MATH 3320, HOMEWORK #4 – SOLUTIONS

1. (10 points) Let p be a prime number. Suppose that a and n are positive numbers such that $\gcd(a, p) = 1$ and $\gcd(n, p-1) = 1$. Determine the number of solutions of the congruence $x^n \equiv a \pmod{p}$.

Solution: It is possible to prove this fairly easily without appealing to the fact that p has a primitive root. However, the proof is a bit more straightforward if we use that fact: Suppose r is a primitive root with respect to p. Then r^0 through r^{p-2} are all noncongruent, so $b = r^\beta$ and $c = r^\gamma$, integers mod p, are congruent if and only if $\beta \equiv \gamma \pmod{p-1}$. Thus, writing a as r^α and x as r^ξ, we obtain that the number of solutions x of our original equation (for a fixed a) is equal to the number of solutions ξ of the equation $n\xi \equiv \alpha \pmod{p-1}$. But this equation has exactly one solution mod $p-1$, as $\gcd(n, p-1) = 1$ (since we may multiply both sides by the inverse n^{-1} mod $p-1$ to get $\xi \equiv n^{-1}\alpha$, and this choice of ξ is easily seen to work). Therefore, for any choice of a, the given equation has one unique solution mod p.

2. (20 points) Let m be a positive integer with a prime factorization

$$m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}.$$

Determine the number of solutions of $x^2 \equiv 1 \pmod{m}$.

Solution: $x^2 \equiv 1 \pmod{m}$ if and only if $x^2 \equiv 1 \pmod{p_i^{e_i}}$ for $i = 1, \cdots, r$, which means

$$(x-1)(x+1) \equiv 0 \pmod{p_i^{e_i}},\ i = 1, \cdots, r$$

For each i, $p_i | p_i^{e_i} | (x-1)(x+1)$, so $p_i | x-1$ or $p_i | x+1$.

Because $(x+1) - (x-1) = 2$, for $p_i > 2$, $x+1$ and $x-1$ cannot be both multiple of p_i at same time. Thus, either $p_i^{e_i} | x+1$ or $p_i^{e_i} | x-1$. We have two cases:

$$x \equiv 1 \pmod{p_i^{e_i}} \text{ or } x \equiv -1 \equiv p_i^{e_i} - 1 \pmod{p_i^{e_i}}.$$

If $p_i = 2$ for some i, consider 3 cases:

- If $e_i = 1$, x can only be $x \equiv 1 \pmod{2}$.
- If $e_i = 2$, x must be odd, and $x \equiv 1 \pmod{2^2}$ or $x \equiv 3 \pmod{2^2}$ are both possible.
- If $e_i \geq 3$, suppose $x - 1 = 2^{a_1} \cdot k_1$ and $x + 1 = 2^{a_2} \cdot k_2$, where k_1, k_2 are odd. Then $k_1 + k_2 \geq e_i$. Because $(x+1) - (x-1) = 2$, one from a_1, a_2 is 1, and the other one $\geq e_i - 1$. There are four possibilities:
  - $x \equiv 2^{e_i - 1} + 1 \pmod{2^{e_i}}$
  - $x \equiv 2^{e_i - 1} - 1 \pmod{2^{e_i}}$
  - $x \equiv 1 \pmod{2^{e_i}}$
  - $x \equiv -1 \equiv 2^{e_i} - 1 \pmod{2^{e_i}}$

Because $p_i^{e_i}$ are relatively prime to each other, given the congruence of x to each $p_i^{e_i}$, there is only one solution module m. So the number of solutions (m) is the product of solution number for each $x^2 \equiv 1 \pmod{p_i^{e_i}}$. In sum, the result is

- If there is no $p_i = 2$, the solution is 2^r.
- If there is a $p_=2$ and $e_i = 1$, the solution is $1 \cdot 2^{r-1} = 2^{r-1}$.
- If there is a $p_=2$ and $e_i = 2$, the solution is $2 \cdot 2^{r-1} = 2^r$.
- If there is a $p_=2$ and $e_i \geq 3$, the solution is $4 \cdot 2^{r-1} = 2^{r+1}$.

3. (15 points) Let a and m be relatively prime positive integers. Prove that a is a primitive root modulo m if and only if $a^{\phi(m)/p} \not\equiv 1 \pmod{m}$ for all prime factors p of $\phi(m)$.

Solution: We must prove two directions. First, for the easy one: Suppose a is a primitive root mod m. Then $a^k \not\equiv 1$ for all integers $0 < k < \phi(m)$. But $\phi(m)/p$ is an integer in that range. The required statement follows.

We now proceed to prove the reverse direction. Suppose (in order to establish the contrapositive) that there exists some prime factor p of $\phi(m)$ such that $a^{\phi(m)/p} \equiv 1 \pmod{m}$. Then $\text{ord}_p(a)$ divides $\phi(m)/p$, from which it follows that the order must be strictly less than $\phi(m)$. It follows that a is not a primitive root mod m.

4.

(a) (5 points) Prove that 3 is a primitive root modulo 17.

Solution: Because 17 is prime, $\phi(17) = 16$. According to problem 3, number 3 is a primitive root if $3^{\phi(17)/p} \not\equiv 1 \pmod 17$. Because $\phi(17) = 16 = 2^4$, it only has prime factor 2. $3^{16/2} = 3^8 \equiv 16 \not\equiv 1 \pmod 17$. So 3 is a primitive root.

Comment: Checking the congruence of every power of 3 needs more computing complexity, therefore is not a good method. Notice that $3^8 = \left((3^2)^2\right)^2$, we actually only need doing 3 computations to compute $3^8 \pmod 17$.

(b) (10 points) Solve the congruence $8x^5 \equiv 5 \pmod{17}$.

Solution: Because 3 is a primitive root, by calculating the congruence of the powers of 3, we obtain

$$8 \equiv 3^{10} \pmod{17}, \quad 5 \equiv 3^5 \pmod{17}.$$

Assume $x = 3^n$, we have

$$3^{10} \cdot 3^{5n} \equiv 3^5 \pmod{17},$$

$$5n + 10 \equiv 5 \pmod{16} \quad \Rightarrow \quad n \equiv 15 \pmod{16}.$$

As a result, $x \equiv 3^n \equiv 3^{15} \equiv 6 \pmod{17}$.

Comment: Most happened in computing the 16 congruence, $3^i \pmod{17}$ for $i = 0, 1, \cdots, 15$. You will get points off if your solution has higher complexity, or hard to generalize to similar problems.

(c) (10 points) Find all integers x such that $7^x \equiv 4 \pmod{17}$.

Solution: $7 \equiv 3^{11} \pmod{17}$, $4 \equiv 3^{12} \pmod{17}$. We have

$$3^{11x} \equiv 3^{12} \pmod{17},$$

$$11x - 12 \equiv 0 \pmod{16}.$$

Let $f(x) = 11x - 12$, we solve the modular equation

$$f(x) \equiv 0 \pmod{2^4}$$

and get $x \equiv 4 \pmod{16}$.

5. (Extra Credit) A positive number m is called a *pseudoprime* (a.k.a. *Carmichael number*, see p. 169 of Davenport) if it satisfies the following two conditions:

(i) m is a composite number;
(ii) $a^{m-1} \equiv 1 \pmod{m}$ for all integers a which are relatively prime to m.

For (15 points), show that m is a Carmichael number if and only if m is a product of at least two distinct primes $p_1, p_2, \ldots, p_r$ such that $p_i - 1$ divides $m - 1$ for $i = 1, 2, \ldots, r$.

In the Section 1 lecture, we called n a pseudoprime, if it is a composite number such that only $2^n \equiv 2\ (mod n)$. Use the definition given in Problem 5 for the extra credit, not the one given in class.

Solution: First, we suppose that m can be written as a product of distinct primes $p_1p_2\cdots p_r$ $(r \geq 2)$ where $p_i - 1$ divides $m-1$ for each i. Then we wish to show $a^{m-1} \equiv 1 \pmod{m}$ for each a relatively prime to m. Pick any such a. Then a is relatively prime to each of the primes p_i. It follows that $a^{p_i-1} \equiv 1 \pmod{p}_i$. Since $p_i - 1|m$, we get $a^m \equiv 1 \pmod{p}_i$. Now, by the Chinese Remainder Theorem, it follows that a^m is congruent to only one possible equivalence class mod m, and thus to 1. The number m is composite (provided we assume $r \geq 2$).

Now suppose that m is a Carmichael number. Suppose m has $p_1^{e_1}p_2^{e_2}\cdots p_n^{e_n}$ as its prime-power factorization. For each p_i, let a_i be a primitive root with respect to $p_i^{e_i}$, and let a be the integer mod m satisfying each of the congruences $a = a_i \pmod{p}_i$. Such a primitive root must exist by Problem 2 of Homework 5 if p_i is odd. If p_i is 2, then we take a_i to be the primitive root of $p_i^{e_i}$ if $e_i = 1$ (namely 1) and to be an element of order 2, say $-1 \pmod{p_i^{e_i}}$, otherwise. In any event we have $(p_i - 1)p_i^{\min\{1, e_i - 1\}}|\mathrm{ord}_{p_i}(a_i)$ for each i. But we also have that $a_i^{m-1} \equiv 1 \pmod{p_i}$ since $a^m \equiv 1 \pmod{m}$. This means that $\mathrm{ord}_{p_i}(a_i)$ must divide $m-1$. Observe that if $e_1 > 1$, then p_i divides both m and $m-1$, hence divides 1, a contradiction, so $e_i = 1$. In addition, we have that $p_i - 1|m-1$. Hence, m can be written in the form $p_1p_2\cdots p_r$ $(r \geq 2)$ where each p_i is distinct and satisfies $p_i - 1|m-1$.