IMO 2017

Aufgabe 1: Für jede ganze Zahl $a_0 > 1$ sei die Folge a_0, a_1, a_2, ... gegeben durch

$$a_{n+1} = \begin{cases} \sqrt{a_n} & \text{falls } \sqrt{a_n} \text{ ganzzahlig,} \\ a_n + 3 & \text{sonst,} \end{cases} \qquad \text{für alle } n \geqslant 0.$$

Man bestimme alle Werte von a_0, so dass es eine Zahl A gibt, mit $a_n = A$ für unendlich viele Werte von n.

Lösung: Wir stellen zunächst fest, dass die Existenz eines Paares von Indizes $m > n$ mit $a_m = a_n$ unmittelbar zur Konsequenz hat, dass die Folge periodisch wird, was die Existenz eines Wertes A der geforderten Art garantiert.

Gibt es einen Index n, sodass $a_n \equiv 2 \pmod 3$ gilt, so gilt auch $a_m \equiv 2 \pmod 3$ für alle $m \geq n$. Da 2 kein quadratischer Rest modulo 3 ist, kann es somit in der Folge a_n für Indizes $m \geq n$ keine Quadratzahlen geben. Es gilt somit für all diese Indizes $a_{m+1} = a_m + 3 > a_m$, und die Folge ist ab dem n-ten Glied streng monoton steigend. In diesem Fall gibt es also keinen Wert A der geforderten Art. Für $a_0 \equiv 2 \pmod 3$ gibt es also niemals einen derartigen Wert A.

Nun beobachten wir, dass $a_n \equiv 0 \pmod 3 \Leftrightarrow a_{n+1} \equiv 0 \pmod 3$ unmittelbar aus der Definition der Rekursion folgt.

Betrachten wir nun Ausgangswerte $a_0 \equiv 1 \pmod 3$, sehen wir, dass es in der Folge keinen Index n mit $a_n \equiv 0 \pmod 3$ geben kann. Es muss aber in diesem Fall einen Index k mit $a_k \equiv 2 \pmod 3$ geben. Nehmen wir nämlich an, dass alle a_i der Folge kongruent 1 modulo 3 seien, so folgt für $a_n = (3k+1)^2$ wegen

$$3k + 1 = (3k - 1) + 2 \leq (3k - 1) \cdot 2 \leq (3k - 1)^2 < (3k + 1)^2$$

und $(3k-1)^2 \equiv 1 \pmod 3$, dass die nächste Quadratzahl in der Folge kleiner als $(3k+1)^2$ sein muss, und somit $a_m < 3k + 1$ für einen Index $m > n$. Dies kann aber nur endlich oft der Fall sein, und wir erhalten einen Widerspruch zur Annahme, dass dies in der Folge unendlich oft geschieht. In der Folge gibt es also sicher ein Glied $a_k \equiv 2 \pmod 3$, und somit gibt es auch in diesem Fall niemals ein A der geforderten Art.

Nun verbleiben die durch 3 teilbare Werte von a_0. Wir zeigen, dass es in diesem Fall auf jeden Fall einen Wert A der geforderten Art gibt; sogar drei davon. Zu diesem Zweck beweisen wir zunächst das folgende Lemma.

Lemma: Gilt $a_n \equiv 0 \pmod 3$ und $a_n > 9$, so gibt es einen Index m mit $m > n$ und $a_m < a_n$.

Beweis des Lemmas: Sei t^2 die größte Quadratzahl kleiner als a_n. Wegen $a_n > 9$ gilt $t \geq 3$. Die erste Quadratzahl in der Folge $a_n, a_n + 3, a_n + 6, \ldots$ ist also eine der Zahlen $(t+1)^2$, $(t+2)^2$ oder $(t+3)^2$, und es gibt somit einen Index m mit $a_m \leq t + 3 < t^2 < a_n$, wie behauptet. Die Gültigkeit des Lemmas ist somit gezeigt.

Nun betrachten wir einen beliebigen Wert a_n mit $a_n \equiv 0 \pmod 3$. Für $a_n \in \{3, 6, 9\}$ ist die Folge jedenfalls ab diesem Glied der Gestalt $(3), (6), 9, 3, 6, 9, \ldots$, und es gibt drei Werte A der geforderten Art, nämlich 3, 6 und 9. Ist $a_n > 9$, sei j ein Index, sodass a_j das kleinste Element der Menge $\{a_{n+1}, a_{n+2}, \ldots\}$ ist. Aufgrund des Lemmas muss aber $a_j \leq 9$ gelten. Somit kommen wir auch in diesem Fall in den Zyklus $3, 6, 9, 3, 6, 9, \ldots$, und auch in diesem Fall gibt es dieselben Werte von A.

Wir sehen zusammenfassend, dass es einen Wert A der geforderten Art genau für die durch 3 teilbaren Werte von a_0 gibt. □

Aufgabe 2: Es sei $\mathbb{R}$ die Menge der reellen Zahlen. Man bestimme alle Funktionen $f\colon \mathbb{R} \to \mathbb{R}$, so dass für alle reellen Zahlen x und y gilt

$$f\left(f(x)f(y)\right) + f(x+y) = f(xy).$$

Lösung: Es gibt drei derartige Funktionen, nämlich

$$x \mapsto 0, \quad x \mapsto x-1 \quad \text{und} \quad x \mapsto 1-x.$$

Es ist leicht einzusehen, dass diese drei Funktionen tatsächlich Lösungen der Funktionalgleichungen sind. Es bleibt also zu zeigen, dass es keine weiteren gibt.

Zu diesem Zweck stellen wir zunächst fest, dass die Tatsache, dass eine bestimmte Funktion $f(x)$ eine Lösung ist, zur Konsequenz hat, dass auch $-f(x)$ eine Lösung ist. Wir können also im weiteren oBdA annehmen, dass $f(0) \leq 0$ gilt. Wir wollen also zeigen, dass in diesem Fall entweder $f(x) = 0$ oder $f(x) = x-1$ gelten muss.

Nun beobachten wir, dass es zu jedem $x \neq 1$ einen eindeutigen Wert y mit $y = \frac{x}{x-1} \Leftrightarrow x+y = xy$ gibt. Setzen wir diesen Wert in der gegebenen Gleichung ein, sehen wir, dass

$$f\left(f(x) \cdot f\left(\frac{x}{x-1}\right)\right) = 0 \tag{1}$$

für alle $x \neq 1$ gelten muss. Setzen wir speziell in dieser Gleichung den Wert $x = 0$ ein, sehen wir, dass f zumindest eine Nullstelle besitzen muss, nämlich $(f(0))^2$. Nun haben wir vorausgesetzt, dass $f(0) \leq 0$ gilt, und es gibt daher zwei Fälle zu unterscheiden.

Fall1: $f(0) = 0$

Setzen wir in diesem Fall in der gegebenen Funktionalgleichung $y = 0$ ein, erhalten wir

$$f(f(x)f(0)) + f(x) = f(0),$$

und somit $f(x) = 0$ für alle reellen Werte von x. Dies liefert also die Lösung $f(x) = 0$.

Fall 2: $f(0) < 0$

In diesem Fall beweisen wir zuerst die Gültigkeit der folgenden Behauptung:

Behauptung 1: Es gelten

$$f(1) = 0, \quad f(a) = 0 \Rightarrow a = 1 \quad \text{und} \quad f(0) = -1.$$

Wir wollen also zunächst zeigen, dass 1 die eindeutige Nullstelle von f ist. Aufgrund der Beziehung $f((f(0))^2) = 0$ hat f jedenfalls zumindest eine Nullstelle a. Gilt $a \neq 1$, können wir in (1) $x = a$ setzen, und erhalten die Beziehung $f(0) = 0$, also einen Widerspruch zur Annahme $f(0) < 0$. $x = 1$ ist somit die eindeutige Nullstelle von f. Aus der Beziehung $f((f(0))^2) = 0$ erhalten wir somit $(f(0))^2 = 1$, und somit wegen der Voraussetzung $f(0) < 0$, sicher $f(0) = -1$.

Nun erhalten wir durch Einsetzen von $y = 1$ in der ursprünglichen Gleichung

$$f(f(x)f(1)) + f(x+1) = f(x) \iff f(0) + f(x+1) = f(x) \iff f(x+1) = f(x) + 1$$

für alle reellen Zahlen x. Einfache Induktion liefert somit auch $f(x+n) = f(x)+n$ für alle reellen Werte von x und alle ganzzahligen Werte von n. Nun können wir also die nächste Behauptung beweisen:

Behauptung 2: f ist injektiv.

Wir nehmen an, es gelte $f(a) = f(b)$ mit $a \neq b$. Wegen $f(x+n) = f(x) + n$, gilt dann

$$f(a+N+1) = f(b+N) + 1$$

für alle ganzen Zahlen N. Wählt man eine beliebige ganze Zahl $N < -b$, so gibt es nach dem Satz von Vieta sicher reelle Zahlen x_0 und y_0 mit $x_0 + y_0 = a + N + 1$ und $x_0 y_0 = b + N$. Wegen $a \neq b$ gilt $x_0 \neq 1$ und $y_0 \neq 1$. Würde nun $x_0 = 1$ gelten, so hätten wir $1 + y_0 = a + N + 1$ und $y_0 = b + N$ und somit $a = b$. Es gilt daher sicher $x_0 \neq 1$ und analog auch $y_0 \neq 1$. Setzen wir also x_0 und y_0 in der ursprünglichen Gleichung ein, erhalten wir

$$\begin{aligned} f(f(x_0)f(y_0)) + f(a+N+1) = f(b+N) &\iff f(f(x_0)f(y_0)) + 1 = 0 \\ &\iff f(f(x_0)f(y_0) + 1) = 0 \\ &\iff f(x_0)f(y_0) = 0, \end{aligned}$$

da 1 die einzige Nullstelle von f ist. Da aber weder x_0 noch y_0 gleich 1 sein können, kann auch weder $f(x_0)$ noch $f(y_0)$ gleich 0 sein, und wir erhalten einen Widerspruch. f ist also sicher injektiv.

Nun können wir, um den Beweis abzuschließen, einen beliebigen reellen Wert t annehmen, und $(x, y) = (t, -t)$ in der ursprünglichen Gleichung einsetzen. Dies ergibt

$$\begin{aligned} f(f(t)f(-t)) + f(0) = f(-t^2) &\iff f(f(t)f(-t)) = f(-t^2) + 1 \\ &\iff f(f(t)f(-t)) = f(-t^2 + 1) \\ &\iff f(t)f(-t) = -t^2 + 1. \end{aligned}$$

Setzen wir andererseits $(x, y) = (t, 1-t)$ ein, erhalten wir

$$\begin{aligned} f(f(t)f(1-t)) + f(1) = f(t(1-t)) &\iff f(f(t)f(1-t)) = f(t(1-t)) \\ &\iff f(t)f(1-t) = t(1-t). \end{aligned}$$

Wegen $f(1-t) = 1 + f(-t)$ gilt aber somit

$$\begin{aligned} f(t)f(1-t) = t(1-t) &\iff f(t)(1 + f(-t)) = t(1-t) \\ &\iff f(t) + (-t^2 + 1) = t(1-t) \\ &\iff f(t) = t - 1. \end{aligned}$$

Wir erkennen also, dass es tatsächlich außer den genannten drei Funktionen keine weiteren Lösungen der gegebenen Funktionalgleichung geben kann. □

Aufgabe 3: Ein Jäger und ein unsichtbarer Hase spielen in der euklidischen Ebene ein Spiel. Der Ausgangspunkt A_0 des Hasen und der Ausgangspunkt B_0 des Jägers sind gleich. Nach $n-1$ Runden des Spiels befinden sich der Hase im Punkt A_{n-1} und der Jäger im Punkt B_{n-1}. Die n-te Runde des Spiels besteht aus drei Schritten in der angegebenen Reihenfolge:

(i) Der Hase bewegt sich unsichtbar zu einem Punkt A_n, so dass der Abstand zwischen A_{n-1} und A_n genau eins ist.

(ii) Ein Ortungsgerät meldet dem Jäger einen Punkt P_n. Die einzige Garantie, die das Ortungsgerät dem Jäger gibt, ist, dass der Abstand zwischen P_n und A_n höchstens eins ist.

(iii) Der Jäger bewegt sich sichtbar zu einem Punkt B_n, so dass der Abstand zwischen B_{n-1} und B_n genau eins ist.

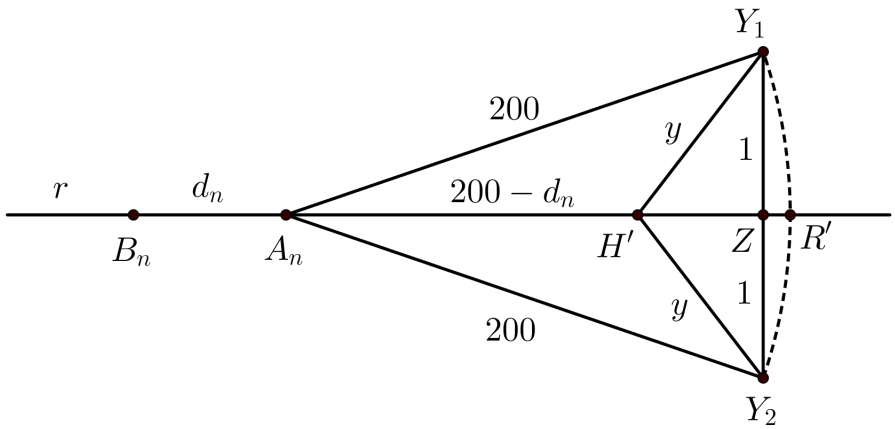
Ist es immer möglich, egal wie sich der Hase bewegt und egal welche Punkte das Ortungsgerät meldet, dass der Jäger seine Bewegungen so wählen kann, dass der Abstand zwischen ihm und dem Hasen nach 10^9 Runden höchstens 100 ist?

Lösung: Es gibt keine Taktik, die dem Jäger dies ermöglicht.

Würde es eine derartige Taktik geben, so hätte der Jäger eine Strategie, die "funktionieren" würde, unabhängig davon, wie sich der Hase bewegt und davon, wo sich die vom Ortungsgerät gemeldeten Punkte P_n befinden. Im Folgenden zeigen wir, dass das Gegenteil der Fall ist. Meldet das Ortungsgerät unter ganz bestimmten Umständen ganz bestimmte Punkte, gibt es vielmehr keine Taktik, die es dem Jäger ermöglicht, den Abstand nach 10^9 Runden sicher unter 100 zu halten.

Zu diesem Zweck bezeichne d_n den Abstand zwischen dem Jäger und dem Hasen nach n Runden. Gilt $d_n \geq 100$ für irgendein $n < 10^9$, so hat der Jäger sicher verloren, da sich der Hase ab diesem Zeitpunkt nur mehr in einer geraden Linie weg vom Jäger bewegen muss, um den Abstand zu halten.

Wir werden nun zeigen, dass es dem Hasen, unter der Voraussetzung, dass $d_n < 100$ gilt, unabhängig von der Taktik des Jägers möglich ist, das Quadrat d_n^2 des Abstands innerhalb von 200 Runden um mindestens $\frac{1}{2}$ zu erhöhen, sofern die gemeldeten Punkte P_n für den Hasen günstig sind. So erreicht der Wert von d_n^2 innerhalb von weniger als $2 \cdot 10^4 \cdot 200 = 4 \cdot 10^6 < 10^9$ Runden einen Wert von mindestens 10^4.



Nehmen wir an, der Jäger würde sich im Punkt B_n befinden, und der Hase im Punkt A_n. Wir können o.B.d.A. sogar annehmen, dass die Position des Hasen zu diesem Zeitpunkt dem Jäger bekannt ist, womit wir alle vorangegangenen Informationen vernachlässigen können. Es bezeichne r die Verbindungsgerade von A_n und B_n, und es seien Y_1 und Y_2 die Punkte, die von A_n die Entfernung 200 haben, und von r den Abstand 1, wie in der Abbildung zu sehen.

Der Hase wählt nun eine der beiden Punkte Y_1 und Y_2 und macht 200 Sprünge in Richtung dorthin. Da alle Sprünge im Abstand weniger als 1 von r bleiben, können alle der 200 dazu gemeldeten Punkte P_i auf der Gerade r liegen. Der Jäger hat dabei keine Möglichkeit zu entscheiden, ob sich der Hase in Richtung Y_1 oder in Richtung Y_2 bewegt.

Nun stellt sich in diesem Fall die Frage nach der optimalen Taktik des Jägers für die nächsten 200 Runden. Bewegt er sich jeweils um genau 1 nach rechts, endet er im Punkt H' der Abbildung auf

r. Er hat aber auch keine bessere Alternative zur Verfügung. Bei jeder anderen Vorgangsweise endet er nach 200 Runden sicher an einem Punkt links von H'. Hat ihn sein Weg oberhalb von r geführt, so ist es möglich, dass der Hase sich in Richtung Y_2 bewegt hat, und sein Abstand vom Hasen ist somit sicher größer als wäre er nach H' gegangen. Landet er unterhalb von r, so gilt dasselbe für seine Lage relativ zu Y_1. Egal welche Strategie der Jäger auch wählt, ist sein Abstand vom Hasen nach 200 Runden mindestens so groß wie der Abstand y von H' zu Y_1 bzw. zu Y_2.

Um nun y^2 abzuschätzen, sei Z der Mittelpunkt der Strecke Y_1Y_2. Bezeichnen wir den Punkt auf r, dessen Entfernung von A_n (also R_n in der Zeichnung) 200 beträgt mit R', so bezeichne ε den Abstand $|ZR'|$. Offensichtlich gilt $|A_nB_n| = |H'R'|$, und wir erhalten

$$y^2 = 1 + |H'Z|^2 = 1 + (d_n - \varepsilon)^2,$$

wobei

$$\varepsilon = 200 - |R_nZ| = 200 - \sqrt{200^2 - 1} = \frac{1}{200 + \sqrt{200^2 - 1}} > \frac{1}{400}$$

gilt. Wegen

$$\varepsilon^2 + 1 = 200^2 + (200^2 - 1) - 2 \cdot 200 \cdot \sqrt{200^2 - 1} + 1 = 400\varepsilon$$

gilt somit

$$y^2 = d_n^2 - 2\varepsilon d_n + \varepsilon^2 + 1 = d_n^2 + \varepsilon(400 - 2d_n).$$

Da wir nun gezeigt haben, dass $\varepsilon > \frac{1}{400}$ gilt, und wir die Annahme getroffen haben, dass auch $d_n < 100$ gilt, sehen wir, dass $y^2 > d_n^2 + \frac{1}{2}$ gelten muss.

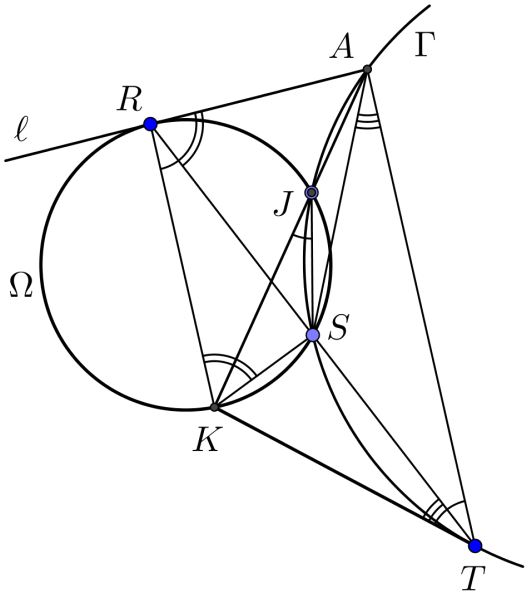
Wir sehen also, dass es tatsächlich der Fall ist, dass unter diesen Umständen $d_{n+200}^2 > d_n^2 + \frac{1}{2}$ gilt. Der Jäger kann also, wie behauptet, keine Taktik finden, die den Abstand unter der geforderten Schranke hält. □

Aufgabe 4: Es seien R und S verschiedene Punkte auf einem Kreis Ω, so dass RS kein Durchmesser ist. Es sei ℓ die Tangente an Ω in R. Der Punkt T liegt so, dass S der Mittelpunkt der Strecke RT ist. Ein Punkt J ist auf dem kleineren Bogen RS von Ω so gegeben, dass der Umkreis Γ des Dreiecks JST die Gerade ℓ in zwei verschiedenen Punkten schneidet. Es sei A derjenige gemeinsame Punkt von Γ und ℓ, der näher an R liegt. Die Gerade AJ schneidet Ω in einem weiteren Punkt K.

Man beweise, dass die Gerade KT den Kreis Γ berührt.

Lösung: Betrachten wir die beiden Kreise, gilt wegen des Peripheriewinkelsatzes in Ω und wegen des Sehnenvierecks $AJST$

$$\angle KRS = \angle KJS = 180^\circ - \angle AJS = \angle ATS.$$



Da RA eine Tangente von Ω ist, gilt auch aufgrund des Sehnen-Tangentenwinkelsatzes $\angle SKR = \angle SRA$. Die Dreiecke ART und SKR sind also ähnlich, und wegen $SR = ST$ gilt somit

$$\frac{TR}{RK} = \frac{AT}{SR} = \frac{AT}{ST}.$$

Nun gilt aber auch $\angle ATS = \angle KRT$, und somit sind auch die Dreiecke AST und TKR ähnlich, womit auch $\angle SAT = \angle RTK$ gilt.

Aus dem Sehnen-Tangentenwinkelsatz folgt somit, dass KT eine Tangente des Umkreises von SAT sein muss, was den Beweis abschließt. □

Aufgabe 5: Gegeben sei eine ganze Zahl $N \geqslant 2$. Eine Gruppe von $N(N+1)$ Fußballspielern, von denen keine zwei gleich groß sind, steht in einer Reihe. Pelé möchte $N(N-1)$ Spieler so aus dieser Reihe entfernen, dass eine neue Reihe von $2N$ Spielern verbleibt, in der die folgenden N Bedingungen gelten:

(1) Niemand steht zwischen den beiden größten Spielern.

(2) Niemand steht zwischen dem drittgrößten und dem viertgrößten Spieler.

⋮

(N) Niemand steht zwischen den beiden kleinsten Spielern.

Man zeige, dass dies immer möglich ist.

Lösung: Wir bezeichnen die Größen der Spieler (und die Spieler selbst) in der Reihenfolge ihres Erscheinens in der Reihe von links nach rechts mit $x_1, x_2, \ldots, x_{N(N+1)}$. OBdA können wir annehmen, dass $(x_1, x_2, \ldots, x_{N(N+1)})$ eine Permutation von $(1, 2, \ldots, N(N+1))$ ist.

Pelé teilt Leiberln in N Farben an die Spieler aus, wobei jeweils $N+1$ Spieler mit "angrenzender" Größe dieselbe Farbe erhalten. Mit anderen Worten, alle Spieler der Größe

$$k(N+1)+1, k(N+1)+2, \ldots, (k+1)(N+1)$$

erhalten jeweils ein Leiberl der Farbe k.

Nun betrachtet er die Leiberlfarben der Spieler einzeln in der Reihenfolge von links nach rechts, also in der Reihenfolge $x_1, x_2, \ldots$, bis eine Farbe zum zweiten Mal vorkommt. Seien die Spieler x_i und x_j (mit $i < j$) diejenigen, die als erstes Leiberl der gleichen Farbe tragen, und sei dies die Farbe c_1. Pelé eliminiert alle Spieler $x_1, x_2, \ldots, x_{j-1}$ außer x_i aus der Reihe, sowie alle Spieler mit Leiberln der Farbe c_1 außer dem Paar (x_i, x_j). Dabei werden höchstens $(N-1)+(N-1) = 2(N-1)$ Spieler eliminiert, und es verbleiben in der Reihe somit neben dem Paar (x_i, x_j) mindestens $(N-1)(N-2)$ Spieler mit Leiberln in $N-1$ Farben.

Dieses Verfahren kann nun induktiv für jede weitere Farbe analog fortgesetzt werden, wobei in jedem Schritt ein zusammenstehendes Paar neu entsteht, das jeweils Leiberln derselben Farbe trägt. Das bedeutet aber, dass sie in der Reihenfolge der verbleibenden Spieler in der Reihe ein Paar bilden, das auch der Größe nach zusammen gehört.

Mit diesem Verfahren ist es Pelé also gelungen, Spieler so zu entfernen, dass die Verbleibende Reihe die gewünschte Eigenschaft besitzt. □

Aufgabe 6: Ein geordnetes Paar (x, y) ganzer Zahlen heißt *teilerfremder Gitterpunkt*, wenn der größte gemeinsame Teiler von x und y eins ist. Für eine gegebene endliche Menge S teilerfremder Gitterpunkte beweise man, dass es eine positive ganze Zahl n und ganze Zahlen a_0, a_1, …, a_n gibt, so dass für alle (x, y) in S gilt:

$$a_0 x^n + a_1 x^{n-1} y + a_2 x^{n-2} y^2 + \cdots + a_{n-1} x y^{n-1} + a_n y^n = 1.$$

Lösung: Wir stellen vorbereitend fest, dass es genügt, die Existenz eines homogenen Polynoms $f(x, y)$ mit $f(x_i, y_i) = \pm 1$ für alle Indizes i nachzuweisen, weil dann sicher $f^2(x_i, y_i) = 1$ für alle Indizes i gilt.

Liegen zwei Punkte (x_i, y_i) und (x_j, y_j) auf derselben Verbindungsgeraden mit dem Ursprung, muss aufgrund der Teilerfremdheit sicher $(x_j, y_j) = (-x_i, -y_i)$ gelten. In diesem Fall gilt aber für jedes homogene Polynom f sicher $f(x_j, y_j) = \pm f(x_i, y_i)$, und wir dürfen somit oBdA annehmen, dass keine zwei der gegebenen Punkte auf einer gemeinsamen Verbindungsgeraden mit dem Ursprung liegen, da wir die Gültigkeit der Beziehung schlimmstenfalls durch nachträgliches Quadrieren für etwaige zunächst ignorierte Punkte garantieren können.

Wir nehmen also im Weiteren an, dass dies für keine zwei Punkte gilt, und konstruieren induktiv ein homogenes Polynom mit $f(x_i, y_i) = 1$ für alle $1 \leq i \leq n$.

Für $n = 1$ gibt es, da x_1 und y_1 relativ prim sind, sicher ganze Zahlen c und d, sodass $cx_1 + dy_1 = 1$ gilt. Das Polynom $f(x, y) = cx + dy$ erfüllt also die geforderte Bedingung.

Nun sein $n \geq 2$. Aufgrund der Induktionshypothese dürfen wir annehmen, dass es ein homogenes Polynom $g(x, y)$ mit

$$g(x_1, y_1) = \ldots = g(x_{n-1}, y_{n-1}) = 1$$

gibt. Wir definieren $j := \deg g$,

$$g_n(x, y) := \prod_{k=1}^{n-1} (y_k x - x_k y)$$

und $a_n := g_n(x_n, y_n)$. Aufgrund der Voraussetzungen gilt sicher $a_n \neq 0$. Wir können sicher ganze Zahlen c und d wählen mit $cx_n + dy_n = 1$, und wir wollen nun ein Polynom der geforderten Art der Gestalt

$$f(x, y) = g(x, y)^K - C \cdot g_n(x, y) \cdot (cx + dy)^L$$

konstruieren, wobei K und L positive ganze Zahlen sein sollen und C eine ganze Zahl. Dabei können wir annehmen, dass $L = Kj - n + 1$ gilt, damit f sicher homogen ist.

Wegen $g(x_1, y_1) = \ldots = g(x_{n-1}, y_{n-1}) = 1$ und $g_n(x_1, y_1) = \ldots = g_n(x_{n-1}, y_{n-1}) = 0$, gilt $f(x_1, y_1) = \ldots = f(x_{n-1}, y_{n-1}) = 1$ automatisch für jede beliebige Wahl der Konstanten K, L und C.

Weiters gilt

$$\begin{aligned} f(x_n, y_n) &= g(x_n, y_n)^K - C \cdot g_n(x_n, y_n) \cdot (cx_n + dy_n)^L \\ &= g(x_n, y_n)^K - C \cdot a_n. \end{aligned}$$

Haben wir also einen Exponenten K mit $g(x_n, y_n)^K \equiv 1 \pmod{a_n}$, ist es sicher möglich, ein geeignetes C zu finden mit $f(x_n, y_n) = 1$. Wir müssen also als Nächstes zeigen, wie ein derartiges K gefunden werden kann.

Zu diesem Zweck sei p ein beliebiger Primteiler von a_n. Wegen

$$p \mid a_n = g_n(x_n, y_n) = \prod_{k=1}^{n-1} (y_k x_n - x_k y_n)$$

existiert sicher ein Index $1 \leq k < n$ mit $x_k y_n \equiv x_n y_k \pmod{p}$. Nun können wir zeigen, dass $x_k x_n$ oder $y_k y_n$ nicht durch p teilbar ist. Im Fall $x_k y_n \equiv x_n y_k \equiv 0 \pmod{p}$ ist dies trivial. Andernfalls gilt jedenfalls $x_k y_n \equiv x_n y_k \equiv 0 \pmod{p}$. Gilt $p \mid x_k$, so folgt sicher $p \nmid y_k$, da (x_k, y_k) teilerfremd ist. Somit gilt sicher $p \mid x_n$, und somit $p \nmid y_n$, da auch (x_n, y_n) teilerfremd ist. Aus $p \mid x_k$ folgt also $p \nmid y_k y_n$, und analog folgt aus $p \mid y_n$ auch $p \nmid x_k x_n$.

Da g homogen mit Grad j ist, gilt somit

$$x_k^j \cdot g(x_n, y_n) = g(x_k x_n, x_k y_n) \equiv g(x_k x_n, y_k x_n) = x_n^j \cdot g(x_k, y_k) = x_n^j \pmod{p} \tag{1}$$

und

$$y_k^j \cdot g(x_n, y_n) = g(y_k x_n, y_k y_n) \equiv g(x_k y_n, y_k y_n) = y_n^j \cdot g(x_k, y_k) = y_n^j \pmod{p}. \tag{2}$$

Gilt nun $p \nmid x_k x_n$, so betrachten wir die $(p-1)$-te Potenz von (1), und andernfalls die $(p-1)$-te Potenz von (2), und erhalten nach dem kleinen Satz von Fermat

$$g(x_n, y_n)^{p-1} \equiv 1 \pmod{p}.$$

Für $p^\alpha \mid m$ erhalten wir also

$$g(x_n, y_n)^{p^{\alpha-1}(p-1)} \equiv 1 \pmod{p^\alpha},$$

womit wir sehen, dass der Exponent $K = n \cdot \varphi(a_n)$, der sicher ein Vielfaches aller Werte der Form $p^{\alpha-1}(p-1)$ ist, eine geeignete Wahl darstellt. (Der Faktor n stellt sicher, dass $K \geq n$, und somit $L > 0$, sicher gilt.) $\square$