Homework 4 Written Solutions

Written Part

In class we showed that an Elgamal oracle can solve the Diffie-Hellman problem. Let's show the other direction, and conclude that Elgamal and Diffie-Hellman are equally difficult.

2. Suppose you have access to an oracle who can solve the Diffie-Hellman problem. That is, for any prime p, given g^a and $g^b \mod p$, the oracle can tell you $g^{ab} \mod p$. Show that you can use this oracle to crack the Elgamal Public Key Cryptosystem. Precisely, suppose Alice publishes a prime p, an element $g \in \mathbb{F}_p^*$, and a public key A, and Bob sends the cipher text (c_1, c_2). Consult with the oracle to find the message Bob sent.

   Proof. We know (or have intercepted) A, c_1, and c_2. We also know the encryption means, so that Alice has a secret key a, and Bob chose a random k and is encrypting a message m. We don't know a, k, or m, but we do know:

   $$\begin{aligned} A &\equiv g^a \mod p \\ c_1 &\equiv g^k \mod p \\ c_2 &\equiv mA^k \mod p \end{aligned}$$

   We then consult with our Diffie Hellman Oracle, having them solve the DHP for $A = g^a$ and $c_1 = g^k$. They return $g^{ak} = A^k$. We then compute the inverse $A^{-k} \mod p$ (which is fast) and multiply by c_2 to recover m. □

Problem 2.10 in [HPS] gives an example of a cryptosystem where Alice and Bob need to send two rounds of messages back and forth to communicate. We reproduce it here. It might be fun to follow along on cocalc!

3. Alice and Bob decide on a prime $p = 32611$. The rest is secret. But any information crossing the middle channel (via the arrows) should be assumed to be intercepted by Eve.

	Alice	Eve	Bob
1.	Alice has message $m = 11111$		
2.	Alice chooses random $a = 3589$		
3.	Alice computes $u = m^a \mod p = 15950$	$\longrightarrow$	Bob recieves u
4.			Bob chooses random $b = 4037$.
5.	Alice recieves v	$\longleftarrow$	Bob Computes $v = u^b \mod p = 15422$
6.	Alice knows $a' = 15619$		
7.	Alice computes $w = v^{a'} \mod p = 27257$	$\longrightarrow$	Bob recieves w.
8.			Bob knows $b' = 31883$
9.			Bob computes $w^{b'} \mod p = 11111$. That's m!

   (a) Notice how Alice knows a second exponent $a' = 15619$ in step 6. Where does this number come from and how does this relate to $a = 3589$ from step 2? Similarly how do Bob's exponenets $b = 4037$ and $b' = 31883$ relate? Use this information to explain how the algorithm works.
   Notice that

   $$aa' = 56056591 = 1 + 1719 * (32610) \equiv 1 \mod p - 1.$$

So $a' \equiv a^{-1} \mod p-1$. Therefore for every x we have:

$$x^{aa'} = x^{1+1719(p-1)} = x(x^{p-1})^1 719 \equiv x \mod p$$

by Fermat's little theorem. Similarly $bb' \equiv 1 \mod p-1$ so that for all nonzero x we have $x^{bb'} \equiv x \mod p$. Therefore:

$$w^{b'} \equiv v^{a'b'} \equiv u^{ba'b'} \equiv m^{aba'b'} = (m^{aa'})^{bb'} \equiv m \mod p.$$

(b) Formulate a general version of this algorithm using variables and show that it works in general.

We will use a table like above:

	Alice	Eve	Bob
1.	Alice has message m		
2.	Alice chooses a with $\gcd(a, p-1) = 1$		
3.	Alice computes $u = m^a \mod p$	$\longrightarrow$	Bob recieves u
4.			Bob chooses b with $\gcd(b, p-1) = 1$.
5.	Alice recieves v	$\longleftarrow$	Bob Computes $v = u^b \mod p$
6.	Alice computes $a' = a^{-1} \mod p-1$		
7.	Alice computes $w = v^{a'} \mod p$	$\longrightarrow$	Bob recieves w.
8.			Bob computes $b' = b^{-1} \mod p-1$
9.			Bob computes $w^{b'} \mod p$. That's m!

By Fermats little theorem, if $cc' \equiv 1 \mod p-1$ then $cc' = 1 + k(p-1)$ so that for all nonzero x we have

$$x^{cc'} = x(x^{p-1})^k \equiv x \mod p.$$

Then we may compute as above that

$$w^{b'} \equiv v^{a'b'} \equiv u^{ba'b'} \equiv m^{aba'b'} = (m^{aa'})^{bb'} \equiv m \mod p$$

proving correctness.

Although I didn't ask this it is interesting to briefly discuss time complexity. Exponentiating in steps 3,5,7,9 is easy, and computing inverses in steps 6,8 is too. The tricky part may be steps 2 and 4, where Alice and Bob need to choose units $\mod (p-1)$. Checking whether a given number is prime to $p-1$ is easy, but on average how many would they need to check before they stumbled upon a unit? The answer certainly depends on $p-1$. For example, if $\varphi(p-1) = |(\mathbb{Z}/(p-1)\mathbb{Z})^*|$ is large, then you have a high probability of finding a unit. But what if $\varphi(p-1)$ is small?

There are two ways of doing this. First is one could choose a (or b) to be a prime number smaller than $p-1$. Of course, if an attacker knows this they can easily narrow down a search for a (or b) and find the message. That said, on average I believe $\varphi(n) \sim \frac{6}{\pi^2} n$, so you actually have a pretty good shot of finding a number prime to n by randomly guessing. One could also arrange for a prime p where $\varphi(p-1)$ is very large (which is actually protects you against discrete log attacks like we have/will discuss(ed)).

(c) Can a solution to the DLP break this cryptosystem? Justify your answer.

Proof. You can use a DLP oracle to break the cryptosystem. In particular, In step 3 you intercept u. Then in step 5 you intercept $v \equiv u^b$. You consult with the DLP oracle to compute $\log_u(v) = b$, and then can quickly compute $b' = b^{-1} \mod p-1$. In step 7 you intercept w and can yourself compute $w^{b'}$ which recovers m. □

(d) Can a solution to the DHP break this cryptosystem? Justify your answer.

Proof. You intercept $u = m^a = m^{abb'}$, $v = m^{ab}$, and $w = m^{aba'}$. In particular, you ask the Diffie-Hellman oracle to solve the DHP with

$$\begin{aligned} g &= v = m^{ab} \\ g^{a'} &= w = m^{aba'} \\ g^{b'} &= u = m^{aab} \end{aligned}$$

and the oracle tells you $g^{a'b'} = m^{aba'b'} = m$. □

The following exercises are adapted from 2.12-2.15 [HPS], and cover important properties and examples from group theory.

4. Let G be a group, and N a positive integer. The *N-torsion* of G is the set:

$$G[N] := \{g \in G : g^N = e\}.$$

(a) Prove that if $g \in G[N]$, then so is g^{-1}.

Proof. The following lemma helps.

Lemma 1. *For $g \in G$ we have $(g^N)^{-1} = g^{-N}$.*

Proof. Recall that we defined $g^{-N} = (g^{-1})^N$. It suffices to show $g^N * g^{-N} = g^{-N} * g^N = 1$. We will use induction on N. The case $n = 1$ is $g^{-1} = (g)^{-1}$ which is immediate. For the inductive step we may assume $(g^{N-1})^{-1} = g^{-(N-1)}$. Then:

$$\begin{aligned} g^N * g^{-N} &= g^{N-1} * g * g^{-1} * g^{-(N-1)} \\ &= g^{N-1} * e * g^{-(N-1)} \\ &= g^{N-1} * g^{-(N-1)} \\ &= e \end{aligned}$$

as desired. The case for $g^{-N} * g^N$ is identical. □

We also want the following fact.

Lemma 2. $e^{-1} = e$.

Proof. It suffices to show $e * e = e$, which is immediate. □

Now we can prove the exercise. Indeed, applying our lemmas we see

$$(g^{-1})^N = g^{-N} = (g^N)^{-1} = e^{-1} = e,$$

so that g^{-1} is N-torsion and we are done. □

(b) Suppose that G is commutative. Prove that if $a, b \in G[N]$, then so is $a * b$

Proof. We compute:

$$\begin{aligned}(a*b)^N &= \underbrace{(a*b)*\cdots*(a*b)}_{N\text{-times}} \\ &= \underbrace{a*a*\cdots*a}_{N\text{-times}} * \underbrace{b*b*\cdots*b}_{N\text{-times}} \\ &= a^N * b^N \\ &= e*e \\ &= e\end{aligned}$$

□

(c) Suppose that G is commutative. Prove that $G[N]$ is a group.

Proof. We enumerate the four properties necessary.

- *Closure:* We see that $G[N]$ is closed under multiplication by part (b).
- *Identity:* Notice that $e \in G[N]$. Indeed $e^N = \underbrace{e*\cdots*e}_{N\text{-times}} = e$. Since any $g \in G[N]$ is also in g, we inherit that $g * e = e * g = g$ from G.
- *Inverse:* We see that if $g \in G[N]$ then so is g^{-1} by part (a). The fact that $g * g^{-1} = g^{-1} * g = e$ is inherited from G.
- *Associativity:* If $a, b, c \in G[N]$ then since $a*(b*c) = (a*b)*c$ in G, it remains true in $G[N]$.

□

5. Let G and H be groups, and denote their multiplication rules by $*_G$ and $*_H$ respectively. A function $\varphi : G \to H$ is called a *homomorphism* if for all $a, b \in G$:

$$\varphi(a *_G b) = \varphi(a) *_H \varphi(g).$$

Homomorphisms have some nice properties:

(a) Let e_G be the identity of G and e_H the identity of H. Show that if φ is a homomorphism then $\varphi(e_G) = e_H$

Proof. Let $g \in G$ and call $\varphi(g) = h$. We notice that:

$$h = \varphi(g) = \varphi(g *_G e_G) = \varphi(g) *_H \varphi(e_G) = h *_H \varphi(e_G).$$

If we multiply both sides (on the left) by h^{-1}, we get:

$$h^{-1} *_H h = h^{-1} *_H (h *_H \varphi(e_G)).$$

The left hand side of this equation becomes e_H, and by associativity we may move the parenteses on the righthand side so that we have:

$$e_H = (h^{-1} *_H h) *_H \varphi(e_H) = e_H *_H \varphi(e_G) = \varphi(e_G),$$

and we are done. □

(b) Show that $\varphi(g^{-1}) = \varphi(g)^{-1}$ for all $g \in G$.

Proof. Applying part (a) we have:

$$\varphi(g^{-1}) *_H \varphi(g) = \varphi(g^{-1} *_G g) = \varphi(e_G) = e_H,$$

and

$$\varphi(g) *_H \varphi(g^{-1}) = \varphi(g *_G g^{-1}) = \varphi(e_G) = e_H.$$

Therefore $\varphi(g^{-1})$ satisfies the property of being the inverse so we are done. □

(c) Let G be a commutative group, show that the function $\varphi(g) = g^2$ is a homomorphism. Do the same for the function $\psi(g) = g^{-1}$. Highlight the steps whereyou needed G to be commutative.

Proof. We start with φ. The red equals sign is where we used commutativity.

$$\varphi(g * h) = (gh)^2 = g * h * g * h = g * g * h * h = g^2 * h^2 = \varphi(g) * \varphi(h).$$

For ψ, we must show that $\psi(g * h) = \psi(g) * \psi(h)$, i.e., that $(g * h)^{-1} = g^{-1} * h^{-1}$. To do this we check that:

$$(g * h) * (g^{-1} * h^{-1}) = g * g^{-1} * h * h^{-1} = e * e = e.$$

To check that it is an inverse on the left as well is identical (or we could notice that because G is commutative, right multiplication and left multiplication agree). □

(d) Suppose $\varphi : G \to H$ is a homomorphism and is bijective. Show that the inverse $\varphi^{-1} : H \to G$ is a homomorphism as well. Such a map is called an *isomorphism*.

Proof. Fix $h, h' \in H$. Since φ is surjective we know that $h = \varphi(g)$ and $h' = \varphi(g')$ for some $g, g' \in G$. Then

$$h *_H h' = \varphi(g) *_H \varphi(g') = \varphi(g *_G g').$$

In particular

$$\varphi^{-1}(h *_H h') = g *_G g' = \varphi^{-1}(h) *_G \varphi^{-1}(h'),$$

which completes the proof. □

6. Prove that the following maps are homomorphisms.

(a) The map $\varphi : \mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$ taking $a \in \mathbb{Z}$ to $a \mod N \in \mathbb{Z}/N\mathbb{Z}$.

Proof. We must show that if we denote the reduction mod N by $\varphi(a) = \overline{a}$, this comes down to showing that $\overline{a + b} = \overline{a} + \overline{b}$, which is HW1 Problem 8(a). □

(b) The map $\iota : \mathbb{R}^* \to GL_2(\mathbb{R})$ defined by $r \mapsto \begin{pmatrix} r & 0 \\ 0 & r^{-1} \end{pmatrix}$.

Proof. We check that

$$\iota(r)\iota(s) = \begin{pmatrix} r & 0 \\ 0 & r^{-1} \end{pmatrix} \begin{pmatrix} s & 0 \\ 0 & s^{-1} \end{pmatrix} = \begin{pmatrix} rs & 0 \\ 0 & r^{-1}s^{-1} \end{pmatrix} = \iota(rs),$$

where in the last step we use that $r^{-1}s^{-1} = rs^{-1}$ in $\mathbb{R}^*$ □

(c) Show that the discrete log map $\log_g : \mathbb{F}_p^* \to \mathbb{Z}/(p-1)\mathbb{Z}$ is an isomorphism.

Proof. To be a homomorphism we must show $\log_g(ab) = \log_g(a) + \log_g(b)$ which is HW3 5(d). We must show further that it is bijective which is HW3 5(c). □

7. Matrix groups over finite fields are very interesting examples of finite groups, and essential in the study of linear algebra over finite fields. Recall that $GL_2(\mathbb{F}_p)$ is the set of 2 by 2 matrices with entries in $\mathbb{F}_p$ and nonzero determinant.

(a) Prove $GL_2(\mathbb{F}_p)$ is a group under matrix multiplication.

Proof. We will be using the following fact. Let $\overline{A} = \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix}$ be a matrix with entries $\mathbb{F}_p$. Letting $a, b, c, d \in \mathbb{Z}$ reduce to $\overline{a}, \overline{b}, \overline{c}, \overline{d}$, we form a matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. We call A a lift of $\overline{A}$. Since matrix multiplication and determinants only involve addition and multiplication, one easily sees (perhaps leveraging HW1 Problem 8) that:

$$\overline{AB} = (\overline{A})(\overline{B})$$

and

$$\det(\overline{A}) = \overline{\det(A)}.$$

We enumerate the necessary properties.

- *Closure:* Suppose $A, B \in GL_2(\mathbb{F}_p)$. Considering lifts to $\mathbb{Z}$ we see that $\det(AB) = \det(A)\det(B)$ (because it holds over $\mathbb{Z}$). Since $\det(A)$ and $\det(B)$ are nonzero, their product is. Therefore $AB \in GL_2(\mathbb{F}_p)$.
- *Identity:* Let $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Then one easily computes that $AI = IA = A$ for any matrix A.
- *Inverse:* For any $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, we define

$$A^{-1} = (ad - bc)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix},$$

and compute that $AA^{-1} = A^{-1}A = I$.
- *Associativity:* Considering lifts this is inherites from associativity for matrix multiplication over $\mathbb{Z}$.

□

(b) Prove $GL_2(\mathbb{F}_p)$ is noncommutative for every p.

Proof. As in lecture we see that $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 1 & 0 & 1 \end{pmatrix}$ do not commute. We first notice that $\det(A) = \det(B) = 1$ so that both of these matrices are in $GL_2(\mathbb{F}_p)$ (regardless of p 1 is never 0). Then one can compute:

$$\begin{aligned} AB &= \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} \\ BA &= \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \end{aligned}$$

These evidently not equal mod p for any p. □

(c) Write down all the elements of $GL_2(\mathbb{F}_2)$ and the multiplication. There are 16 total 2x2 matrices with binary entries. We notice that any matrix with an entire column or row consisting of 0s automatically has determinant zero. We also check that the matrix all of whose entries are 1 has determinant 0. This leaves:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix},$$

all of which are easily seen to have determinant 1. One then computes the multiplication table. It is arranged below as row×column.

×	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$
$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$
$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$
$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$
$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$

(d) Compute this size of $GL_2(\mathbb{F}_p)$ in terms of p. (*Hint:* How many choices are there for the first column? Once you fix this first column how many choices are there left for the second?)

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. One recalls from linear algebra that the determinant of a 2x2 matrix is nonzero if and only if the columns are linearly independent. Indeed, if the columns are dependant, then simple column operations could make the second column 0 without changing the determinant, hence showing that $\det A$ is zero, and if the columns are independent, then one could row reduce to get an upper triangular matrix with nonzero entries in the diagonal (which therefore has nonzero determinant).

If we could choose any vector for the first column we would have p choice for a and p choices for c. Of course we cannot choose 0 for both so this leaves us with p^2-1 choices for the first column. As above there are naively p^2 choices for the second column, but since it must be independent from the first, it cannot be a multiple of the first column. There are precisely p scalar multiples of the first column: indeed $i\begin{pmatrix}a\\c\end{pmatrix} = j\begin{pmatrix}a\\c\end{pmatrix}$ if and only if $ia \equiv ja \mod p$ and $ic \equiv jc \mod p$. Since one of a or c is nonzero, we can divide by it so that $i \equiv j \mod p$.This means p bad choices for the second column and in total we have: $(p^2-1)(p^2-p)$.

8. Let's play with big $\mathcal{O}$ notation.

   (a) Show that $x^3 + 2x + 5 = \mathcal{O}(x^3)$

   Proof. By L'Hôpital's rule
   $$\lim_{x\to\infty} \frac{x^3+2x+5}{x^3} = 1.$$
   □

   (b) Let $f(x)$ be a polynomial of degree n. Show that $f(x) = \mathcal{O}(x^n)$.

   Proof. Let $f(x) = a_n x^n + \cdots + a_0$ with $a_n \neq 0$. Then again by L'Hôpital's rule we have:
   $$\lim_{x\to\infty} \frac{f(x)}{x^n} = a_n.$$
   □

   (c) Show that $(\ln x)^{500} = \mathcal{O}(x^{.01})$.

   Proof. Taking the derivative of the numerator and denominator of $(\ln x)^n/x^{.01}$ gives:
   $$\frac{n(\ln x)^{n-1}x^{-1}}{.01x^{-.99}} = 100n\frac{(\ln x)^{n-1}}{x^{.01}}.$$
   In particular, appyling L'Hôpital's rule inductively will eventually decrease the exponenent of the numberator to zero while leaving the denominator unchanged, and picking up a constant each time. Therefore the is 0. The moral of the story here is even really slow exponential time is faster than really fast polynomial time. □

   (d) Show that $k^2 2^k = \mathcal{O}(3^k)$

   Proof. One way to see this is that $k^2 2^k/3^k = k^2/((3/2)^k)$. Then applying L'Hôpital's rule twice we get:
   $$\lim_{k\to\infty} \frac{k^2}{(3/2)^k} = \lim_{k\to\infty} \frac{2k}{\ln(3/2)(3/2)^k} = \lim_{k\to\infty} \frac{2}{\ln(3/2)^2(3/2)^k} = 0.$$
   □