Problem Set 1

$\boxed{1}$ Run Euclidean algorithm:

$$240 = 2 \cdot 84 + 72$$
$$84 = 1 \cdot 72 + 12$$
$$72 = 6 \cdot 12 + 0.$$

So
$$\gcd(240, 84) = 12$$
$$= 84 - 1 \cdot 72$$
$$= 84 - [240 - 2 \cdot 84]$$
$$= -240 + 3 \cdot 84.$$

So one solution is $(s, t) := (-1, 3)$.

A pair (s', t') is a solution $\Leftrightarrow$ $240(s'-s) = 84(t-t')$

$\Leftrightarrow$ $20(s'-s) = 7(t-t')$

$\Leftrightarrow$ $\exists i \in \mathbb{Z}$ such that

$s' = s + 7i$ and $t' = t - 20i$.

So the solutions are $\{(-1+7i, 3-20i) : i \in \mathbb{Z}\}$.

$\boxed{2}$ Let $a, b, n \in \mathbb{N}^*$ be arbitrary.

<u>Claim</u>: $\gcd(an, bn) \geq n \gcd(a,b)$.

Pf: $\gcd(a,b) \mid a$ and $\gcd(a,b) \mid b$.

So $n \cdot \gcd(a,b) \mid an$ and $n \cdot \gcd(a,b) \mid bn$.

<u>Claim</u>: $\gcd(an, bn) \leq n \gcd(a,b)$.

Pf: By Euclidean algorithm / Bézout's lemma,

$$\exists\, s, t \in \mathbb{Z} : \quad \gcd(an, bn) = s \cdot an + t \cdot bn$$
$$= n(sa + tb).$$

Define $k := sa + tb$.

By construction, $kn = \gcd(an, bn)$.

So $kn \mid an$ and $kn \mid bn$.

So $k \mid a$ and $k \mid b$.

So $k \leq \gcd(a,b)$.

$\boxed{3}$ Let $a, b, n \in \mathbb{N}^*$ be arbitrary.

Suppose that $n \mid ab$ and $\gcd(a,n) = 1$.

By Euclidean algorithm / Bézout's lemma,

$$\exists\, s,t \in \mathbb{Z} : \quad sa + tn = \gcd(a,n) = 1.$$

So $\quad sab + tnb = b.$

Since (by hypothesis) $n \mid ab$,

we have $n \mid sab + tnb$, ie $n \mid b$.

$\boxed{4}$ Let $n \in \mathbb{N}^*$.

Let $n = \sum_{i=0}^{k} 10^i c_i$ be its base-10 representation.

Since $10 \equiv 1 \pmod{9}$,

$$n \equiv \sum_{i=1}^{k} 10^i c_i \equiv \sum_{i=1}^{k} 1^i c_i \equiv \sum_{i=1}^{k} c_i \pmod{9}.$$

So $9 \mid n$ if and only if $9 \mid \sum_{i=1}^{k} c_i$.

$\boxed{5}$

Let $\mathbb{Z}/m\mathbb{Z} := \{[0], [1], \ldots, [m-1]\}$

be the mod-m congruence classes.

Let $\tilde{F}_1, \tilde{F}_2, \ldots$ be the mod-m reduced Fibonacci sequence,

ie $\forall i$: $\tilde{F}_i \in \mathbb{Z}/m\mathbb{Z}$ and $F_i \in \tilde{F}_i$.

By the pigeonhole principle,

$$\exists\, 0 \leq i < j \leq m^2: \quad \left(\tilde{F}_{2i}, \tilde{F}_{2i+1}\right) = \left(\tilde{F}_{2j}, \tilde{F}_{2j+1}\right).$$

Define $f : (\mathbb{Z}/m\mathbb{Z})^2 \to (\mathbb{Z}/m\mathbb{Z})^2$

$$([a], [b]) \mapsto ([a+b], [2a+b]).$$

Note that f is a bijection and that

$$\forall k \geq 0: \quad f\left(\tilde{F}_k, \tilde{F}_{k+1}\right) = \left(\tilde{F}_{k+2}, \tilde{F}_{k+3}\right).$$

It follows that $\left(\tilde{F}_{2k}, \tilde{F}_{2k+1}\right)_{k \geq 0}$ is $(j-i)$-periodic,

and hence that $(\tilde{F}_k)_{k \geq 0}$ is $2(j-i)$-periodic.