Solution to Homework 3

1. Given: $\mathcal{H}$ is a universal hash family from $\{1, \ldots, U\}$ to $\{0, 1, \ldots, m-1\}$.

We want to find the expected number of steps to do a SUCCESFUL search for x. This is at most the number of element that collide with x plus one (to find x). Define X_{uv} to be 1 is i collides with j. We have that since $\mathcal{H}$ is a universal hash family, $\Pr(x \text{ collides with } y) = \frac{1}{m}$, therefore $\mathbf{E}[X_{ij}] - \frac{1}{m}$ for all i, and j.

$$\text{search time} \leq 1 + \sum_{y \neq x} X_{yx}$$

So,

$$\begin{aligned} \text{expected search time} &\leq \mathbf{E}[1 + \sum_{y \neq x} X_{yx}] \\ &= 1 + \sum_{y \neq x} \mathbf{E}[X_{yx}] && \text{linearity of expectation} \\ &= 1 + (n-1)\frac{1}{m} && \text{universal hash family} \end{aligned}$$

On the other hand, unsuccesful searches, we have:

$$\text{search time} \leq \sum_{y \neq x} X_{yx}$$

Therefore,

$$\begin{aligned} \text{expected search time} &\leq \mathbf{E}[\sum_{y \neq x} X_{yx}] \\ &= \sum_{y \neq x} \mathbf{E}[X_{yx}] && \text{linearity of expectation} \\ &= \frac{n}{m} && \text{universal hash family} \end{aligned}$$

□

2.a. One way to do this is as follows: Fix whatever value of $(ax + by) \bmod p$ you want, say 0. We will generate p distinct pairs (x_i, y_i) such that $ax_i + by_i = 0 \bmod p$. The key idea here is that $a^{p-1} = 1 \bmod p$ for any $a \neq 0 \bmod p$.

Here are the pairs:

$$\begin{aligned}
x_0 &= 0 \\
y_0 &= 0 \\
x_i &= ia^{p-2} \bmod p && \text{for } i = 1, \dots, p-1 \\
y_i &= -ib^{p-2} \bmod p && \text{for } i = 1, \dots, p-1
\end{aligned}$$

First, we check that

$$\begin{aligned}
(ax_i + bx_i) \bmod p &= (ia^{p-1} - ib^{p-1}) \bmod p \\
&= (ia^{p-1}) \bmod p - (ib^{p-1}) \bmod p \\
&= (i - i) \bmod p \\
&= 0
\end{aligned}$$

Next, we check that they are unique, If $ia^{p-2} = ja^{p-2} \bmod p$, then multiplying both sides by a, we have $i = j \bmod p$, therefore, they are all distinct. □

2.b. We have that for two distinct inputs (x, y), and (x', y'), and we would like to find all a and b such that $ax + by = ax' + by' \bmod p$, or

$$a(x - x') = b(y' - y) \bmod p. \tag{1}$$

Assume that, so $y' - y \neq 0 \bmod p$, so similarly to the previous problem, $(y' - y)^{p-1} = (1) \bmod p$. So, again, multiplying both sides of Equation 1 by $(y' - y)^{p-2}$, we have

$$\begin{aligned}
a(x - x')(y' - y)^{p-2} &= (b(y' - y)^{p-1}) \bmod p \\
&= (b) \bmod p
\end{aligned}$$

Therefore, one can fix any a, $b = a(x - x')(y' - y)^{p-2} \bmod p$ would satisfy Equation 1. Since there are exactly p ways to pick a, there are exactly p pairs (a, b) that satisfy the above equation.

□