Math 110 Homework 4 Solutions

February 5, 2015

1. (a) Let p be a positive prime. Define a *primitive root modulo p*.

   (b) Identify all primitive roots modulo 11. Is your solution consistent with the claim that there are $\phi(\phi(p))$ primitive roots modulo p?

   (c) We stated the *Primitive Root Theorem*: If p is prime, then there is at least one primitive root modulo p. Show that this result does not hold for composite n: if n is composite, then there may not be unit that is a multiplicative generator (ie, primitive root) of the set of units modulo n. *Hint:* Check the units modulo 8.

   Solution: A primitive root is an integer a (equivalently, a congruence class $[a] \pmod p$) such that the powers of a generate all units modulo p.

   The primitive roots are $2, 6, 7, 8 \pmod{11}$. To check, we can simply compute the first $\phi(11) = 10$ powers of each unit modulo 11, and check whether or not all units appear on the list. A more sophisticated approach: Once you have a primitive root $a \pmod{11}$, it's a fact that the other primitive roots must be the congruence classes $a^m \pmod{11}$ where $(m, 10) = 1$ (the units modulo 10), so we can take $2, 2^3 \equiv 9 \pmod{10}, 2^7 \equiv 7 \pmod{11}$, and $2^9 \equiv 6 \pmod{11}$. This explains why there are $\phi(\phi(11)) = \phi(10) = 4$ primitive roots modulo 11.

   Let $n = 8$. Then if a is unit modulo n, then a is one of $1, 3, 7, 9$. We can check in each case that $a^2 \equiv 1 \pmod 8$, so the only powers of a are a and 1. No element is a primitive root. There is a primitive root when n is $2, 4, p^r, 2p^r$ where $r \geq 1$ and p is an odd prime.

2. In this question, you will prove the following result which appeared in class and is given in Chapter 3.7 of the textbook. You are welcome to read the proof on page 84, but your solution must be written in your own words.

   Theorem 1. *Let p be a positive prime and g be a primitive root modulo p.*

   1. *Let n be an integer. Then*

   $$g^n \equiv 1 \pmod p \qquad \text{if and only if} \qquad n \equiv 0 \pmod{p-1}.$$

   2. *If j and k are integers, then*

   $$g^j \equiv g^k \pmod p \qquad \text{if and only if} \qquad j \equiv k \pmod{p-1}.$$

   Solution: For the first part, suppose $g^n \equiv 1 \pmod p$. Then as we know $g^{p-1} \equiv 1 \pmod p$, using the division algorithm to write $n = (p-1)s + t$ with $0 \leq t < p-1$ we see that

   $$1 \equiv g^n \equiv g^{(p-1)s} g^t \equiv g^t \pmod p$$

   Suppose $0 < t < p-1$. Then g can have at most t distinct powers: since

   $$g^{at+b} \equiv (g^t)^a g^b \equiv (1)^a g^b \equiv g^b$$

we can always reduce exponents of g modulo t, which implies that there can be at most one distinct power of g for each residue class modulo t. Primitive roots, by definition, have $p-1$ distinct powers (all the units modulo p), and so this contradicts our assumption that g is a primitive root modulo p. Thus $t = 0$ and $n \equiv 0 \pmod{p-1}$. Conversely, if $n = (p-1)s$ then $g^n \equiv \left(g^{p-1}\right)^s \equiv 1^s \equiv 1 \pmod{p}$.

For the second part, the first condition is equivalent to $g^{j-k} \equiv 1 \pmod{p}$ by multiplying by g^{-k}. The second condition is equivalent to $j - k \equiv 0 \pmod{p-1}$. Thus the second part follows from the first.

3. Trappe–Washington Chapter 3 Question 20.

Solution:

(a) By Euler's theorem, $a^{\phi(n)} \equiv 1 \pmod{n}$. Thus the least integer r with $a^r \equiv 1 \pmod{n}$ is at most $\phi(n)$.

(b) Calculate $a^m \equiv (a^r)^k \equiv 1^k \equiv 1 \pmod{n}$.

(c) This is like one direction of the previous problem. Calculate $a^t \equiv a^{qr}a^s \equiv a^s \pmod{n}$ using the previous part.

(d) Suppose $a^t \equiv 1 \pmod{n}$. Then by the previous part, $a^s \equiv 1 \pmod{n}$ while $0 \leq s < r$. As r is the least positive integer such that $a^r \equiv 1 \pmod{n}$, this forces $s = 0$ and hence $a^t \equiv 1 \pmod{n}$ implies $r \mid t$. For the converse, use the second part of this question.

4. Trappe–Washington Chapter 3 Question 21. This question develops a method for finding primitive roots.

Solution:

(a) Consider the prime factorization of 600 and a proper divisor. Each prime (2, 3, 5) occuring in the factorization of the divisor occurs at most as many times as it appears in the factorization of 600, and for at least one prime divisor has strictly fewer. This means any proper divisor must divide 600/2, 600/3, or 600/5.

(b) The order of 7 is a divisor of $\phi(601) = 600$. If it is less than 600, then it must be a proper divisor, so it divides 300, 200, or 120.

(c) If the order of 7 divided any of these, then question 3b would show $7^m \equiv 1 \pmod{601}$ for at least one $m \in \{300, 200, 120\}$. The calculations given show this is not the case.

(d) Therefore the order of 7 is 600. There are 600 units modulo 601. If $7^i \equiv 7^j \pmod{601}$, then $7^{i-j} \equiv 1 \pmod{601}$. Hence $600 | i - j$ (question 2), and hence no two distinct powers of 7 that are less than 600 can be equal. Hence all 600 units occur as powers of 7, so 7 is a primitive root.

(e) In general, let $d_i = \frac{p-1}{q_i}$. Compute $g^{d_i} \pmod{p}$. Following the same reasoning as above, if any of these are 1 then the order of g is less than $p-1$ and g is not a primitive root. If none are congruent to 1, then g is a primitive root.

Note: searching for a primitive root by using this on $2, 3, 5, \ldots$, is reasonable, but hard to analyze. How long it takes depends on the smallest primitive root. Assuming the generalized Riemann Hypothesis, the smallest primitive root is $O(\log(p)^6)$, so this would run in polynomial time. The best unconditional bound is much worse.

5. (a) Define the *discrete logarithm problem* and the function $L_\alpha(\beta)$.

(b) Explain why we can easily determine the parity of $L_\alpha(\beta)$ when α is a primitive root.

(c) Trappe–Washington Chapter 7 Question 3.

Solution: The book does the first part fine on page 201.

We can determine whether $L_\alpha(\beta)$ is even or odd by checking whether $\beta^{\frac{(p-1)}{2}}$ is congruent to 1 or -1 modulo p, respectively. Here's an explanation:

Suppose that α is a primitive root modulo p. Then $\alpha^{\frac{(p-1)}{2}}$ is a square root of 1 modulo p, as

$$(\alpha^{\frac{(p-1)}{2}})^2 \equiv \alpha^{(p-1)} \equiv 1 \pmod{p} \qquad \text{by Fermat's Little Theorem.}$$

But we proved in class that the only square roots of 1 modulo a prime are 1 and -1. Moreover, since α is a primitive root, Part 1 of the theorem in Question 2 implies that $\alpha^{\frac{(p-1)}{2}}$ cannot be congruent to 1, so we must have $\alpha^{\frac{(p-1)}{2}} \equiv -1 \pmod{p}$.

It follows that

$$\beta^{\frac{(p-1)}{2}} \equiv \alpha^{x\frac{(p-1)}{2}} \equiv (\alpha^{\frac{(p-1)}{2}})^x \equiv (-1)^x \pmod{p}$$

and so $\beta^{\frac{(p-1)}{2}}$ will be congruent to 1 if x is even and -1 if x is odd.

The congruence $3^{\frac{(1223-1)}{2}} \equiv 3^{611} \equiv 1 \pmod{1223}$ shows 3 is a square, so the discrete logarithm is even.

6. (a) Describe the Diffie–Hellman Key Exchange (Chapter 7.4).
   (b) Trappe–Washington Chapter 7 Question 10.

Solution: The description in the book is good.

Given the situation described, Eve can compute a multiplicative inverse for b modulo $p-1$. Call it c. Then $bc \equiv 1 \pmod{p-1}$, and hence

$$x_2^c \equiv \alpha^{bc} \equiv \alpha \pmod{p}.$$

7. (a) Describe the ElGamal public key cryptosystem (Chapter 7.5).
   (b) Trappe–Washington Chapter 7 Question 11.

Solution: The description is in the book.

Bob decrypts by computing tr^{-a} in the notation of the book. In this case, $t = 6$ and $r = 7$, so $r^{-a} = 7^{-6} \equiv 7^{10} \equiv 2 \pmod{17}$. Thus the message was 12.

8. At the end of Chapter 3.9 is stated the following principle:

   > Suppose $n = pq$ is the product of two primes congruent to 3 (mod 4), and suppose that y is a number relatively prime to n which has a square root modulo n. Then finding the four solutions $x = \pm a, \pm b$ to $x^2 \equiv y \pmod{n}$ is computationally equivalent to factoring n.

   (a) Explain why if $n = pq$ is the product of *any* two primes p, q, then knowing four square roots of a unit $y \pmod{n}$ enables us factor n.
   (b) Conversely, explain how (if p and q are both congruent to 3 (mod 4)) we can determine all square roots of y modulo $n = pq$. Include the statement of the main proposition in Chapter 3.9.
   (c) Alice and Bob are communicating secretly using the RSA cryptosystem with modulus $n = pq = 830429$. Suppose you learn that 500, 100 424, 730 005, and 829 929 are all square roots of 250 000 modulo n. Find p and q. Show your work.

Solution: Suppose we had four square roots. By the Chinese remainder theorem, the four square roots arise from combining the solutions $x \equiv \pm y_1 \pmod{p}$ and $\equiv \pm y_2 \pmod{q}$. Therefore we can find two of the solutions α and β such that $\alpha \equiv \beta \pmod{p}$ and $\alpha \equiv -\beta \pmod{q}$. Then $\alpha - \beta$ is a multiple of p and not a multiple of q, so $\gcd(\alpha - \beta, n) = p$. This can be computed efficiently using the Euclidean algorithm, so knowing all four square roots gives an effective way to factor n.

The Proposition from 3.9 is stated in the book. It allows one to calculate a square root modulo a prime $p \equiv 3 \pmod 4$ provided one exists by raising to the $\frac{p+1}{4}$th power. The other is the negative. So to compute the square root for y modulo n, compute the square roots modulo p and q using this procedure, and then use the Chinese remainder theorem to find the square roots modulo n.

Take the square roots 500 and 100424. Their difference is 99024. Compute the gcd of this and 830429 using the Euclidean algorithm: you get 757. Then dividing 830429 by 757, you get the other prime factor 1097.

Note that the difficulty of computing square roots modulo $n = pq$ is the foundation for multiple systems in cryptography. The Rabin cryptosystem is the simplest: it is described in Exercise 3.27 (the bonus problem).

9. Trappe–Washington Chapter 3 Question 25.

   Solution: The first step is to solve $x^2 \equiv 133 \equiv 1 \pmod{11}$ and $x^2 \equiv 133 \equiv 3 \pmod{13}$. These are small enough it is easy to spot the answer: $x \equiv \pm 1 \pmod{11}$ and $x \equiv \pm 4 \pmod{13}$. Then combine them using the Chinese remainder theorem as in problem problem 8 of homework 2. The answer is $43, 56, 87, 100 \pmod{143}$.

   Likewise, we solve $x^2 \equiv 0 \pmod{11}$ and $x^2 \equiv 77 \equiv -1 \pmod{13}$. Inspection gives $x \equiv 0 \pmod{11}$ (which explains why there are only two solutions) and $x \equiv \pm 5 \pmod{13}$. Using the Chinese remainder theorem gives $44, 99 \pmod{143}$ as solutions.

10. (**Not for credit**) What topic have you chosen for your WIM? Your answer is non-binding, but please do start thinking about your WIM topic and the specifics of what you might want to include in the paper.

11. (**Bonus**). Trappe–Washington Chapter 3 Question 27.

    Solution: Assuming only one of the four square roots is meaningful, the probability of Alice's machine not returning it is 3/4. The chance of it not returning it n times is $\left(\frac{3}{4}\right)^n$ which goes to 0 quickly as $n \to \infty$. Thus Alice should soon see the correct message.

    If Oscar knows x, to find m would require him to be able to compute the square roots of x modulo n. We know this equivalent to factoring n.

    If Eve can decrypt chosen messages, she would decrypt $x = c^2$ where Eve chooses c at random. Half the time, the square root produced would not equal $\pm c$, which would allow her to factor n.