1 Problem 1

Let $\{a_n\}_{n\geq 0}$ be a sequence defined as follows:

$$a_0 = 0; a_1 = 1; a_2 = 2 \text{ and}$$

$$a_{n+3} = 5^n \cdot a_{n+2} + n^2 \cdot a_{n+1} + 11a_n \text{ for } n \geq 0$$

Prove that there exist infinitely many $n \in \mathbb{N}$ such that $2023 \mid a_n$.

Solution. Let

$$V_n = (\overline{a_{n+2}}, \overline{a_{n+1}}, \overline{a_n}, \overline{5^n}, \overline{n})$$

where $\overline{m}$ is the equivalence class of m modulo 2023. Note that there are only 2023^5 permutations of $(a_{n+2}, a_{n+1}, a_n, 5^n, n)$ when each element is considered modulo 2023, thus there are only 2023^5 possible values of V_n. Furthermore, V_n determines uniquely V_{n+1}: if $V_n = (\overline{v_1}, \overline{v_2}, \overline{v_3}, \overline{v_4}, \overline{v_5})$, then

$$\begin{aligned}
n + 1 &\equiv v_5 + 1 \pmod{2023} \\
5^{n+1} &\equiv 5v_4 \pmod{2023} \\
a_{n+1} &\equiv v_2 \pmod{2023} \\
a_{n+2} &\equiv v_1 \pmod{2023} \\
a_{n+3} &\equiv v_4 v_1 + v_5^2 v_2 + 11v_3 \pmod{2023}
\end{aligned}$$

which determines V_{n+1}. Hence V_n determines uniquely V_{n+i} for all $i \in \mathbb{N}$ (since V_{n+i} is determined by V_{n+i-1}, and V_{n+i-1} is determined by V_{n+i-2}, etc. until we get that it is determined by V_n). Hence, if $V_n = V_m$, we must have $V_{n+i} = V_{m+i}$ for all $i \in \mathbb{N}$.

Let $k = 2023^5 + 1$, and consider V_k. By the pigeon-hole principle, there must exist some $m \leq 2023^5$ such that $V_k = V_m$ and thus we must have that $V_{k+i} = V_{m+i}$ for all $i \in \mathbb{N}$, as we proved before. Hence, $a_{k+i} \equiv a_{m+i} \pmod{2023}$ for all $i \in \mathbb{N}$, since these are just the third element of our V's, which must be equal for equality of V_{k+i} and V_{m+i}. Thus, (a_n) is periodic with period $p = k - m$.

Note that $a_0 = 0$, thus, it is sufficient to show that $\overline{a_0} = \overline{a_{0+p}}$. To prove this, assume for the sake of contradiction that there is some least $j > 0$ where $\overline{a_{j+p}} = \overline{a_j}$ but $\overline{a_{j+p-1}} \neq \overline{a_{j-1}}$ (a_{j-1} will always be defined since $j - 1 \geq 0$). Then $V_j = V_{j+p}$ and $V_{j-1} \neq V_{j+p-1}$. See that

- $a_{j+1} \equiv a_{j+p+1} \pmod{2023}$
- $a_j \equiv a_{j+p} \pmod{2023}$
- $5^j \equiv 5^{j+p} \pmod{2023}$ implies $5^{j-1} \equiv 5^{j+p-1} \pmod{2023}$ since 5 is coprime with 2023 and so we can divide it out
- $j \equiv j + p \pmod{2023}$ implies that $j - 1 \equiv j + p - 1 \pmod{2023}$ (and also $j^2 \equiv (j+p)^2 \pmod{2023}$), which we will make use of later).

Thus, since $V_{j-1} \neq V_{j+p-1}$, since all the other elements are the same, we must have that $a_{j-1} \not\equiv a_{j+p-1} \pmod{2023}$. But since we have $a_{j+2} \equiv a_{j+p+2} \pmod{2023}$, we have

$$5^j \cdot a_{j+1} + j^2 \cdot a_j + 11a_{j-1} \equiv 5^{j+p} \cdot a_{j+p+1} + (j+p)^2 \cdot a_{j+p} + 11a_{j+p-1} \pmod{2023}$$

$$\implies 11a_{j-1} \equiv 11a_{j+p-1} \pmod{2023}$$

$$\implies a_{j-1} \equiv a_{j+p-1} \pmod{2023}$$

since 11 is coprime with 2023 so we can divide out by it. But this contradicts that $V_{j-1} \neq V_{j+p-1}$. Therefore, $j \not> 0$, so $\overline{a_0} = \overline{a_{0+p}} = \overline{0}$, and this infinitly repeats every p, thus there are infinitely many n such that $2023 \mid a_n$.

2 Problem 2

Let $n \in \mathbb{N}$. Find the number of solutions for the congruence equation:

$$x^3 \equiv 1 \pmod{n}$$

Solution. Consider the unique prime factors of n, specifically $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ (where $\alpha_i \geq 1$).

If we have $p_i = 2$, we seek to find the number of solutions to $x^3 - 1 \equiv 0 \pmod{2^{\alpha_i}}$. Notice that we must have $2^{\alpha_i} \mid x^3 - 1$, so $x^3 - 1$ is even, hence x^3 is odd, which implies x is odd. Then, $\frac{d}{dx}(x^3 - 1) = 3x^2$ is not even, so $\frac{d}{dx}(x^3 - 1) \neq 0 \pmod{2^{\alpha_i}}$. Therefore, we can invoke Hensel's lemma: if $x^3 - 1 \equiv 0 \pmod{2}$, the only solution modulo 2 is $x = 1$, thus we know that $x^3 - 1 \equiv 0 \pmod{2^{\alpha_i}}$ has only one solution as well. Thus, there is only one solution to $x^3 \equiv 1 \pmod{p_i^{\alpha_i}}$.

If $p_i \neq 2$, note that since $p \nmid 1$, and $3 \in \mathbb{Z}^+$, by theorem 18.2, we have the number of solutions to $x^3 \equiv 1 \pmod{p_i^{\alpha_i}}$ is $d_i = \gcd(3, p_i^{\alpha_i})$ (note that we never have the 0 solutions case, because $1^{\phi(p_i^{\alpha_i})/d} \equiv 1 \pmod{p_i^{\alpha_i}}$ always). We can now compute d_i:

$$d_i = \gcd(3, \phi(p_i^{\alpha_i})) = \gcd(3, p^{\alpha_i - 1}(p_i - 1))$$

We can have $p_i \equiv 0 \pmod{3}$, $p_i \equiv 1 \pmod{3}$, or $p_i \equiv 2 \pmod{3}$.

In the $0 \pmod{3}$, this says that $3 \mid p_i$, which is only true when $p_i = 3$ (by the definition of a prime). Then if $\alpha_i = 1$, we have $\gcd(3, 2) = 1$. If $\alpha_i > 1$, we have $\gcd(3, 3^{\alpha_i} 2) = 3$.

If $p_i \equiv 1 \pmod{3}$, then $\gcd(3, p_i^{\alpha_i}(p_i - 1)) = 3$ since $3 \mid p_i - 1$ and $p_i^{\alpha_i} \geq 3 + 1$.

If $p_i \equiv 2 \pmod{3}$, then $\gcd(3, p_i^{\alpha_i}(p_i - 1) = 1$, since $3 \nmid p_i^{\alpha_i}$ (by definition of p_i being prime and not 3) and $3 \nmid p_i - 1 = 3k + 1$ by definition of p_i being $2 \pmod{3}$.

Let $N_P(m)$ denote the number of solutions to $x^3 - 1 \equiv 0 \pmod{m}$. From Theorem 8.2, since $p_i^{\alpha_i}$ is coprime with $p_j^{\alpha_j}$ when $i \neq j$, we have $N_P(n) = \prod N_P(p_i^{\alpha_i})$. We can rewrite n as

$$n = 2^l 3^k \prod_{i=1}^{r} p_i^{\alpha_i} \prod_{j=1}^{s} q_i^{\beta_j}$$

where $l, k \in \mathbb{N} \cup \{0\}$, p_i, q_j are prime, $p_i \equiv 1 \pmod{3}$, $q_j \equiv 2 \pmod{3}$ not 2, and r and s are the number of such primes where $\alpha_i, \beta_j \geq 1$.

Thus,

$$N_P(n) = N_P(2^l) N_P(3^k) \prod_{i=1}^{r} N_P(p_i^{\alpha_i}) \prod_{j=1}^{s} N_P(q_i^{\beta_j}) = N_P(3^k) 3^r$$

Hence, we have

$$N_P(n) = \begin{cases} 3^{r+1} & \text{if } k > 1 \\ 3^r & \text{otherwise} \end{cases}$$

3 Problem 3

As always, $\phi(\cdot)$ is the Euler-ϕ function.
Let α be any real number in the interval $[0, 1]$. Prove that there exists an infinite sequence $\{n_k\}_{k\geq 1} \subset \mathbb{N}$ such that

$$\lim_{k\to\infty} \frac{\phi(n_k)}{n_k} = \alpha$$

Solution. For any $n \in \mathbb{N}$, we can take the prime factor decomposition $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ where all $\alpha_i \geq 1$. Furthermore, recall that $\phi(n) = \prod_{i=1}^r p_i^{\alpha_i - 1}(p_i - 1)$, hence

$$\frac{\phi(n)}{n} = \frac{\prod_{i=1}^r p_i^{\alpha_i-1}(p_i - 1)}{\prod_{i=1}^r p_i^{\alpha_i}} = \prod_{i=1}^r \frac{p_i - 1}{p_i}$$

We let $\varepsilon > 0$ be arbitrary. By the Archimedean principle, there exists some $N \in \mathbb{N}$ such that $N > \varepsilon > 0$, so $\frac{1}{N} < \varepsilon$. By the infinitude of primes, there is some $J \in \mathbb{N}$ such that $p_J > N$ so $\frac{1}{p_J} < \varepsilon$ as well. If $j > J$, and we assume that we indexed the primes so that they were increasing, we have that $0 < \frac{1}{p_j} < \varepsilon$ as well.

We now provide the sequence defined by

$$x_n = \prod_{i=0}^n \frac{p_{i+J} - 1}{p_{i+J}}$$

Note that if $m = \prod_{i=0}^n p_{i+J}$, we showed above then that

$$x_n = \frac{\phi(m)}{m}$$

We have $1 > \frac{p_J - 1}{p_J} = x_0 = 1 - \frac{1}{p_J} > 1 - \varepsilon$. Furthermore, for any $n \in \mathbb{N}$, $x_n > x_{n+1}$ since we are multiplying by a value less than one, hencee

$$\begin{aligned}
0 < x_n - x_{n+1} &= \prod_{i=0}^n \frac{p_{i+J} - 1}{p_{i+J}} - \prod_{i=0}^{n+1} \frac{p_{i+J} - 1}{p_{i+J}} \\
&= \prod_{i=0}^n \left(\frac{p_{i+J} - 1}{p_{i+J}} \left(1 - 1 + \frac{1}{p_{n+J+1}}\right)\right) \\
&= \frac{1}{p_{n+J+1}} \prod_{i=0}^n \frac{p_{i+J} - 1}{p_{i+J}} \\
&< \varepsilon \prod_{i=0}^n \frac{p_{i+J} - 1}{p_{i+J}} < \varepsilon
\end{aligned}$$

Now we can invoke the Euler product formula to get

$$\prod_{p \text{ prime}} \left(\frac{1}{1 - \frac{1}{p^s}} \right) = \sum_{n=1}^\infty \frac{1}{n^s}$$

therefore

$$\lim_{n\to\infty} \prod_{i=1}^n \frac{p_i}{p_i - 1} = \lim_{n\to\infty} \prod_{i=1}^n \frac{1}{1 - \frac{1}{p_i}} = \sum_{k=1}^\infty \frac{1}{k} = +\infty$$

which gives that

$$\lim_{n\to\infty} \prod_{i=1}^n \frac{p_i - 1}{p_i} = 0$$

Now, by the definition of the limit, there exists $N \in \mathbb{N}$ such that for all $n > N$, we get

$$\prod_{i=1}^{n} \frac{p_i - 1}{p_i} < \left(\frac{1}{\prod_{i=1}^{J-1} \frac{p_i}{p_i - 1}} \right) \varepsilon$$

Thus

$$x_N = \prod_{i=0}^{J} \frac{p_{i+J} - 1}{p_{i+J}} = \left(\prod_{i=1}^{N+J} \frac{p_i - 1}{p_i} \right) \left(\prod_{i=1}^{J-1} \frac{p_i}{p_i - 1} \right) < \varepsilon$$

Thus, $0 < x_N < \varepsilon$.

Now, we know that after some J, x_n is within ε of 1, the sequence is monotonically decreasing and within ε of each other as well, and for large enough N, we are also within ε of 0. So for any $\alpha \in [0, 1]$, we have that $(x_n) \cap (\alpha - \varepsilon, \alpha + \varepsilon) \neq \emptyset$, and there are infinitly points in the intersection. So $\{x_n\}$ is dense in $[0, 1]$, hence we must always have that α is a limit point for some subsequence of (x_{n_k}) of (x_n). Thus, we can always find a subsequence (n_k) such that

$$\lim_{k \to \infty} x_{n_k} = \lim_{k \to \infty} \frac{\phi(n_k)}{n_k} = \alpha$$