

## Solution 1 (INMO 2020/5)

Let  $F$  be the infinite family and  $d$  be the distance between two closest parallel lines. Let the parallel diagonals  $PQ$  and  $RS$  have lengths  $2R \sin \frac{2\pi}{n}$  and  $2R \sin \frac{4\pi}{n}$ . If lines  $MP, NR \in F$  such that  $QM \perp PM$  and  $SN \perp RN$  then  $\triangle PQM \sim \triangle RSN$ . As  $QM$  and  $SN$  are integral multiples of  $d$ ,  $\frac{RS}{PQ} = \frac{SN}{QM}$  is rational.

$$\frac{RS}{PQ} = \frac{2R \sin \frac{4\pi}{n}}{2R \sin \frac{2\pi}{n}} = 2 \cos \frac{2\pi}{n}$$

So  $\cos \frac{2\pi}{n}$  is rational. By Niven's theorem,  $\cos \frac{2\pi}{n} \in \{-1, -\frac{1}{2}, 0, \frac{1}{2}, 1\}$  and this gives  $n = 3, 4, 6$ . It can be easily checked that all three solutions work.

## Solution 2 (BAMO 2018/5)

At a vertex,  $\frac{\pi(n-2)}{n} = \theta_1 + \dots + \theta_k$  where  $\cos \theta_1, \sin \theta_1 \dots \in \mathbb{Q}$ . So  $\cos \frac{2\pi}{n}, \sin \frac{2\pi}{n} \in \mathbb{Q}$ . By Niven's theorem,  $n = 4$ . It is possible for this case by dividing the square into  $3 \times 4$  rectangles.

## Solution 3 (Black MOP 2010)

Assign complex numbers  $1, \omega^1, \omega^2, \dots, \omega^{n-1}$  to the lamps where 1 is the lamp which is initially on and  $\omega = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$ . If the lamps on a regular polygon are toggled, the sum of their weights is zero. So if we add half of the weights of each lamp when toggled, the sum is zero. 1 is toggled an odd number of times, say  $2k+1$  times.  $\omega^1, \omega^2, \dots, \omega^{n-1}$  each are toggled an even number of times,  $2r_1, 2r_2, \dots, 2r_{n-1}$ . So  $0 = \frac{2k+1}{2} + r_1\omega^1 + r_2\omega^2 + \dots + r_{n-1}\omega^{n-1}$  or  $\frac{-1}{2} = k + r_1\omega^1 + r_2\omega^2 + \dots + r_{n-1}\omega^{n-1}$ . The left hand side is not an algebraic integer, but the right hand side is an algebraic integer, a contradiction. So it is not possible for any  $n$ .

## Solution 5 ( $\infty$ MO 2018/5)

The characteristic polynomial of this sequence is

$$X^k = c_1 X^{k-1} + c_2 X^{k-2} + \dots + c_k$$

with roots  $r_1, \dots, r_k$ . So

$$a_n = d_1 r_1^n + d_2 r_2^n + \dots + d_k r_k^n$$

We take  $a_1, \dots, a_k$  such that  $d_1 = \dots = d_k = 1$ .

$r_1^n + \dots + r_k^n$  is rational by the theorem of symmetric polynomials, and it is an algebraic integer, so it is a rational integer.

$\frac{(r_1 + \dots + r_k)^p - (r_1^p + \dots + r_k^p)}{p}$  is rational, and expanding by binomial theorem (by induction), it is an algebraic integer. So

$$a_p = r_1^p + \dots + r_k^p \equiv (r_1 + \dots + r_k)^p = a_1^p \pmod{p}$$

## Solution 6 (APMO 2018/5)

Assume  $P(0) = 0$ . Let  $p$  be a large prime. If  $P(x) - p = f(x)g(x)$  such that  $g(0) = 1$  then  $\alpha$  is a root of  $g(x)$  such that  $|\alpha| \leq 1$ . Then  $|P(\alpha) - p| \geq p - |P(\alpha)| > 0$ . Therefore  $P(x) - p$  is irreducible over the integers. Choose real  $k$  such that  $P(k) - p = 0$ . Then  $P(x) - p \mid P(mx) - P(mk)$ . As their degree is same, we compare coefficients to get  $P(x) = cx^n$ . If  $P(a) = 1$  then  $P(a^2) = \frac{1}{c}$  is an integer. So the answer is  $\pm x^n + b$ .

## Solution 9 (IMO 2006/5)

If  $Q(t) = t$ , then  $P(t) = t$  or we get a sequence of distinct integers  $x_1, x_2, \dots, x_m$  where  $t = x_1$  and  $m \leq k$ .

$(x_1 - x_2) \mid P(x_1) - P(x_2) = (x_2 - x_3)$  and similar equations give  $|x_1 - x_2| = |x_2 - x_3| = \dots = |x_k - x_1|$

As they are distinct,  $x_1 = x_3 = x_5 = \dots$  and  $x_2 = x_4 = \dots$  so  $P(P(t)) = t$ .

Let  $P(a) = b$  and  $P(b) = a$  where  $a \neq b$ . If such  $a$  and  $b$  do not exist then  $Q(t) = t \implies P(t) = t$  which has at most  $n$  roots.

Now if  $P(c) = d$  and  $P(d) = c$  where these are not equal to any of  $a$  or  $b$ , then  $(b - c) \mid P(b) - P(c) = (a - d)$  and similar divisibility relations give  $|a - d| = |b - c|$  and  $|a - c| = |b - d|$ . Denote these as  $x$ -coordinates of points  $A, B, C, D$  on the  $x$ -axis and  $M$  is the midpoint of  $AB$ . If we fix  $A, B, C$  then there are two positions for  $D$  satisfying  $AD = BC$ . But for only one of these,  $AC = BD$  and  $M$  is the midpoint of  $CD$  in this case. So  $a + b = c + d$ . This is a constant and also holds for  $c = d$ .

So  $Q(t) = t \implies H(t) = a + b - P(t) - t = 0$ . But  $H(x)$  has degree  $n$ , so has at most  $n$  roots.

## Solution 10 (TSTST 2016/1)

Perform the division algorithm on  $A$  and  $B$  for the variable  $x$ , so  $A = B \cdot Q + R$  where  $R$  is a polynomial in  $x$  with coefficients as rational functions of  $y$ . The degree of  $R$  is less than the degree of  $B$  with respect to  $x$ . Now, it is given that for infinitely many values of  $y$ ,  $R = 0$ , i.e. each coefficient of  $R$  is zero. So  $R$  is the zero polynomial. Taking the rational functions of  $y$  in the coefficients of  $y$  into the numerator and denominator by adding all terms, we can write  $Q$  as  $Q = \frac{Q_1(x, y)}{F(y)}$ . Doing the same by interchanging  $x$  and  $y$ , we write in lowest terms  $\frac{A(x, y)}{B(x, y)} = \frac{Q_1(x, y)}{F(y)} = \frac{Q_2(x, y)}{G(x)}$ . So  $F(y) \mid Q_1(x, y)G(x)$ , so  $F(y)$  and  $G(x)$  are constant polynomials.

## Solution 12 (HMIC 2014/4)

Let  $\zeta_j = e^{\frac{2\pi i}{k_j}}$ . Define

$$B = \{a_1\zeta_1^{r_1} + a_2\zeta_2^{r_2} + \dots + a_n\zeta_n^{r_n} \mid \gcd(r_j, k_j) = 1, 1 \leq j \leq n\}$$

$$P(X) = \prod_{\beta \in B} (X - \beta)$$

By the theorem of symmetric polynomials,  $P(X)$  has integer coefficients. As  $P(\alpha) = 0$ , the minimal polynomial of  $\alpha$  divides  $P(X)$ . So the Galois conjugates of  $\alpha$  belong to  $B$ . Now we get a condition from  $\alpha\bar{\alpha} = 1$ . The Galois conjugates of  $\alpha$  satisfy this, so they lie on the unit circle. By Kronecker's theorem,  $\alpha$  is a root of unity.

### Solution 13 (OMO 2015 S28)

We factor both sides as

$$(P(x)+iQ(x))(P(x)-iQ(x)) = (x-1)^2(x+1)^2 \prod_{k=1}^{n-1} (x^{2^k}+1)^2 = (x-1)^2(x+1)^2 \prod_{k=1}^{n-1} (x^{2^{k-1}}-i)^2(x^{2^{k-1}}+i)^2$$

Now we can distribute  $(x^{2^{k-1}}-i)^2(x^{2^{k-1}}+i)^2$  as  $((x^{2^{k-1}}-i)^2, (x^{2^{k-1}}+i)^2), ((x^{2^{k-1}}+i)^2, (x^{2^{k-1}}-i)^2)$  or  $((x^{2^{k-1}}-i)(x^{2^{k-1}}+i), (x^{2^{k-1}}-i)(x^{2^{k-1}}+i))$  as  $P(x)+iQ(x)$  and  $P(x)-iQ(x)$  are conjugates. Multiplying by  $1, -1, i, -i$  we get 4 ordered pairs after the distribution. So the answer is  $4 \cdot 3^{n-1}$ .

### Solution 14 (Taiwan TST 2016/3J/1)

Let  $\lambda = \beta^3$ , the other two roots of the equation  $x^3 = x^2 + 1$  are complex conjugates  $z$  and  $\bar{z}$ .  $\beta^{900} + z^{900} + \bar{z}^{900}$  is an integer, so we can look at 2 times the real part of  $z^{900}$ , which is less than  $4^{-100}$ .

### Solution 16 (USA TST 2017/6)

If  $1 + \omega + \omega^2 = 0$ ,  $g(x) = p(x - \omega)^2(x - \omega^2)^2$  and  $f(x) = (x + 1)^p - x^p - 1$ , then  $f(\omega) = f(\omega^2) = f'(\omega) = f'(\omega^2) = 0$  only when  $3 \mid (p - 1)$ .

So  $p(x^2 + xy + y^2) \mid (x + y)^p - x^p - y^p$ . For every such prime, we choose  $x$  and  $y$  such that  $(xy^{-1})^3 \equiv 1 \pmod{p^2}$  and  $p^2 \mid g(x)$ .

### Solution 20 (Shortlist 2003 N7)

Let  $2a_k = b_k + \frac{1}{b_k}$ . Then  $b_{k+1} = b_k^{\pm 2}$ . As  $b_0 = 2 \pm \sqrt{3}$ ,

$$a_n = \frac{(2 + \sqrt{3})^{2^n} + (2 - \sqrt{3})^{2^n}}{2}$$

We work in  $\mathbb{F}_{p^2}$ . If  $p \mid a_n$ , then  $\alpha = (2 + \sqrt{3}) = \frac{(1 + \sqrt{3})^2}{2} = m^2$  as  $8 \mid p^2 - 1$  and  $\alpha^{2^{n+1}} = m^{2^{n+2}} = -1$ . So  $2^{n+3}$  is the order of  $m$  and divides  $p^2 - 1$ .

### Mini Survey

(a)

It took around 11 hours.

(b)

Problems 2, 3 and 14 were especially nice.