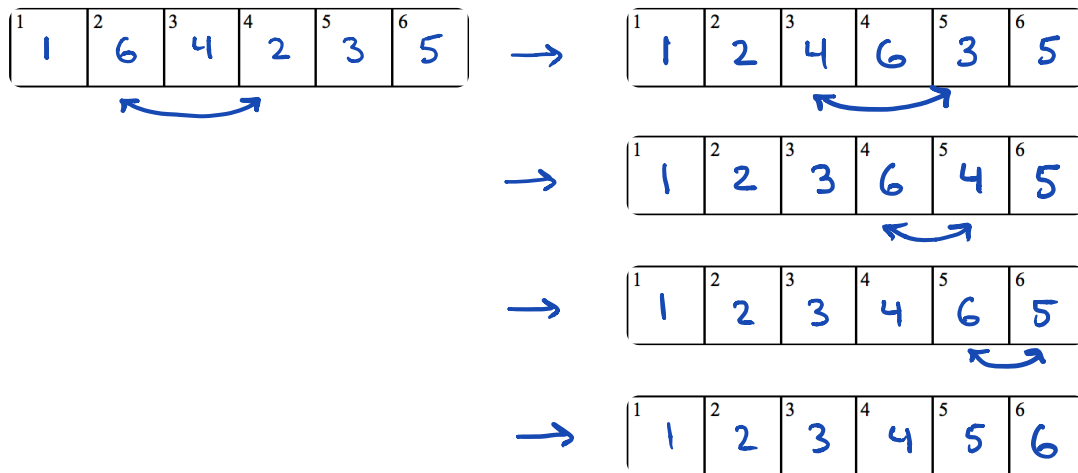


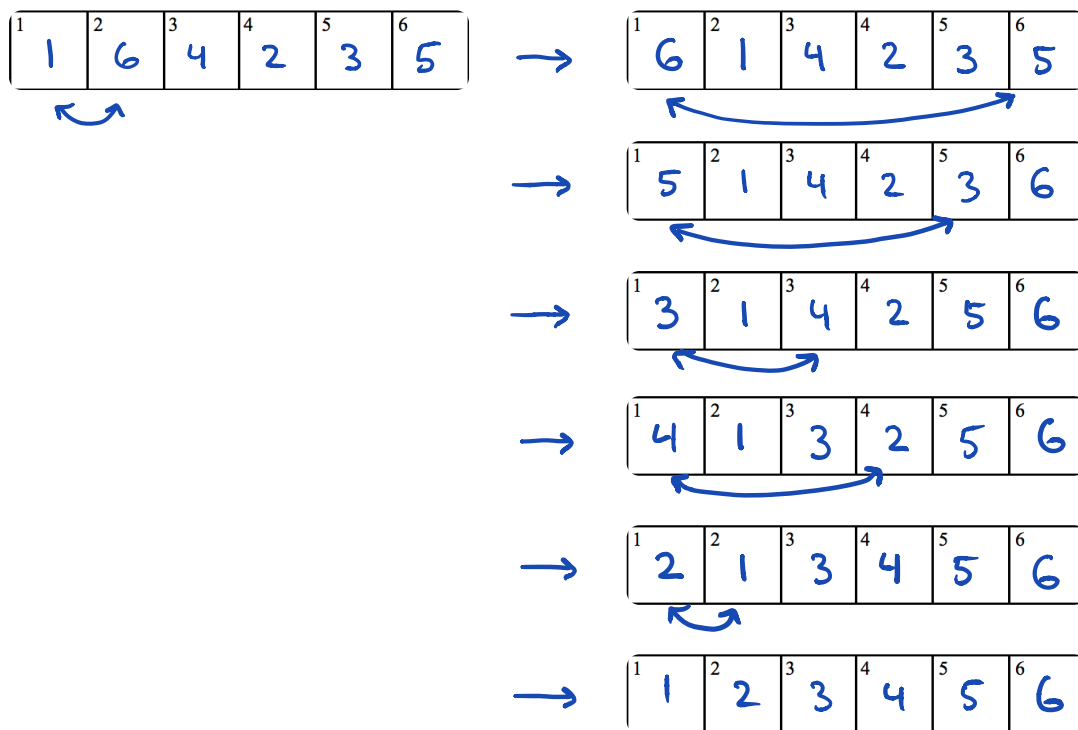
# Math 304 Assignment 1 - Solutions

(a) Legal moves : swap contents of any two boxes  
Here is one of many possible solutions :

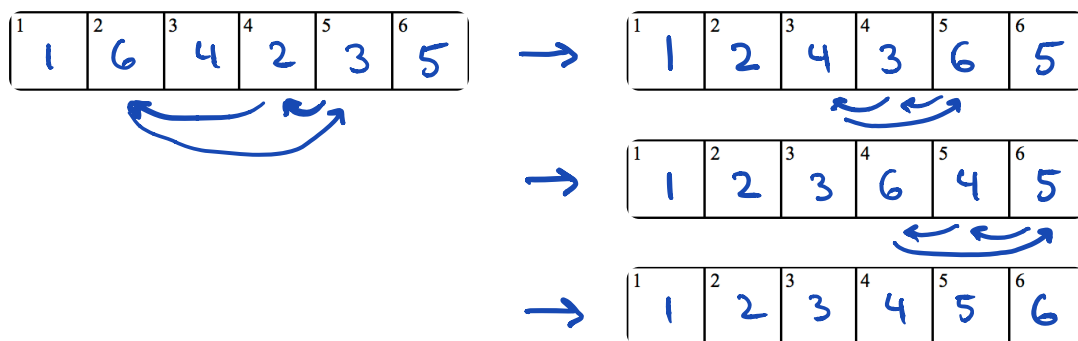


which is a solution using 4 moves.

(b) Legal moves : swap contents of any box with box 1 :



(c) Legal moves : 3-cycles



2. Legal moves : 3-cycles

$$(a) \quad \underline{264135} \rightarrow \underline{164325} \rightarrow \underline{124635} \rightarrow 123465$$

←
←
←

Which is the desired arrangement.

$$(b) \quad \underline{264135} \rightarrow \underline{614235} \rightarrow 612345 \text{ . Which is the arrangement.}$$

←
←

(c) We already know from (a) that we can put it in the order 123465. So if we can swap 6 and 5 by a sequence of 3-cycles then we are done. However, this seems impossible. (will develop the tools to show this is impossible shortly.)

3. (a)  $\{0, 2\}$   
 (b)  $\{0, 3, 6, 9, 12, 15, 18, 21, 24\}$   
 (c)  $\{7, 13, 19\}$

4. Since  $d|a, b$  then there exists integers  $k, l$  such that  
 $a = kd$  and  $b = ld$ .

Then

$$a + b = kd + ld = (k+l)d$$

which means  $d | a + b$ .

5. (a) 306, 702

Euclidean Alg.:

$$\begin{aligned} \gcd(702, 306) &= \gcd(306, 90) \\ &= \gcd(90, 36) \\ &= \gcd(36, 18) \\ &= \gcd(18, 0) \\ &= 18 \end{aligned}$$

$$\therefore \gcd(702, 306) = 18 \quad \text{and} \quad 7(702) - 16(306) = 18$$

Extended Euclidean Alg.:

$$\begin{aligned} 702 &= 2 \cdot 306 + 90 \\ 306 &= 3 \cdot 90 + 36 \\ 90 &= 2 \cdot 36 + 18 \\ 36 &= 2 \cdot 18 + 0 \end{aligned}$$

$18 = 90 - 2(36)$   
 $= 90 - 2(306 - 3 \cdot 90)$   
 $= 7(90) - 2(306)$   
 $= 7(702 - 2(306)) - 2(306)$   
 $= 7(702) - 16(306)$

(b) 888, 3071

Euclidean Alg.:

$$\begin{aligned} \gcd(3071, 888) &= \gcd(888, 407) \\ &= \gcd(407, 74) \\ &= \gcd(74, 37) \\ &= \gcd(37, 0) \\ &= 37 \end{aligned}$$

$$\therefore \gcd(3071, 888) = 37 \quad \text{and} \quad 11(3071) - 38(888) = 37$$

Extended Euc. Alg.:

$$\begin{aligned} 3071 &= 3(888) + 407 \\ 888 &= 2(407) + 74 \\ 407 &= 5(74) + 37 \\ 74 &= 2 \cdot 37 + 0 \end{aligned}$$

$37 = 407 - 5(74)$   
 $= 407 - 5(888 - 2(407))$   
 $= 11(407) - 5(888)$   
 $= 11(3071 - 3(888)) - 5(888)$   
 $= 11(3071) - 38(888)$

6. Let  $\gcd(a,b) = d$ .

Suppose  $g = \gcd(a/d, b/d)$ . Then  $g|a/d$  and  $g|b/d$ .

Therefore,

$$gd|a \quad \text{and} \quad gd|b$$

Since  $gd$  is a common divisor of  $a$  and  $b$ , but  $d$  is the greatest such common divisor, then

$$gd \leq d.$$

It follows that  $g=1$ , hence  $\gcd(a/d, b/d) = 1$ .

7. If there were integers  $x, y$  such that

$$1034x + 444y = 1$$

then since the LHS is even (divisible by 2) it must follow that the RHS is even. But 1 is odd, thus we have a contradiction. Therefore, no such integers  $x$  and  $y$  exist.

8. No. For example,  $6|2 \cdot 3$  but  $6 \nmid 2$  and  $6 \nmid 3$ .

9. (a) Let  $\gcd(a,b) = d$  and suppose  $c|a, b$ .

Then by the Ext. Euclidean Alg there exists integers  $u, v$  such that

$$au + bv = d.$$

Since  $c|a, b$  then  $c|au + bv \Rightarrow c|d$ .

(b) Let  $d|ab$  and  $\gcd(d,a) = 1$ .

Then by the Ext. Euclidean Alg. there exists integers  $u, v$  such that

$$du + av = 1.$$

Multiplying by  $b$  we get:

$$bd u + abv = b.$$

Since  $d$  divides each term on the LHS (i.e.  $d|bd u$  &  $d|abv$ ) then  $d$  divides the LHS. Hence  $d$  divides the RHS, so

$$d|b.$$

$$10. \quad \phi(42) = \phi(2 \cdot 3 \cdot 7) = (2-1)(3-1)(7-1) = 1 \cdot 2 \cdot 6 = 12$$

$$\phi(420) = \phi(2^2 \cdot 3 \cdot 5 \cdot 7) = 2^1(2-1)(3-1)(5-1)(7-1) = 2(2)(4)(6) = 96$$

$$\phi(4200) = \phi(2^3 \cdot 3 \cdot 5^2 \cdot 7) = 2^2(2-1)(3-1)5(5-1)(7-1) = 2^2 \cdot 2 \cdot 5 \cdot 4 \cdot 6 = 960$$

$$11. \quad 1848 \equiv 1914 \pmod{m} \quad \Leftrightarrow m | 1914 - 1848 = 66$$

$$\Leftrightarrow m = 1, 2, 3, 6, 11, 22, 33, 66.$$

12. We want to find  $3^{2027} \pmod{10}$  and  $3^{2027} \pmod{100}$ .

mod 10: First notice that

$$3^2 \equiv 9 \pmod{10}$$

$$3^3 \equiv 7 \pmod{10}$$

$$3^4 \equiv 1 \pmod{10}$$

$\rightarrow$  this is the useful congruence.

Now,

$$\begin{aligned} 3^{2027} &= 3^{4 \cdot 506 + 3} \\ &= (3^4)^{506} 3^3 \\ &\equiv 1^{506} \cdot 3^3 \pmod{10} \\ &\equiv 7 \pmod{10} \end{aligned}$$

Therefore, the ones digit of  $3^{2027}$  is 7.

mod 100: First notice that  $3^{20} \equiv 1 \pmod{100}$  (this is the smallest power with this property).

Now,

$$\begin{aligned} 3^{2027} &= 3^{20(101) + 7} \\ &= (3^{20})^{101} 3^7 \\ &\equiv 1^{101} 3^7 \pmod{100} \\ &\equiv 2187 \pmod{100} \\ &\equiv 87 \pmod{100} \end{aligned}$$

Therefore, the last two digits are 87.

13. We wish to determine  $1 + 2 + 2^2 + 2^3 + \dots + 2^{2020} + 2^{2021} \pmod{3}$ .

First observe  $2^2 \equiv 1 \pmod{3}$ , therefore,

$$2^m \equiv \begin{cases} 1 \pmod{3} & \text{if } m \text{ even} \\ 2 \pmod{3} & \text{if } m \text{ odd} \end{cases}$$

Therefore,

$$\begin{aligned} 1 + 2 + 2^2 + 2^3 + \dots + 2^{2020} + 2^{2021} &\equiv 1 + 2 + 1 + 2 + \dots + 1 + 2 \pmod{3} \\ &\quad \rightarrow \text{there are 1011 1's and 1011 2's listed here} \\ &\equiv (1011)1 + (1011)2 \pmod{3} \\ &\equiv 3(1011) \pmod{3} \\ &\equiv 0 \pmod{3} \end{aligned}$$

$\therefore 1 + 2 + 2^2 + \dots + 2^{2021}$  is divisible by 3.