The Forty-Eighth Annual William Lowell Putnam Competition
Saturday, December 5, 1987

Done: all

A–1 Curves A, B, C and D are defined in the plane as follows:

$$\begin{aligned} A &= \left\{(x,y) : x^2 - y^2 = \frac{x}{x^2+y^2}\right\}, \\ B &= \left\{(x,y) : 2xy + \frac{y}{x^2+y^2} = 3\right\}, \\ C &= \left\{(x,y) : x^3 - 3xy^2 + 3y = 1\right\}, \\ D &= \left\{(x,y) : 3x^2y - 3x - y^3 = 0\right\}. \end{aligned}$$

Prove that $A \cap B = C \cap D$.

Solution: *If (x,y) is in D then $x = 0$ implies $y = 0$. But $(0,0)$ is not in C so $(x,y) \in C \cap D$ implies $x \neq 0$. Similarly we deduce $(x,y) \in C \cap D$ implies $y \neq 0$. Check from the definition of B that $y = 0$ is impossible for $x \neq 0$ and let me assume that $(0,0)$ is automatically excluded from the definition of both A and B. From B we learn $x = 0$ implies $y = 1/3$ but this does not belong to A.*

We now assume that all four sets exclude any point with either co-ordinate 0 and rewrite A as

$$A = \left\{(x,y) : y^4 = x^4 - x\right\}$$

B as

$$B = \left\{(x,y) : 2x^3y + 2xy^3 + y = 3x^2 + 3y^2\right\}$$

C as

$$C = \left\{(x,y) : 3x^2y^2 - 3xy = x^4 - x\right\},$$

and D as

$$D = \left\{(x,y) : y^4 = 3x^2y^2 - 3xy\right\}.$$

Let

$$\begin{aligned} a &= y^4 - x^4 - x \\ b &= 2x^3y + 2xy^3 + y - 3x^2 - 3y^2 \\ c &= 3x^2y^2 - 3xy - x^4 + x \\ d &= 3x^2y - 3x - y^3 \end{aligned}$$

Note that $A = \{(x,y) : a = 0\}$ and so on. Then

$$a = -yd - xc \quad \textit{and} \quad b = xd - yc$$

so that $c = d = 0$ implies both $a = 0$ and $b = 0$. Conversely

$$c = -\frac{xa + yb}{x^2 + y^2} \quad \textit{and} \quad d = \frac{xb - ya}{x^2 + y^2}$$

so that $a = b = 0$ implies $c = d = 0$ as desired.

A–2 The sequence of digits

$$12345678910111213141516171819202 1\ldots$$

is obtained by writing the positive integers in order. If the 10^n-th digit in this sequence occurs in the part of the sequence in which the m-digit numbers are placed, define $f(n)$ to be m. For example, $f(2) = 2$ because the 100th digit enters the sequence in the placement of the two-digit integer 55. Find, with proof, $f(1987)$.

Solution: *There are 9 1-digit numbers, 90 2-digit numbers and in general* $9 \times 10^{m-1}$ m*-digit numbers. The* m *digit numbers therefore occupy places* M_m *to* $M_m + m9 \times 10^{m-1} - 1$ *where*

$$\begin{aligned} M_m &= \sum_{j=1}^{m-1} j9 \times 10^{j-1} + 1 = 9 \sum_{j=1}^{m-1} \sum_{i=1}^{j} 10^{j-1} + 1 = 9 \sum_{i=1}^{m-1} \sum_{j=i}^{m-1} 10^{j-1} + 1 \\ &= \sum_{i=1}^{m-1} \frac{9(10^{m-i} - 1)10^{i-1}}{10 - 1} + 1 \\ &= \sum_{i=1}^{m-1} 10^{m-1} - \sum_{i=1}^{m-1} 10^{i-1} + 1 \\ &= (m-1)10^{m-1} - \frac{10^{m-1} - 1}{10 - 1} + 1 = m10^{m-1} - 10^m/9 + 10/9. \end{aligned}$$

In order to compute $f(1987)$ *we must find* m *so that*

$$M_m \leq 10^{1987} < M_{m+1}$$

Rewrite these inequalities as

$$(m - 10/9) \leq 10^{1988-m} - 10^{2-m}/9 < 10(m + 1 - 10/9)$$

For $m = 1984$ *the middle term is between 9999 and 10000 while the first term is 1982+8/9 and the last term is 19838+8/9. Thus* $f(1987) = 1984$*.*

A–3 For all real x, the real-valued function $y = f(x)$ satisfies

$$y'' - 2y' + y = 2e^x.$$

(a) If $f(x) > 0$ for all real x, must $f'(x) > 0$ for all real x? Explain.

(b) If $f'(x) > 0$ for all real x, must $f(x) > 0$ for all real x? Explain.

Solution: *The function* $g(x) = y \exp(-x)$ *has derivative* $(y' - y) \exp(-x)$ *and second derivative* $(y'' - 2y' + y) \exp(-x)$*.Thus*

$$g''(x) = 2.$$

Thus

$$g(x) = x^2 + ax + b$$

for some real constants a *and* b *and*

$$f(x) = (x^2 + ax + b)e^x.$$

The sign of g *is the same as the sign of* f *for all* x*. Moreover* $f' = (g' + g) \exp(x)$ *so that* f' *has the same sign as* $g' + g$*.*

Write

$$g(x) = (x + a/2)^2 + b - a^2/4$$

and see that $f(x) > 0$ *for all* x *if and only if* $b > a^2/4$*. Now* $g' + g = x^2 + (2 + a)x + a + b$ *can be rewritten as*

$$(x + 1 + a/2)^2 + b + a - (1 + a/2)^2 = (x + 1 + a/2)^2 + b - a^2/4 - 1.$$

The minimum value of this will be negative if

$$a^2/4 < b < a^2/4 + 1.$$

For part a) the answer is no.

For the converse the function f' *is everywhere positive if and only if* $b - a^2/4 - 1 > 0$*. If this condition is satisfied then certainly* $b - a^2/4 > 0$ *and so* $g(x) > 0$ *for all* x *and so* $f(x) > 0$ *for all* x*.*

A–4 Let P be a polynomial, with real coefficients, in three variables and F be a function of two variables such that

$$P(ux, uy, uz) = u^2 F(y - x, z - x) \quad \text{for all real } x, y, z, u,$$

and such that $P(1, 0, 0) = 4$, $P(0, 1, 0) = 5$, and $P(0, 0, 1) = 6$. Also let A, B, C be complex numbers with $P(A, B, C) = 0$ and $|B - A| = 10$. Find $|C - A|$.

Solution: *Write P in the form*

$$P(x, y, z) = \sum_{r=0}^{d} Q_r(x, y, z)$$

where Q_r is homogeneous of degree r. Then

$$P(ux, uy, uz) = \sum_{r=0}^{d} u^r Q_r(x, y, z) = u^2 F(y - x, z - x)$$

shows that $Q_r \equiv 0$ for all $r \neq 2$. Thus

$$P(x, y, z) = ax^2 + by^2 + cz^2 + dxy + exz + fyz$$

for some reals a, b, c, d, e, f. Putting $x = y = z$ gives

$$P(ux, ux, ux) = u^2 F(0, 0)$$

from which we deduce $F(0, 0) = 0$ (by say taking $x = 1/u$). That is, $P(1, 1, 1) = a + b + c + d + e + f = 0$. Then $P(1, 0, 0) = a = 4$, $P(0, 1, 0) = b = 5$ and $P(0, 0, 1) = c = 6$. Notice that

$$P(0, y, z) = 5y^2 + 6z^2 + fyz = F(y, z).$$

Thus

$$P(x, y, z) = 5(y - x)^2 + 6(z - x)^2 + f(y - x)(z - x)$$

The coefficient of x^2 is $5 + 6 + f = 4$ so $f = -7$.

The complex numbers A, B and C satisfy

$$5(B - A)^2 + 6(C - A)^2 - 7(B - A)(C - A) = 0.$$

Let $v = B - A$ and $w = C - A$ and get

$$w = \frac{7v \pm \sqrt{49v^2 - 120v^2}}{12} = v\frac{7 \pm \sqrt{71}i}{12}.$$

The modulus of this is

$$|v|\sqrt{7^2 + 71}/12 = 10\sqrt{120/144} = 10\sqrt{5/6}.$$

This seems a particularly unlikely answer.

A–5 Let

$$\vec{G}(x, y) = \left(\frac{-y}{x^2 + 4y^2}, \frac{x}{x^2 + 4y^2}, 0 \right).$$

Prove or disprove that there is a vector-valued function

$$\vec{F}(x, y, z) = (M(x, y, z), N(x, y, z), P(x, y, z))$$

with the following properties:

(i) M, N, P have continuous partial derivatives for all $(x, y, z) \neq (0, 0, 0)$;

(ii) $\mathrm{Curl}\,\vec{F} = \vec{0}$ for all $(x, y, z) \neq (0, 0, 0)$;

(iii) $\vec{F}(x, y, 0) = \vec{G}(x, y)$.

Solution: *A curl free function on an open, simply connected subset of R^3 is the gradient of potential function ϕ so the line integral of F around any curve must be 0. But the line integral of $\int F \cdot dl$ around the eliipse $x^2 + 4y^2 = 1$ in the plane $z = 0$ is not 0. Specifically the parametrization $x = \cos(\theta)$ and $2y = \sin(\theta)$ gives*

$$\int_0^{2\pi} \left\{ -\frac{1}{2}\sin^2(\theta) - \frac{1}{2}\cos^2(\theta) \right\} d\theta = -\pi \neq 0.$$

So no such vector field F exists. Notice that R^3 minus the origin is simply connected.

A–6 For each positive integer n, let $a(n)$ be the number of zeroes in the base 3 representation of n. For which positive real numbers x does the series

$$\sum_{n=1}^{\infty} \frac{x^{a(n)}}{n^3}$$

converge?

Solution: *Call the sum S. Consider integers n with*

$$3^{m-1} \leq n < 3^m$$

Such integers have m ternary digits with the leading digit being a 1 or a 2, of course. For such integers we have

$$\frac{1}{3^{3m}} \leq \frac{1}{n^3} \leq \frac{1}{3^{3(m-1)}} \quad \textit{or} \quad \frac{1}{27^m} \leq \frac{1}{n^3} \leq \frac{27}{27^m}.$$

We now count the number of such n with $a(n) = k$ for $k = 0, \ldots, m-1$. There are $\binom{m}{j}$ integers n with leading digit 1 and j 0s and the same number with leading digit 2. This tells us that there are $2\binom{m}{j}$ integers n in the given range with $a(n) = j$ so that the sum is bounded by

$$2\sum_m \frac{\sum_{j=0}^m \binom{m}{j} x^j}{27^m} \leq S \leq 54 \sum_m \frac{\sum_{j=0}^m \binom{m}{j} x^j}{27^m}.$$

The sums over j can be done by the binomial expansion to show

$$2\sum_m \frac{(1+x)^m}{27^m} \leq S \leq 54 \sum_m \frac{(1+x)^m}{27^m}.$$

The bounding geometric sums converge if and only if

$$\frac{1+x}{27} < 1$$

or

$$x < 26$$

apparently.

B–1 Evaluate

$$\int_2^4 \frac{\sqrt{\ln(9-x)}\, dx}{\sqrt{\ln(9-x)} + \sqrt{\ln(x+3)}}.$$

Solution: *The substitution* $9 - x = y + 3$ *shows that*

$$I_1 \equiv \int_2^4 \frac{\sqrt{\ln(9-x)}\,dx}{\sqrt{\ln(9-x)}+\sqrt{\ln(x+3)}} = \int_2^4 \frac{\sqrt{\ln(y+3)}\,dy}{\sqrt{\ln(y+3)}+\sqrt{\ln(9-y)}} \equiv I_2.$$

But

$$I_1 + I_2 = \int_2^4 \frac{\sqrt{\ln(9-x)}+\sqrt{\ln 3+x}}{\sqrt{\ln(9-x)}+\sqrt{\ln(x+3)}}dx = \int_2^4 1dx = 2.$$

So

$$I_1 = 1.$$

B–2 Let r, s and t be integers with $0 \le r$, $0 \le s$ and $r + s \le t$. Prove that

$$\frac{\binom{s}{0}}{\binom{t}{r}} + \frac{\binom{s}{1}}{\binom{t}{r+1}} + \cdots + \frac{\binom{s}{s}}{\binom{t}{r+s}} = \frac{t+1}{(t+1-s)\binom{t-s}{r}}.$$

Solution: *You have* $t + 1$ *balls of which* s *are silver. You pick balls at random without replacement until you get something* $r + 1$ *red balls. The chance that you get* j *silver balls is the chance that draw number* $r + j + 1$ *is red and* j *of the first* $j + r$ *draws are silver. There are* $\binom{s}{j}$ *ways to pick* j *silver balls from the* s, $\binom{t-s}{r}$ *ways to pick* r *red balls from the* $t - s$ *red balls other than the one picked on trial* $r + j + 1$ *and a total of* $\binom{t}{r+j}$ *ways to pick a total of* $r + j$ *balls from the* t *other than the one you picked on draw* $r + j + 1$. *So:*

$$P(j \text{ silver balls drawn}) = \left(1 - \frac{s}{t+1}\right)\frac{\binom{s}{j}\binom{t-s}{r}}{\binom{t}{r+j}}$$

Adding over j *must give 1 because the number of silver balls must be some* $j \in \{0, 1, \ldots, s\}$.

B–3 Let F be a field in which $1 + 1 \ne 0$. Show that the set of solutions to the equation $x^2 + y^2 = 1$ with x and y in F is given by $(x, y) = (1, 0)$ and

$$(x, y) = \left(\frac{r^2-1}{r^2+1}, \frac{2r}{r^2+1}\right)$$

where r runs through the elements of F such that $r^2 \ne -1$.

Solution: *It is straightforward algebra to check that any order pair of the given form must have* $x^2 + y^2 = 1$ *because* $(r^2 - 1)^2 + (2r)^2 = (r^2 + 1)^2$. *For the converse suppose* (x, y) *is such a pair with* $x \ne 1$. *We want* $x = (r^2 - 1)/(r^2 + 1)$ *for some* r *we wish to find. Then*

$$r^2(1 - x) = (1 + x)$$

For $x^2 \ne 1$ *we then get*

$$r^2 = (1 + x)(1 - x)^{-1} = (1 + x)^2(1 - x^2)^{-1} = (1 + x)^2(y^2)^{-1}.$$

Take square roots to get

$$r = (1 + x)y^{-1}.$$

Note that if $x^2 \ne 1$ *we have* $y^2 \ne 0$ *so* $y \ne 0$ *so* y *is invertible. Check that for* r *as defined we have* $(r^2 - 1)/(r^2 + 1) = x$ *and* $2r/(1 + r^2) = y$. *It remains to consider the possibility that* $x^2 = 1$ *so that* $y = 0$ *but* $x \ne 1$. *In this case* $1 - x^2 = (1 - x)(1 + x) = 0$ *so that one of the two terms is 0 and either* $x = 1$ *or* $x = -1$. *In the latter case we take* $r = 0$ *and check that we have a solution. Finally notice that if we had* $x = 1$ *for the* r *we have found then we would have* $r^2 - 1 = r^2 + 1$ *or* $1 + 1 = 0$.

B–4 Let $(x_1, y_1) = (0.8, 0.6)$ and let $x_{n+1} = x_n \cos y_n - y_n \sin y_n$ and $y_{n+1} = x_n \sin y_n + y_n \cos y_n$ for $n = 1, 2, 3, \ldots$. For each of $\lim_{n\to\infty} x_n$ and $\lim_{n\to\infty} y_n$, prove that the limit exists and find it or prove that the limit does not exist.

Solution: *Define the function*

$$T(x, y) = (x', y') \equiv (x\cos(y) - y\sin(y), x\sin(y) + y\cos(y)).$$

Check that $x^2 + y^2 = 1$ *implies* $(x')^2 + (y')^2 = 1$ *so that* T *maps the unit circle to the unit circle. If* $(x, y) = (\cos(\theta), \sin(\theta))$ *then using standard trigonometric identities we see*

$$T(x, y) = (\cos(\theta + y), \sin(\theta + y)).$$

The map

$$g : \theta \mapsto \theta + \sin\theta$$

has the following properties. First it is monotone increasing on $[0, \pi]$ *and strictly so on the open interval* $(0, \pi)$. *Since* $g(0) = 0$ *and* $g(\pi) = \pi$ *we see that* g *is a bijection of* $[0, \pi]$ *to* $[0, \pi]$. *Suppose now that* $(x, y) = (\cos\theta, \sin\theta)$ *is a point on the unit circle with* $y > 0$. *It follows that*

$$x' = \cos(\theta + \sin(\theta)) < x$$

and $y' > 0$. *Then* $y\sin(y) > 0$ *so*

$$x' = x\cos(y) - y\sin(y) < x\cos(y).$$

Thus we have

$$x_1 > x_2 > \cdots$$

and

$$0 < \theta_1 < \theta_2 < \cdots < \pi.$$

Thus the sequence θ_n *has some limit* θ *in* $(0, \pi]$. *Since* g *is continuous we find*

$$\theta = \lim_n \theta_n = \lim_n \theta_{n+1} = \lim_n g(\theta_n) = g(\theta).$$

But $g(\theta) = \theta \in (0, \pi]$ *implies* $\theta = \pi$ *so that both the sequences* x_n *and* y_n *have limits* $x = -1$ *and* $y = 0$.

B–5 Let O_n be the n-dimensional vector $(0, 0, \cdots, 0)$. Let M be a $2n \times n$ matrix of complex numbers such that whenever $(z_1, z_2, \ldots, z_{2n})M = O_n$, with complex z_i, not all zero, then at least one of the z_i is not real. Prove that for arbitrary real numbers $r_1, r_2, \ldots, r_{2n}$, there are complex numbers $w_1, w_2, \ldots, w_n$ such that

$$\mathrm{re}\left[M\begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix}\right] = \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix}.$$

(Note: if C is a matrix of complex numbers, $\mathrm{re}(C)$ is the matrix whose entries are the real parts of the entries of C.)

Solution: *Write* $M = A + iB$ *with* A *and* B *real. Write* $z = u + iv$ *with* u *and* v *real. Then*

$$zM = uA - vB + i(uB + vA) = O$$

implies both $uB + vA = 0$ *and* $uA - vB = 0$. *We are given that these equations and* $v = 0$ *imply* $u = 0$. *Let* C *be the matrix which puts* A *and* B *side by side. We have learned* $uC = 0$ *implies* $u = 0$ *so that* C *has full rank,* $2n$, *and is invertible. Now write* $w = x + iy$ *with* x *and* y *real and then*

$$re(Mw) = Ax - By = C\begin{bmatrix} x \\ -y \end{bmatrix}.$$

Let $s = C^{-1}r$ *and let* x *be the first* n *elements of* s *and* y *be the negative of the last* n *elements of* s. *This* x *and* y *solve the problem.*

B–6 Let F be the field of p^2 elements, where p is an odd prime. Suppose S is a set of $(p^2-1)/2$ distinct nonzero elements of F with the property that for each $a \neq 0$ in F, exactly one of a and $-a$ is in S. Let N be the number of elements in the intersection $S \cap \{2a : a \in S\}$. Prove that N is even.

Solution: *For any non-zero $x \in F$, the set $O_x = \{x, 2x, 4x, \cdots\} = \{x, 2x, \ldots, 2^{r-1}x\}$, where r is the least integer for which $2^r = 1$, has cardinality r. For any two non-zero x and y either $O_x = O_y$ or the two are disjoint. Two cases arise. In Case A, r is even and $2\ell = r$. Then $2^\ell = -1$ (because $x^2 - 1 = 0$ factors the only square roots of 1 are 1 and -1 and 1 is ruled out by definition of r). In Case B r is odd.*

Case A. In this case for each $y \in O_x$ we have $-y = 2^\ell x \in O_x$ so exactly half the elements of O_x are in S; that is, ℓ of the elements of O_x are in S. Let $J_+ = \{j : 2^j x \in S, 0 \leq j \leq \ell - 1\}$. Let $J_- = \{j : 2^j x \in S, \ell \leq j \leq r-1\}$ and notice that $J_- = J_+ + \ell$, that is, J_- is determined by J_+. The cardinality of $C \cap O_x$ is

$$\sum_{0 \leq j \leq r-1} 1(y \in S, y/2 \in S) = \sum_{j \in J_+, j>0} 1(j-1 \in J_+) + \sum_{j \in J_-, j > \ell} 1(j-1 \in J_-) + 1(0 \in J_+, r-1 \in J_-) + 1(\ell \in J_-, \ell - 1 \in J_+).$$

Consider making a new subset J_+^* of $\{0, \ldots, \ell - 1\}$ from a given set J_+ by removing some j_0 from J_+. To maintain the required properties of S we would have to add $j_0 + \ell$ to J_-. The sum on the right hand side above changes as follows. If $j_0 - 1$, j_0 and $j_0 + 1$ were all in J_+ then the first term decreases by 2. Moreover, none of $j_0 + \ell - 1$, $j_0 + \ell$, or $j_0 + \ell + 1$ were in J_- so none of the other three terms is changed. That is, the parity of J_+ is unchanged as is the parity of J_-. If j_0 and $j_0 + 1$ were in J_+ but $j_0 - 1$ was not then the first term has decreased by 1 but the second term has increased by 1. Similar arguments apply if $j_0 - 1$ and j_0 are both in J_+ but $j_0 + 1$ is not and if neither $j_0 - 1$ nor $j_0 + 1$ are in J_+. The cases of $j_0 = 0$ or $j_0 = \ell$ are also similar. In every case the parity is unchanged. Every possible J_+ can be obtained by deleting elements one at a time from the initial set $\{0, \ldots, \ell - 1\}$. For this set the sum indicated is $\ell - 1$ so: when ℓ is even the cardinality of $O_x \cap C$ is odd and vice-versa. In both cases the cardinality of C is the sum over a suitable set of x values of the cardinalities of $O_x \cap C$. Since the parities are all the same the parity of the sum is the number of terms in a partition of the non-zero elements of F into these orbits O_x. The number of orbits required is $(p^2-1)/r = (p+1)(p-1)/r$. Since r is the order of a cylic subgroup of the multiplicative group of nonzero elements of F we see that r divides $p - 1$, that is, $(p-1)/r$ is an integer. Since p is odd we see $(p+1)$ is even and $(p^2-1)/r$ is an even integer.

Case B. In this case O_x and O_{-x} are disjoint for any x and every O_x has cardinality r. Find $x_1, \ldots, x_m$ such that the sets $O_{x_1}, O_{-x_1}, \ldots, O_{x_m}, O_{-x_m}$ form a partition of the set of non-zero elements of F. Thus $2mr = p^2 - 1$. I claim that the cardinality of $\{y \in O_x : y \in S, y/2 \in S\}$ is the same as the cardinality of $\{y \in O_{-x} : y \in S, y/2 \in S\}$. Thus $\{y \in (O_x \cup O_{-x}) : y \in S, y/2 \in S\}$ has even cardinality. Then I partition the non-zero elements of F into a disjoint union over a collection of x values such that

$$F \setminus \{0\} = \cup_x \{O_x \cup O_{-x}\}.$$

to see that N is a sum of even numbers, so even.

To prove the claim let

$$a = \sum_{y \in O_x} 1(y \in S, y/2 \in S)$$

and

$$b = \sum_{y \in O_{-x}} 1(y \in S, y/2 \in S)$$

I will show that $a + b$ has the same parity as the cardinality of O_x so is the same for all x. The parity of N is thus the parity of m times the cardinality r of any O_x.Since $2mr = p^2 1 = (p+1)(p-1)$ is divisible by 4 (both $p+1$ and $p-1$ are even) we must have mr is even. It remains to show that $a + b \equiv r$ modulo 2. Let

$$c = \sum_{y \in O_x} 1(y \in S, y/2 \notin S) = \sum_{y \in O_x} 1(y \notin S, y/2 \in S)$$

and

$$d = \sum_{y \in O_{-x}} 1(y \in S, y/2 \notin S) = \sum_{y \in O_{-x}} 1(y \notin S, y/2 \in S)$$

Then

$$\begin{aligned} a + c &= \sum_{y \in O_x} 1(y \in S, y/2 \in S) + \sum_{y \in O_x} 1(y \in S, y/2 \notin S) \\ &= \sum_{y \in O_x} 1(y \in S) \end{aligned}$$

and

$$\begin{aligned} b + d &= \sum_{y \in O_{-x}} 1(y \in S, y/2 \in S) + \sum_{y \in O_{-x}} 1(y \in S, y/2 \notin S) \\ &= \sum_{y \in O_{-x}} 1(y \in S) \\ &= \sum_{y \in O_x} 1(-y \in S) \\ &= \sum_{y \in O_x} 1(y \notin S) \end{aligned}$$

Thus

$$a + b + c + d = \sum_{y \in O_x} 1(y \in S) + \sum_{y \in O_x} 1(y \notin S) = \#O_x.$$

Next

$$\begin{aligned} d = \sum_{y \in O_{-x}} 1(y \notin S, y/2 \in S) &= \sum_{-y \in O_x} 1(y \notin S, y/2 \in S) \\ &= \sum_{y \in O_x} 1(-y \notin S, -y/2 \in S) \\ &= \sum_{y \in O_x} 1(y \in S, y/2 \notin S) \\ &= \sum_{y \in O_x} 1(y \notin S, y/2 \in S) \\ &= c \end{aligned}$$

So

$$a + b + 2c = \#O_x.$$

This establishes the claim.

Two special cases, $p = 3$ and $p = 5$ have more structure. For $p = 3$ we have $N = 0$ and for $p = 5$ we have $N = 6$. Consider first the case $p = 3$. Then for any a we have $a + 2a = 3a = 0$ so $2a = -a$. Since either a or $-a$ is in S but not both we find that C is empty so $N = 0$. For the case $p = 5$ notice that $2^4 = 1$ and $2^2 = 4 = -1$ in this field. For any non-zero $x \in F$ consider the set $O_x = \{x, 2x, 4x, 8x\}$. The set of 24 non-zero elements of F can be split into 6 disjoint sets $O_{x_1}, \ldots, O_{x_6}$. As above 2 of the four elements on O_x must be in S. Without loss, then, we may assume each $x_i \in S$. For each i either $2x_i \in S$ or $8x_i \in S$ but not both. If $2x_i \in S$ then $C \cap O_{x_i} = 2x_i$ while if $8x_i \in S$ then $x_i = 2 \cdot 8x_i \in C$ and $C \cap O_{x_i} = \{x_i\}$. In either case the cardinality of $O_{x_i} \cap C$ is 1 and so the cardinality of C is $N = 6$ which is even.