Math 3110: Quiz #4 – Solutions

April 13, 2019

Name:

Question 1

(16 minutes / 16 points) Short answers. Each question is worth 2 points.

1. Give the definition of the *multiplicative order* of a modulo n (for invertible elements a modulo n, $n \geq 1$).

   Solution. Let a and n be integers, $n \geq 1$. Suppose a is invertible modulo n. The *multiplicative order* of a modulo n is the smallest positive integer x such that $a^x \equiv 1 \pmod{n}$.

   Note: The most common error here was forgetting part or all of *smallest positive*.

2. Compute $3^{68} \pmod{7}$ (simplify so that the answer is the natural representative).

   Solution. By Fermat's Little Theorem, $3^6 \equiv 1 \pmod{7}$. Therefore $3^{68} \equiv (3^6)^{11} \cdot 3^2 \equiv 1^{11} \cdot 9 \equiv 2 \pmod{7}$.

3. Compute $\Phi(12)$ and $\phi(12)$.

   Solution. $\Phi(12)$ is the set of elements of $\{1, 2, \ldots, 12\}$ which are coprime to 12. Thus

   $$\Phi(12) = \{1, 5, 7, 11\}$$

   Therefore $\phi(12) = |\Phi(12)| = 4$.

4. Draw the multiplicative dynamics of 2 modulo 6.

   See text for examples.

5. It is true that $303^{100018} \equiv 1 \pmod{100019}$. Using only this information, what can we conclude about 100019 (circle one)?

   definitely prime   definitely composite   probably prime   probably composite

   Solution. The FLT primality test (page 160) tells us that it is probably prime, but this is not enough information to be sure.

6. What is the discrete logarithm $\log_3(2)$ for the modulus 7?

   Solution. Trying some powers, we have $3^1 \equiv 3 \pmod 7$ and $3^2 \equiv 2 \pmod 7$. This latter fact tells us that $\log_3(2) = 2$.

7. (True/False) The only square roots of 1 modulo a prime p are ± 1.

   Solution. True. This is Proposition 6.21, rephrased.

8. (True/False) Let p be a prime. If a is an element of order λ modulo p, then all other elements of order λ are powers of a.

   Solution. True. This is one of the steps of the proof of the existence of primitive roots. See the class notes or handout on this topic.

Question 2

(10 minutes / 10 points)

Prove the following theorem (i.e. the Totient Sum Formula). Hint: Count the fractions in the unit interval in two different ways.

Theorem 1. *Let $n > 1$ be an integer. Then*

$$\sum_{d|n} \phi(d) = n.$$

Solution. See the handout on the proof of existence of primitive roots.

Question 3

(10 minutes / 10 points)

You are Alice, and your secret key is $a = 3$. You are doing a Diffie-Hellman Key Exchange with Bob. You agree to use public prime $p = 17$ and primitive root $g = 3$. Bob tells you that his public key is $B = 10$.

1. What is the shared secret?

   Solution You must compute $B^a \equiv 10^3 \pmod{17}$. This is mildly annoying, but easier if you compute $10^2 \equiv 100 \equiv 15 \pmod{17}$ (note that $5 \cdot 17 = 85$), and then $10^3 \equiv 10 \cdot 15 \equiv 150 \equiv 100 + 50 \equiv 15 + 50 \equiv 65 \equiv 14 \pmod{17}$ (note that $3 \cdot 17 = 51$).

2. What is Bob's secret key?

   Solution You must find the discrete logarithm base 3 of 10. We try $3^1 \equiv 3$, $3^2 \equiv 9$, $3^3 \equiv 27 \equiv 10$ and we discover he used secret key 3 also. (That was unfortunate!)

3. You find out that you made a mistake in reading the info and the primitive root being used was actually $g = 5$. Which of the following is true (circle the right ones):

   (a) The shared secret you computed above must change.

   (b) The public key you gave to Bob has to be fixed.

   Solution Interestingly, the shared secret doesn't need to be recomputed (Alice computes it by B^a which doesn't depend on knowing g), but your public key is wrong (Alice computs g^a, which depends on g), so Bob won't get the same shared secret until you fix that.

Question 4

(10 minutes / 10 points)

Prove the following. Let p be an odd prime.

1. The only two residues a modulo p which are *self-inverse* (i.e. $a^{-1} \equiv a \pmod{p}$) are 1 and -1.

   Solution 1. If $a^{-1} \equiv a \pmod{p}$ then $a^2 \equiv 1 \pmod{p}$ so these are roots of the polynomial $T^2 \equiv 1$. Clearly 1 and -1 work, but we know a polynomial of degree 2 has at most two solutions, so nothing else works.

   Solution 2. Starting the same way, we have $0 \equiv a^2 - 1 \equiv (a-1)(a+1) \pmod{p}$. Since p is prime, we can conclude either $a - 1 \equiv 0$ or $a + 1 \equiv 0$.

2. Prove that $2 \cdot 3 \cdot 4 \cdots (p-4) \cdots (p-3) \cdots (p-2) \equiv 1 \pmod{p}$. Hint: Use the previous problem.

   Solution. None of these elements is self-inverse, but all non-self-inverse elements are included, so they are all paired up with their inverses, cancelling.

3. Prove that $(p-1)! \equiv -1 \pmod{p}$. Hint: Use the previous part.

   Solution. We have

$$(p-1)! \equiv 1 \cdot 2 \cdot 3 \cdots (p-2) \cdots (p-1) \equiv 1 \cdot 1 \cdot (p-1) \equiv -1 \pmod{p}.$$

   by the previous part.

4. Prove that if $n \geq 2$ is composite, then $(n-1)! \not\equiv -1 \pmod{n}$.

   Solution. If n is composite, let $n = de$ be a factorization into proper divisors of n. Then d and e both appear in $(n-1)!$, hence

$$(n-1)! \equiv 0 \pmod{n}.$$

   Alternate solution. If n is composite, then there is an element x in the range $1 < x < n$ which is not invertible. Then $(n-1)!$ is a multiple of this element x, hence also not invertible. But -1 is invertible, hence $(n-1)! \not\equiv -1 \pmod{n}$.

Note. This gives an impractical but interesting primality test.

Note on grading. As 10 isn't divisible by 4, but I didn't want to weight one part more than some other part, I graded each problem as X (0 points), ϵ (1 point), $\checkmark-$ (2 points), or $\checkmark$ (3 points), and then did a conversion from a scale on 12 points to a scale on 10 points ($x \mapsto x$ for $x \in \{0,1,2,3\}$, $x \mapsto x-1$ for $x \in \{4,5,6,7\}$ and $x \mapsto x-2$ for $x \in \{8,9,10,11,12\}$).