# Practice problems for Test 1

## Solutions

1. (a) $85 = 51 \cdot 1 + 34$
   $51 = 34 \cdot 1 + 17$
   $34 = 17 \cdot 2$
   So $(51, 85) = 17$.

   (b) $17 = 51 - 34 \cdot 1 = 51 - (85 - 51 \cdot 1) \cdot 1 = 51 - 85 + 51 \cdot 1 = 51 \cdot 2 - 85$
   Thus $d = 51 \cdot 2 + 85(-1)$, so $m = 2$ and $n = -1$.

2. $(\Rightarrow)$
   $b|a \Rightarrow a = bc$ for some integer $c$.
   Then $x \in a\mathbb{Z} \Rightarrow x = am$ for some $m \in \mathbb{Z} \Rightarrow x = bcm = b(cm) \Rightarrow x \in b\mathbb{Z}$.
   $(\Leftarrow)$
   $a\mathbb{Z} \subset b\mathbb{Z} \Rightarrow a = a \cdot 1 \in b\mathbb{Z} \Rightarrow a = bm$ for some $m \in \mathbb{Z} \Rightarrow b|a$.

3. (a) $15x \equiv 21 (\text{mod } 24)$
   Since $(15, 24) = 3$ and $3|21$, this congruence has 3 solutions mod 24, which are congruent mod 8.
   Divide by 3: $5x \equiv 7 (\text{mod } 8)$
   Again, we see that since $(5, 8) = 1$, this congruence has a unique solution mod 8.
   Multiply by 5 (which is the inverse of $[5]_8$): $25x \equiv 35 (\text{mod } 8)$
   Reduce: $x \equiv 3 (\text{mod } 8)$.

   (b) $15x \equiv 8 (\text{mod } 24)$
   Since $(15, 24) = 3$ and $3 \nmid 8$, this congruence has no solutions.

4. $x \equiv 6 (\text{mod } 25)$, $x \equiv 2 (\text{mod } 11)$.
   Since $(25, 11) = 1$, by the Chinese Remainder Theorem the system has a unique solution modulo $25 \cdot 11 = 275$.
   $25 = 11 \cdot 2 + 3$
   $11 = 3 \cdot 3 + 2$
   $3 = 2 \cdot 1 + 1$
   $1 = 3 - 2 \cdot 1 = 3 - (11 - 3 \cdot 3) \cdot 1 = 3 - 11 \cdot 1 + 3 \cdot 3 = 3 \cdot 4 - 11 \cdot 1 = (25 - 11 \cdot 2) \cdot 4 - 11 \cdot 1 = 25 \cdot 4 - 11 \cdot 8 - 11 \cdot 1 = 25 \cdot 4 - 11 \cdot 9$.
   Now, $2 \cdot 25 \cdot 4 - 6 \cdot 11 \cdot 9 = 200 - 594 = -394$ is a solution.
   Since $-394 \equiv 156 (\text{mod } 275)$, we can write the answer as $x \equiv 156 (\text{mod } 275)$.

5. (a) $\phi(n)$ is the number of positive integers less than or equial to $n$ that are relatively prime to $n$.

   (b) List all positive integers from 1 to 15, and exclude those which are not relatively prime to 15, that is, which are divisible by 3 or 15.
   All: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15
   Divisible by 3: 3, 6, 9, 12, 15
   Divisible by 5: 5, 10, 15
   The rest are relatively prime to 15: 1, 2, 4, 7, 8, 11, 13, 14 - there are 8 integers in this list, therefore $\phi(15) = 8$.

   (c) $\phi(pq) = pq\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right) = pq\frac{p-1}{p}\frac{q-1}{q} = (p-1)(q-1) = pq - p - q + 1.$

6. $[101]^2_{1000} = [201]_{1000}$, $[101]^3_{1000} = [301]_{1000}$, $[101]^4_{1000} = [401]_{1000}$, $[101]^5_{1000} = [501]_{1000}$, $[101]^6_{1000} = [601]_{1000}$, $[101]^7_{1000} = [701]_{1000}$, $[101]^8_{1000} = [801]_{1000}$, $[101]^9_{1000} = [901]_{1000}$, $[101]^{10}_{1000} = [1]_{1000}$, therefore the multiplicative order of $[101]^2_{1000}$ is 10, and the multiplicative inverse is $[901]_{1000}$.

7. (a) $f : \mathbb{Z}_8 \to \mathbb{Z}_{12}$ given by $f([x]_8) = [3x]_{12}$ is well-defined because
   $[x]_8 = [y]_8 \Rightarrow 8|(x-y) \Rightarrow 24|3(x-y) \Rightarrow 12|3(x-y) \Rightarrow 12|(3x-3y) \Rightarrow [3x]_{12} = [3y]_{12}$

   (b) $f : \mathbb{Z}_8 \to \mathbb{Z}_{16}$ given by $f([x]_8) = [-x]_{16}$ is not well-defined because
   $f([0]_8) = [0]_{16}$ but $f([8]_8) = [-8]_{16} \neq [0]_{16}$ while $[0]_8 = [8]_8$.

8. $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ by $f([x]_{mn}) = ([x]_m, [x]_n)$.
Each element of $\mathbb{Z}_{mn}$ can be written as $[x]_{mn}$ for some integer $x$, and $f$ can be defined by the above formula. We have to show that $f$ is well-defined.
If $[x]_{mn} = [y]_{mn}$ then $mn|(x-y)$. Then $m|(x-y)$ and $n|(x-y)$, so $[x]_m = [y]_m$ and $[x]_n = [y]_n$. Therefore $([x]_m, [x]_n) = ([y]_m, [y]_n)$.
Now we show that if $f$ is onto then $(m, n) = 1$. Let's prove by contradiction. Suppose $(m, n) = d > 1$. Then we claim that $f$ is not onto because, for example, the pair $([0]_m, [1]_n)$ is not in the image: $([x]_m, [x]_n) = ([0]_m, [1]_n)$ would imply that $[x]_m = [0]_m$ and $[x]_n = [1]_n$, then $m|x$ and $n|(x-1)$, so $d|x$ and $d|(x-1)$, therefore $d|1$ which is impossible. So we have a contradiction.
Conversely, if $(m, n) = 1$, then by the Chinese Remainder Theorem for each pair $(a, b)$ there exists $x$ such that $x \equiv a (\text{mod } m)$ and $x \equiv b (\text{mod } n)$. Then $([x]_m, [x]_n) = ([a]_m, [b]_n)$, so each pair $([a]_m, [b]_n)$ is in the image, and thus $f$ is onto.

9. (a) $x \sim y$ if $|x - y| \leq 1$ is not an equivalence relation because the transitive law is not satisfied. For example, $4 \sim 5$ and $5 \sim 6$ but $4 \not\sim 6$ according to the given rule.

   (b) $x \sim y$ if $|x| = |y|$ is an equivalence relation.
   Reflexive law: $x \sim x$ for all $x$ because $|x| = |x|$.
   Symmetric law: if $x \sim y$ then $|x| = |y|$ then $|y| = |x|$ then $y \sim x$.
   Transitive law: if $x \sim y$ and $y \sim z$, we have $|x| = |y|$ and $|y| = |z|$, then $|x| = |z|$, so $x \sim z$.
   There are infinitely many equivalence classes. One consists of just one element 0, and all other equivalence classes consist of 2 elements, one positive and one negative, of the form $\{a, -a\}$. E.g. $\{1, -1\}$, $\{3, -3\}$, etc.

   (c) $x \sim y$ if $xy > 0$ is not an equivalece relation because the reflexive law is not satisfied: $0 \not\sim 0$ according to the given rule.

   (d) $x \sim y$ if either $xy > 0$ or $x = y = 0$ is an equivalence relation.
   Reflexive law: $x \sim x$ for all $x$ because either $x \cdot x > 0$ or $x = x = 0$.
   Symmetric law: if $x \sim y$ then either $xy > 0$ or $x = y = 0$, then either $yx > 0$ or $y = x = 0$, so $y \sim x$.
   Transitive law: if $x \sim y$ and $y \sim z$, then either $xy > 0$ (in which case $y \neq 0$, so $yz \neq 0$) and $yz > 0$, or $x = y = 0$ and $y = z = 0$. In the first case we have $xy > 0$ and $yz > 0$, then $xy^2z > 0$, so $xz > 0$ (since $y^2 > 0$). In the second case we have $x = z = 0$. Thus in both cases $x \sim z$.
   There are 3 equivalence classes: one class consists of 0 alone, one class consists of all positive numbers, and the third class consists of all negative numbers.

10. (a) $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 1 & 6 & 2 \end{pmatrix}$, $\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 6 & 2 & 3 & 4 \end{pmatrix}$.

   (b) $\sigma$ and $\tau$ do not commute because $\sigma\tau \neq \tau\sigma$.

(c) $\sigma^{-1} = \begin{pmatrix} 3 & 1 & 6 & 4 & 5 & 2 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 4 & 5 & 3 \end{pmatrix}$,

$\tau^{-1} = \begin{pmatrix} 1 & 4 & 5 & 2 & 3 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 5 & 2 & 3 & 6 \end{pmatrix}$.

(d) $\sigma = (1362)$, $\tau = (24)(35)$

(e)


(f) $\sigma = (1362) = (13)(36)(62)$

(g) $\sigma$ is odd because it can be written as a product of 3 (which is an odd number) transpositions, and $\tau$ is even because it can be written as a product of 2 (which is an even number) transpositions.