Polynomial PSet Solutions

Note: Problems A1, A2, B2, B8, C2, D2, E3, and E6 were done in class.

(A) Values and Roots

1. Rearrange to get
$$(x+1)P(x) - x = 0 \text{ for } x = 0, 1, \ldots, n.$$
Since this equation has roots $x = 0, 1, \ldots, n$, and the left-hand side has degree $n+1$,
$$(x+1)P(x) - x = kx(x-1)\cdots(x-n)$$
for some integer k. Then
$$P(x) = \frac{kx(x-1)\cdots(x-n)+x}{x+1}.$$
The numerator must be divisible by $x+1$ so must have $x=-1$ as a zero. Plugging in, we get $(-1)^{n+1}(n+1)!k - 1 = 0$, or $k = \frac{(-1)^{n+1}}{(n+1)!}$. Plugging in $x = n+1$ gives
$$P(n+1) = \begin{cases} 1, & n \text{ odd} \\ \frac{n}{n+2}, & n \text{ even} \end{cases}$$

2. This time it's easier to guess the solution. The polynomial
$$Q(x) = \sum_{i=0}^{n} \binom{x}{i} (r-1)^i$$
has degree n and by the Binomial Theorem, satisfies the given conditions. Since $P(x) = Q(x)$ for $n+1$ values of x, actually P, Q are the same polynomial, and
$$P(n+1) = Q(n+1) = \left(\sum_{i=0}^{n+1} \binom{n+1}{i} (r-1)^i\right) - (r-1)^{n+1} = r^{n+1} - (r-1)^{n+1}.$$

3. Letting ray OQ_1 be the positive real axis, Q_i represent the nth roots of unity ω^i in the complex plane. Hence PQ_i equals $|2 - \omega^i|$. The roots of $x^n - 1 = 0$ are just the nth roots of unity, so $x^n - 1 = \prod_{i=0}^{n-1}(x - \omega^i)$. Plugging in $x = 2$ gives $\prod_{k=1}^{n} |PQ_i| = 2^n - 1$.

4. The given condition says
$$f(x)^2 = x(x-1)\cdots(x-n)Q(x) + x^2 + 1 \tag{1}$$
for some polynomial $f(x)$ of degree at most n. Plugging $x = 0, 1, \ldots, n$ into (1) gives
$$f(x) = \pm\sqrt{x^2+1}, \text{ when } x = 0, 1, \ldots, n. \tag{2}$$

The following is key: Given $n+1$ points $(x_0, y_0), \ldots, (x_n, y_n)$ with distinct x-coordinates, there exists exactly one polynomial f of degree at most n so that $f(x_i) = y_i$ for $i = 0, 1, \ldots, n$.

Applying this to (2) we get 2^{n+1} possibilities for $f(x)$ since we have 2 choices of sign for each of $x = 0, 1, \ldots, n$. If $f(x)$ is a solution to (2) then so is $-f(x)$; we get 2^n possibilities for $f(x)^2$. Solve (1) to get 2^n possibilities for $Q(x)$:

$$Q(x) = \frac{f(x)^2 - x^2 - 1}{x(x-1)\cdots(x-n)}$$

Each such polynomial is a valid solution because $f(x)^2 - x^2 - 1$ is zero at $x = 0, 1, \ldots, n$ and hence is divisible by $x(x-1)\cdots(x-n)$.

5. Clearing denominators,

$$\sum_{i=1}^{5} \left[a_i x \prod_{i \neq j, 1 \leq j \leq 5} (x+j) \right] - (x+1)(x+2)(x+3)(x+4)(x+5) = 0$$

for $x = 1, 4, 9, 16, 25$. Let $f(x)$ denote the LHS. Since $f(x) = 0$ has the roots $x = 1, 4, 9, 16, 25$, we conclude that $(x-1)(x-4)\cdots(x-25)$ divides $f(x)$. Since $f(x)$ has degree at most 5,

$$f(x) = k(x-1)(x-4)(x-9)(x-16)(x-25)$$

for some constant k. However, equating

$$f(0) = [-(x+1)(x+2)(x+3)(x+4)(x+5)]_{x=0} = -5!$$

and $f(0) = -k \cdot 5!^2$ gives $k = \frac{1}{5!}$. Thus

$$f(x) = \frac{1}{5!}(x-1)(x-4)(x-9)(x-16)(x-25).$$

Then

$$\begin{aligned} \sum_{i=1}^{5} \frac{a_i}{6^2+i} &= \frac{f(6^2)}{x(x+1)(x+2)(x+3)(x+4)(x+5)|_{x=6^2}} - \frac{1}{6^2} \\ &= \frac{187465}{6744582}. \end{aligned}$$

6. Suppose $|p(x) - r^x| < 1$ for $x = 0, 1, \ldots, n$. Let $y_i = p(i)$ for $0 \leq i \leq n$. By the Lagrange Interpolation Formula,

$$p(x) = \sum_{i=0}^{n} \left[y_i \prod_{j \neq i} \frac{x-j}{i-j} \right].$$

When $r^i - 1 \le y_i \le r^i + 1$, $p(n+1)$ is maximized when we take $y_i = r^i - 1$ when the product is negative (i.e. when $n - i$ is odd) and y_i when the product is positive (i.e. when $n - i$ is even):

$$\begin{aligned} p(n+1) &< \sum_{i=0}^{n} (r^i + (-1)^{n-i}) \prod_{j \neq i} \frac{(n+1) - j}{i - j} \\ &= \sum_{i=0}^{n} (r^i + (-1)^{n-i})(-1)^{n-i} \frac{(n+1)!}{i!(n+1-i)!} \\ &= \sum_{i=0}^{n} \left[\binom{n+1}{i} r^i (-1)^{n-i} + \binom{n+1}{i} \right] \\ &= -((r-1)^{n+1} - r^{n+1}) + (2^{n+1} - 1) \qquad \text{by the Binomial Theorem} \\ &= r^{n+1} - 1 + 2^{n+1} - (r-1)^{n+1} \le r^{n+1} - 1 \end{aligned}$$

An alternate solution is to use Lagrange Interpolation with $n+2$ points and show that the coefficient of x^{n+1} cannot be 0.

7. Given two points (x_1, y_1) and (x_2, y_2) the equation

$$\frac{y - y_1}{y_2 - y_1} = \frac{x - x_1}{x_2 - x_1} \implies (y - y_1)(x_2 - x_1) = (x - x_1)(y_2 - y_1)$$

represents the line passing through these two points (it is a linear equation satisfied by the coordinares of the two points). It follows that three points (x_1, y_1), (x_2, y_2) and (x_3, y_3) lie on the same line if and only if the condition

$$(y_3 - y_1)(x_2 - x_1) = (x_3 - x_1)(y_2 - y_1) \tag{3}$$

holds. Now suppose that (x_1, y_1), (x_2, y_2) and (x_3, y_3) represent the (changing) coordinates of the three ducks as they waddle along their paths. Each coordinate is a linear function of time t, so (3) is an equation in t of degree at most 2 (i.e., is a quadratic). If such an equation has more than 2 solutions then it must reduce to an identity and thus hold true for all values of t. That is, if the ducks are in a row at more than two times, then they are always in a row.

8. Note that $g(x)$ is one of the 16 integer divisors of 2008 for each of the 81 integer roots. There must be at least 6 roots of $f(x)$ for which $g(x)$ has the same value. Since $g(x)$ is nonconstant, its degree must be greater than 5.

9. Let $p(x)$ be the monic real polynomial of degree n. If $n = 1$, then $p(r) = r + a$ for some real number a, and $p(x)$ is the average of x and $x + 2a$, each of which has 1 real root. Now we assume that $n > 1$. Let

$$g(x) = (x-2)(x-4)\cdots(x-2(n-1)).$$

The degree of $g(x)$ is $n - 1$. Consider the polynomials

$$q(x) = x^n - kg(x), r(x) = 2p(x) - q(x) = 2p(x) - x^n + kg(x).$$

We will show that for large enough k these two polynomials have n real roots. Since they are monic and their average is clearly $p(x)$, this will solve the problem.

Consider the values of the polynomial $g(x)$ at n points $x = 1, 3, 5, \ldots, 2n-1$. These values alternate in sign and are at least 1 (since at most two of the factors have magnitude 1 and the others have magnitude at least 2). On the other hand, there is a constant $c > 0$ such that for $0 \leq x \leq n$, we have $|x^n| < c$ and $|2p(x) - x^n| < c$. Take $k > c$. Then we see that $q(x)$ and $r(x)$ evaluated at n points $x = 1, 3, 5, \ldots, 2n-1$ alternate in sign. Thus $q(x)$ and $r(x)$ each has at least $n-1$ real roots. However since they are polynomials of degree n, they must have n real roots, as desired.

10. Without loss of generality, suppose $n = \deg(f) \geq \deg(g)$. Let $r_1, \ldots, r_k$ be the distinct roots of f and let $s_1, \ldots, s_l$ be the distinct roots of $f - 1$.

We claim that $k + l \geq n + 1$. Indeed, suppose

$$f(x) = (x - r_1)^{p_1} \cdots (x - r_k)^{p_k}.$$

Then

$$(x - r_1)^{p_1 - 1} \cdots (x - r_k)^{p_k - 1} \mid f'.$$

Similarly, if

$$f(x) - 1 = (x - s_1)^{q_1} \cdots (x - s_l)^{q_l},$$

then

$$(x - s_1)^{q_1 - 1} \cdots (x - s_l)^{q_l - 1} \mid f'.$$

Since the roots of f and $f - 1$ are distinct,

$$(x - r_1)^{p_1 - 1} \cdots (x - r_k)^{p_k - 1} (x - s_1)^{q_1 - 1} \cdots (x - s_l)^{q_l - 1} \mid f'.$$

Since f' has degree $n - 1$,

$$(p_1 - 1) + \ldots + (p_k - 1) + (q_1 - 1) + \ldots (q_l - 1) \leq n - 1.$$

Since $p_1 + \ldots + p_k = q_1 + \ldots + q_l = n$, this gives $(n - k) + (n - l) \leq n - 1$, or $k + l \geq n + 1$.

Now $f - g$ has degree at most n and has at least $n+1$ distinct roots $r_1, r_2, \ldots, r_k, s_1, \ldots, s_l$, so it must be identically 0, and $f = g$.

11. Suppose f, g have no common nonconstant factor. Consider f, g as elements of $\mathbb{C}(x)[y]$. Since $\mathbb{C}(x)$ is a field, $\mathbb{C}(x)[y]$ is a principal ideal domain. From Gauss's Lemma applied to the ring $\mathbb{C}[x]$ and its fraction field $\mathbb{C}(x)$, any two polynomials with no common factor in $\mathbb{C}[x][y]$ have no common factor in $\mathbb{C}(x)[y]$. Hence the greatest common divisor of f, g in $\mathbb{C}(x)[y]$ is 1, and we can write

$$1 = u(x, y) f(x, y) + v(x, y) g(x, y)$$

for some $u, v \in \mathbb{C}(x)[y]$. Multiplying to clear denominators in u, v, we get

$$p(x) = s(y) f(x, y) + t(y) g(x, y).$$

Any zero (x, y) of both f and g must satisfy $p(x) = 0$. Since p is a nonzero polynomial, it has finitely many zeros, i.e. there are finitely many possibilities for x. Each value gives a polynomial equation in y, which again has finitely many zeros.

(B) Arithmetic Properties

1. Take n so that $P(n)$ is nonzero. Suppose it is prime. Now $P(n) \mid P(n + kP(n)) - P(n) \Rightarrow P(n) \mid P(n + kP(n))$ for all $k \in \mathbb{Z}$. If $P(x)$ is not composite for all integer x, then $P(n + kP(n))$ is $\pm P(n)$ or 0 for all $k \in \mathbb{Z}$. P attains one of these values infinitely many times so is constant.

2. If not, then no two are equal. Without loss of generality, assume that c is between a and b. Then
$$|P(a) - P(b)| = |c - b| < |b - a|.$$
However, $b - a \mid P(b) - P(a)$, a contradiction.

3. We first show that every fixed point x of Q is in fact a fixed point of $P \circ P$. Consider the sequence given by $x_0 = x$ and $x_{i+1} = P(x_i)$ for $i \geq 0$. Assume $x_k = x_0$. Then
$$d_i := x_{i+1} - x_i | P(x_{i+1}) - P(x_i) = x_{i+2} - x_{i+1} = d_{i+1}$$
for all i, which together with $d_k = d_0$ implies $|d_0| = |d_1| = \cdots = |d_k|$. Suppose $d_1 = d_0 = d \neq 0$. Then $d_2 = d$ as otherwise $x_3 = x_1$ and x_0 will never occur in the sequence again. Similarly $d_i = d$ for all i and $x_i = x_0 + id \neq x_0$ for all i, a contradition. It follows that $d_1 = -d_0$, as claimed. Thus we can assume $Q = P \circ P$.

   If every integer t with $P(P(t)) = t$ also satisfies $P(t) = t$, the number of solutions is at most $\deg(P) = n$. Suppose $P(t_1) = t_2, P(t_2) = t_1, P(t_3) = t_4, P(t_4) = t_3$, where t_1 is not equal to any of t_2, t_3, t_4. Since $t_1 - t_3$ divides $t_2 - t_4$ and vice versa, we conclude $t_1 - t_3 = \pm(t_2 - t_4)$. Assume $t_1 - t_3 = t_2 - t_4$, i.e. $t_1 - t_2 = t_3 - t_4 = u \neq 0$. Since the relation $t_1 - t_4 = \pm(t_2 - t_3)$ similarly holds, we obtain $t_1 - t_3 + u = \pm(t_1 - t_3 - u)$, which is impossible. Therefore, we must have $t_1 - t_3 = t_4 - t_2$, which gives us $P(t_1) + t_1 = P(t_3) + t_3 = c$ for some c. It follows that all integral solutions t of the equation $P(P(t))$ satisfy $P(t) + t = c$, and their number does not exceed n.

4. Induct on the degree. If f has degree n with leading coefficient c, then the first nonzero term in the representation must be $\frac{c}{u_n} p_n(x)$ and $f(x) - \frac{c}{u_n} p_n(x)$ can be uniquely written as $a_{n-1}p_{n-1}(x) + \ldots + a_1 p_1(x) + a_0 p_0(x)$ by the induction hypothesis.

5. The assertions $(a) \Rightarrow (b)$ and $(c) \Rightarrow (a)$ are clear ($\binom{x}{i}$ are integers for all integers x and nonnegative integers i).

   Suppose (b) holds. First assume that $f(x)$ takes on integer values at $0, 1, \ldots, n$. We inductively build the sequence $a_0, a_1, \ldots$ so that the polynomial
$$P_m(x) = a_m \binom{x}{m} + a_{m-1} \binom{x}{m-1} + \cdots + a_0 \binom{x}{0}$$
matches the value of $f(x)$ at $x = 0, \ldots, m$. Define $a_0 = f(0)$; once $a_0, \ldots, a_m$ have been defined, let
$$a_{m+1} = f(m + 1) - P_m(m + 1).$$
Noting that $\binom{x}{m+1}$ equals 1 at $x = m+1$ and 0 for $0 \leq x \leq m$, this gives $P_{m+1}(x) = f(x)$ for $x = 0, 1, \ldots, m + 1$. Now $P_n(x)$ is a degree n polynomial that agrees with $f(x)$ at $x = 0, 1, \ldots, n$, so they must be the same polynomial.

Now if f takes on integer values for any $n+1$ consecutive values, then by the argument above on the translated function it takes on integer values for all x; in particular, for $x = 0, 1, \ldots, n$. Use the above argument to get the desired representation in (c).

6. Replacing $f(x)$ by $f(x) - f(n)$ as necessary, it suffices to show

$$\operatorname{lcm}[1, 2, \ldots, \deg(f)] \cdot \frac{f(m)}{m} \in \mathbb{Z}.$$

Letting $d = \deg(f)$ and writing f as in Problem 5, the above expression equals

$$\operatorname{lcm}(1, 2, \ldots, d) \sum_{i=0}^{d} \frac{a_i}{m} \binom{m}{i} = \operatorname{lcm}(1, 2, \ldots, d) \sum_{i=0}^{d} \frac{a_i}{i} \binom{m-1}{i-1}.$$

Each term is an integer because $i \mid \operatorname{lcm}(1, 2, \ldots, d)$ for all $1 \le i \le d$.

7. **Step 1** Suppose P has degree d. Let Q be the polynomial of degree at most d with $Q(x) = q_x$ for $0 \le x \le d$. Since the q_x are all integers, Q has rational coefficients, and there exists k so that kQ has integer coefficients. Then $m - n | kQ(m) - kQ(n)$ for all $m, n \in \mathbb{N}_0$.

Step 2 We show that Q is the desired polynomial.

Let $x > n$ be given. Now

$$kq_x \equiv kq_m \pmod{x - m} \text{ for all integers } m \in [0, d]$$

Since $kQ(x)$ satisfies these relations as well, and $kq_m = kQ(m)$,

$$kq_x \equiv kQ(x) \pmod{x - m} \text{ for all integers } m \in [0, d]$$

and hence

$$kq_x \equiv kQ(x) \pmod{\operatorname{lcm}(x, x-1, \ldots, x-d)}. \tag{4}$$

Now

$$\begin{aligned}
\operatorname{lcm}(x, x-1, \ldots, x-i-1) &= \operatorname{lcm}[\operatorname{lcm}(x, x-1, \ldots, x-i), x-i-1] \\
&= \frac{\operatorname{lcm}(x, x-1, \ldots, x-i)(x-i-1)}{\gcd[\operatorname{lcm}(x, x-1, \ldots, x-i), (x-i-1)]} \\
&\ge \frac{\operatorname{lcm}(x, x-1, \ldots, x-i)(x-i-1)}{\gcd[x(x-1)\cdots(x-i), (x-i-1)]} \\
&\ge \frac{\operatorname{lcm}(x, x-1, \ldots, x-i)(x-i-1)}{(i+1)!}
\end{aligned}$$

so by induction $\operatorname{lcm}(x, x-1, \ldots, x-d) \ge \frac{x(x-1)\cdots(x-d)}{d!(d-1)!\cdots 1!}$. Since $P(x), Q(x)$ have degree d, for large enough x (say $x > L$) we have $\left|Q(x) \pm \frac{x(x-1)\cdots(x-d)}{kd!(d-1)!\cdots 1!}\right| > P(x)$. By (4) kq_x must differ by a multiple of $\operatorname{lcm}(x, x-1, \ldots, x-d)$ from $kQ(x)$; hence q_x must differ by a multiple of $\frac{x(x-1)\cdots(x-d)}{kd!(d-1)!\cdots 1!}$ from $Q(x)$, and for $x > L$ we must have $kq_x = kQ(x)$ and $q_x = Q(x)$.

Now for any y we have $kQ(y) \equiv kQ(x) \equiv kq_x \equiv kq_y \pmod{x - y}$ for any $x > L$. Since $x - y$ can be arbitrarily large, we must have $Q(y) = q_y$, as needed.

8. For $i \in \mathbb{N}$, let

$$P_i(x) = \prod_{k=1}^{i}(x - (2k-1)).$$

(Define $P_0(x) = 1$.)

Step 1 By Problem 4, any polynomial with integer coefficients can be written in the form $\sum_{0 \le i \le n} c_i P_i(x)$.

Step 2 Let $a_i = \sum_{k=0}^{\infty} \left\lfloor \frac{i}{2^k} \right\rfloor$. We claim that $2^{a_i} \mid P_i(x)$ for all $i \in \mathbb{N}$ and all odd x. For a prime p and $n \in \mathbb{Z}$, denote by $v_p(n)$ the exponent of the highest power of p dividing n (by convention $v_p(0) = \infty$). For given odd x let $f(\alpha)$ be the number of values of k $(0 \le k \le i-1)$ where $2^\alpha \mid x - 1 - 2k$. Then

$$v_2(P_i(x)) = \sum_{k=0}^{i-1} v_2(x - 1 - 2k) = \sum_{\alpha=1}^{\infty} f(\alpha)$$

since each k with $2^\alpha \,||\, x - 1 - 2k$ is counted α times in either sum.

Since any set of $2^{\alpha-1}$ consecutive even integers has one divisible by 2^α, any set of i consecutive even integers has at least $\left\lfloor \frac{i}{2^{\alpha-1}} \right\rfloor$ integers divisible by 2^α. Hence $f(\alpha) \ge \left\lfloor \frac{i}{2^{\alpha-1}} \right\rfloor$, and $v_2(P_i(x)) \ge \sum_{\alpha=0}^{\infty} \left\lfloor \frac{i}{2^\alpha} \right\rfloor$ as desired.

Note $a_0 = 0, a_1 = 1, a_2 = 3, a_3 = 4, a_4 = 7, a_5 = 8$, and $a_i \ge 10$ for $i \ge 6$.

Step 3 Next, we claim that if $P(x) = \sum_{0 \le i \le n} c_i P_i(x)$ has a complete remainder sequence then c_1 is odd. (c_0 obviously needs to be odd.) We have $4 \mid P(4k+i) - P(i)$ for any integer i; hence $r(4k+1) \equiv r(1) \pmod 4$ and $r(4k+3) \equiv r(3) \pmod 4$ for each k. In order for the remainder sequence to be complete, we need $r(1) \not\equiv r(3) \pmod 4$. But noting that $a_i \ge 2$ and $P_i(x) \equiv 0 \pmod 4$ for odd x and $i \ge 2$, we have $P(3) - P(1) \equiv c_1(P_1(3) - P_1(1)) \equiv 2c_1 \pmod 4$. Hence c_1 is odd.

Step 4 Since for any odd x, $P_i(x)$ is divisible by 2^{a_i}, if we mod out c_i by 2^{10-a_i}, and delete the terms with P_i for $i \ge 6$ (where $a_i \ge 10$), we get a polynomial with the same remainder sequence as P_i. If $P(x)$ gives a complete remainder sequence, then c_0 is odd, so there are 2^9 choices for it; c_1 is odd, so there are at most 2^8 choices for $c_1 \pmod{2^9}$ ($a_1 = 1$); for $2 \le i \le 5$ there are at most 2^{10-a_i} choices for $c_i \pmod{2^{10-a_i}}$. Hence the number of complete remainder sequences is at most

$$2^9 \cdot 2^8 \cdot \prod_{i=2}^{5} 2^{10-\alpha_i} = 2^9 \cdot 2^8 \cdot 2^7 \cdot 2^6 \cdot 2^3 \cdot 2^2 = 2^{35}.$$

9. **Step 1** Let $k \ge 1$ be an integer and p be a prime. Call

$$(f(0), \ldots, f(i)) \pmod{p^k}$$

the $(i+1)$-subsignature of f modulo p^k.

By Problem 4, each polynomial $f \in (\mathbb{Z}/p^k\mathbb{Z})[x]$ can be uniquely represented as

$$f(x) = \sum_{i \ge 0} a_i x^{\underline{i}}, a_i \in \mathbb{Z}/p^k\mathbb{Z} \tag{5}$$

The following are clear:

(a) The term $a_i x^{\underline{i}}$ does not affect the value of $f(0), \ldots, f(i-1)$.

(b) $p \nmid i!$ for $0 \leq i < p$.

(c) $p||i!$ for $p \leq i < p^2$.

(d) $p|x^{\underline{i}}$ when $i \geq p$.

(e) $p^2|x^{\underline{i}}$ when $i \geq 2p$.

We show that for $m \leq p$, the p^{km} choices for $a_0, \ldots, a_{m-1}$ give the p^{km} distinct m-term sequences modulo p^k as m-subsignatures. This is clear for $m = 1$. Suppose this is true for a certain $m < p$. Given a sequence $(y_0, \ldots, y_m)$, we can find $a_0, \ldots, a_{m-1}$ in (5) such that $f(i) = y_i$ for $0 \leq i < m$. Next note the term $a_m x^{\underline{m}}$ ranges over all of $\mathbb{Z}/p^k\mathbb{Z}$ for $x = m$ since $p \nmid m!$ implies $m!$ is invertible modulo p^k. Hence we can choose a_m to make $f(m) = y_m$ (this does not affect $f(0), \ldots, f(m-1)$ by item (a) above), and all $p^{k(m+1)}$ distinct $(m+1)$-term sequences modulo p^k are $(m+1)$-subsignatures.

Hence there are p^{kp} possible p-subsignatures modulo p^k. In particular, there are p possible signatures modulo p and p^2 p-subsignatures modulo p^2.

Step 3 Now, we show there are p^{3p} $2p$-subsignatures $(y_0, y_1, \ldots, y_{2p-1})$ modulo p^2, corresponding to the sequences

$$(a_0 \bmod p^2, \ldots, a_{p-1} \bmod p^2, a_p \bmod p, \ldots, a_{2p-1} \bmod p). \tag{6}$$

Again, we induct on the following statement: there are $p^{2p}p^k$ $(p+k)$-subsignatures $(y_0, y_1, \ldots, y_{p+k-1})$ modulo p^2, corresponding to the coefficients

$$(a_0 \bmod p^2, \ldots, a_{p-1} \bmod p^2, a_p \bmod p, \ldots, a_{p+k-1} \bmod p). \tag{7}$$

This is true for $k = 0$ by Step 2; once it has been established for some $k < p$, note that $a_{p+k}x^{\underline{p+k}}$ ranges over p residues modulo p^2 when $x = p + k$, as $p||(p+k)!$. Hence given the coefficients (7) there are exactly p possible values for $f(p+k)$, giving $p^{2p}p^{k+1}$ possible $(p+k+1)$-subsignatures. The claim follows.

Step 4 The $2p$-subsignature modulo p^2 completely determines the signature modulo p^2.

From Step 3, each such subsignature corresponds to a sequence as in (6). Since $p^2|x^{\underline{i}}$ for $i \geq 2p$ and $p|x^{\underline{i}}$ for $i \geq p$,

$$f(x) = \sum_{i \geq 2p} a_i \underbrace{x^{\underline{i}}}_{0 \bmod p^2} + \sum_{p \leq i < 2p} \underbrace{a_i}_{\text{determined mod } p} \underbrace{x^{\underline{i}}}_{0 \bmod p} + \sum_{i<p} \underbrace{a_i}_{\text{determined mod } p^2} x^{\underline{i}}$$

is determined modulo p^2 for each x.

Step 5 If $p||n$ then there are p^p possible signatures modulo p and if $p^2||n$ then there are p^{3p} possible signatures modulo p^2. Hence, since a sequence modulo $p^{v_p(n)}$ for every prime $p|n$ uniquely determines the sequence modulo n by the Chinese Remainder Theorem, there are at most

$$\left(\prod_{p||n} p^p\right)\left(\prod_{p^2||n} p^{3p}\right) = \left(\prod_{p|n} p^p\right)\left(\prod_{p^2|n} p^{2p}\right)$$

possible signatures modulo n. All of these are attainable: it suffices to show that given a valid signature s_p modulo $p^{v_p(n)}$ for every prime $p|n$, we can find a polynomial that has signature s_p modulo $p^{v_p(n)}$ for every prime $p|n$. There exists a polynomial R_p with signature s_p; then

$$f = \sum_{\text{prime } p|n} \left[\left(\prod_{q|n, q\neq p} q^2 \right) \left(\left(\prod_{q|n, q\neq p} q^2 \right)^{-1} \pmod{p^2} \right) R_p \right]$$

is the desired polynomial.

10. **Step 1** A polynomial $P(x)$ has all terms divisible by a prime p if and only if $x(x-1)\cdots(x-(p-1)) \mid P(x)$ in $\mathbb{Z}/p\mathbb{Z}$. Call a polynomial p-valid if $x(x-1)\cdots(x-(p-1)) \nmid P(x)$ modulo p.

    Step 2 A polynomial is fine if and only if it is p-valid for every prime p. Indeed, the forward assertion follows from Step 1. Conversely, suppose that the polynomial is p-valid for every prime p; then there does not exist a prime p such that $x(x-1)\cdots(x-(p-1)) \mid P(x)$ in $\mathbb{Z}/p\mathbb{Z}$. Given $k \in \mathbb{N}$, let $p_1, \ldots, p_j$ be all the primes dividing k. Then, for $1 \leq i \leq j$, there exists $x_i \in \mathbb{Z}/p\mathbb{Z}$ such that $P(x_i) \not\equiv 0 \pmod{p_i}$ for all $1 \leq i \leq j$. Then any $x' \in \mathbb{N}$ with $x' \equiv x_i \pmod{p_i}$ causes $P(x')$ to not be divisible by any of $p_1, \ldots, p_j$ and hence relatively prime to k. By the Chinese Remainder Theorem we can find infinitely many such x', so $P(x)$ is fine.

    Step 3 Let $p_1 < \ldots < p_m$ be all primes less than n. In S the proportion of p_i-valid polynomials modulo p_i is $1 - \frac{1}{p_i^{p_i}}$. Indeed, write

    $$P(x) \equiv x(x-1)\cdots(x-(p_i-1))Q(x) + R(x) \pmod{p_i},$$

    where $R(x)$ is the remainder upon dividing $P(x)$ by $R(x)$. $Q(x)$ can be any polynomial of degree $n - p_i$, and for any choice of $Q(x)$, exactly $p_i^{p_i} - 1$ out of $p_i^{p_i}$ choices for $R(x)$ are possible, namely any polynomial of degree less than p_i except the zero polynomial.

    Step 4 The equations $P(x) \equiv R_i(x) \pmod{p_i}$ uniquely determine $P(x)$ modulo $p_1 p_2 \cdots p_m$. (This is a direct application of the Chinese Remainder Theorem.) Since the proportion p_i-valid polynomials modulo p_i is $1 - \frac{1}{p_i^{p_i}}$, the proportion of polynomials in S that are p_i-valid for each i is $\prod_{i=1}^{m} \left(1 - \frac{1}{p_i^{p_i}}\right)$. Now $p_1 p_2 \cdots p_m | n!$ so there are a fixed number of polynomials corresponding to each polynomial modulo $p_1 \cdots p_m$ that is p_i-valid for each i. Hence the proportion of fine polynomials is at most $\prod_{i=1}^{m} \left(1 - \frac{1}{p_i^{p_i}}\right)$.

(C) Divisibility, GCD, and Irreducibility

1. There exist polynomials $u, v \in \mathbb{Q}[x]$ so that $uf + vg = 1$. Clearing denominators we get the desired representation. Now if $uf + vg = k$ for $f, g \in \mathbb{Z}[x]$ then replacing u by (u mod g) and v by (v mod g), we get $u'f + v'g = k$ (why?) with u', v' having degrees less than $\deg(f)$, $\deg(g)$, respectively. Note that u', v' are uniquely determined up to

a constant multiple, since we need $u'f \equiv -k \pmod{g}$, and u' is determined modulo g up to a constant factor. Letting c be $\gcd(a_0, \ldots, a_m, b_0, \ldots, b_n)$, we necessarily have $u_1 = \pm u/c$, and $v_1 = \pm v/c$, giving that $k = \pm ck_0$.

2. We have $uf(n)+vg(n) = k$ for some $u, v \in \mathbb{Z}$ and nonzero . Hence $\gcd(f(n), g(n)) \mid k$.

3. Let f^n denote f iterated n times. We will encode the statement of the problem in polynomials. For a polynomial $p(x) = c_n x^n + \cdots + c_1 x + c_0$, we will denote by $p(f)$ the function $c_n f^n(x) + \cdots + c_1 f(x) + c_0 x$. We are given $(x^3 + 2x^4 + x - 4)f = 0$ and $(x^{2009} - 1)f = 0$. Since $\gcd(x^3 + 2x^2 + x - 4, x^{2009} - 1) = x - 1$ and hence there exist polynomials $u(x), v(x) \in \mathbb{Q}[x]$ for which $u(x)(x^3+2x^2+x-4)+v(x)(x^{2009}-1) = x-1$. Then

   $$0 = (u(x)(x^3 + 2x^2 + x - 4)f)(t) + (v(x)(x^{2009} - 1)f)(t) = ((x - 1)f)(t) = f(t) - t$$

   as desired.

4. First we prove uniqueness. In any nonzero multiple of $(x+2)(x+5) = x^2+7x+10$, the coefficient of the term with smallest exponent must be divisible by 10.

   Any two polynomials both satisfying the given condition must have difference divisible by $(x + 2)(x + 5)$. Given any two distinct polynomials Q and R having difference divisible by $x^2 + 7x + 10$, one coefficient must differ by at least 10, so the coefficients of Q and R cannot all be in $[0, 10)$.

   Now we show existence. Start with the polynomial n and repeat the following process. If the smallest term with coefficient 10 or greater is $a_n x^n$, add $x^n(x + 2)(x + 5)(x - 1) = x^n(x^3 + 6x^2 + 3x^2 - 10)$ to this polynomial (call this *firing* at position n). Changing the polynomial by a multiple of $(x + 2)(x + 5)$ does not change its value at $-2, -5$. Furthermore, note the sum of coefficients stays the same. If at some time the polynomial has all coefficients less than 10 we are done.

   Suppose this process goes on forever. Consider the sequence of triplets (a_n, a_{n-1}, a_{n-2}) where a_n is the leading coefficient of the polynomial. By our process, $n - 3$ must have fired in the previous step; positions less than $n-23$ will never fire again; terms $x^i, i < n - 3$ have coefficients less than 10. Since there are a finite number of possibilities for (a_n, a_{n-1}, a_{n-2}) (as their sum is bounded), at some later time the same triplet must appear twice, say as the coefficients of x^n, x^{n-1}, x^{n-2} at step t_1 and as the coefficients of x^m, x^{m-1}, x^{m-2} at step $t_2 > t_1$. The coefficients of $x^{n-3}, \ldots, 1$ have not changed in the intervening steps. Then the difference between the polynomials at these two times is $(x^{m-n} - 1)(a_n x^2 + a_{n-1}x + a_{n-2})$. Since $x^2 + 7x + 10$ must divide this polynomial but it has no factor in common with $x^{m-n} - 1$, it must divide $a_n x^2 + a_{n-1}x + a_{n-2}$. This means that $a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2}$ evaluates to 0 at $-2, -5$. Hence if we remove these terms at time t_1, then we get a polynomial satisfying the desired conditions.

5. By division with remainder we can write $f(x) = q(x)g(x) + r(x)$ where $\deg(r) < \deg(f)$. Then

   $$\frac{f(n)}{g(n)} = q(x) + \frac{r(n)}{g(n)}.$$

When $|n|$ is large enough, $|r(n)| < |g(n)|$. Hence $r(n) = 0$ for infinitely many n, and in fact $r(x) = 0, g \mid f$.

6. Let $f(x) = x^n + x^2 - 1$ and $g(x) = x^m + x - 1$. By the previous problem, we need $f(x)|g(x)$. Both f, g have a unique root in $(0, 1)$, since both are increasing and go from -1 to 1. This must be the same root since $g|f$; call it α.

   We use α to show $m < 2n$. Certainly $\alpha > \phi$ where ϕ is the positive root of $h(x) := x^2 - x + 1 = 0$. This is because f is increasing in $(0, 1)$ and $f(\phi) < h(\phi) = 0 = f(\alpha)$. On the other hand, if $m \geq 2n$ then $1 - \alpha = \alpha^m \leq (\alpha^n)^2 = (1 - \alpha^2)^2$ and the outer terms rearrange to give $\alpha(\alpha - 1)(\alpha^2 - \alpha + 1) \geq 0$, which requires $\alpha \leq \phi$, a contradiction.

   We show that the only solution with $m < 2n$ is $(m, n) = (5, 3)$. Since $x^n + x^2 - 1|(x^{m-n}(x^n + x^2 - 1) - (x^m + x - 1))$, $x^n + x^2 - 1|x^{m-n+2} - x^{m-n} - x + 1$. Since $x^{m-n+2} - x^{m-n} - x + 1$ is not identically 0, and since $m \leq 2n-1$, $m-n+2$ is either m or $m+1$. In the first case, we must have $x^{m-n+2} - x^{m-n} - x + 1 = x^n + x^2 - 1$, which is impossible. In the second case, we must have $(x-1)(x^n + x^2 - 1) = x^{n+1} - x^{n-1} - x + 1$ so $-x^{n-1} = -x^n + x^3 - x^2$, which can only happen if $n = 3$, and therefore $m = 5$. As $(x^3 + x^2 - 1)(x^2 - x + 1) = (x^5 + x - 1)$, this solution works.

7. In light of Problem 1, we just need to find u, v with $uf + vg$ a constant, $\deg(u) < \deg(g)$, and with the coefficients of f, g together having gcd 1. This constant will be the desired k_0. For polynomials f, g define $(f \bmod g)$ to be the remainder when f is divided by g. For an integer d and $f \in \mathbb{Z}$ we write $d||f$ if d is the maximal positive integer that divides every coefficient of f. We need the following facts.

   (a) (from Gauss's Lemma) If $p, q \in \mathbb{Z}[x]$ and $d||p, e||q$ then $de||pq$.

   (b) For integer $n \geq 1$, integer k, $0 < k < 2^n$, $\binom{2^n}{k}$ is even. Moreover,

   $$\gcd\left(\binom{2^n}{1}, \ldots, \binom{2^n}{2^n - 1}\right) = 2.$$

   (c) If $u, v \in \mathbb{Z}[x]$, v is monic, there exist $q, r \in \mathbb{Z}[x]$ such that $u = qv + r$, $\deg(r) < \deg(u)$.

   Let $P(x) = \frac{(x^n-1)^n}{(-2)^n}$. Note the roots of $x^n + 1$ are $e^{\pi k/n}$ for k odd, $0 < k < 2n$. For any root x of $x^n + 1 = 0$,

   $$P(x) = \frac{(x^n - 1)^n}{(-2)^n} = \frac{(-2)^n}{(-2)^n} = 1.$$

   So $P(x) \equiv 1 \pmod{x^n + 1}$. Since $(-1)^n - 1 = 0$, $x + 1$ divides $x^n - 1$. Hence $(x + 1)^n \mid \frac{(x^n-1)^n}{(-2)^n}$ or

   $$P(x) \equiv 0 \pmod{(x + 1)^n}.$$

   Therefore, for some polynomials f, g,

   $$P(x) = (x + 1)^n f = -(x^n + 1)g + 1.$$

We have $f(x) = \left(\frac{x^n-1}{(-2)(x+1)}\right)^n$, and

$$(-2)^n = \left(\frac{x^n-1}{x+1}\right)^n (x+1)^n + (-2)^n g(x)(x^n+1).$$

We can write

$$\left(\frac{x^n-1}{x+1}\right)^n = s(x)(x^n+1) + t(x)$$

where $\deg(t) < \deg(x^n+1) = n$, and find

$$(-2)^n = t(x)(x+1)^n + [(-2)^n g(x) + s(x)(x+1)^n](x^n+1).$$

Now we find the $d \in \mathbb{N}$ such that $d||t(x)$.

Claim 1 $2^{(2^r-1)q}$ is the highest power of 2 dividing $\left[\left(\frac{x^n-1}{x+1}\right)^n \bmod x^{2^r}+1\right]$.

We have

$$\frac{x^n-1}{x+1} = (x-1)(x^2-1)\cdots(x^{2^r}-1)(x^{2^r(q-1)}+\cdots+x+1).$$

For $0 \le i < r$

$$(x^{2^i}-1)^{2^{r-i}} = \sum_{k=0}^{2^{r-i}} \binom{2^{r-i}}{k} x^{2^i k}(-1)^k \equiv \sum_{k=1}^{2^{r-i}-1} \binom{2^{r-i}}{k} x^{2^i k}(-1)^k \pmod{x^{2^r}+1}.$$

By item (c), $2|\binom{2^{r-i}}{k}$ for $1 \le k \le 2^{r-i}-1$. Let $f_i(x) = \frac{1}{2}\sum_{k=1}^{2^{r-i}-1}\binom{2^{r-i}}{k}x^{2^i k}(-1)^k$. Note that $f_i \in \mathbb{Z}[x]$ and

$$f_i(1) = \frac{1}{2}((x^{2^i}-1)^{2^{r-i}}-2)|_{x=1} = -1.$$

We have

$$(x^{2^i}-1)^{2^r q} = [(x^{2^i}-1)^{2^{r-i}}]^{2^i q} \equiv 2^{2^i q} f_i(x)^{2^i q} \pmod{x^{2^r}+1}$$

Multiplying these equations for $0 \le i < r$ we get

$$\begin{aligned}[(x-1)(x^2-1)\cdots(x^{2^r-1}-1)]^n &= 2^{(2^0+2^1+\cdots+2^{r-1})q}\prod_{i=0}^{r-1} f_i(x)^{2^i q} \\ &= 2^{(2^r-1)q}\prod_{i=0}^{r-1} f_i(x)^{2^i q} \pmod{x^{2^r}+1}\end{aligned}$$

Let $w(x) = \left[\left(\prod_{i=0}^{r-1} f_i(x)^{2^i q}\right)(x^{2^r(q-1)}+\cdots+x+1)^n\right]$. By item 3, we can write, $w(x) = w_1(x)(x^{2^r}+1) + w_2(x); w_1, w_2 \in \mathbb{Z}[x]$. Then $w(1)$ is odd so the sum of coefficients of $w(x)$ is odd and not all coefficients of $w_2(x)$ are even. Hence

$$\begin{aligned}\left(\frac{x^n-1}{x+1}\right)^n \bmod x^{2^r}+1 &= [(x-1)(x^2-1)\cdots(x^{2^{r-1}}-1)(x^{2^r(q-1)}+\cdots+x+1)]^n \bmod x^{2^r}+1 \\ &= 2^{(2^r-1)q}[w(x) \bmod x^{2^r}+1]\end{aligned}$$

and $2^{(2^r-1)q}$ is the highest power of 2 dividing $\frac{x^n-1}{x+1} \bmod x^{2^r}+1$.

Claim 2 2^{2^rq} is the highest power of 2 dividing $\left(\frac{x^n-1}{x+1}\right)^n \bmod x^{2^r(q-1)} - \cdots - x^{2^r} + 1$.

We have

$$x^{2^r(q-1)} + \cdots + x^{2^r} + 1 \equiv \sum_{0<i<q-1, i \text{ odd}} 2x^{2^ri} \pmod{x^{2^r(q-1)} - \cdots - x^{2^r} + 1}$$

so $\left(\frac{x^n-1}{x+1}\right)^n$ is congruent to

$$[(x-1)(x^2-1)\cdots(x^{2^r}-1)(x^{2^r(q-1)} + \cdots + x^{2^r} + 1)]^n$$
$$\equiv [(x-1)(x^2-1)\cdots(x^{2^r}-1)]^n 2^n \left(\sum_{0<i<q-1, i \text{ odd}} x^{2^ri}\right)^n \pmod{x^{2^r(q-1)} - \cdots - x^{2^r} + 1}$$

and the claim follows.

Let $R_1 = \left(\frac{x^n-1}{x+1}\right)^n \bmod x^{2^r}+1$ and $R_2 = \left(\frac{x^n-1}{x+1}\right)^n \bmod x^{2^r(q-1)} - \cdots - x^{2^r} + 1$. Let $Q = \sum_{0<i<q, i \text{ odd}} x^{2^ri}$, $P_1 = \sum_{1\le i<q} x^{2^ri}$, $P_2 = x^{2^r}+1$. Then

$$P_1 = QP_2 + 1$$
$$R_1 - R_2 = (R_1 - R_2)(P_1 - qP_2)$$
$$R_1 - P_1(R_1 - R_2) = R_2 - P_2Q(R_1 - R_2)$$

Let $F = R_1 - P_1(R_1 - R_2)$. Then $F \equiv R_1 \pmod{x^{2^r}+1}$ and $F \equiv R_2 \pmod{x^{2^r(q-1)} - \cdots - x^{2^r} + 1}$. Hence by the Chinese Remainder Theorem, since $t(x) \equiv R_1 \pmod{x^{2^r}+1}$, $t(x) \equiv R_2 \pmod{x^{2^r(q-1)} - \cdots - x^{2^r} + 1}$, and $\deg(F) < n$ we have $F(x) = t(x)$. Let $G(x) = (-2)^n g(x) - s(x)(x+1)^n$. Then

$$(-2)^n = F(x)(x+1)^n + G(x)(x^n+1).$$

Note $2^{(2^r-1)q}$ is the highest power of 2 dividing R_1, and $2^{2^rq} | R_2$, $F(x) = R_1(x) - P_1(x)(R_1(x) - R_2(x)) = (1 - P_1(x))R_1(x) + P_1(x)R_2(x)$. $2 \nmid 1 - P_1(x)$ so $2^{(2^r-1)q}$ is the highest power of 2 dividing $S_1(x) = (1 - P_1(x))R_1(x)$. There exists j so that the coefficient u_j of x^j in $S_1(x)$ is not divisible by $2^{(2^r-1)q+1}$. Let the coefficient of x^j in $P_1(x)R_2(x)$ be b_j. Note $2^{2^rq} | R_2$ implies $2^{2^rq} || b_j$. Hence $2^{(2^r-1)q+1} \nmid a_j + b_j$, and $2^{(2^r-1)q+1} \nmid F(x)$. Let $\mathcal{F}(x) = \frac{F(x)}{2^{(2^r-1)q}}$ and $\mathcal{G}(x) = \frac{G(x)}{2^{(2^r-1)q}}$. Then $\mathcal{F}(x) \in \mathbb{Z}[x]$. Let $\mathcal{F}(x) = \sum_{i=0}^{l} c_i x^i, \mathcal{G}(x) = \sum_{i=0}^{m} d_i x^i$. Then

$$2^q = 2^{2^rq - (2^r-1)q} = \mathcal{F}(x)(x+1)^n + \mathcal{G}(x)(x^n+1).$$

Since $(x^n+1) | 2^q - \mathcal{F}(x)(x+1)^n$ in $\mathbb{Q}[x]$, by divisibility holds in $\mathbb{Z}[x]$, i.e. $\mathcal{G}(x) \in \mathbb{Z}[x]$. $2 \nmid \gcd(c_0, \ldots, c_l)$ and $\gcd(c_0, \ldots, c_l, d_0, \ldots, d_m) | 2^q$. Hence the gcd is 1. By Problem 1, $k_0 = 2^q$.

(D) Algebraic Numbers

1. Let β be the root of greatest absolute value. Suppose by way of contradiction $f(\alpha^3+1) = 0$. Since $f(x)$ is irreducible and $f(\alpha) = 0$, it is the minimal polynomial of α. Since the polynomial $g(x) = f(x^3+1)$ has α as a root $f(x) \mid f(x^3+1)$. Hence $f(\beta) = f(\beta^3+1) = 0$. Let $r = |\beta|$. Now $r^3 - r - 1 > 0$ for $r \ge \frac{3}{2}$, so $|\beta^3+1| \ge |\beta|^3 - 1 > |\beta|$, contradicting the maximality of β.

2. Suppose the LHS is not 0. The conjugates of $c_1a_1 + \ldots + c_na_n$ are among the numbers $c_1b_1 + \ldots + c_nb_n$ where b_i is a conjugate of a_i. Each of these have absolute value at most $|c_1a_1'| + \cdots + |c_na_n'|$. The product of all conjugates (including $c_1a_1 + \ldots + c_na_n$) is an integer because it is the constant term of the minimal polynomial of $c_1a_1 + \ldots + c_na_n$; hence it is at least 1. The conjugates multiply to an integer with absolute value at least 1, they number at most $d_1 \cdots d_n$ and each is at most $|c_1a_1'| + \cdots + |c_na_n'|$; hence each is at least $\left(\frac{1}{|c_1a_1'|+\cdots+|c_na_n'|}\right)^{d_1d_2\cdots d_n-1}$.

3. This time we can do better than in Problem 2. Suppose $\omega_1, \ldots, \omega_k$ are the roots of unity. We claim that

$$\prod_{i=1}^{p-1}(x - (\omega_1^i + \ldots + \omega_k^i)) \tag{8}$$

has integer coefficients since each coefficient. Indeed, we can write each coefficient in the form

$$a_0 + a_1\omega + \cdots + a_{p-2}\omega^{p-2}, \tag{9}$$

where ω is a primitive pth root of unity. If we replace ω by ω^i for some $1 \le i \le p-1$, then the product in (8) stays the same. Hence (9) stays the same as well, and since $1, \omega, \ldots, \omega^{p-2}$ satisfy no linear dependency relation, we must have $a_0 = \cdots = a_{p-2}$, and (9) is an integer. (A more advanced way of looking at this is the following: the coefficients are in the fixed field of all automorphisms of $\mathbb{Q}(\omega)$ fixing $\mathbb{Q}$; Galois Theory allows us to conclude that these coefficients are actually in $\mathbb{Q}$.)

Thus the conjugates of $\omega_1 + \cdots + \omega_k$ are among the $\omega_1^i + \ldots + \omega_k^i$. Since each has absolute value at most k, and their product is a nonzero integer (and hence has absolute value at least 1), each must be at least $\frac{1}{k^{p-2}}$.

(E) Cyclotomic and Chebyshev Polynomials

1. Let the side lengths be $a_0, \ldots, a_{p-1}$. Then letting ω be the pth root of unity,

$$a_{p-1}\omega^{p-1} + \cdots + a_0 = 0$$

Hence ω satisfies the polynomial equation $a_{p-1}x^{p-1} + \cdots + a_0$. Since the minimal polynomial of ω is $\Phi_p = x^{p-1} + \cdots + x + 1$, $x^{p-1} + \cdots + x + 1 \mid a_{p-1}x^{p-1} + \cdots + a_0$, i.e. $a_{p-1} = \cdots = a_0$.

2. The factorization of $x^n - 1$ into irreducible (monic) factors $P_1 \cdots P_k$ gives a (not necessarily complete) factorization of $2^n - 1$. If P_i has degree d then $P_i(2) \le 3^d$ since

$$P_i(2) = \prod_{\omega \text{ root of } P_i} (2 - \omega)$$

and all roots have absolute value 1. Letting ω be a primitive nth root of unity, the irreducible factor containing ω^i is $\Phi_{n/\gcd(n,i)}$, which has degree $\varphi(m) \le \varphi(n)$ for some factor m of n. Hence it suffices to find n so that $3^{\varphi(n)} \le 2^{\frac{n}{1993}}$, or

$$\varphi(n) \le \frac{n\ln(2)}{1993\ln(3)}.$$

However, for any $C > 0$ we can find n so that $\varphi(n) < Cn$. The product $\prod_{p \text{ prime}} \frac{p}{p-1}$ is infinite (rewrite as geometric series, expand to get the harmonic series). Hence $\prod_{p \text{ prime}} \frac{p-1}{p} = 0$, and taking $n = p_1 \cdots p_k$ for sufficiently many distinct primes p_i we find that we can make $\varphi(n)/n = \prod_{i=1}^{k} \frac{p_i - 1}{p_i}$ as close to 0 as desired.

3. (A) Let $\omega = \cos(p\pi) + i\sin(p\pi)$. Then ω is a root of unity and hence an algebraic integer; similarly $\overline{\omega}$ is as well. Hence $2\cos(p\pi) = \omega + \overline{\omega}$ is an algebraic integer; since it is rational it is a rational integer. Hence we must have $2\cos(p\pi) = 0, \pm 1, \pm 2$, giving $p = 0, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, 1$.

   (B)
   Step 1 If a is nonreal, $a\overline{a} \in \mathbb{Q}$ and the irreducible polynomial of a over $\mathbb{Q}$ has degree n, then the irreducible polynomial of $a + \overline{a}$ has degree $n/2$. Indeed, $[\mathbb{Q}(a) : \mathbb{Q}(a + \overline{a})] = 2$ since a satisfies a quadratic equation in $\mathbb{Q}[a + \overline{a}]$ (namely $x^2 - (a + \overline{a})x + a\overline{a} = 0$), and $a \notin \mathbb{R}$ implies $a \notin \mathbb{Q}(a + \overline{a})$. Since

$$n = [\mathbb{Q}(a) : \mathbb{Q}] = [\mathbb{Q}(a) : \mathbb{Q}(a + \overline{a})][\mathbb{Q}(a + \overline{a}) : \mathbb{Q}],$$

   the desired result follows. In particular, this holds for roots of unity.

   Step 2 If $\cos(p\pi) = \frac{1}{2}(\omega + \overline{\omega})$ has degree n over $\mathbb{Q}$, then ω has degree $2n$. However, if $2p = \frac{q}{r}$ in reduced form, then ω is a rth root of unity, and its irreducible polynomial is the cyclotomic polynomial Φ_r. Hence $2n = \varphi(r)$. If $n = 2$, then $r = 4$, and the solutions to $\varphi(r) = 4$ are $5, 10, 12$. Hence in addition to the p above, rational p with denominators 5 or 6 also work.

   Try to use this method to describe the factorization of Chebyshev polynomials!

4. It is easy to check that $\sqrt{n+1} + \sqrt{n}$ is a conjugate of $\sqrt{n+1} - \sqrt{n}$. If $\cos p\pi = \frac{1}{2}(\sqrt{n+1} - \sqrt{n})$ then $\frac{1}{2}(\sqrt{n+1} - \sqrt{n})$ is a zero of some Chebyshev polynomial. But then $\frac{1}{2}(\sqrt{n+1} + \sqrt{n}) > 1$ is also a zero, a contradiction since all zeros of Chebyshev polynomials are in $[-1, 1]$.

5. **Solution 1** Let $\cos(k\theta) = p \in \mathbb{Q}, \cos[(k+1)\theta] = q \in \mathbb{Q}$. Then

$$\begin{aligned} \cos\theta &= \cos[(k+1)\theta]\cos\theta \pm \sin[(k+1)\theta]\sin k\theta \\ &= pq \pm \sqrt{(1-p^2)(1-q^2)} \\ &= a \pm \sqrt{b} \end{aligned}$$

   for some $a, b \in \mathbb{Q}$ such that b is not a perfect square. Now $T_k(a \pm \sqrt{b}) = T_k(\cos(\theta)) = \cos(k\theta) = p$ so either $a + \sqrt{b}$ or $a - \sqrt{b}$ is a zero of the polynomial $T_k(x) - p \in \mathbb{Q}[x]$. The minimal polynomial in $\mathbb{Q}[x]$ having $a + \sqrt{b}$ (or $a - \sqrt{b}$) as a root is $R(x) = [x - (a + \sqrt{b})][x - (a - \sqrt{b})]$ so $R(x) | T_k(x) - p$. Now if $a \mp \sqrt{b} \notin [-1, 1]$ then we have $T_k(a \mp \sqrt{b}) \notin [-1, 1]$ and hence not equal to p, a contradiction. So there must exist ϕ so that $\cos(\phi) = a \mp \sqrt{b}$. By similar reasoning $a \mp \sqrt{b}$ is a root of $T_{k+1}(x) - q = 0$.

Now $\cos(k\phi) = T_k(a \mp \sqrt{b}) = p$ and similarly $\cos[(k+1)\phi] = q$. In summary,

$$\cos\theta = a \pm \sqrt{b} \tag{10}$$

$$\cos\phi = a \mp \sqrt{b} \tag{11}$$

$$\cos k\theta = \cos k\phi = p \tag{12}$$

$$\cos[(k+1)\theta] = \cos[(k+1)\phi] = q \tag{13}$$

Now (12) implies $k\phi = 2\pi j \pm k\theta$ for some $j \in \mathbb{Z}$, or

$$\phi = \frac{2\pi j}{k} \pm \theta \tag{14}$$

and (13) implies

$$\phi = \frac{2\pi l}{(k+1)} \pm \theta \tag{15}$$

for some $l \in \mathbb{Z}$. Since $b \neq 0$, $a + \sqrt{b} \neq a - \sqrt{b}$ and $\cos\theta \neq \cos\phi$. If (14) or (16) hold true for the same sign, then $\frac{2\pi j}{k} = \frac{2\pi l}{k+1}$ and $j(k+1) = lk$; since $\gcd(k, k+1) = 1$ but $k \nmid j$ this is a contradiction. So equating (14) and (16) gives

$$\theta = 2\pi \cdot \frac{m}{2k(k+1)}$$

for some $m \in \mathbb{Z}$. Since $\cos(\theta)$ is the root of a quadratic, we know by Problem 3 that $\cos\theta = \sqrt{3}/2, 1/2, (\sqrt{5} \pm 1)/2$. It is easy to check that $\theta = \pi/6$ is the only solution.

Solution 2 We claim that if $\cos k\theta$ and $\cos l\theta$ are rational for relatively prime positive integers k, l, then either $\cos\theta$ is rational or θ is a rational multiple of π.

Let $\cos k\theta = p$ and $\cos l\theta = q$ as before. Noting that $e^{i\phi} + \frac{1}{e^{i\phi}} = 2\cos\phi$, we have that $e^{i\theta}$ is a root of

$$x^k + \frac{1}{x^k} = 2p \implies x^{2k} - 2px^k + 1 = 0 \tag{16}$$

$$x^l + \frac{1}{x^l} = 2q \implies x^{2l} - 2qx^l + 1 = 0 \tag{17}$$

Suppose θ is not a rational multiple of π. Then the numbers $e^{\pm i\theta + \frac{2\pi ij}{k}}$ for $0 \leq j < k$ are all distinct. They are the roots of (16). Similarly, $e^{\pm i\theta + \frac{2\pi ij}{l}}$ are the roots of (17). Since θ is not a rational multiple of π and k, l are relatively prime, we have that the only solution to $e^{\pm i\theta + \frac{2\pi ij_1}{k}} = e^{\pm i\theta + \frac{2\pi ij_2}{k}}$ for $0 \leq j_1 < k$ and $0 \leq j_2 < l$ for some choices of signs is when $j_1 = j_2 = 0$. Thus the only roots the two polynomials share in common are $\omega = e^{i\theta}$ and $\bar{\omega} = -e^{i\theta}$, and hence the polynomial

$$g(x) := (x - e^{i\theta})(x - e^{-i\theta})$$

is the greatest common divisor of polynomials $x^{2k} - 2px^k + 1$ and $x^{2l} - 2qx^l + 1$, which have rational coefficients. Hence $g(x)$ has rational coefficients, and $e^{i\theta} + e^{-i\theta} = 2\cos\theta$ is rational.

Now by Problem 3, the only rational multiples of π that give a rational values for cosine are multiples of $\frac{\pi}{6}$. By our claim, θ is a rational multiple of π. Hence $k\theta$ and $(k+1)\theta$ are both multiples of $\frac{\pi}{6}$, and so must θ. Since $\cos\theta$ is irrational, $\theta = \frac{\pi}{6}$.

6. Let $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Since $x \in [-1, 1]$, we set $x = \cos(\theta)$.

   Step 1 Write $p(\cos\theta)$ in the form

   $$p(\cos\theta) = b_n \cos(n\theta) + b_{n-1}\cos((n-1)\theta) + \cdots + b_0.$$

   We know that $\cos n\theta = T_n(\cos\theta)$, so this is possible by Problem B4. Moreover, since the leading coefficient of T_n is 2^{n-1} (by induction), we must have $b_n = \frac{1}{2^{n-1}}$.

   Step 2 The maximum of $h(\cos\theta) = c_n\cos(n\theta) + \cdots + c_1\cos\theta + c_0$ is at least $|c_n|$.

   Assume WLOG $c_n > 0$. Suppose by way of contradiction that $\max|h(\cos\theta)| < c_n$. Then

   $$c_n T_n\left(\cos\left(\frac{k\pi}{n}\right)\right) - h\left(\cos\left(\frac{k\pi}{n}\right)\right) = (-1)^k c_n - h\left(\cos\left(\frac{k\pi}{n}\right)\right)$$

   is positive for even k and negative for odd k in the range $0 \le k \le n$. We conclude that $c_nT_n(x) - h(x)$ has at least n roots in $[0, 1]$. However this polynomial has degree less than n, contradiction.

   Applying Step 2 to p gives the desired result.

7. By induction, the constant term of T_k is 0 for k odd and ± 1 for k even, and the leading coefficient is 2^k. Hence by Vieta's formula, the product of the roots of T_{2n} is

   $$\cos\frac{\pi}{4n}\cdot\cos\frac{3\pi}{4n}\cdots\cos\frac{(4n-1)\pi}{4n} = \frac{\pm 1}{2^{2n-1}}.$$

   Since $\cos\frac{\pi}{4n}\cdot\cos\frac{3\pi}{4n}\cdots\cos\frac{(2n-1)\pi}{4n} = \pm\cos\frac{(2n+1)\pi}{4n}\cdot\cos\frac{(2n+3)\pi}{4n}\cdots\cos\frac{(4n-1)\pi}{4n}$, we get

   $$\cos\frac{\pi}{4n}\cdot\cos\frac{3\pi}{4n}\cdots\cos\frac{(2n-1)\pi}{4n} = \frac{1}{2^{n-\frac{1}{2}}}.$$

(F) Polynomials in Number Theory

1. By Fermat's Little Theorem, $x^{p-1} \equiv 1 \pmod p$. Thus in $\mathbb{Z}/p\mathbb{Z}$,

   $$x^{p-1} - 1 \equiv \prod_{i=1}^{p-1}(x - i) \pmod p. \tag{18}$$

   Write $(x-1)^{\underline{p-1}} = \sum_{i=0}^{p-1} a_i x^i$. Then matching coefficients on both sides of (18) gives

   $$a_i \equiv 0 \pmod p \text{ for all } 1 \le i < p-1. \tag{19}$$

   Since $p \ge 5$, letting $x = p$ gives

   $$(p-1)! = (x-1)^{\underline{p-1}} = p^{p-1} + \left(\sum_{i=2}^{p-2} a_i p^i\right) + a_1 p + (p-1)!$$

   since $(-1)(-2)\cdots(-p+1) = (-1)^{p-1}(p-1)! = (p-1)!$. Subtracting $(p-1)!$ on both sides,

   $$0 = p^{p-1} + \left(\sum_{j=2}^{p-1} a_i p^i\right) + a_1 p.$$

Using (19), $p^3 \mid a_i p^i$ for $2 \le i \le p-1$. Hence, since $p \ge 5$, $p^3 \mid p^{p-1} + \sum_{i=2}^{p-1} a_i p^i$. Since p^3 divides the LHS, $p^3 \mid a_1 p$ and $p^2 \mid a_1$. Now $p^3 \mid (kp)^{p-1} + \left(\sum_{i=2}^{p-2} a_i (kp)^i\right)$ as well and we get

$$\begin{aligned}(kp-1)^{\underline{p-1}} &= (x-1)^{\underline{p-1}}|_{x=pk} \\ &= (kp)^{p-1} + \left(\sum_{j=2}^{p-1} a_i (kp)^i\right) + a_1 p + (p-1)! \\ &\equiv (p-1)! \pmod{p^3}. \end{aligned} \tag{20}$$

Now,

$$\begin{aligned}\binom{pa}{pb} &= \frac{(pa)^{\underline{pb}}}{(pb)!} \\ &= \frac{\prod_{i=a-b+1}^{a}[(pi)(pi-1)^{\underline{p-1}}]}{\prod_{i=1}^{b}[(pi)(pi-1)^{\underline{p-1}}]} \\ &= \frac{a^{\underline{b}}}{b!}\left[\prod_{i=1}^{b} \frac{[p(i+a-b)-1]^{\underline{p-1}}}{(pi-1)^{\underline{p-1}}}\right] \\ &= \frac{a^{\underline{b}}}{b!}\left[\prod_{i=1}^{b} \frac{[p(i+a-b)-1]^{\underline{p-1}}}{(pi-1)^{\underline{p-1}}}\right] \end{aligned} \tag{21}$$

By (20), $[p(i+a-b)-1]^{\underline{p-1}} \equiv (pi-1)^{\underline{p-1}} \pmod{p^3}$. Hence (21) becomes $\binom{a}{b}$ modulo p^3, as needed.

2. Continuing the above, we have by Viete's formula that

$$a_1 = (p-1)!\left(1 + \frac{1}{2} + \cdots + \frac{1}{p-1}\right).$$

We've shown that $p^2 | a_1$, as needed.

3. Rearranging, it suffices to show $(p^2-1)^{\underline{p-1}} \equiv (p-1)! \pmod{p^4}$

Continuing the above, if we plug in p^2 into the polynomial $(x-1)^{\underline{p-1}}$ we get

$$(p^2-1)^{\underline{p}} = p^{2(p-1)} + \sum_{i=2}^{p-2} a_i p^{2i} + a_1 p^2 + (p-1)! \equiv (p-1)! \pmod{p^4}.$$

4. Consider the polynomial

$$P(x) = (x+a)(x+b)(x+c) - (x-d)(x-e)(x-f) = Sx^2 + Qx + R$$

where $Q = ab + bc + ca - de - ef - fd$ and $R = abc + def$. Since $S | Q, R$, it follows that $S | P(x)$ for every $x \in \mathbb{Z}$. Hence $S | P(d) = (d+a)(d+b)(d+c)$. Since $S > d+a, d+b, d+c$ and thus cannot divide any of them, it follows that S must be composite.

5. Note that for any odd p, $p|n!+1$ has a finite number of positive integer solutions because for $n \geq p$, $p|n!$, $p \nmid n!+1$. Suppose the solutions to

$$n! + 1 \equiv 0 \pmod{p}$$

are exactly $n_1 < n_2 < \cdots < n_m$ with $m > 1$. Then for each i, $1 \leq i < m$ we have

$$\begin{aligned} n_{i+1}! &\equiv -1 \pmod{p} \\ n_i! &\equiv -1 \pmod{p} \end{aligned}$$

Dividing these 2 relations gives

$$(n_i + 1)(n_i + 2) \cdots (n_{i+1}) \equiv 1 \pmod{p}.$$

Letting $k = n_{i+1} - n_i$, we see that $x = n_i$ is a solution to

$$(x + 1)(x + 2) \cdots (x + k) \equiv 1 \pmod{p}.$$

For each k, $1 \leq k < p$ the polynomial

$$(x + 1)(x + 2) \cdots (x + k) - 1 \in \mathbb{Z}/p\mathbb{Z}[x]$$

has at most k roots modulo p. Therefore, there are at most k indices i where $n_{i+1} - n_i = k$, for each k with $1 \leq k < p$.

Now let j be the smallest positive integer such that $m \geq \frac{j(j+1)}{2}$. Then $\frac{(j+1)(j+2)}{2} \geq m \geq \frac{j(j+1)}{2}$ and

$$\begin{aligned} p > n_m - n_1 &= \sum_{i=1}^{m-1} (n_{i+1} - n_i) \\ &\geq \sum_{i=1}^{j} i^2 \\ &= \frac{j(j+1)(2j+1)}{6} \end{aligned}$$

where the second inequality follows from the fact that for a fixed k, $1 \leq k < p$, $n_{i+1} - n_i$ has at most k solutions. Since $m \geq \frac{j(j+1)}{2} = \sum_{i=1}^{j} j$, when the differences $n_{i+1} - n_i$ are written in ascending order, the first is at least 1, the next two are at least 2, and so on, each time the next i differences are at least i and hence sum to at least i^2, up to $i = j$. Now since

$$\lim_{j \to \infty} \frac{j(j+1)(2j+1)/6}{((j+1)(j+2)/2)^{3/2}}$$

is finite and greater than 0, there exists a constant $0 < c_1 < 1$ such that this expression is greater than c_1 for each $j \in \mathbb{N}$; letting $c = \frac{1}{c_1}$ we see that

$$p > \frac{j(j+1)(2j+1)}{6} \geq c_1 \left(\frac{(j+1)(j+2)}{2} \right)^{3/2} \geq c_1 m^{3/2}$$

or $m < cp^{2/3}$. (Requiring $c_1 < 1$ leads to $cp^{2/3} > 1$ so this is true even if $m = 0, 1$.)

6. We continue from Problems 1-3. The numerator of $f_p(x) - f_p(y)$ in lowest terms is divisible by p^3 iff

$$\sum_{k=1}^{p-1} \frac{1}{(px+k)^2} - \sum_{k=1}^{p-1} \frac{1}{(py+1)^2} \equiv 0 \pmod{p^3},$$

where the inverse is taken modulo p^3. First note that since

$$p \mid a_j = (-1)^{p-1-j}(p-1)! \sum_{1 \le i_1 < \cdots < i_j \le p-1} \frac{1}{i_1 i_2 \cdots i_j}$$

for $1 \le j \le p-1$ by Vieta's formula,

$$\sum_{1 \le i_1 < \cdots < i_j \le p-1} \frac{1}{i_1 i_2 \cdots i_j} \equiv 0 \pmod{p}.$$

From Problem 2,

$$\sum_{i=1}^{p-1} \frac{1}{i} \equiv 0 \pmod{p^2}.$$

Now

$$\sum_{1 \le i < j < k \le p-1} \frac{1}{ijk} = \left(\sum_{1 \le i \le p-1} \frac{1}{i} \right)^3 - \left(\sum_{1 \le i \le p-1} \frac{1}{i^3} \right) - 3 \left(\sum_{1 \le i < j \le p-1} \frac{1}{ij} \right) \left(\sum_{1 \le i \le p-1} \frac{1}{i} \right).$$

Hence by Vieta's,

$$a_3 = (p-1)! \left(\sum_{1 \le i < j < k \le p-1} \frac{1}{ijk} \right) \equiv 0 \pmod{p^2}.$$

Let $P(x) = (x-1)^{\underline{p}}$. Write

$$f(t) := \prod_{i=1}^{p-1} [t - (px+i)] = t^{p-1} + b_{p-2}t^{p-2} + \cdots + b_1 t + b_0.$$

Then

$$t_{p-1} + b_{p-2}t^{p-2} + \cdots + b_0 = (t-px)^{p-1} + a_{p-2}(t-px)^{p-2} + \cdots + a_1(t-px) + a_0.$$

Matching the coefficient of t^2 on both sides, using the Binomial Theorem,

$$\begin{aligned} b_n &\equiv \sum_{n=2}^{p-1} a_n \binom{n}{2} (px)^{n-2} \\ &\equiv a_2 + a_3 p + a_4 p^2 \equiv a_2 \pmod{p^3} \end{aligned}$$

(We used $p > 5 \Rightarrow p|a_4$.) By Vieta's formula,

$$b_2 = (px + p - 1)^{\underline{p-1}} \left(\sum_{1 \le i < j \le p-1} \frac{1}{(px+i)(px+j)} \right).$$

By Wolstenholme,

$$(px - 1)^{\underline{p-1}} \equiv (py - 1)^{\underline{p-1}} \pmod{p^3}.$$

Using Wolstenholme and $a_2 \equiv b_2 \pmod{p^3}$, we get

$$\sum_{1 \le i < j \le p-1} \left(\frac{1}{(px+i)(px+j)} \right) \equiv \sum_{1 \le i < j \le p-1} \pmod{p^3}.$$

So

$$\begin{aligned}
\sum_{k=1}^{p-1} \frac{1}{(px+k)^2} &\equiv \left(\sum_{k=1}^{p-1} \frac{1}{(px+k)^2} \right)^2 - 2 \sum_{1 \le i < j \le p-1} \frac{1}{(px+i)(px+j)} \\
&\equiv 0 - 2 \sum_{1 \le i < j \le p-1} \frac{1}{(px+i)(px+j)} \\
&\equiv \left(\sum_{k=1}^{p-1} \frac{1}{(py+k)^2} \right)^2 - 2 \sum_{1 \le i < j \le p-1} \frac{1}{(py+i)(py+j)} \\
&\equiv \sum_{k=1}^{p-1} \frac{1}{(py+k)^2} \pmod{p^3}
\end{aligned}$$