HW0 SOLUTION

JI ZENG

Problem.A

For (a), we have $a = 1 \cdot a$.

For (b), $a|b$ and $b|c$ give integers p, q s.t.(such that) $b = pa$ and $c = qb$, then there's integer, namely pq, s.t. $c = (pq)a$. So $a|c$.

Now suppose $a|b$ and $b|a$, it's not necessary that $a = b$. A counterexample is $a = 1$ and $b = -1$. Clearly $a|b$ as $b = (-1) \cdot a$ and $b|a$ as $a = (-1) \cdot b$.

Problem.B

(a) $2019 = 17 \cdot 118 + 13$.

(b) $d|b$ and $d|a$ means there're integers m, n s.t. $b = md$ and $a = nd$. Then by $b = qa + r$, we have $r = b - qa = md - qnd = (m - qn)d$, which implies $d|r$.

(c) Write $g = gcd(221, 143)$. Notice $221 = 1 \cdot 143 + 78$, so by (b) $g|78$. Notice $78 = 2 \cdot 3 \cdot 13$, so g may only contain $\{2, 3, 13\}$ as factors (with multiplicity one). Notice $2 \not| 143$, $3 \not| 143$ and $13|143$. So $g = 13$.

To get wanted x, y, we apply the Euclid algorithm,

$$\begin{aligned} 221 &= 1 \cdot 143 + 78, \\ 143 &= 1 \cdot 78 + 65, \\ 78 &= 1 \cdot 65 + 13. \end{aligned}$$

Hence

$$\begin{aligned} 13 &= 78 - 1 \cdot 65 \\ &= 78 - (143 - 1 \cdot 78) \\ &= (221 - 1 \cdot 143) - (143 - (221 - 1 \cdot 143)) \\ &= 2 \cdot 221 - 3 \cdot 143. \end{aligned}$$

Problem.C

(a) $2, 3, 5, 7, 11, 13, 17, 19$.

(b) $60 = 2 \cdot 2 \cdot 3 \cdot 5$.

(c) No there isn't. Use the binomial theorem

$$4^n = (3+1)^n = \sum_{i=0}^{n} \binom{n}{i} 3^i.$$

We have $4^n - 1 = \sum_{i=1}^{n} \binom{n}{i} 3^i$ so clearly $3|4^n - 1$ and $3 < 4^n - 1$. So $4^n - 1$ isn't a prime.

Problem.D

(a) For $n = 1$, the identity degenerates to $1 = 1$.

Suppose now that the identity is proved for n, let's consider $n+1$,

$$\begin{aligned}\frac{x^{n+1}-1}{x-1} &= \frac{x^{n+1}-x^n+x^n-1}{x-1}\\ &= \frac{x^{n+1}-x^n}{x-1}+\frac{x^n-1}{x-1}\\ &= x^n+\frac{x^n-1}{x-1}\\ &= x^n+x^{n-1}+x^{n-2}+\cdots+1, \text{ by induction hypothesis.}\end{aligned}$$

Hence we conclude the proof.
(b) Apply the identity to $x=6$, we have $6^n-1=(\sum_{i=0}^{n-1}6^i)\cdot 5$, as wanted.

Problem.E
(a) $|A|=8$ and $|B|=6$.
(b) $A\cup B=\{1,2,3,4,5,7,11,13,17,18,19\}$.
$A\cap B=\{3,11,17\}$.
(c) There're $2^{|B|}=2^6$ subsets.
(d) Only (v) is true.

Problem.F
To verify $GL(N,\mathbb{R})$ is a group, we need to verify:
1. Multiplication is associative: this is because matrix multiplication is associative. (You should learned this in your linear algebra course.)
2. Existence of identity: the identity matrix $I\in GL(N,\mathbb{R})$ serves the group identity.
3. Existence of inverses: for any matrix $A\in GL(N,\mathbb{R})$, by definition A is invertible. So A^{-1} exists and is in $GL(N,\mathbb{R})$.

(a) Firstly we verify the identity for $n\geq 0$ by induction. For $n=0,1$, this is trivial. Suppose we have verified the identity for n, and we consider for $n+1$, then

$$\begin{aligned}\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}^{n+1} &= \begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}^{n}\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}\\ &= \begin{pmatrix}1 & na\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}\\ &= \begin{pmatrix}1 & (n+1)a\\ 0 & 1\end{pmatrix}, \text{ by matrix computation.}\end{aligned}$$

Now we verify the identity for $n=-1$, which requires as to show that $\begin{pmatrix}1 & -a\\ 0 & 1\end{pmatrix}=\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}^{-1}$. Indeed, by matrix multiplication, $\begin{pmatrix}1 & -a\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$.
Then we verify the identity for $n\leq -1$, write $n=-m$ for some $m\geq 1$. Then

$$\begin{aligned}\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}^{n} = \begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}^{-1\cdot m} &= \begin{pmatrix}1 & -a\\ 0 & 1\end{pmatrix}^{m}\\ &= \begin{pmatrix}1 & m(-a)\\ 0 & 1\end{pmatrix}, \text{ apply above identity with } -a \text{ and } m\geq 1\end{aligned}$$

$$= \begin{pmatrix} 1 & na \\ 0 & 1 \end{pmatrix},$$

as wanted.

(b) Consider the rotation matrix $A_\theta = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$ with $\theta = \frac{2\pi}{n}$. We know that i-th time rotation of angel θ is equivalent to rotation of $i\theta$. So $A_\theta^i = A_{i\theta}$ for all $i \in \mathbb{N}$. We also know that identity is exactly rotation of angel 2π. So $A_\theta^n = I$ and $A_\theta^i \neq I$ for $i = 1, \ldots, n-1$.