Math 304 Assignment 1 – Solutions

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

1	2	3	4	5	6
1	6	4	2	3	5

→

1	2	3	4	5	6
1	2	4	6	3	5

→

1	2	3	4	5	6
1	2	3	6	4	5

→

1	2	3	4	5	6
1	2	3	4	6	5

→

1	2	3	4	5	6
1	2	3	4	5	6

which is a solution using 4 moves.

(b) Legal moves: swap contents of any box with box <u>1</u>:

1	2	3	4	5	6
1	6	4	2	3	5

→

1	2	3	4	5	6
6	1	4	2	3	5

→

1	2	3	4	5	6
5	1	4	2	3	6

→

1	2	3	4	5	6
3	1	4	2	5	6

→

1	2	3	4	5	6
4	1	3	2	5	6

→

1	2	3	4	5	6
2	1	3	4	5	6

→

1	2	3	4	5	6
1	2	3	4	5	6

(c) Legal moves: 3-cycles

1	2	3	4	5	6
1	6	4	2	3	5

→

1	2	3	4	5	6
1	2	4	3	6	5

→

1	2	3	4	5	6
1	2	3	6	4	5

→

1	2	3	4	5	6
1	2	3	4	5	6

2. Legal moves : 3-cycles

(a) 264135 $\rightarrow$ 164325 $\rightarrow$ 124635 $\rightarrow$ 123465

which is the desired arrangement.

(b) 264135 $\rightarrow$ 614235 $\rightarrow$ 612345 . 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 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 $d \mid a, b$ then there exists integers k, ℓ such that

$$a = kd \quad \text{and} \quad b = \ell d .$$

Then

$$a+b = kd + \ell d = (k+\ell)d$$

which means $d \mid a+b$.

5. (a) 306, 702

Euclidean Alg.:

$\gcd(702, 306)$
$= \gcd(306, 90)$
$= \gcd(90, 36)$
$= \gcd(36, 18)$
$= \gcd(18, 0)$
$= 18$

$702 = 2 \cdot 306 + 90$
$306 = 3 \cdot 90 + 36$
$90 = 2 \cdot 36 + 18$
$36 = 2 \cdot 18 + 0$

Extended Euclidean Alg:

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

$\therefore \gcd(702, 306) = 18$ and $7(702) - 16(306) = 18$.

(b) 888, 3071

Euclidean Alg:

$\gcd(3071, 888)$
$= \gcd(888, 407)$
$= \gcd(407, 74)$
$= \gcd(74, 37)$
$= \gcd(37, 0)$
$= 37$

$3071 = 3(888) + 407$
$888 = 2(407) + 74$
$407 = 5(74) + 37$
$74 = 2 \cdot 37 + 0$

Extended Euc. Alg:

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

$\therefore \gcd(3071, 888) = 37$ and $11(3071) - 38(888) = 37$.

6. Let $\gcd(a,b)=d$.
Suppose $g=\gcd(a/d, b/d)$. Then $g \mid a/d$ and $g \mid b/d$.
Therefore,
$$gd \mid a \quad \text{and} \quad gd \mid b$$
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, $6 \mid 2\cdot 3$ but $6 \nmid 2$ and $6 \nmid 3$.

9. (a) Let $\gcd(a,b)=d$ and suppose $c \mid a, b$.
Then by the Ext. Euclidean Alg there exists integers u, v such that
$$au + bv = d.$$
Since $c \mid a, b$ then $c \mid au+bv \Rightarrow c \mid d$.

(b) Let $d \mid ab$ 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:
$$bdu + abv = b.$$
Since d divides each term on the LHS (i.e. $d \mid bdu$ & $d \mid abv$) then d divides the LHS. Hence d divides the RHS, so
$$d \mid b.$$

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

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

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

11. $1848 \equiv 1914 \bmod m \iff m \mid 1914-1848 = 66$
$\iff m = 1, 2, 3, 6, 11, 22, 33, 66.$

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

mod 10: First notice that

$$3^2 \equiv 9 \bmod 10$$
$$3^3 \equiv 7 \bmod 10$$
$$3^4 \equiv 1 \bmod 10 \quad \rightsquigarrow \text{this is the useful congruence.}$$

Now,

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

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

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

Now,

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

Therefore, the last two digits are 87.

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

First observe $2^2 \equiv 1 \bmod 3$, therefore,

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

Therefore,

$$1+2+2^2+2^3+\cdots+2^{2020}+2^{2021} \equiv 1+2+1+2+\cdots+1+2 \bmod 3$$

↳ there are 1011 1's and 1011 2's listed here

$$\begin{aligned} &\equiv (1011)1 + (1011)2 \bmod 3 \\ &\equiv 3(1011) \bmod 3 \\ &\equiv 0 \bmod 3 \end{aligned}$$

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