and try to unwind the ideas in the proof to the special situation in this problem.)

Solution. Let n_1 have factorization $p_1^{e_1} \dots p_r^{e_r}$, and let n_2 have factorization $p_1^{f_1} \dots p_r^{f_r}$, where we use the convention that e_i, f_i might equal 0, but not both at the same time. Then the congruence $x \equiv a_1 \mod n_1$ is equivalent to $x \equiv a_1 \mod p_i^{e_i}$, for all i, and similarly $x \equiv a_2 \mod n_2$ is equivalent to $x \equiv a_2 \mod p_i^{f_i}$.

For a fixed p_i, consider the pair of congruences corresponding to moduli $p_i^{e_i}, p_i^{f_i}$ as given above. We know that pair has a solution if and only if $a_2 \equiv a_1 \mod p_i^{\min(e_i,f_i)}$, and if so that solution is unique mod $p_i^{\max(e_i,f_i)}$. So the original pair of congruences has a simultaneous solution if and only if $p_i^{\min(e_i,f_i)}$ divides $a_1 - a_2$ for all i. (We use the fact that all the prime powers $p_i^{\cdots}$ are mutually coprime.) However, since these powers of p_i are all relatively prime, this implies that their product divides $a_1 - a_2$, and that product is $\gcd(n_1, n_2)$. If this is the case, since the congruences $x \equiv a_1 \mod p_i^{e_i}, x \equiv a_2 \mod p_i^{f_i}$ has a unique solution mod $p_i^{\max(e_i,f_i)}$, the CRT tells us that these congruences taken together over all p_i have a unique solution mod their product, which is just $\operatorname{lcm}(n_1, n_2)$. □

(4) Let $f(x)$ be a polynomial with integer coefficients. Consider the equation $f(x) \equiv 0 \mod n$. If $f(x)$ is a linear polynomial, is it possible for $x \equiv 1, 4, 7, 11 \mod 12$ to be the solution set of the linear congruence $f(x) \equiv 0 \mod n$?

Solution. The answer is no. Recall that the solutions to any linear congruence $ax + b \equiv 0 \mod n$ have the form $x \equiv x_0 + nt/d \mod n$, where $d = \gcd(a, n)$, x_0 is any particular solution, and t is an integer. In particular, the solutions to a linear congruence form an arithmetic progression. However, the numbers which satisfy $x \equiv 1, 4, 7, 11 \mod 12$ do not form an arithmetic progression, since $11 - 7 \neq 7 - 4$. Therefore, $x \equiv 1, 4, 7, 11 \mod 12$ cannot possibly be the solution set of a linear congruence. □

(5) (a) Compute the remainder when 4^{6303} is divided by 31.
(b) Compute the remainder when 7^{7^7} is divided by 11.

Solution.

(a) Fermat's Little Theorem applied to the prime $p = 31$ and $a = 4$ yields $4^{30} \equiv 1 \mod 31$. As $6303 = 210(30) + 3$, $4^{6303} \equiv 4^3 \mod 31$, and $4^3 = 64 \equiv 2 \mod 31$.
(b) Fermat's Little Theorem applied to the prime $p = 11$ and $a = 7$ yields $7^{10} \equiv 1 \mod 11$. Therefore, to compute $7^{7^7} \mod 11$, we want to find the remainder of 7^7 when we divide by 10; in other words, we want to find the last digit of 7^7. Since $7^4 \equiv 1 \mod 10$, $7^7 \equiv 7^3 \equiv 3 \mod 10$. Therefore $7^{7^7} \equiv 7^3 \equiv 2 \mod 11$. □

(6) Let p be a prime, and let a be an integer relatively prime to p. Suppose that d is the smallest positive integer such that $a^d \equiv 1 \mod p$. Show that $d|(p-1)$. (This d is sometimes called the *order* of a mod p; the terminology comes from abstract algebra.)

Solution. Since $a^{p-1} \equiv 1 \mod p$ by Fermat's Little Theorem, $p - 1 \geq d$. Perform a Euclidean division of $p - 1$ by d; one gets $p - 1 = qd + r$ for some $0 \leq r < d$. Therefore $a^{p-1} \equiv a^{qd}a^r \equiv 1 \mod p$. Since $a^d \equiv 1 \mod d$, we have $a^r \equiv 1 \mod p$. But $0 \leq r < d$, and d is the smallest positive integer for which $a^d \equiv 1 \mod p$, so we must have $r = 0$. This means $d \mid (p - 1)$, as desired. □