

## CAS CS 538. Solutions to Problem Set 4

Due electronically via gradescope, **Tuesday February 17, 2026 11:59pm**

Om Khadka, U51801771

**Problem 1.** (34 points) Problem 3.2 from Boneh-Shoup. Let  $\mathcal{E} = (E, D)$  be a cipher defined over  $(\mathcal{K}, \mathcal{M}, \mathcal{C})$  where  $\mathcal{K} \subseteq \mathcal{M}$ . Let  $\mathcal{E}' = (E', D')$  be a cipher where encryption is defined as  $E'((k_1, k_2), m) := (E(k_1, k_2), E(k_2, m))$ . Show that if  $\mathcal{E}$  is semantically secure then so is  $\mathcal{E}'$ . Note that problem is analogous to problem 3 on problem set 1, replacing perfect secrecy with semantic security.

**Hint:** use a hybrid argument with two intermediate games between Semantic Security Experiment 0 and Semantic Security Experiment 1. You will need to define two other games; let's call them Game h0 and Game h1 ("h" is for "hybrid"). Then you will have three separate proofs:

- Semantic Security Experiment 0 is indistinguishable from Game h0.
- Game h0 is indistinguishable from Game h1.
- Game h1 is indistinguishable from Semantic Security Experiment 1.

We suggest denoting by  $p_0, p_{h0}, p_{h1}, p_1$  the probability that the adversary outputs 1 in each of the games.

Each of these three proofs will be, itself, a reduction. Recall that a reduction itself has two parts: an algorithm and an analysis of advantage (which consists of computing two probabilities and subtracting them). The probability computations will be very simple in this problem.

**Solution.** The solution to this proof will be (like the hint stated) done via chaining the various changes we do in the encryption scheme, proving and reducing each part until we end up with the final product. By proving each part of the chain is semantically secure, I can prove via transitivity that the end-product will then also be secure.

Let  $\mathcal{E}$  be the defined cipher stated above. Then,  $\mathcal{E}'$  will be defined as the following:

- Key space is  $\mathcal{K}' = \mathcal{K} \times \mathcal{K}$
- Encryption is  $\mathcal{E}'((k_1, k_2), m) = (\mathcal{E}(k_1, k_2), E(k_2, m))$

Let  $\mathcal{A}$  be some efficient adversary, that'll attack the semantic security of  $\mathcal{E}'$ . I will now split this game up into 4 games, bounded to  $\mathcal{A}$ 's advantage. Also, fix some element  $k_0 \in \mathcal{K}$  (since  $\mathcal{K} \neq \emptyset$ ).

- $(\mathcal{E}(k_1, k_2), \mathcal{E}(k_2, m_0))$ 
  - Game 0; The actual  $\mathcal{E}'$  experiment.
- $(\mathcal{E}(k_1, k_0), \mathcal{E}(k_2, m_0))$ 
  - Game 1; Encrypting with  $k_0$  instead of  $k_2$
- $(\mathcal{E}(k_1, k_0), \mathcal{E}(k_2, m_1))$ 
  - Game 2; Encrypting  $m_1$  instead of  $m_0$

- $(\mathcal{E}(k_1, k_2), \mathcal{E}(k_2, m_1))$ 
  - Game 3; Actual  $\mathcal{E}'$  experiment, but now with  $m_0$ .

Let  $W_j$  denote the chance that  $\mathcal{A}$  outputs 1 in game  $j$ . Then, by the triangle inequality:

$$\text{SSadv}[\mathcal{A}, \mathcal{E}'] = |\Pr[W_0] - \Pr[W_3]| \leq |\Pr[W_0] - \Pr[W_1]| + |\Pr[W_1] - \Pr[W_2]| + |\Pr[W_2] - \Pr[W_3]|$$

I'll go into the reduction of each term to prove  $\mathcal{E}'$ 's semantic security.

### Game 0 $\approx$ Game 1

Let  $\mathcal{B}_1$  be an adversary attacking  $\mathcal{E}$ :

- Gets challenge ciphertext  $c^*$  from  $\mathcal{E}'$  (either  $k_2, k_0$ ).
- Samples  $k_2 \leftarrow \mathcal{K}$  independently.
- Computes  $c_2 \leftarrow \mathcal{E}(k_2, m_0)$ .
- Gives  $(c^*, c_2)$  to  $\mathcal{A}$ .
- Outputs the result of  $\mathcal{A}$ .

Looking at this now, note two key things. Firstly, if  $c^* = \mathcal{E}(k_1, k_2)$ , then  $\mathcal{B}_1$  simulates Game 0 perfectly. Also, if  $c^* = \mathcal{E}(k_1, k_0)$ ,  $\mathcal{B}_1$  will then also simulate Game 1 perfectly. Thus,

$$|\Pr[W_0] - \Pr[W_1]| = \text{SSadv}[\mathcal{B}_1, \mathcal{E}]$$

### Game 1 $\approx$ Game 2

Now let  $\mathcal{B}_2$  attack  $\mathcal{E}$ :

- Gets challenge ciphertext  $c^*$  from  $\mathcal{E}'$  (either  $m_0, m_1$  under key of  $k_2$ ).
- Samples  $k_1 \leftarrow \mathcal{K}$  independently.
- Computes  $c_1 \leftarrow \mathcal{E}(k_1, k_0)$ .
- Gives  $(c_1, c^*)$  to  $\mathcal{A}$ .
- Outputs result of  $\mathcal{A}$ .

Now look at this game. If  $c^* = \mathcal{E}(k_2, m_0)$ , then  $\mathcal{B}_2$  will perfectly simulate Game 1. In the same manner, if  $c^* = \mathcal{E}(k_2, m_1)$ , then  $\mathcal{B}_2$  will perfectly simulate Game 2. Thus,

$$|\Pr[W_1] - \Pr[W_2]| = \text{SSadv}[\mathcal{B}_2, \mathcal{E}]$$

### Game 2 $\approx$ Game 3

Let  $\mathcal{B}_3$  attack  $\mathcal{E}$  now (symmetric to  $\mathcal{B}_1$  btw).

- Gets challenge ciphertext  $c^*$  from  $\mathcal{E}'$  (either  $k_0, k_2$ ).
- Samples  $k_2 \leftarrow \mathcal{K}$  independently, then compute  $c_2 \leftarrow \mathcal{E}(k_2, m_1)$ .
- Give  $(c^*, c_2)$  to  $\mathcal{A}$ .
- Output result of  $\mathcal{A}$ .

This game also ends up with a similar result as the previous games; If  $c^* = \mathcal{E}(k_1, k_0)$ , then  $\mathcal{B}_3$  simulates Game 2 perfectly, and if  $c^* = \mathcal{E}(k_1, k_2)$ , then  $\mathcal{B}_3$  simulates Game 3 perfectly. Thus,

$$|\Pr[W_2] - \Pr[W_3]| = \text{SSadv}[\mathcal{B}_3, \mathcal{E}]$$

By combining these 3 bounds:

$$\text{SSadv}[\mathcal{A}, \mathcal{E}'] \leq \text{SSadv}[\mathcal{B}_1, \mathcal{E}] + \text{SSadv}[\mathcal{B}_2, \mathcal{E}] + \text{SSadv}[\mathcal{B}_3, \mathcal{E}]$$

And since  $\mathcal{E}$  is semantically secure, then each  $\text{SSadv}[\mathcal{B}_i, \mathcal{E}]$  will then be negligible. Thus, the sum will also be negligible, and  $\therefore \text{SSadv}[\mathcal{A}, \mathcal{E}']$  is negligible from all efficient  $\mathcal{A}$ , proving the initial statement.

**Problem 2. NOTE: We are postponing this problem. This problem will appear on Discussion 5 on Feb 18; a different problem related to the symmetric ratchet will appear on the next homework assignment. So if you have done this problem, you have not wasted time.**

The Signal protocol is the most widely used end-to-end encrypted messaging protocol in the world, used by over a billion people daily. It's the core cryptography underneath WhatsApp, Google Messages, Facebook Messenger, and the eponymous Signal app.

An important property Signal provides is *forward secrecy*: each time a message is sent, the encryption key is changed so that message remains hidden from this moment forward, even if an attacker obtains future encryption keys. The mechanism Signal uses to update the keys is called a *symmetric ratchet*<sup>1</sup>. The core ingredients to a symmetric ratchet are a PRG  $G$  and a semantically secure cipher (Enc, Dec).

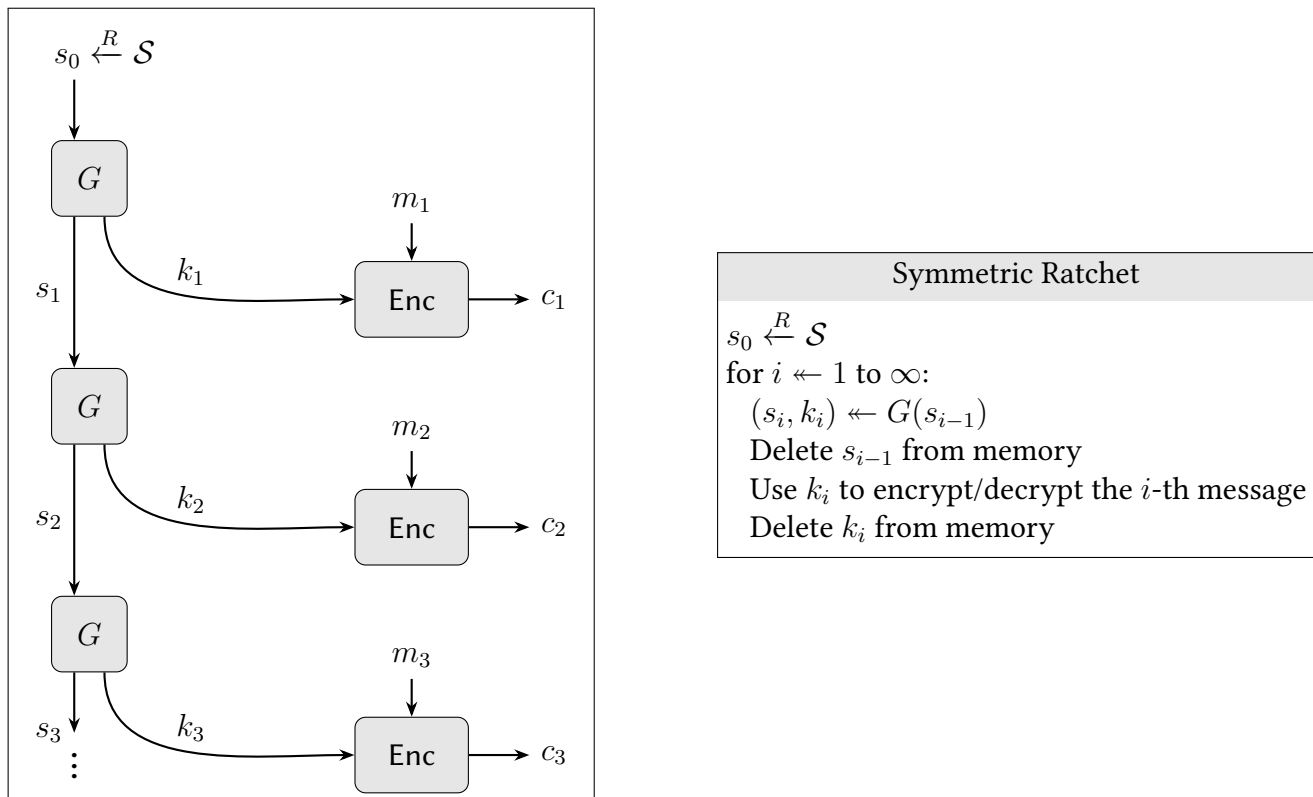


Figure 1: The Signal symmetric ratchet

When Alice and Bob want to communicate with a symmetric ratchet, they begin by agreeing on a uniformly random PRG seed  $s_0$ . If Alice is sending the first message, she runs the seed  $s_0$  through  $G$  to obtain a new seed  $s_1$  as well as a key  $k_1$ . She encrypts her message under  $k_1$  with Enc and send the ciphertext to Bob. Now Bob runs his copy of  $s_0$  through  $G$  to learn the same key  $k_1$  and decrypt the message. This process can repeat essentially forever: with each new message, Alice and Bob use the PRG to update their state and produce a fresh encryption key. Every time Alice or Bob updates their state with  $G$ , they delete the previous state and key from memory. This ensures that if they are compromised, the attacker only learns the current state.

<sup>1</sup>The full Signal protocol is sometimes called the double ratchet protocol, because it interleaves a symmetric ratchet with another mechanism called an asymmetric ratchet. The asymmetric ratchet provides backwards security, meaning that messages are secure from key compromises that occurred in the past.

This mechanism is called a *ratchet* because it's easy to advance the state forward, but it's hard to recover a previous state once you've deleted it from memory.

In this problem you'll show that the symmetric ratchet has a property necessary for forward secrecy: specifically, that there is no efficient way to learn a past key given a later state and key. (This property is necessary, but not sufficient, because what you really want is that past encryptions are still semantically secure; but we are giving you a simpler problem here.) Let  $G : \{0, 1\}^\ell \rightarrow \{0, 1\}^{2\ell}$  be a secure PRG. For all  $n \in \mathbb{N}$ , let  $G^n : \{0, 1\}^\ell \rightarrow \{0, 1\}^{(n+1)\ell}$  be the  $n$ -wise sequential composition of  $G$ , i.e.

$G^n(s)$
$s_0 \leftarrow s$ <b>for</b> $i \leftarrow 1$ <b>to</b> $n$ : $(k_i, s_i) \leftarrow G(s_{i-1})$ <b>output</b> $(k_1, \dots, k_n, s_n)$

Prove that there does not exist a PPT algorithm  $\mathcal{A}$  such that  $\Pr[\mathcal{A}(k_n, s_n) == k_{n-1}]$  is non-negligible, when  $k_n, s_n$ , and  $k_{n-1}$  are values produced by  $G^n$  with a random seed.

*You can use the fact that  $G^n$  is a secure PRG, as proven in section 3.4.2 of the textbook. Suppose there exists such an algorithm  $\mathcal{A}$ , and use it to construct an adversary that breaks the PRG game for  $G^n$ .*

**Solution.** *Skipped for now.*

**Problem 3.** (66 points, at 8 each except (c) which is 2)

Your proofs for this problem may rely only on the theorems we provide below (note the optional references to their proofs in Shoup's *A Computational Introduction to Number Theory and Algebra* <https://shoup.net/ntb>) and problems from Discussion 3, which is posted also under Piazza resources. In particular, you may not (and do not need to) invoke other theorems from number theory or abstract algebra. When proving each part, it may be very helpful to use previous parts. The parts will be graded independently, so you can use the previous parts even if you have not solved them.

**Theorem 1** (Division theorem, Shoup Theorem 1.4). *Let  $a, b \in \mathbb{Z}$  with  $b > 0$ . Then there exists unique  $q, r \in \mathbb{Z}$  such that  $a = bq + r$  and  $0 \leq r < b$ . ( $q$  is called “quotient” and  $r$  is called “remainder”.)*

A divisor  $d$  of  $a$  is any integer  $d$  such that there exists an integer  $q$  with  $qd = a$ . A common divisor of  $a$  and  $b$  is an integer that is a divisor of  $a$  and a divisor of  $b$ .

**Theorem 2** (Greatest common divisor theorem, Shoup Theorem 1.7). *Let  $a, b \in \mathbb{Z}$ . Unless  $a = b = 0$ , the set of common divisors of  $a$  and  $b$  has a maximum, called the greatest common divisor of  $a$  and  $b$  and denoted by  $\gcd(a, b)$ . We will say that  $a$  and  $b$  are relatively prime whenever  $\gcd(a, b) = 1$ .*

**Theorem 3** (Shoup Theorem 4.4). *Let  $a, b \in \mathbb{Z}$ . The extended Euclidean algorithm computes  $d, s, t \in \mathbb{Z}$  in time polynomial in  $\log a \cdot \log b$ , such that  $d = \gcd(a, b)$  and*

$$as + bt = d. \quad (1)$$

Equation (1) is also known as the Bézout's identity, and the integers  $s$  and  $t$  are called Bézout's coefficients for  $(a, b)$ .

Thus, if  $a$  and  $n$  are relatively prime, then Extended Euclidean Algorithm gives us  $s$  and  $t$  such that  $as + nt = 1$ , so  $as = 1 - nt \equiv_n 1$ , and therefore  $s \bmod n \in \mathbb{Z}_n$  is the number that, when multiplied by  $a$ , is congruent to 1 modulo  $n$ . We will call  $s$  a *multiplicative inverse of  $a$  modulo  $n$* , write  $s = a^{-1} \bmod n$ , and, when working modulo  $n$ , we will use the term “divide by  $a$ ” to mean “multiply by  $s$ ” (just like in arithmetic over real numbers).

Note that division does not always exist — it exists if and only if  $a$  and  $n$  are relatively prime.

Let  $p$  be a prime. Since every element of  $\mathbb{Z}_p^*$  is relatively prime with  $p$  whenever  $p$  is prime, inverses for elements of  $\mathbb{Z}_p^*$  always exist.

(a) Prove that for any integer  $a \in \mathbb{Z}_p^*$ , the values  $a, 2a, 3a, \dots, (p-1)a$  (all reduced modulo  $p$ ) hit every element in the set  $\mathbb{Z}_p^* = \{1, 2, 3, \dots, p-1\}$  exactly once.

*Hint: think of multiplication by  $a$  modulo  $p$  as a function. The statement is simply asking you to prove that it is a bijection. Since the domain and the target are finite and of the same size, it suffices to prove that it is a surjection (onto) or injection (1-to-1). You can choose whether to prove surjectivity or injectivity, and then simply write “a surjective (respectively, injective) function between domain and range of the same finite size is bijective.” The existence of multiplicative inverses proven could be useful.*

**Solution.** Firstly, I define the function  $f_a : \mathbb{Z}_p^*$  by  $f_a(x) = ax \bmod p$ . To show that the values  $a, 2a, \dots, (p-1)a$  hit every element of  $\mathbb{Z}_p^*$  exactly once, I'll just prove how  $f_a$  is injective. Since  $\mathbb{Z}_p^*$  is finite, and  $|\mathbb{Z}_p^*| = p-1$ , this should be enough to prove how  $f_a$  is ultimately a bijection.

Now, let  $x, y \in Z_p^*$  such that  $f_a(x) = f_a(y)$  (basically that  $ax \equiv_p ay$ ). Then,

$$ax - ay \equiv_p 0 \rightarrow a(x - y) \equiv_p 0.$$

And since  $a \in Z_p^*$ , and  $p$  is prime, then the  $\gcd(a, p) = 1$  by the definition of  $Z_p^*$ . By (3), there should exist ints  $s, t$  such that:

$$as + pt = 1.$$

And since reducing modulo  $p$  gives  $as \equiv_p 1$ , then  $s$  is a multiplicative inverse of  $a \pmod p$ .

Multiplying both sides of  $a(x - y) \equiv_p 0$  by  $s$  gives the following:

$$s \times a(x - y) \equiv_p s \times 0 \rightarrow (sa)(x - y) \equiv_p 0 \rightarrow 1 \times (x - y) \equiv_p 0.$$

And thus,  $x \equiv_p y$ . Since  $x, y \in \{1, 2, \dots, p-1\}$ , then I can conclude that  $x = y$ .

$\therefore f_a$  is injective, and since  $f_a$  is an injective function from a finite set to itself (of equal cardinality), it is then ALSO a bijection.

Thus, we prove the original statement.

**(b)** Fermat's little theorem: prove that for any  $a \in \mathbb{Z}_p^*$ ,  $a^{p-1} \equiv_p 1$ . (Or equivalently,  $a^{p-1} = 1$  if you consider multiplications modulo  $p$ . Here, we write  $\equiv_p$  to emphasize the underlying modulus.)

*Hint: multiply together the  $(p-1)$  values  $a, 2a, 3a, \dots, (p-1)a$  and use part (a).*

**Solution.** This problem will have to utilize Theorems (2) and (3), to prove parts of the mathematics for this. I'll also use the result from (a) to show the bijection/permutation property of this problem.

Let  $p$  be prime, and  $a \in Z_p^* = \{1, 2, \dots, p-1\}$ .

By (a), the map  $x \mapsto ax \pmod p$  is a bijection on  $Z_p^*$ . Therefore, the sets of

$$\{1, 2, \dots, p-1\} \text{ and } \{a \times 1, a \times 2, \dots, a \times (p-1)\} \pmod p$$

will have exactly the same elements (just in a different order).

Taking the product of all elements in each set, and by reducing modulo  $p$ ,

$$1 \times 2 \times \dots \times (p-1) \equiv_p (a \times 1) \times (a \times 2) \times \dots \times (a \times (p-1))$$

The left-hand side effectively becomes  $(p-1)!$ , meaning I can simplify the right-hand side to be

$$a^{p-1} \times (1 \times 2 \times \dots \times (p-1)) = a^{p-1} \times (p-1)!$$

And therefore

$$(p-1)! \equiv_p a^{p-1} \times (p-1)! \pmod p$$

Now, since  $p$  is prime, and every factor in  $(p-1)!$  is strictly less than  $p$ , then none of these factors can be divisible by  $p$ . By (2), the GCD will exist, and therefore

$$\gcd((p-1)!, p) = 1$$

By (3), since  $\gcd((p-1)!, p) = 1$ , then there will exist ints  $s, t$  such that

$$s \times (p-1)! + t \times p = 1$$

And by reducing this equation mod  $p$ , you'll get

$$s \times (p-1)! \equiv_p 1 \pmod{p}$$

This then shows how  $s$  is multiplicative inverse of  $(p-1)! \pmod{p}$ .

Now multiplying both sides of the equation by  $s$ , I get

$$\begin{aligned} s \times (p-1)! &\equiv_p s \times a^{p-1} \times (p-1)! \pmod{p} \\ 1 &\equiv_p a^{p-1} \times 1 \pmod{p} \\ a^{p-1} &\equiv_p 1 \end{aligned}$$

$\therefore$  I have shown the proof for Fermat's Little Theorem.

(c) Watch this video <https://www.youtube.com/watch?v=sB8v1bsssUo>. Pronounce Fermat correctly as the video explains. We will give you two points on an honor system if you tell us you did it.

**Solution.** I got it (plz trust me!!!) I know from my spanish dormmate (who studies French) that typically the last letter in words in French are usually vocally omitted, so it sounds more like 'Fear-maa', with no 't' sound.

(d) Let  $a \in \mathbb{Z}_p^*$ . The order of  $a$ , denoted by  $\text{ord}(a)$  is the smallest positive integer  $k$  such that  $a^k \equiv_p 1$ . Prove that  $k$  divides  $p-1$ .

*Hint: do a proof by contradiction. Let  $p-1 = kq + r$ , where  $q, r \in \mathbb{Z}$  and  $0 \leq r < k$  by the division theorem. Consider  $a^r$ .*

**Solution.** So by using (1) to initialize the proof, this question will basically use modular exponentiation and that minimality property of  $k$  to prove the underlying question of this problem.

Let  $k = \text{ord}(a)$ , meaning that

- $k > 0$  is the smallest int that satisfies  $a^k \equiv_p 1$ , and
- For all ints  $0 < j < k$ , we'll have  $a^j \not\equiv_p 1$ .

By (b), I already know that  $a^{p-1} \equiv_p 1$ . And since  $k > 0$ , by (1), there exists unique ints  $q, r$  such that

$$p-1 = kq + r \text{ where } 0 \leq r < k.$$



Now by computing  $a^{p-1}$  by using the decomposition of  $a^r \pmod p$ , I get

$$a^{p-1} = a^{kq+r} = (a^k)^q \times a^r \equiv_p 1^q \times a^r \equiv_p a^r.$$

But since (b) shows us how  $a^{p-1} \equiv_p 1$ , then

$$a^r \equiv_p 1.$$

Now by the minimality of  $k = \text{ord}(a)$ ,

- If  $r > 0$ , then this could contradict the minimality of  $k$  (since  $r < k$ , but also  $a^r \equiv_p 1$ ).
- $\therefore r = 0$ .

Since  $r = 0$ , the division equation becomes  $p - 1 = kq$ , which then means that  $k \mid (p - 1)$ .

$\therefore$  the order of any element  $a \in \mathbb{Z}_p^*$  will divide by  $p - 1$ .

(e) Again, let  $\text{ord}(a) = k$ . Prove that the  $k$  powers of  $a$  modulo  $p$  (namely  $\{1 = a^0, a = a^1, a^2, \dots, a^{k-1}\}$ ) are all distinct.

**Solution.** This is just a result of the problem we proved from (d), or of the minimality of  $k$ . If any 2 powers  $a^i, a^j$ , with  $0 \leq j < k$ , were equal modulo  $p$ , then we should be able to derive a contradiction to the minimality of  $k$ .

Assume, for contradiction, that 2 distinct powers were congruent modulo  $p$ . That is, suppose there exists ints  $i, j$  such that:

- $0 \leq i < j \leq k - 1$ , and
- $a^i \equiv_p a^j$ .

Now, since  $a \in \mathbb{Z}_p^*$  and  $p$  is prime, we'll have  $\gcd(a, p) = 1$ . By constantly applying (3),  $a^i$  will then also have multiplicative inverse modulo  $p$ . *Specifically*, since  $\gcd(a, p) = 1$ , there should exist  $s \in \mathbb{Z}$  such that  $as \equiv_p 1$ . Then,  $(a^i)(s^i) \equiv_p 1$ , so then therefore  $s^i$  is also a multiplicative inverse of  $a^i \pmod p$ .

Now multiply both sides of  $a^i \equiv_p a^j$  with this inverse:

$$\begin{aligned} a^i \times (a^i)^{-1} &\equiv_p a^j \times (a^j)^{-1} \pmod p \\ 1 &\equiv_p a^{i-j} \pmod p \end{aligned}$$

Now, since  $j - i > 0$  (since  $j > i$ ), and  $j - i < k$  (since  $j \leq k - 1$  and  $i \geq 0$ ), then therefore  $0 < j - i < k$  and  $a^{j-i} \equiv_p 1$ . BUT, this contradicts the initial definition of  $k = \text{ord}(a)$  as the SMALLEST + INT satisfying  $a^k \equiv_p 1$ .

$\therefore$  our assumption is false, and the original statement must be true.

(f) Prove that if the order of  $a$  is  $k$  and  $x \equiv_k y$  for some integers  $x$  and  $y$ , then  $a^x \equiv_p a^y$  (note the different subscripts of  $\equiv$ ).

**Solution.** Well now here, the congruence of mod  $k$  really means that  $x, y$  differ by a multiple of  $k$ . And since  $a^k \equiv_p 1$  by the def. of order, then any multiple of  $k$  in the exponent should contribute a factor of 1 mod  $p$ , leaving the value unchanged.

Assume  $x \equiv_k y$ . By the def. of congruence modulo  $k$ , then this means that  $k|(x - y)$ . Equivalently, there will exist an int  $q$  such that:

- $x - y = kq$ , or
- $x = y + kq$ .

Now computing  $a^x \pmod p$  using this decomposition:

$$a^x = a^{y+kq} = a^y \times a^{kq} = a^y \times (a^k)^q.$$

And since  $k = \text{ord}(a)$ , by def. we have  $a^k \equiv_p 1$ . Therefore,

$$(a^k)^q \equiv_p 1^q \equiv_p 1.$$

Subbing this back gets us:

$$a^x \equiv_p a^y \times 1 \equiv_p a^y.$$

$\therefore a^x \equiv_p a^y$  whenever  $x \equiv_k y$ .

(g) Prove the converse of part (f): if the order of  $a$  is  $k$  and  $a^x \equiv_p a^y$  for some integers  $x$  and  $y$ , then  $x \equiv_k y$  (note the different subscripts of  $\equiv$ ). Thus combining this part and the previous part, you know that for any  $a$  of order  $k$ , exponents work modulo  $k$ .

**Solution.** Ok well this is just the inverse of the last problem. Where the last problem shows how congruent exponents mod  $k$  yield the same mod  $p$ , this is now asking to show how congruent powers mod  $p$  have to come from congruent exponents mod  $k$ .

Assume  $a^x \equiv_p a^y$ . Just assume  $x \geq y$  (if not, just swap the vars; the argument is symmetric).

Since  $a \in \mathbb{Z}_p^*$  and  $p$  is prime, we get  $\gcd(a, p) = 1$ . By the use of (3),  $a^y$  will have a multiplicative inverse modulo  $p$ . And because of this, there'll exist  $s \in \mathbb{Z}$  such that  $as \equiv_p 1$ . Then  $(a^y)(s^y) \equiv_p 1$ , and therefore  $s^y$  is a multiplicative inverse of  $a^y \pmod p$ .

Multiplying both sides with this inverse:

$$\begin{aligned} a^x \times (a^y)^{-1} &\equiv_p a^y \times (a^y)^{-1} \pmod p \\ a^{x-y} &\equiv_p 1 \pmod p \end{aligned}$$

By (1) to  $x - y, k$ , with  $k > 0$ , There'll exist unique ints  $q, r$  such that:

$$x - y = kq + r \text{ where } 0 \leq r < k.$$

Computing  $a^{x-y} \pmod p$  w/ this decomposition gets us:

$$a^{x-y} = a^{kq+r} = (a^k)^q \times a^r \equiv_p 1^q \times a^r \equiv_p a^r.$$

But since we've alr established that  $a^{x-y} \equiv_p 1$ , then:

$$a^r \equiv_p 1.$$

By the def. of  $k = \text{ord}(a)$ , and since  $0 \leq r < k$ , the only possibility for  $r$  is  $r = 0$ , since otherwise  $r$  would be a smaller + exponent yielding 1, contradicting minimality.

$\therefore x - y = kq$ , which means  $k | (x - y)$ . By def. of congruence modulo  $k$ , this mens that:

$$x \equiv_k y.$$

And therefore, if  $a^x \equiv_p a^y$ , then  $x \equiv_k y$ .

**(h)** Let  $b = a^x \pmod p$ . Let  $c$  be the multiplicative inverse of  $b$ . Prove that  $c$  is a nonnegative power of  $a$ : that is, prove that there exists a nonnegative integer  $y$  such that  $a^y \equiv_p c$ .

**Solution.** For this question, since  $a^k \equiv_p 1$ , where  $k = \text{ord}(a)$ , the inverse of  $a^x$  is just  $a^{k-x}$  since  $a^x \times a^{k-x} = a^k \equiv_p 1$ . Also from (f) (g), we alr know that exponents will work mod  $k$ , so its always possible to find a non-neg num.  $y \in \{0, 1, \dots, k-1\}$  for the exponent  $k-x$ .

Let  $k = \text{ord}(a)$ , so  $a^k \equiv_p 1$  and the minimality property of  $k$  is implied from prev. problems. By (1), there'll exist ints  $q, r$  such that  $x = kq + r$  where  $0 \leq r < k$ .

By (f), since  $x \equiv_k r$ , then  $a^x \equiv_p a^r$ .

Now looking at  $a^{k-r}$ , we can compute:

$$a^r \times a^{k-r} = a^k \equiv_p 1.$$

Thus  $a^{k-r}$  is just a multiplicative inverse of  $a^r \pmod p$ , and since  $a^x \equiv_p a^r$  and multiplicative inverses modulo a prime are unique (from (3)),  $a^{k-r}$  is also the multiplicative inverse of  $a^x$ . Therefore  $c \equiv_p a^{k-r}$ .

Now I'll show that  $k-r$  can be replaced by a non-neg. exponent in  $\{0, 1, \dots, k-1\}$ :

- **Case 1:**  $r = 0$

Then,  $k-r = k$ , but  $a^k \equiv_p 1 = a^0$  by def. of order. So then  $c \equiv_p a^0$ , so we can just take  $y = 0$ .

- **Case 2:**  $r > 0$

Then  $0 < k-r < k$ , so  $y = k-r$ , which is alr a non-neg. int in  $\{1, 2, \dots, k-1\}$ .

In both cases, there'll exist a non-neg. int  $y \in \{0, 1, \dots, k-1\}$ , such that  $a^y \equiv_p c$ .

Therefore the multiplicative inverse of any power of  $a$  is itself a non-neg. power of  $a$ .

(i) Suppose  $g$  has order  $p-1$  (we know such a  $g$  exists for any prime  $p$ , though we have not proven this fact). Suppose  $k \mid p-1$ . We want to show that there exists an element of order  $k$ . Specifically, show that  $g_k := g^{(p-1)/k}$  has order  $k$ .

**Solution.** Ok so this final question kinda has 2 parts to it. Since  $g$  has maximal order of  $p-1$ , then rising it to the power of  $(p-1)/k$  will essentially 'compress' its cycle length to be  $k$ . Then the rest is just showing how  $(g_k)^k \equiv_p 1$ , and how no smaller + exponent  $j < k$  can satisfy  $(g_k)^j \equiv_p 1$  (order divides AND is exactly  $k$ ).

Let  $d = \text{ord}(g_k)$ , so  $d$  is the smallest + int such that  $(g_k)^d \equiv_p 1$ . I'll now show how  $d = k$ .

Computing  $(g_k)^k$  gets us the following:

$$(g_k)^k = (g^{(p-1)/k})^k = g^{(p-1)/k \times k} = g^{p-1}.$$

By (b),  $g^{p-1} \equiv_p 1$ , so:

$$(g_k)^k \equiv_p 1.$$

And by (a), then  $d \mid k$ .

By the def. of  $(g_k)^d \equiv_p 1$ , we get:

$$(g^{(p-1)/k})^d \equiv_p 1 \rightarrow g^{d(p-1)/k} \equiv_p 1.$$

And because  $\text{ord}(g) = p-1$ , (d) tells us tht  $p-1$  divides any exponent yielding 1 modulo  $p$ , therefore:

$$p-1 \mid \frac{d(p-1)}{k}.$$

This means that there exist an int,  $q$ , such that:

$$\frac{d(p-1)}{k} = q(p-1).$$

And since  $p-1 > 0$ , then we can divide both sides by  $p-1$  to get:

$$\frac{d}{k} = q \rightarrow d = qk.$$

$\therefore k \mid d$ .

Since I've shown that we get both  $d \mid k, k \mid d$ , and since  $d, k$  are both + ints, this implies that  $d = k$ .  
 $\therefore \text{ord}(g_k) = k$ .

For any  $k$  that divides  $p - 1$ , we can consider the set  $G_k$  of powers of  $g_k$ . This set has size  $k$  (because powers of  $g_k$  repeat after  $k$  multiplications by  $g_k$ ). Multiplying elements of  $G_k$  gives you other elements of  $G_k$  (because  $g_k^x \cdot g_k^y = g_k^{x+y}$ ), as does dividing (by part (h)). Thus,  $G_k$  is a cyclic group of order  $k$ : “cyclic” because it consists of all the powers of one element  $g_k$ , “group” because it is closed under multiplication and division, “of order  $k$ ” because it contains  $k$  elements. We will use such groups throughout the semester. The value  $g_k$  is called a *generator* of  $G_k$ , and  $G_k$  is sometimes denoted by  $\langle g_k \rangle$ .