Problem Set 1 Solutions

1. (a) Note that $ar+bs = as - nab + nab + bs$

$$= a(r-nb) + b(s+na), \quad \forall n, s, r \in \mathbb{Z}.$$

So if $ab-a-b = ax+by$ for $x, y \in \mathbb{Z}_{\geq 0}$,

then $ab = a(x+1) + b(y+1)$

& we may replace $(x+1, y+1)$ by $(x+1-nb, y+1+na)$ for any $n \in \mathbb{Z}$.

$\Rightarrow$ may assume $0 \leq x+1 < b$.

On the other hand,

$$ab = a(x+1) + b(y+1) \Rightarrow b \mid (a(x+1) + b(y+1))$$

$$\Rightarrow b \mid a(x+1).$$

As $\gcd(a,b)=1$, $b \mid a(x+1) \Rightarrow b \mid (x+1) \Rightarrow x+1 \geq b$.

This is a contradiction. So $ab-a-b \neq ax+by$, $\forall x, y \in \mathbb{Z}$.

(b) Consider $S = \{x \in \mathbb{Z} : b \mid n-ax,\ x \geq 0\}$

$$\Rightarrow S \text{ is a nonempty finite set.}$$

$\Rightarrow \exists y \in S$ s.t. $by = n-ax$ ($\Leftrightarrow n = ax+by$).

It suffices to show $y \geq 0$.

By (a), may assume $x \leq b-1$.

So $n - ax > ab-a-b-ax = ab-a-b-ab+a = -b$

$\Rightarrow by > -b \Rightarrow y > -1 \Rightarrow y \geq 0$.

2. Given $f(a,b) = f(b,a) = f(b-a,a)$. We have

$$f(a,b) = f(a-b,b) = f(a-2b,b) = \cdots = f(a-tb,b), \ \forall t \in \mathbb{N}.$$

Assume $a > b$ without loss of generality.

Write $a = qb + r$ for $0 \le r < b$ by Euclid division.

$$\Rightarrow f(a,b) = f(a-qb,b) = f(r,b), \quad 0 \le r < b.$$

Write $b = mr + n$ for $0 \le n < r$ by Euclid division.

$$\Rightarrow f(r,b) = f(r, b-mr) = f(r,n).$$

Do this process iteratively,

Euclidean algorithm

$$\Rightarrow f(a,b) = f(r,b) = f(r,n) = \cdots = f(\gcd(a,b), \gcd(a,b))$$
$$= f(\gcd(a,b), 0).$$

3. Construct $f: \mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0} \longrightarrow \mathbb{Z}_{\geq 0}$ by defining

$$f(m,n) = \gcd(a^m - 1, a^n - 1).$$

Check: (1) $f(m,n) = f(n,m)$ is clear

(2) $\gcd(a^m-1, a^n-1) = \gcd((a^m-1)-(a^n-1), a^n-1)$

$= \gcd(a^m - a^n, a^n - 1)$

$= \gcd(a^n(a^{m-n}-1), a^n-1)$

$= \gcd(a^{m-n}-1, a^n-1)$ as $\gcd(a^n, a^n-1) = 1$.

$\Rightarrow f(m,n) = f(m-n, n)$.

So f is a function satisfying Problem 2.

$\Rightarrow f(m,n) = f(\gcd(m,n), 0)$

$\Rightarrow \gcd(a^m-1, a^n-1) = \gcd(a^{\gcd(m,n)}-1, a^0-1)$

$= a^{\gcd(m,n)} - 1.$

4. We have $\frac{1}{x}+\frac{1}{y}=\frac{1}{z} \Rightarrow xy = z(x+y)$.

$\Rightarrow \forall p$ prime, $v_p(x)+v_p(y) = v_p(z)+v_p(x+y)$.

So to show $x+y$ = perfect square, it suffices to show

$\forall p$ prime, $v_p(x)+v_p(y)-v_p(z)$ is even.

Known: $\gcd(x,y,z)=1 \Rightarrow$ at least one of $v_p(x), v_p(y), v_p(z)$ must equal 0.

Let n be any integer. ($n \| m$ means $v_n(m)=1$.)

Case (1): $n \| x$, $n \nmid y \Rightarrow n \| xy = z(x+y)$, $n \nmid (x+y) \Rightarrow n \| z$

$\Rightarrow v_n(z) = v_n(x)$, $v_n(y)=0$.

Case (2): $n \| y$, $n \nmid x \Rightarrow n \| xy$, $n \nmid (x+y) \Rightarrow n \| z$.

$\Rightarrow v_n(z) = v_n(y)$, $v_n(x)=0$.

Case (3): $n \| x$, $n \| y \Rightarrow n \nmid z \Rightarrow v_n(x) = v_n(y)$, $v_n(z)=0$

Case (4): $n \nmid x$, $n \nmid y \Rightarrow n \nmid xy = z(x+y) \Rightarrow n \nmid z$.

$\Rightarrow v_n(x) = v_n(y) = v_n(z) = 0$.

Conclusion: $\forall p$ prime, $v_p(x)+v_p(y) = v_p(z)$ is even.

5. Let $p \neq q$ be two primes. Then

$$\gcd(a_p, a_q) = \gcd(p, q) = 1$$

$$\gcd(a_p, a_{pq}) = \gcd(p, pq) = p \Rightarrow p \mid a_p,\ p \mid a_{pq}$$

$$\gcd(a_q, a_{pq}) = \gcd(q, pq) = q \Rightarrow q \mid a_q,\ q \mid a_{pq}.$$

$$\Rightarrow pq \mid a_{pq}.$$

$$\forall r \in \mathbb{N},\quad \gcd(a_{p^r}, a_{p^{r+1}}) = \gcd(p^r, p^{r+1}) = p^r \Rightarrow p^r \mid a_{p^r}$$

So we know:

(a) $\forall p$ prime, $p \mid a_p$.

(b) $\forall r \in \mathbb{N}$ & p prime, $p^r \mid a_{p^r}$

(c) $\forall p_1, \dots, p_k$, $p_1 \cdots p_k \mid a_{p_1 \cdots p_k}$.

Hence $\forall m \in \mathbb{N}$, $m \mid a_m$ by writing $m = p_1^{r_1} \cdots p_k^{r_k}$.

Write $a_n = k_n \cdot n$ for all $n \in \mathbb{N}$ (with some $k_n \in \mathbb{N}$).

$\Rightarrow \gcd(a_m, a_n) = \gcd(k_m \cdot m, k_n \cdot n) = \gcd(m, n)$

$\Rightarrow \gcd(k_m, k_n) = \gcd(k_m, n) = \gcd(k_n, m) = 1$ for any m, n.

$\Rightarrow k_m = k_n = 1$

$\Rightarrow a_m = m$ for all $m \in \mathbb{N}$.