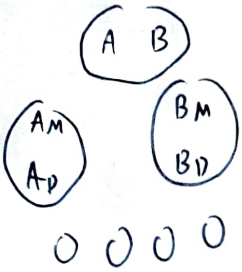
Zhuang Jianning TO3A

A0214561M

Q1 a) i.



Let Aiken and Betty, Aiken's parents, Betty's parents each be 1 unit

Together with the other 4 relatives, there are 7 units

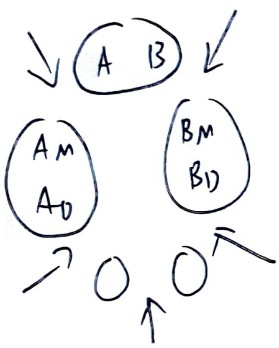
7 units can be arranged in a circle in $(7-1)!$ ways.

Within the units with 2 people, there are $2!$ ways to arrange themselves within the unit

Hence, total number of ways $= 6! \times 2! \times 2! \times 2!$

$= \underline{5760}$ //

ii.



Excluding Uncle Pete and Aunt Jemima first

There are $(5-1)!$ ways to arrange the other 5 units in (i.)

There are 5 spaces between the 5 units, which can be occupied by Uncle Pete and Aunt Jemima in ${}^5P_2$ ways.

3 of the units are still made up of pairs of people.

Hence, total number of ways $= 4! \times 2! \times 2! \times 2! \times 5 \times 4$

$= \underline{3840}$ //

b) i.

The number of size r multisets selected from a set of n elements is $\binom{r+n-1}{r}$

$r = 6$, $n = 4$

Hence, total ways to buy food for the Flaming Six $= \binom{6+4-1}{6}$

$= \underline{84}$ //

ii. combinations that are not permissible ① 0 vegetarian 6 meat
② 1 vegetarian 5 meat

2 vegetarian options, 2 meat options.

case ① ways to choose 0 vegetarian $= \binom{0+2-1}{0} = 1$

ways to choose 6 meat $= \binom{6+2-1}{6} = 7$

total ways $= 1 \times 7 = 7$

case ② ways to choose 1 vegetarian $= \binom{1+2-1}{1} = 2$

ways to choose 5 meat $= \binom{5+2-1}{5} = 6$

total ways $= 2 \times 6 = 12$

ways to buy food considering 2 vegetarian = total ways − case ① − case ②

$= 84 - 7 - 12$

$= \underline{\underline{65}}$

2. 1. Let $a \in \mathbb{Z}_{\geq 2}$. Suppose that $\forall m, n \in \mathbb{Z}^+$, if $a | mn$, then $a | m$ or $a | n$

2. a is either composite or prime

2.1 Case 1: a is composite

2.1.1 Then $\exists m' \in \mathbb{Z}^+$ such that m' is a divisor of a with $1 < m' \leq \sqrt{a}$ (Theorem 7.15)

2.1.2 Then $\exists n' \in \mathbb{Z}^+$ such that $a = m'n'$ and $\sqrt{a} \leq n' < a$ (Definition 7.1)

2.1.3 Then $a | m'n'$ and $|a| = |m'||n'|$

2.1.4 $|a| > |m'|$ as $|n'| > 1$ and $|a| > |n'|$ as $|m'| > 1$

2.1.5 If $|a| > |m'|$ and $|a| > |n'|$ then $(a \nmid m'$ or $m' = 0)$ and $(a \nmid n'$ or $n' = 0)$ (contrapositive of Theorem 7.4)

2.1.6 $|m'| \neq 0$ and $|n'| \neq 0$

2.1.7 Hence $\exists m', n' \in \mathbb{Z}^+$ such that $a \nmid m'$ and $a \nmid n'$.

2.1.8 As this a contradiction, a cannot be composite.

2.2 Case 2: a is prime

2.2.1 Then $\forall m \in \mathbb{Z}^+$, $\gcd(a,m) = 1$ or $\gcd(a,m) = a$ (Definition of prime and gcd)

2.2.2 $\forall n \in \mathbb{Z}^+$, if $a|mn$ and $\gcd(a,m) = 1$, then $a|n$ (Theorem 8.3)

2.2.3 $\forall n \in \mathbb{Z}^+$, if $a|mn$ and $\gcd(a,m) = a$, then $a|m$ (Definition of gcd)

2.2.4 From 2.2.2 and 2.2.3, $\forall m, n \in \mathbb{Z}^+$, if $a|mn$, then $a|m$ or $a|n$

2.2.5 a can be prime

3. From case 1 and case 2, a must be prime.

3. $42x + 15y = 6$

a	b	$\text{rem}(a,b) = a - kb$	
42	15	12	$= 42 - 2 \cdot 15$
15	12	3	$= 15 - 1 \cdot 12$ $= 15 - 1 \cdot (42 - 2 \cdot 15)$ $= 3 \cdot 15 - 1 \cdot 42$
12	$\boxed{3}$	0	

$\gcd(42, 15) = 3$. Thus, Bezout's lemma tells us that 3 is an integer linear combination of 42 and 15

From Euclidean Algorithm above, $3 = -1 \cdot 42 + 3 \cdot 15$

$$6 = -2 \cdot 42 + 6 \cdot 15$$

Hence, integers (x,y) that satisfy $42x + 15y = 6$ are $(-2, 6)$

$$6 = 42(-2) + 15(6) + 42(15k) - 15(42k)$$
$$= 42(-2+15k) + 15(6-42k)$$

$(x,y) = (-2+15k,\ 6-42k)$ $\forall k \in \mathbb{Z}$ (family of solutions)

4. a) 1. ("Reflexivity")

1.1 Let $x \in \{0, 1, \dots, n-1\}$ and $a \in \{1, 2, \dots, n-1\}$

1.2 Then $(ax - ax) = 0$

1.3 $\forall n \in \mathbb{Z}_{\geq 2}$, $n \mid 0$ (Theorem 7.2)

1.4 Thus $n \mid (ax - ax)$

1.5 Hence $ax \equiv ax \pmod{n}$ (definition of congruence relation)

2. ("Symmetry")

2.1. Let $x, y \in \{0, 1, \dots, n-1\}$ and $a \in \{1, 2, \dots, n-1\}$ such that xRy

2.2. Then $ax \equiv ay \pmod{n}$ (definition of R)

2.3 Thus $n \mid (ax - ay)$ (definition of congruence relation)

2.4 Thus $\exists k \in \mathbb{Z}$ such that $(ax - ay) = kn$ (definition of divides)

2.5 Then $(ay - ax) = -kn$

2.6 Thus $n \mid (ay - ax)$ (definition of divides)

2.7 Hence $ay \equiv ax \pmod{n}$ (definition of congruence relation)

b) $n = 4$

i) 0 —— 2 $\qquad 4 \mid (2 \cdot 0 - 2 \cdot 2) \Rightarrow 0R2$, $2R0$

1 —— 3 $\qquad 4 \mid (2 \cdot 1 - 2 \cdot 3) \Rightarrow 1R3$, $3R1$

ii) R is reflexive and symmetric $\forall n \in \mathbb{Z}_{\geq 2}$ (part a)

R is also transitive as $\forall x, y, z \in \{0, 1, 2, 3\}$, $xRy \wedge yRz \rightarrow xRz$

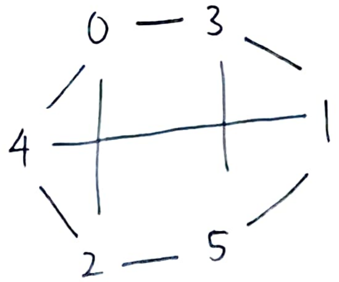
$0R0 \wedge 0R0 \rightarrow 0R0$	$2R0 \wedge 0R0 \rightarrow 2R0$	$1R1 \wedge 1R1 \rightarrow 1R1$	$3R1 \wedge 1R1 \rightarrow 1R1$
$0R0 \wedge 0R2 \rightarrow 0R2$	$2R0 \wedge 0R2 \rightarrow 2R2$	$1R1 \wedge 1R3 \rightarrow 1R3$	$3R1 \wedge 1R3 \rightarrow 3R3$
$0R2 \wedge 2R0 \rightarrow 0R0$	$2R2 \wedge 2R0 \rightarrow 2R0$	$1R3 \wedge 3R1 \rightarrow 1R1$	$3R3 \wedge 3R1 \rightarrow 3R1$
$0R2 \wedge 2R2 \rightarrow 0R2$	$2R2 \wedge 2R2 \rightarrow 2R2$	$1R3 \wedge 3R3 \rightarrow 1R3$	$3R3 \wedge 3R3 \rightarrow 3R3$

$[0]_R = \{0, 2\}$

$[1]_R = \{1, 3\}$

c) $n = 6$

i)



ii) R is reflexive and symmetric $\forall n \in \mathbb{Z}_{\geq 2}$ (part a)

However, it is not transitive because $0 R 2$ and $2 R 5$ but $0 \not R 5$. Hence, it is not transitive and not an equivalence relation.

5.

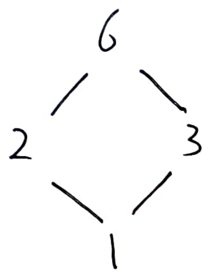
1. Let $B = A$ and f be the identity function on A
2. Then, $f : A \to A$ can be defined such that $\forall x \in A$, $f(x) = x$
3. As the identity function is bijective, it is both injective and surjective
4. Hence f is surjective
5. Let $\mathcal{C}$ be a partition of A such that it is made up of sets of the individual elements of A $\{\{a_1\}, \{a_2\} \dots \{a_n\}\}$ (mutually disjoint and $\bigcup_{1}^{n}\{a_i\} = A$ i
6. Thus $\mathcal{C} = \{\{x \in A : i_A(x) = x\} : x \in A\}$
7. Hence, there exists a set $B = A$ and surjective function $f : A \to B$ such that $\mathcal{C} = \{\{x \in A : f(x) = y\} : y \in B\}$

6. a)

$a = 8$

$D_a = \{1, 2, 4, 8\}$

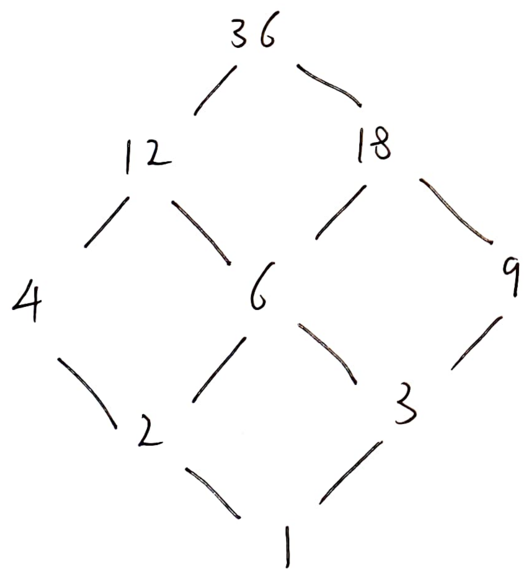
b)



$b = 6$

$D_b = \{1, 2, 3, 6\}$

c)



$c = 36$

$D_c = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$

* odd number of divisors $\Rightarrow$ square number