1. (a) CS70 $\leftrightarrow$ A

CS61A $\leftrightarrow$ C

CS61B $\leftrightarrow$ B

(b) CS70 $\leftrightarrow$ B

CS61A: $\leftrightarrow$ C

CS61B $\leftrightarrow$ A

(c) CS70 $\leftrightarrow$ A, C

CS61A $\leftrightarrow$ D

CS61B $\leftrightarrow$ B

(d) Moving D out of his 1st preference (CS61A) is undesirable, so we cannot swap D.

This leaves the swaps (A, B), and (C, B), but (A, B) is undesirable to CS70, and (C, B) is also undesirable to CS70.

2. After using the algorithm,

We have

(Jerry, Megan)

(Sam, Eric)

(Angelina, Lucy)

J	~~E~~	M	L	~~S~~	~~A~~
E	~~M~~	S	~~J~~	~~A~~	~~L~~
S	~~J~~	~~M~~	E	L	A
L	~~L~~ A	J	E	S	M
M	J	A	~~E~~	~~L~~	~~S~~
A	S	L	~~M~~	~~J~~	~~E~~

3.

(a) $2x = 14, \quad x = 7$

$2y = 4, \quad y = 2$

(b) $x + y \equiv 4 \pmod 5$

(c) $x - y \equiv 0 \pmod 5$

(d) $4(x+y) - (x-y) = 4 \cdot 4 - 0 \mod (5)$

$3x \equiv 1 \pmod 5$

(e) $x \equiv 2 \pmod 5$

(f) $(x+y) - (x-y) \equiv 4 - 0 \pmod 5$

$2y \equiv 4 \mod (5)$

(g) $y \equiv 2 \mod (5)$

(h) $y \equiv 2 \mod (5)$ and $y = 2$

(i) They're the same in mod 5.

(j) No, but it is mod 5.

4. (a) After calculation,

$d = 1$, $a = -2$, $b = 3$

where $31a + 21b = d$.

(b) To make coefficients positive

we first have

$(a, b) = (-2020, 3030)$ as a solution,

and then have

$a = -2020 + 21 \cdot 97$, $b = 3030 - 31 \cdot 97$

$a = 17$

$b = 23$

(c) Since all solutions are a shift of either

$(a+21, b-31)$ or $(a-21, b+31)$,

$(a, b) = (17, 23)$ is the only solution that doesn't result in negative values.

5. (a) Pour full #5 into #3, resulting in 2-ounces in #5.

Pour the 2-ounces into #3. Then pour full #5 into #3, resulting in 4 ounces.

(b) Keep pouring full a's into the p-tumbler.

If the next pour will overfill p, fill up p and dump the full p-tumbler, and then pour remaining contents of a-tumbler into p.

Apply the algorithm again.

The contents inside p will be of the form $ka \pmod p$, which will cycle through all values of $\{0,1,2,\ldots,p\}$ in some order.

~~Take the set G of all numbers coprime to~~

6. Note that the map ~~[illegible]~~

$\{x : x \in S_n\} \rightarrow \{xa\}$

multiplying all elements in S_n is a ~~[illegible]~~ bijection to itself, because two elements mapping to the same element implies $xa \equiv \cancel{y}a \mod (n)$, which implies $x \equiv y \pmod{n}$ because a is coprime.

Then taking the product of ~~[illegible]~~ each set's elements gives the same value, or

$a^{|S_n|} \cdot P \equiv P \pmod{n}$, $\iff$ $a^{|S_n|} \equiv 1 \pmod{n}$

because P is coprime to n, as it is the product of coprime elements

7. (a) $(p-1)(q-1)$ must be coprime to 3,

so p, q are of form $3k+2$.

(b) $(x^{17})^d \equiv x \mod (37 \cdot 13)$,

or

$17d \equiv 1 \mod (36 \cdot 12)$

solving gives $d = 305$

(c) $91 \equiv x^{17} \mod (37 \cdot 13)$,

$91^{305} \equiv x \mod (37 \cdot 13)$,

$x \equiv 13 \mod (37 \cdot 13)$

(d) $8^{25} \mod (7 \cdot 3) \equiv 8 \mod (7 \cdot 3)$

(e) since $x^{p-1} \equiv 1 \mod (p)$, this implies from FLT,

we can subtract multiples of $p-1$ on the exponent,

so $x^e \equiv x^{k(p-1)+1} \equiv x^1 \mod (p)$.

similarly $x^e \equiv x^{l(q-1)+1} \equiv x^1 \mod (q)$,

so by CRT, $x^e \equiv x^1 \mod (pq)$.