Putnam 2023 Solutions

Session A

A1. For a positive integer n, let $f_n(x) = \cos(x)\cos(2x)\cos(3x)\cdots\cos(nx)$. Find the smallest n such that $|f_n''(0)| > 2023$.

Answer. $n = 18$.

Solution. Denote $p_j(x) = \cos(jx)$. Then $f_n(x) = p_1(x)\cdots p_n(x)$. By product rule, we have

$$f_n'(x) = \sum_{i=1}^{n} p_i'(x) \prod_{j\neq i} p_j(x)$$

and

$$f_n''(x) = \sum_{i=1}^{n} p_i''(x) \prod_{j\neq i} p_j(x) + \sum_{i\neq j} p_i'(x)p_j'(x) \prod_{k\neq i,j} p_k(x)\,.$$

Notice that $p_j'(x) = -j\sin(jx)$, so $p_j'(0) = 0$ for all $j \geq 1$. Also, $p_j''(x) = -j^2\cos(jx)$m so $p_j''(0) = -j^2$. This gives $f_n''(x) = \sum_{i=1}^{n} -i^2$ and our task is to determine the smallest n such that $\frac{n(n+1)(2n+1)}{6} = \sum_{i=1}^{n} i^2 > 2023$. We have $\frac{17(18)(35)}{6} = 1785$ and $\frac{18(19)(37)}{6} = 2109$, thereby giving the answer $n = 18$.

A2. Let n be an even positive integer. Let p be a monic, real polynomial of degree $2n$; that is to say, $p(x) = x^{2n} + a_{2n-1}x^{2n-1} + \cdots + a_1x + a_0$ for some real coefficients $a_0, \ldots, a_{2n-1}$. Suppose that $p(1/k) = k^2$ for all integers k such that $1 \leq |k| \leq n$. Find all other real numbers x for which $p(1/x) = x^2$.

Answer. $x = \pm\frac{1}{n!}$.

Soluton. Consider the polynomial $Q(x) = x^2p(x) - 1$. It has degree $2n+2$, and also monic. By looking at the constant coefficient, the product of all roots in Q is -1, and by looking at the linear coefficient, we have $\sum_r \frac{P}{r} = 0$, where the sum is taken over all the roots.

By the problem condition, we are given that $2n$ of the roots are $\frac{1}{k}$ for $k = \pm1, \cdots, \pm n$, leaving us two more roots to be found, namely a and b. We now have $-1 = ab\prod_{k=1}^{n}\frac{1}{k}\cdot\frac{1}{-k} = \frac{1}{(n!)^2}$, so $ab = -(n!)^2$. In addition, $0 = \sum_r \frac{1}{r} = \frac{1}{a} + \frac{1}{b} + \sum_{k=1}^{n} k + (-k)$, and therefore $a + b = 0$. Thus we have $b = -a$ and $\{a, b\} = \{n!, -n!\}$, giving the roots above as desired.

A3. Determine the smallest positive real number r such that there exist differentiable functions $f : \mathbb{R} \to \mathbb{R}$ and $g : \mathbb{R} \to \mathbb{R}$ satisfying

(a) $f(0) > 0$;

(b) $g(0) = 0$;

(c) $|f'(x)| \leq |g(x)|$ for all x;

(d) $|g'(x)| \leq |f(x)|$ for all x; and

(e) $f(r) = 0$.

Answer. $r = \frac{\pi}{2}$.

Solution. The example can be taken with $f(x) = \cos x$ and $g(x) = \sin x$, so all the inequalities become equality.

To show that no smaller r is possible, consider any functions f and g satisfying the conditions above. Let r be smallest possible choice for which $f(r) = 0$; we have $f(x) > 0$

for all $x \in (0, r)$, and thus $f(x) = |f(x)|$. Denote, now, $F(x) = \int_0^x f(y)dy$, then

$$|g(x)| = \left| \int_0^x g'(y)dy \right| \leq \int_0^x |g'(y)|dy \leq \int_0^y f(y)dy = F(x)$$

and therefore $-f'(x) \leq |g(x)| \leq F(x)$.

Now consider the following integration by parts procedure, bearing in mind that $\sin(0) = f(r) = F(0) = 0$:

$$\begin{aligned}\int_0^r f(x)\cos x dx &= \sin r f(r) - \sin 0 f(0) - \int_0^r f'(x)\sin x dx \\ &\leq \int_0^r F(x)\sin x dx \\ &= -F(r)\cos r + F(0)\cos 0 + \int_0^r f(x)\cos x dx\end{aligned}$$

and therefore $F(r)\cos r \leq 0$. Since $f(x) > 0$ for $x \in (0, r)$, we have $F(r) > 0$. Thus $\cos r \leq 0$ and so $r \geq \frac{\pi}{2}$.

A5. For a nonnegative integer k, let $f(k)$ be the number of ones in the base 3 representation of k. Find all complex numbers z such that

$$\sum_{k=0}^{3^{1010}-1} (-2)^{f(k)}(z+k)^{2023} = 0$$

Answer. There are three roots, given by $\ell = -\frac{3^{1010}-1}{2}$ and $\ell \pm \frac{\sqrt{3^{2020}-1}}{4} i$.

Solution. We define the polynomial

$$P(z, a, b, n) = \sum_{k=0}^{3^b-1} (-2)^{f(k)}(z+ak)^n$$

noting that $P(z, a, 0, n) = z^n$.

We first show that $P(z, a, b, n)$ is a linear combination of $P(z+a, 3a, b-1, n')$ for $\{n' : 0 \leq n' < n, n-n' \text{ even}\}$. Indeed, we first note that $f(3k) = f(3k+2) = f(k)$ while $f(3k+1) = f(k)+1$. Thus:

$$\begin{aligned}P(z, a, b, n) &= \sum_{k=0}^{3^{b-1}-1} (-2)^{f(3k)}(z+3ak)^n + (-2)^{f(3k+1)}(z+a(3k+1))^n + (-2)^{f(3k+1)}(z+a(3k+2))^n \\ &= \sum_{k=0}^{3^{b-1}-1} (-2)^{f(k)}\left((z+a(3k+1)-a)^n - 2(z+a(3k+1))^n + (z+a(3k+1)+a)^n\right) \\ &= \sum_{k=0}^{3^{b-1}-1} (-2)^{f(k)} \sum_{m=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2m} a^{2m}(z+a(3k+1))^{n-2m} \\ &= \sum_{m=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2m} a^{2m} \left(\sum_{k=0}^{3^{b-1}-1} (-2)^{f(k)}(z+a(3k+1))^{n-2m} \right) \\ &= \sum_{m=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2m} a^{2m} P(z+a, 3a, b-1, n-2m)\end{aligned}$$

Next, we show that $P(z, a, b, n) = 0$ if $n < 2b$. Here, we will induct on b for $b \geq 1$. For $b = 1$, we note that by the expansion above, if $n \leq 1$ then $P(z, a, b, n) = 0$. Now for some $b > 1$ and $n < 2b$, suppose the induction hypothesis holds for $b-1$. Note now that $P(z,a,b,n)$ is a linear combination of $P(z,a,b-1,m)$ where $m \le n-2$. Thus $m = n-2 < 2b-2 = 2(b-1)$, completing the induction.

We now get back to our problem, with $b = 1010$ and $n = 2b+3$, where all we need to do is to consider the following two expressions:

$$P(z,a,b,2b+1) = a^2\binom{2b+1}{2}P(z+a,3a,b-1,2b-1)$$

$$P(z,a,b,2b{+}3) = a^2\left(\binom{2b+3}{2}P(z+a,3a,b-1,2b+1) + \binom{2b+3}{4}a^2P(z+a,3a,b-1,2b-1)\right)$$

Note that for any $k \le b$ we can show that $P(z,a,b,2b+3) = x_{b,k}P(z+(3^{k-1}+\cdots+1)a, 3^ka, b-k, 2(b-k)+3) + y_{b,k}P(z+(3^{k-1}+\cdots+1)a, 3^ka, b-k, 2(b-k)+1)$ for some numbers $x_{b,k}$ and $y_{b,k}$. In addition, we have $x_{b,0} = 1$, $y_{b,0} = 0$, and the following recursive formula:

$$x_{b,k+1} = (3^ka)^2\binom{2(b-k)+3}{2}x_{b,k} \qquad y_{b,k+1} = (3^ka)^4\binom{2(b-k)+3}{4}x_{b,k}{+}(3^ka)^2\binom{2(b-k)+1}{2}y_{b,k}$$

Let $C(a,k) = \prod_{j=0}^{k-1}(3^ja)^2$, then $x_{b,k} = C(a,k)\prod_{j=0}^{k-1}\binom{2(b-j)+3}{2} = C(a,k)\cdot\frac{P(2b+3,2k)}{2^k}$ where $P(n,k) = n(n-1)\cdots(n-k+1)$ for $k \le n$ (i.e. $P(n,n) = n!$), and also

$$y_{b,k} = C(a,k)(1+(3a)^2+\cdots+(3a)^{2(k-1)})\cdot\frac{P(2b+3,2(k+1))}{4!\cdot 2^{k-1}}$$

Finally, denote $\ell_b = 3^{b-1}{+}3^{b-2}{+}\cdots 1 = \frac{3^b-1}{2}$. Then our original polyomial $P(z,a,b,2b{+}3)$ can now be written as (where $k = b$)

$$P(z,a,b,2b+3) = x_{b,b}P(z+\ell_ba, 3^ba, 0, 3) + y_{b,b}P(z+\ell_ba, 3^ba, 0, 1)$$

$$= C(a,b)\frac{P(2b+3,2b)}{2^b}(z{+}\ell_ba)^3{+}C(a,b){\cdot}\frac{P(2b+3,2(b+1))}{4!\cdot 2^{b-1}}(z{+}\ell_ba)(1{+}(3a)^2{+}\cdots{+}(3a)^{2(b-1)})$$

$$= C(a,b)\frac{P(2b+3,2b)}{2^b}(z+\ell_ba)\left((z+\ell_ba)^2 + \frac{1}{2}\cdot\frac{(3a)^{2b}-1}{9a-1}\right)$$

Since $C(a,b)$ and $\frac{P(2b+3,2b)}{2^b}$ are nonzero, it then follows that the roots are $-\ell_ba$ and $-\ell_ba \pm \sqrt{\frac{(3a)^{2b}-1}{2(9a-1)}}$.

In particular, by subtituting $a = 1$ and $b = 1010$ we get our answer.

Session B

B1. Consider an m-by-n grid of unit squares, indexed by (i,j) with $1 \le i \le m$ and $1 \le j \le n$. There are $(m-1)(n-1)$ coins, which are initially placed in the squares (i,j) with $1 \le i \le m-1$ and $1 \le j \le n-1$. If a coin occupies the square (i,j) with $i \le m-1$ and $j \le n-1$ and the squares $(i+1,j)$, $(i,j+1)$, and $(i+1,j+1)$ are unoccupied, then a legal move is to slide the coin from (i,j) to $(i+1,j+1)$. How many distinct configurations of coins can be reached starting from the initial configuration by a (possibly empty) sequence of legal moves?

Answer. $\binom{m+n-2}{m-1}$.

Solution. Instead of moving coins, we 'move' holes determined by those squares with no coin. Notice that in the beginning there are $m+n-1$ holes on the top edge (m,j) and the right edge (i,n). A valid move of sliding hole at (i,j) with $i \ge 2, j \ge 2$ is as follows: $(i-1,j)$ and $(i,j-1)$ are both holes, and $(i-1,j-1)$ is not a hole (we say it's occupied, i,e, with a coin), and then we slide the hole from (i,j) from $(i-1,j-1)$. Now for a hole at (i,j), consider the difference of coordinates $y-x$ as $d(i,j)=j-i$. Note that this opertion stays the same after the move. Considering that the initial positions of the holes are $(m,1),(m,2),\cdots,(m,n),(m-1,n),\cdots,(1,n)$, the $d(\cdot)$ of the coins are $1-m,2-m,\cdots,n-1$, which are $m+n-1$ distinct integers. It follows that at any stage, for each $x\in\{1-m,\cdots,n-1\}$ we have exactly each hole with $d(\cdot)$ of x.

We now show that the configuration is valid if and only if there exists a path joining the holes in the form $u_1\to u_2\to\cdots\to u_{m+n-1}$, such that if $u_i=(i,j)$ then u_{i+1} is either $(i-1,j)$ or $(i,j+1)$. In the beginning we have

$$(m,1)\to(m,2)\to\cdots\to(m,n)\to(m-1,n)\to\cdots\to(1,n)$$

Now suppose we are to move (i,j) to $(i-1,j-1)$, we know that $(i-1,j)$ and $(i,j-1)$ are holes, and so we have the path sequence $(i,j-1)\to(i,j)\to(i-1,j)$. Note that after that we still have $(i,j-1)\to(i-1,j-1)\to(i-1,j)$, showing that this invariant is maintained.

Conversely, to show that all such configurations are attainable, consider the path $(i,j)\to(i-1,j)$ as 'left' (L) and $(i,j)\to(i,j+1)$ as 'up' (U). Initially, we have $n-1$ consecutive U's, followed by $m-1$ consecutive L's; thereafter, any switch that swaps a consecutive segment (U, L) to (L, U) is valid. Thus one algorithm would be to move each L's iteratively to the left by swapping with the U's to their target positions, starting from the leftmost L.

Thus we have a sequence of path of length $m+n-2$, with $m-1$ 'left's and $n-1$ 'up's. This gives the desired $\binom{m+n-2}{m-1}$ choices.

B2. For each positive integer n, let $k(n)$ be the number of ones in the binary representation of $2023\cdot n$. What is the minimum value of $k(n)$?

Answer. $k(n)=3$.

Solution. We first see that $2023=7\times17^2$. Write $n=2^{a_1}+\cdots+2^{a_k}$, with $0\le a_1<\cdots<a_k$. We need $k>0$ for $n>0$. We show that $k\ge3$ is necessary for $3\mid n$. To see why, observe that $7\nmid 2^j$ for all $j\ge0$; and given that $2^j\in\{1,2,4\}\pmod 7$, we see that 2^j+2^m cannot be divisible by 7 considering all possible combinations (since $7-1=6,7-2=5$ and $7-4=3$ are not a value of 2^j).

To give such a construction, we notice that $2^4=16$, and $2^{68}=(17-1)^{17}\equiv-1\pmod{17^2}$, hence $2^{69}\equiv-2\pmod{17^2}$. We also have $2^{136}\equiv1\pmod{17^2}$. Thus we want to look for distinct a,b,c such that $a\equiv69,b\equiv0,c\equiv0\pmod{136}$, which ensures $17^2\mid2^a+2^b+2^c$ (remainder $-2,1,1$). In addition, since the order of 2 modulo 7 is 3, we may also consider a,b,c such that $a\equiv2,b\equiv1,c\equiv0\pmod3$, giving $7\mid2^a+2^b+2^c$ (remainder 4, 2, 1). Finally, note that we need (a,b,c) to simultaneously fulfill both the conditions, which is doable via Chinese Remainder Theorem since $\gcd(3,136)=1$. In particular we may take:

$$a=341,b=136,c=408\,.$$

B3. A sequence $y_1,y_2,\dots,y_k$ of real numbers is called *zigzag* if $k=1$, or if $y_2-y_1,y_3-y_2,\dots,y_k-y_{k-1}$ are nonzero and alternate in sign. Let $X_1,X_2,\dots,X_n$ be chosen independently from the uniform distribution on $[0,1]$. Let $a\left(X_1,X_2,\dots,X_n\right)$ be the largest value of k for which there exists an increasing sequence of integers $i_1,i_2,\dots,i_k$ such that $X_{i_1},X_{i_2},\dots X_{i_k}$ is zigzag. Find the expected value of $a\left(X_1,X_2,\dots,X_n\right)$ for $n\ge2$.

Answer. $\frac{2n+2}{3}$.

Solution. Let X_j be a valley if $2\le j\le n-1$ and $X_j<\min\{X_{j-1},X_{j+1}\}$, and peak if $2\le j\le n-1$ and $X_j>\max\{X_{j-1},X_{j+1}\}$. Collectively we call a point a turning point if it's a valley or a peak. We claim that $a\left(X_1, X_2, \ldots, X_n\right)$ is 2+number of turning points. Indeed, an example will be to include X_1, X_n, and all the turning points, which is valid since the turning points must alternate between valleys and peaks (i.e. every two valleys must have a peak in between, and vice versa). Conversely, if $y_1, y_2, \cdots, y_k \subseteq X_1, \cdots, X_n$ is zigzag, consider, iteratively, $y_{i-1}, y_i, y_{i+1} = X_{a_{i-1}}, X_{a_i}, X_{a_{i+1}}$. If $y_i > y_{i-1}$ and $y_{i+1} > y_i$, we may replace y_i with $\max\{X_j : a_{i-1} < j < a_{i+1}\}$, so this new y_i is itself a peak (we may similarly do so for the opposite case). Repeating this for $i = 2, \cdots, k-1$ yields that there must be a sequence of length k with all (except the endpoints) being turning points, thus establishing the upper bound.

We now proceed iteratively, where for $n = 2$ we have $X_1 \neq X_2$ almost certainly, so $\mathbb{E}[a(X_1, X_2)] = 2$. We now consider what happens as we add in another number, by considering the position of the biggest number M. We show that the expected gain of $a()$ is $\frac{2}{3}$. Note that this biggest number has $\frac{1}{n+1}$ of being before X_1, and after X_n, respectively. Then the same probability between X_i and X_{i+1} for each $i = 1, \cdots, n-1$.

If M is inserted before X_1, this X_1 is a newly installed turning point if and only if $X_1 < X_2$, which happens with probability $\frac{1}{2}$. Thus the expected gain in this case is $\frac{1}{2}$, and by symmetry this also holds if M is inserted after X_n. Otherwise, consider the case where M is inserted between X_i and X_{i+1}. We see that M is always going to be a turning point (i.e. the extra addition), so it really depends on whether X_i or X_{i+1} gains or loses their status as a turning point.

By symmetry, we will only consider X_i. If $i = 1$, there is nothing to be done. Otherwise, there are two cases, depending on whether $X_i < X_{i+1}$ or $X_i > X_{i+1}$. Denote, now, $\triangle(X_i)$ as whether X_i gains $(+1)$, loses (-1), or remains (0)its turing point status. If $X_i < X_{i+1}$, then from $X_i < M$, we see that X_i is a turning point if and only if $X_{i-1} > X_i$, and that would not change after addition of M in between X_i and X_{i+1}. Thus, $\triangle(X_i) = 0$. Otherwise, $X_i > X_{i+1}$, so X_i either gains or loses its status as a turning point, depending on whether $X_{i-1} > X_i$.

In this sequel, we claim that $\mathbb{P}[X_{i-1} > X_i \mid X_i > X_{i+1}] = \frac{1}{3}$. Indeed, we see that given 3 independent uniform variables a, b, c in $[0, 1]$, we have $\mathbb{P}[a > b \mid b > c] = \frac{\mathbb{P}[a>b \wedge b>c]}{\mathbb{P}[b>c]} = 2\int_0^1 b(1-b)db = \frac{1}{3}$, as desired. In other words, conditioned on $X_i > X_{i+1}$, $\triangle(X_i)$ is 1 with probability $\frac{1}{3}$, and -1 with probability $\frac{2}{3}$, so for $i > 1$,

$$\mathbb{E}[\triangle(X_i)] = \frac{1}{2}\mathbb{E}[\triangle(X_i) \mid X_i < X_{i+1}] + \frac{1}{2}\mathbb{E}[\triangle(X_i) \mid X_i > X_{i+1}] = 0 - \frac{1}{2} \cdot \frac{1}{3} = -\frac{1}{6}$$

Thus, considering the $n+1$ possible positions of M, we have

$$\mathbb{E}[a(X_1, \cdots, X_i, M, X_{i+1}, \ldots, X_n)] - \mathbb{E}[a(X_1, \cdots, X_n)] = \frac{2}{n+1} \cdot \frac{1}{2} + \frac{n-1}{n+1} - 2 \cdot \frac{1}{6} \cdot \frac{n-2}{n+1} = \frac{2}{3}$$

establishing the conclusion.

B4. For a nonnegative integer n and a strictly increasing sequence of real numbers $t_0, t_1, \ldots, t_n$, let $f(t)$ be the corresponding real-valued function defined for $t \geq t_0$ by the following properties:

(a) $f(t)$ is continuous for $t \geq t_0$, and is twice differentiable for all $t > t_0$ other than $t_1, \ldots, t_n$;

(b) $f\left(t_0\right) = 1/2$;

(c) $\lim_{t \to t_k^+} f'(t) = 0$ for $0 \leq k \leq n$;

(d) For $0 \leq k \leq n-1$, we have $f''(t) = k+1$ when $t_k < t < t_{k+1}$, and $f''(t) = n+1$ when $t > t_n$.

Considering all choices of n and $t_0, t_1, \ldots, t_n$ such that $t_k \geq t_{k-1} + 1$ for $1 \leq k \leq n$, what is the least possible value of T for which $f\left(t_0 + T\right) = 2023$?

Answer. $T = 29$.

Solution. Consider $t \in [t_k, t_{k+1})$ (if $k = n$, we let $t_{n+1} = \infty$). We claim that $f(t) - f(t_k) = \frac{k+1}{2} \cdot (t - t_k)^2$. Note that for $t_k < t < t_{k+1}$ we have $f'(t) = \int_{t_k}^{t} f''(x)dx = \int_{t_k}^{t} (k+1)dx = (k+1)(t - t_k)$, givnen that $\lim_{t \to t_k^+} f'(t) = 0$. Thus we have $f(t) - f(t_k) = \int_{t_k}^{t} f'(x)dx = \int_{t_k}^{t} (k+1)(x - t_k)dx = \frac{k+1}{2} \cdot (t - t_k)^2$. Consequently, if $t \in [t_k, t_{k+1})$, then by the continuity of f we have $f(t) = f(t) - f(t_k) + f(t_0) + \sum_{\ell=1}^{k} f(t_\ell) - f(t_{\ell-1}) = \frac{k+1}{2} \cdot (t - t_k)^2 + \frac{1}{2} + \sum_{\ell=1}^{k} \frac{\ell}{2}(t_\ell - t_{\ell-1})^2$.

Having established that, we first give an example for $T = 29$. Consider $n = 9$, and $t_k = k$. Then $f(t_0 + T) = \frac{1}{2} + 5 \cdot (29 - 9)^2 + \sum_{\ell=1}^{9} \frac{\ell}{2} = 2023$.

To show this T is the minimum we can get, we show that $f(t_0 + T) < 2023$ must hold if $T < 29$. Denote $g_k(T) \triangleq \frac{k(k+1)}{4} + \frac{k+1}{2}(T - k)^2$.

$$f(t_0 + T) \leq \frac{1}{2} + \max_{0 \leq k \leq T} \{g_k(T)\}$$

Indeed, consider k such that $t_k \leq t_0 + T < t_{k+1}$ (so $T \geq k$), and let $d_i = t_i - t_{i-1} - 1$ for $i = 1, \cdots, d$ (so $d_i \geq 0$); we want to bound $f(t_k)$. Indeed,

$$f(t_k) - f(t_0) = \sum_{\ell=1}^{k} \frac{\ell}{2}(1 + d_i)^2 = \sum_{\ell=1}^{k} \frac{\ell}{2}(1 + d_i^2 + 2d_i) \leq \sum_{\ell=1}^{k} \left(\frac{\ell}{2} + \frac{k}{2} \cdot d_i^2 + kd_i\right)$$

$$= \frac{k(k-1)}{4} + \frac{k}{2}(1 + 2\sum_{\ell=1}^{k} d_i + \sum_{\ell=1}^{k} d_i^2) \leq \frac{k(k-1)}{4} + \frac{k}{2}(1 + 2\sum_{\ell=1}^{k} d_i + (\sum_{\ell=1}^{k} d_i)^2)$$

$$= \frac{k(k-1)}{4} + \frac{k}{2}\left(1 + \sum_{\ell=1}^{k} d_i\right)^2$$

I.e. $f(t_k) - f(t_0) \leq \frac{k(k-1)}{4} + \frac{k}{2}(t_k - t_0 - (k-1))^2$. Next, we have $f(f_0 + T) - f(t_0) \leq \frac{k(k-1)}{4} + \frac{k}{2}(t_k - t_0 - (k-1))^2 + \frac{k+1}{2}(f_0 + T - f_k)$. The function

$$\frac{k(k-1)}{4} + \frac{k}{2}(t_k - t_0 - (k-1))^2 + \frac{k+1}{2}(t_0 + T - t_k)^2$$

is convex in t_k, subject to the constraint $t_0 + k \leq t_k \leq t_0 + T$. Thus the maximum is attained when t_k is either $t_0 + k$ or $t_0 + T$, giving us the value either $g_k(T)$ or $g_{k-1}(T)$, establishing our claim.

Next, fixing T, we have $g_k(T) - g_{k-1}(T) = \frac{(T-k)(T-3k)}{2}$, suggesting that this is > 0 when $T > 3k$ and < 0 when $T < 3k$. In particular, when $T = 29$ the optimum k is $k = 9$, and $g_9(29) = 2023 - \frac{1}{2}$, so $f(t_0 + 29) \leq 2023$. Given also that f is strictly monotone increasing, we have $f(t_0 + T) < f(t_0 + 29)$ for all $T < 29$.

B5. Determine which positive integers n have the following property: For all integers m that are relatively prime to n, there exists a permutation $\pi : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ such that $\pi(\pi(k)) \equiv mk (\mathrm{mod} n)$ for all $k \in \{1, 2, \ldots, n\}$.

Answer. $n = 1$ and all $n \equiv 2 \pmod 4$.

Solution. We first charaterize all permutations ρ of $1, 2, \ldots, n$ such that there exists a permutation π with $\rho = \pi^2$. We claim that ρ fulfills this condition if and only if the following holds: let $c_\rho(m)$ be the number of cycles in ρ with size m, then $c_\rho(m)$ is even for all even m. To see why, consider π with cycles $C_1, \cdots, C_k$, Consider any cycle

$C_i = a_{i,1} \to a_{i,2} \to \cdots \to a_{i,m} \to a_{i,1}$ (that is, $u \to v$ denoted by $\pi(u) = v$). If the size m is odd, then in π^2, the set of C_i is retained, except in different order $a_{i,1} \to a_{i,3} \to \cdots \to a_{i,m} \to a_{i,2} \to \cdots \to a_{i,m-1} \to a_{i,1}$. Otherwise, in π^2, C_i is split into two cycles of the same size $\frac{m}{2}$:

$$a_{i,1} \to a_{i,3} \to \cdots \to a_{i,m-1} \to a_{i,1} \qquad a_{i,2} \to \cdots \to a_{i,m} \to a_{i,2}$$

Therefore, all the odd cycles are repermuted and all the even cycles are broken into two, giving us the following:

$$c_\rho(m) = \begin{cases} c_\pi(m) + 2c_\pi(2m) & m \text{ odd} \\ 2c_\pi(2m) & m \text{ even} \end{cases}$$

(note that $c_\pi(m) = 0$ for all $m > n$), so $c_\rho(m)$ is indeed even for m even.

Conversely, if $c_\rho(m)$ is even for all even m, then we may construct π by pairing all even cycles in ρ, and retain the odd cycles (again, repermuting). That is, for a cycle $C_i = a_{i,1} \to a_{i,2} \to \cdots \to a_{i,m} \to a_{i,1}$ with odd m, we permute the elements in a way such that $a_{i,j} \to a_{i,j+\frac{m+1}{2}}$, and for two cycles of length m (with m even) $C_i = a_{i,1} \to a_{i,2} \to \cdots \to a_{i,m} \to a_{i,1}$ and $C_j = a_{j,1} \to a_{j,2} \to \cdots \to a_{j,m} \to a_{i,1}$, we may merge them together and obtain

$$a_{i,1} \to a_{j,1} \to a_{i,2} \to a_{j,2} \to \cdots \to a_{i,m} \to a_{j,m} \to a_{i,1}$$

Now going back to the problem, we first identify a construction for $n = 4k + 2$. Now if $\gcd(m, n) = 1$, then m is odd. We note that $mk \equiv k \pmod 2$, so each cycle must have all its elements of the same parity. In addition, there exists an injective map φ from $\{1, 3, \cdots, n-1\} \to \{2, 4, \cdots, n\}$ such that $\varphi(m) \equiv 2m$, because if $m \neq k$ are odd then $\frac{n}{2} \nmid m - k$ (note that $\frac{n}{2}$ is odd here) and therefore $n \nmid 2(m-k)$. Thus, for each cycle $C_i = a_{i,1} \to a_{i,2} \to \cdots \to a_{i,m} \to a_{i,1}$ with all elements odd (via the map $u \to ku$), it follows that we also have another cycle $2a_{i,1} \to 2a_{i,2} \to \cdots \to 2a_{i,m} \to 2a_{i,1}$, all of even parity. It follows that all odd cycles can have an 'even' cycle partner to be paired up, so the permutation $\rho(m) = km$ has $c_\rho(m)$ even for all $m = 1, \cdots, n$.

To show that these are the only solutions, we first consider $n = 4k$, and $m = n - 1$. Then $km \equiv -m$, so we have the following cycles:

$$(n), (\frac{n}{2}), (1, n-1), \cdots, (\frac{n}{2} - 1, \frac{n}{2} + 1)$$

Notice that there are $\frac{n}{2} - 1$ cycles of length 2, i.e. odd quantity. Thus this n cannot work.

Now suppose $n > 1$ is odd. Denote its prime factorization as $\prod_{i=1}^{\ell} p_i^{\alpha_i}$, and let $p \geq 3$ be the smallest such prime. Consider, now, q_i as a primitive root of $p_i^{\alpha_i}$, and choose $k \equiv q_i \pmod{p_i}$ for all $i = 1, \cdots, \ell$ (which exists by Chinese Remainder Theorem). We show that under $\rho(m) = km$, only one cycle can have length $p - 1$ (which is even). First, consider the numbers $\{m \cdot \frac{n}{p} : m = 1, 2, \cdots, p-1\}$; this forms its own (single) cycle because the minimum positive j with $p \mid k^j - 1$ is $j = p - 1$. To show no other numbers can in a cycle of length $p - 1$, we note that by our choice of k, $k^j - 1$ cannot be divisible by q for other prime divisors $q \neq p$ of n, and in addition, if $p^2 \mid n$, cannot be divisible by p^2. It follows that for each m with $k^{p-1}m \equiv m \pmod n$, we have $\frac{n}{p} \mid m$, showing that m is either n (cycle length 1) or in the form of $m' \cdot \frac{n}{p}$. Thus this completes the proof showing that $n > 1$ odd cannot be.