Name: \_\_\_\_\_

1. [2 points] How many equivalence relations are there on  $\{1, 2, 3\}$ ?

2. [2 points] A 6-slot database uses a hashing strategy to store numbers; the hash function is  $h(x) = x \mod 6$ . Initially, the database is empty. Show a picture of the hash table after the numbers 843, 145, 1932, 533, 204 are inserted in the given order. Collisions are resolved by linear probing.

- 3. [2 points] Let  $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$ . We consider permutations on A.
  - (a) Let  $f = (25471) \circ (8742)$ . Express f as the composition of disjoint cycle permutations.

(b) Find the inverse  $f^{-1}$  in tabular form.

4. [2 points] Decide whether the given functions are one-to-one/injective, onto/surjective, or bijective. For each blank cell in the table, write "Yes" if the function has the property, and "No" otherwise. You do not need to show your work.

In the following, let  $A^*$  be the set of finite strings of *a*'s and *b*'s. For example, *aaba*, *bb*, and the empty string  $\lambda$  are all in  $A^*$ . Recall that  $\mathbb{N} = \{0, 1, 2, ...\}$  and  $\mathbb{Z}$  is the set of integers.

Function	one-to-one	onto	bijective
$f: \mathbb{Z} \to \mathbb{Z}$ where $f(x) = x + 6$			
$f: \mathbb{Z} \to \mathbb{Z}$ where $f(x) = x^2 - 1$			
$f: \mathbb{Z} \to \mathbb{Z}$ where $f(x) = x^3 - 1$			
$f\colonA^*\to{\rm I\!N}$ where $f(x)$ equals the length of $x$			
$f \colon A^* \to A^*$ where $f(x) = xx$			
$f \colon A^* \to A^*$ where $f(x)$ equals the reverse of $x$			

5. [2 points] In RSA, let p = 47 and q = 43. Then n = 2021 and  $\phi(n) = 1932$ . Pick e = 541. Use the Euclidean algorithm to find the value of d.