21-127 HW10
SOL'NS

1) <u>Prop 1</u>: Let $d_i \mid a \wedge d_i \mid b$
and $(q \mid a \wedge q \wedge b) \to (q \mid d_i)$

hold for $i = 1, 2$. Then

$d_1 \mid a \wedge d_1 \mid b$, so $d_1 \mid d_2$. On the other hand,
$d_2 \mid a \wedge d_2 \mid b$, so $d_2 \mid d_1$. Thus $\exists n, k$ st

$d_1 = n d_2$, $d_2 = k d_1 \Rightarrow d_1 = n k d_1 \Rightarrow n \cdot k = 1$

so $n, k \in \{1, -1\}$ and thus $d_1 = \pm d_2$.

<u>Prop 2</u>:

i) Note ~~$k|0$ since $a|0 \geq 0$ and~~ $k \mid 0 \ \forall k \in \mathbb{Z}$.
Thus since a is greatest so that $a \mid a$,
$\gcd(0, a) = a$.

ii) Note $k \mid 1 \Rightarrow k = \pm 1$. Since $1 \mid a$,
$\gcd(1, a) = 1$.

iii) Note $l \mid a \Rightarrow l \leq a$. Since $a \mid a$ and
$a \mid ka$, it is the greatest possible common
divisor. (if $a \neq 0$)

2) <u>Prop 3</u>

i) FTSOC, say $m > 1$ has $m \mid \frac{a}{d}$, $m \mid \frac{b}{d}$.

Then $\exists\, n, k \in \mathbb{Z}$ st $mn = \frac{a}{d}$, $mk = \frac{b}{d}$, so

$mdn = a$, $mkd = b$. Then $md \mid a$ and $md \mid b$,

but $md \nmid d$, contradicting $d = \gcd(a,b)$.

ii) $a \mid dy \Rightarrow \exists\, n \in \mathbb{Z}$, $an = dy$. Then

$dkn = dy \Rightarrow kn = y \Rightarrow k \mid y$.

---

3) Lemma: If $y = \prod_{i=1}^{r} p_i^{k_i}$, p_i distinct primes, $k_i \geq 0$,

Then $x \mid y \iff x = \prod_{i=1}^{r} p_i^{n_i}$, $n_i \leq k_i$.

PF of Lemma:

"$\Leftarrow$": If $x = \prod_{i=1}^{r} p_i^{n_i}$, then $\frac{y}{x} = \prod_{i=1}^{r} p_i^{k_i - n_i}$,

where $k_i - n_i \geq 0$ $\forall i \in [r]$, so $\frac{y}{x} \in \mathbb{Z}$.

"$\Rightarrow$": FTSOC, say $x = \prod_{i=1}^{r} p_i^{n_i} \times q$

where q is coprime to $p_1, \dots, p_r$. Then $q \mid x$, so

$q \mid y$, but q is coprime to $p_1, \dots, p_r$ and so coprime to y.

$\ast$.

Thus $x = \prod_{i=1}^{r} p_i^{n_i}$. We see $n_i \le k_i \ \forall i$ since

<u>if</u> $n_i > k_i$, then $p^{n_i} / x \Rightarrow p^{n_i} / y$, but

$\dfrac{\prod_{j=1}^{r} p_j^{k_j}}{p_i^{n_i}}$ does <u>not</u> cleanly divide, since $n_i > k_i$.

and $\gcd(p_i, p_j) = 1 \ \forall j \neq i$.

With the lemma, now, letting

$d = \prod_{i=1}^{n} p_i^{m_i}$, we claim

i) $d \mid a \wedge d \mid b$

ii) $q \mid a \wedge q \mid b \Rightarrow q \mid d$.

i): Since $d = \prod_{i=1}^{r} p_i^{m_i}$ and $m_i = \min(k_i, j_i) \le k_i$,

$d \mid a$. Similarly, $m_i = \min(k_i, j_i) \le j_i$, so

$d \mid b$.

ii) Let $q \mid a$ and $q \mid b$. Thus $q = \prod_{i=1}^{r} p_i^{n_i}$

where $n_i \le k_i$ and $n_i \le j_i$. But then

$n_i \le \min(k_i, j_i)$, so $q \mid d$.

Since d satisfies (i) & (ii),

$d = \gcd(a, b)$.

4)

a) $12a + 9b = 15$

$\gcd(12,9) = 3 \qquad 3 \mid 15$ ✓

Solve $12a' + 9b' = 3$ using Euclidean algorithm:

$12 = 9 \cdot 1 + 3 \qquad 12 \cdot 1 + 9 \cdot (-1) = 3.$

$\Rightarrow \quad 12 \cdot 5 + 9 \cdot (-5) = 15$

Solutions: $a = 5 + \frac{9}{\gcd(9,12)} k = 5 + 3k$

$b = -5 - \frac{12}{\gcd(9,12)} k = -5 - 4k$, $k \in \mathbb{Z}$.

b) $12a + 9b = 1 \qquad \gcd(12,9) = 3 \nmid 1$

$\Rightarrow$ no solutions

c) $2a + 3b = 1$

one solution is $a = -1, b = 1$.

Then all solutions are $a = -1 + 3k$, $b = 1 - 2k$ $\quad k \in \mathbb{Z}$.

d) $2 \mid 50000$

$2 \mid 18412$ $\Rightarrow 1 \neq \gcd(50000, 18412)$

so <u>no</u> solutions.

5) $a \perp b \Rightarrow \exists x, y \in \mathbb{Z},\ ax + by = 1$

(Bézout's Lemma)

$a \mid (bc) \Rightarrow \exists k \in \mathbb{Z},\ ak = bc.$

so $acx + bcy = c$

$\Rightarrow acx + aky = c \Rightarrow a(cx + ky) = c$

$\Rightarrow a \mid c.$

6) If we let $S = \{q \in \mathbb{N} \mid a \mid q \wedge b \mid q\}$,

a) claim $\operatorname{lcm}(a,b)$ is the minimal element of S.

(Since $ab \in S$, $S \neq \emptyset$, so it has a minimal element by W.O.P.

Claim: $m = \min(S)$ satisfies 1) $a \mid m \wedge b \mid m$

2) $a \mid q \wedge b \mid q \Rightarrow m \mid q$.

Since $m \in S$, 1) is automatic.

Now, if $a \mid q \wedge b \mid q$, then $q \in S$. Consider $\gcd(m,q)$. Note $a \mid m \wedge b \mid m$ and $a \mid q \wedge b \mid q$, so $a \mid \gcd(m,q) \wedge b \mid \gcd(m,q)$, so $\gcd(m,q) \in S$.

But then $\gcd(m,q) \geq m$, and $m \leq q$, so $\gcd(m,q) = m$ and thus $q \mid m$. We conclude that m satisfies 2).

b) Suffices to show $\frac{ab}{d} = m$. Let $m' := \frac{ab}{d}$.

Note that since $\frac{a}{d} \in \mathbb{Z}$, $\frac{b}{d} \in \mathbb{Z}$,

$m' = a\frac{b}{d} = b\frac{a}{d}$

$\Rightarrow a \mid m', \; b \mid m'$.

Now, let $q \in \mathbb{Z}$ satisfy

$a \mid q \wedge b \mid q$.

b) Let $d = \gcd(a,b)$, $d' = \frac{ab}{\operatorname{lcm}(a,b)}$.

Claim: $d' = d$.

Note $\frac{a}{d'} = \frac{m}{b} \in \mathbb{Z}$ since $b \mid m$

$\frac{b}{d'} = \frac{m}{a} \in \mathbb{Z}$ since $a \mid m$, so $d' \mid a \wedge d' \mid b$.

Now, let $q \mid a \wedge q \mid b$, so $\frac{ab}{q} \in \mathbb{Z}$. Since

$a \mid \frac{ab}{q}$ and $b \mid \frac{ab}{q}$, $m \mid \frac{ab}{q}$. So,

$\frac{ab}{mq} = \frac{d'}{q} \in \mathbb{Z}$, so $q \mid d'$, so in fact $d' = d$.

7) No, it fails to be ~~transitive~~ ~~NOT~~ ~~not~~ reflexive.

$\gcd(2,2) = 2$, so $2 \not\sim 2$.

---

8) Yes. Reflexive: Since $f(x) = f(x)$ $\forall x \in X$, $x \sim x$.

Symmetric: Let $x_1, x_2 \in X$, $x_1 \sim x_2$. Then $f(x_1) = f(x_2)$, so $f(x_2) = f(x_1)$, so $x_2 \sim x_1$.

Transitive: Let $x_1, x_2, x_3 \in X$, $x_1 \sim x_2$, $x_2 \sim x_3$. Then $f(x_1) = f(x_2)$ and $f(x_2) = f(x_3)$, so $f(x_1) = f(x_3)$ and $x_1 \sim x_3$.

---

9) Reflexive: Since $\forall x \in X$, $x \sim_1 x$ and $x \sim_2 x$, we have $x \sim x$.

Symmetric: Let $x, y \in X$, $x \sim y$.

Then $x \sim_1 y$ and $x \sim_2 y$, so $y \sim_1 x$ and $y \sim_2 x$, so $y \sim x$.

Transitive: Let $x, y, z \in X$, $x \sim y \wedge y \sim z$.

Then $x \sim_1 y$, $x \sim_2 y$ and $y \sim_1 z$, $y \sim_2 z$.

$x \sim_1 y \wedge y \sim_1 z \rightarrow x \sim_1 z$

$x \sim_2 y \wedge y \sim_2 z \rightarrow x \sim_2 z$

$\rightarrow x \sim z$.

Note $[x] = \{y \in X \mid x \sim y\} = \{y \in X \mid x \sim_1 y \wedge x \sim_2 y\}$

$= \{y \in X \mid x \sim_1 y\} \cap \{y \in X \mid x \sim_2 y\}$

$= [x]_1 \cap [x]_2$.

---

10) a) True. Proof by induction: If $a \equiv b \mod n$, $\forall k \in \mathbb{N}$, $a^k \equiv b^k \mod n$.

Base case: $a^1 \equiv a \equiv b \equiv b^1 \mod n$ ✓

Inductive step: Assume $a^k \equiv b^k \mod n$ for some k.

Then $a^{k+1} \equiv a^k \cdot a \equiv a^k \cdot b \equiv b^k \cdot b \equiv b^{k+1} \mod n$ ✓

Thus $a^{k+1} \equiv b^{k+1} \mod n$.

b) False, let $n = 3$, $a = 2$, $k = 1$, $l = 4$.

Then $4 \equiv 1 \mod 3$, but

$2^4 \equiv 16 \equiv 1 \mod 3$ while $2^1 \equiv 2 \mod 3$.

---

11) "$\Rightarrow$" Clearly u, u' both inverses $\Rightarrow$ u is an inverse.

Now, note $u(u'a) \equiv u \cdot 1 \equiv u \mod n$ but

$u'(ua) \equiv u' \cdot 1 \equiv u' \mod n$.

Thus $u' \equiv u \mod n$.

"$\Leftarrow$" Since $u \equiv u'$, we have $a \cdot u \equiv a \cdot u' \bmod n$ and since u is an inverse, $a \cdot u \equiv 1 \bmod n$ so $a \cdot u' \equiv 1 \bmod n$.

---

12) Note that in the range $1, \ldots, p^k$, a ~~number~~ number is <u>coprime</u> to p^k if and only if it is <u>not</u> divisible by p.

~~The~~ Every p^{th} number is divisible by p, so there are $p^k \cdot \frac{1}{p}$ numbers <u>not</u> coprime to p^k in the range $1, \ldots, p^k$.

Thus, there are $p^k - p^{k-1}$ numbers coprime to p^k, so $\phi(p^k) = p^k - p^{k-1}$.

5

$1, 2, 3, 4$

$2^2 \equiv 4$ $\quad 3^2 \equiv 4$

$2^3 \equiv 3$ $\quad 3^3 \equiv$

$2^4 \equiv 1$

4^2

$a^{\varphi(n)-1} \cdot a = 1$

$a^k \equiv 1$

$\boxed{5}$

$5 \cdot 2 = 10$

$2 \cdot 5 = 10$