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. 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. Furthermore, $a_{n+2} \pmod{2023}, a_{n+1} \pmod{2023}, a_n \pmod{2023}, 5^n \pmod{2023}, n \pmod{2023}$ determines the value $a_{n+3} \pmod{2023}$, since ff (need to consider $n \implies n^2$).

Let $k = 2023^5 + 1$, and consider the a_k. By the pigeon-hole principle, there must exist some m such that $(a_{k+2}, a_{k+1}, a_k, 5^k, k) = (a_{m+2}, a_{m+1}, a_m, 5^m, m)$ (recall that these are all modulo 2023), and thus we must have that $a_{k+i} = a_{m+i}$ for all $i \in \mathbb{N}$, as we proved before. Thus, (a_n) is periodic with period $p = k - m$.

Note that $a_0 = 0$, thus, it is sufficient to show that $a_0 = a_{0+p}$. To prove this, assume for the sake of contradiction that there is some least $j > 0$ where $a_{j+p} = a_j$ but $a_{j+p-1} \neq a_{j-1}$. Then $(a_{j+2}, a_{j+1}, a_j, 5^j, j) = (a_{j+p+2}, a_{j+p+1}, a_{j+p}, 5^{j+p}, j+p)$ and $(a_{j+1}, a_j, a_{j-1}, 5^{j-1}, j-1) \neq (a_{j+p+1}, a_{j+p}, a_{j+p-1}, 5^{j+p-1}, j+p-1)$. But then we have one of $a_{j-1} \neq a_{j+p-1} \pmod{2023}$, $5^{j-1} \neq 5^{j+p-1} \pmod{2023}$, or $j - 1 \neq n + p - 1 \pmod{2023}$. ff

ff we can repeat this process with $j - 1$, until we get to $j = 0$.

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 $p_i = 2$, then $x^3 \equiv 1 \pmod{2}$ is solved whenever x^3 is odd, which has one solution mod 2, namely $x = 1$. 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. If $n = \prod_{i=1}^{\pi(n)} p_i^{\alpha_i}$, then

$$\phi(n) = \prod_{i=1}^{\pi(n)} (p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = n \prod_{\substack{p|n \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right)$$

Thus

$$\frac{\phi(n)}{n} = \prod_{\substack{p|n \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right)$$

To show that $\{\frac{\phi(n)}{n}\}$ is dense in $(0, 1)$, let $x, y \in (0, 1)$ where $x < y$, then we claim there exists n such that $x < \frac{\phi(n)}{n} < y$. It is sufficient to consider when $x, y \in \mathbb{Q} \cap (0, 1)$. Let $x = p_1'/q_1$ and $y = p_2'/q_2$ where $p_i' < q_i$ and $\gcd(p_i', q_i) = 1$. We can rewrite them to have the same denomonator: $x = p_1/q$ and $y = p_2/q$, where $p_1 < p_2 < q$. Note $1 - \frac{1}{p} = \frac{p-1}{p}$. Choose the p such that $p \mid q$ (I want something more, like the product of all the primes is q). So let's just assume that q's prime decomposition only has exponents 1 (and then could show this is dense) so then we want $p_1 < \prod(p - 1) < p_2$. Perhaps if it is too big, then we find more p later and multiply it down. If it is too small, ff

This is the problem: we can't write every rational number as a product of $(p-1)/p$, or even every rational with denominator whose prime number decomposition do not have extra exponents. But somehow we achieve density.

Note that $\prod(1 - \frac{1}{p})$ converges iff $\sum -\frac{1}{p}$ converges (stack exchange link in source code). But I don't think we really care.

Maybe useful: the rationals in simplified form do not contain any shared primes between the numerator and denominator.

Maybe we do a completely different approach to density. What if $n = q$ or something.