Math374 **Quiz #6** **15 November 2011**

Name: Solutions

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

1 part: $\{1,2,3\}$

2 parts: $12|3$, $1|23$, $13|2$

3 parts: $1|2|3$

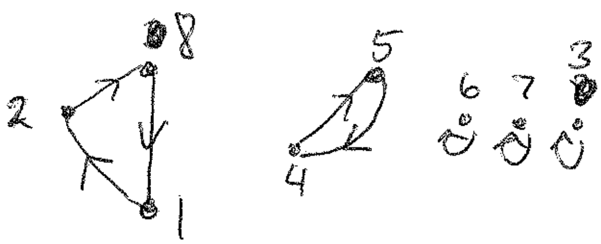
Total number: $\boxed{5}$

2. [**2 points**] A 6-slot database uses a hasing 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.

0	1	2	3	4	5
1932	145	204	843		533

3. [**2 points**] Let $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$. We consider permutations on A.

(a) Let $f = (2\ 5\ 4\ 7\ 1) \circ (\cancel{3}\ 8\ 7\ 4\ 2)$. Express f as the ~~disjoint union~~ composition of disjoint cycle permutations.



$$\boxed{\begin{array}{c} f = (1\,2\,8) \circ (4\,5) \\ \text{or} \\ f = (4\,5) \circ (1\,2\,8) \end{array}}$$

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

$$f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 1 & 3 & 5 & 4 & 6 & 7 & 2 \end{pmatrix}$$

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 λ are all in A^*. Recall that $\mathbb{N} = \{0, 1, 2, \ldots\}$ and $\mathbb{Z}$ is the set of integers.

Function	one-to-one	onto	bijective
$f\colon \mathbb{Z} \to \mathbb{Z}$ where $f(x) = x + 6$	Yes	Yes	Yes
$f\colon \mathbb{Z} \to \mathbb{Z}$ where $f(x) = x^2 - 1$	No	No	No
$f\colon \mathbb{Z} \to \mathbb{Z}$ where $f(x) = x^3 - 1$	Yes	No	No
$f\colon A^* \to \mathbb{N}$ where $f(x)$ equals the length of x	No	Yes	No
$f\colon A^* \to A^*$ where $f(x) = xx$	Yes	No	No
$f\colon A^* \to A^*$ where $f(x)$ equals the reverse of x	Yes	Yes	Yes

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.

Want: $d' \cdot 541 + f \cdot 1932 = 1$

$1932 = 3 \cdot 541 + 309$

$541 = 1 \cdot 309 + 232$

$309 = 1 \cdot 232 + 77$

$232 = 3 \cdot 77 + 1$

$1 = 232 - 3 \cdot 77$

$1 = 232 - 3(309 - 1 \cdot 232)$

$1 = 4 \cdot 232 - 3 \cdot 309$

$1 = 4(541 - 1 \cdot 309) - 3 \cdot 309$

$1 = 4 \cdot 541 - 7 \cdot 309$

$1 = 4 \cdot 541 - 7 \cdot (1932 - 3 \cdot 541)$

$1 = 25 \cdot 541 - 7 \cdot 1932$

So $d' = 25$ and $d = 25 \bmod 1932 = \boxed{25}$.