Justin Li
2/9/23

COEN 379 HW 4

1. $h_a(x)$ = (ax mod p) mod m
   Following the universal hashing property proof we did in class:
   Suppose $h_a(x1)$ and $h_a(x2)$ are the same
   Then, r = ax1 != ax2 = s (mod p) because p is prime, a!=0 and x1!=x2
   Thus, there are at most p-1/m values s mod p such that r = s (mod m)
   But r != s mod p
   So, the probability of such a collision is at most p(p-1)/m/(p-1) = p/m, which is greater than 1/m, not following the universal property.

2. Using the proof we did in class that we did in order to find the expected total number of horizontal moves of a fair coin, we can apply the same logic to find the expected total number of horizontal moves for a coin with any probability p.
   E[L] = E[Sum(i>=0) Li] = Sum(i>=0) E[Li]
   = Sum(i=0 to i=$\log_{1/p}$(n)) E[Li] + Sum(i>=1+$\log_{1/p}$(n)) E[Li]

   Here, E[Li], or the expected number of horizontal moves on level i is the geometric random variable counting the number of heads before a tails is observed, which is 1/p in this case.
   <= Sum(i=0 to i=$\log_{1/p}$(n)) 1/p + Sum(i>=1+$\log_{1/p}$(n)) E[Si]

   Here, E[Si] is the expected size of the level-i list, which is Sum(j=0 to n) p^i = np^i
   = 1/p * (1 + $\log_{1/p}$(n)) + Sum(i>=1+$\log_{1/p}$(n)) np^i
   np^(1+$\log_{1/p}$(n)) = n(p*1/n) = p
   np^(2+$\log_{1/p}$(n)) = n(p^2*1/n) = p^2
   …
   np^(n+$\log_{1/p}$(n)) = n(p^n*1/n) = p^n
   …
   = 1/p + (1/p)*$\log_{1/p}$(n) + Sum(i>=1)p^i

   Here, we can generalize 1/p and Sum(i>=1)p^i both to be O(1) since 0<p<1
   Thus,
   E[L] <= (1/p)*$\log_{1/p}$(n) + O(1)

   Now, let's see for what value of p this expression is minimized with examples:
   E[L] = 1/(0.1)*$\log_{1/0.1}$(n) + O(1)

$<= 10*\log_{10}(n) + O(1)$
vs.
$E[L] = 1/(0.9)*\log_{1/0.9}(n) + O(1)$
$<= 1.11*\log_{1.11}(n) + O(1)$

Here, the top value is much significantly lower than the bottom value, demonstrating that a lower value of p leads to an overall lower value. Thus, the expression is minimized when p approaches 0