
Inseln der Ordnung unter den Primzahlen – Primzahlserien in Polynomen

Albrecht Schultz

Albrecht Schultz, Jahrgang 1946, unterrichtet an einem rheinland-pfälzischen Gymnasium Mathematik und Physik. Da er auch eine Arbeitsgruppe Astronomie und einen Mathematikzirkel leitet, beschäftigt er sich oft mit Fragen, die am Rand des Unterrichtpensums liegen. Problemstellungen und Lösungen, wie sie hier in seinem Beitrag zur Sprache kommen, fallen ihm auf langen Spaziergängen im Pfälzerwald ein; während der Ferien kann das auch auf Bergwanderungen in den Alpen eintreten, vorzugsweise im Engadin und im Wallis.

Überblick

Es geht hier um Primzahlen in den Wertemengen von Polynomen zweiten Grades, vornehmlich um Primzahlserien. Zuerst werden die Polynome herausgestellt, die von ihrem Aufbau her zusammenhängende Primzahlserien liefern können; dabei werden Polynome mit identischen Wertemengen jeweils auf "Grundpolynome" reduziert. Ein zahlentheoretischer Zusammenhang zwischen den Diskriminanten und den Primteilern von Polynomgliedern liefert den Schlüssel für eine gezielte Suche nach primzahlreichen Polynomen; eine Auswahl der mit entsprechenden Suchprogrammen erhaltenen Ergebnisse wird vorgestellt und diskutiert. Schließlich wird ein graphisches Suchverfahren präsentiert: Knickt man den Strahl der natürlichen Zahlen zu einer Vieleckspirale und hebt darin die Glieder eines gegebenen Polynoms unter zusätzlicher Kennzeichnung der Primzahlen hervor, so werden die in den quadratischen Polynomen versteckten bruchstückhaften Ordnungen

Die Mathematik kennt über die Verteilung der Primzahlen heute eine grosse Anzahl von tiefliegenden Sätzen statistischer und asymptotischer Natur. Trotzdem aber birgt das Gebiet noch viele Rätsel, und die Verteilung von Primzahlen erscheint uns im Grunde immer noch als "ungeordnet" und "gesetzlos". Umso überraschender sind Aussagen, die geordnete Teilbereiche aufzeigen; ein Beispiel einer solchen Aussage liefert das Polynom $n^2 + n + 41$: Man weiss seit Euler, dass seine Werte für $n = 0, 1, \dots, 39$ eine ununterbrochene Serie von Primzahlen bilden. Albrecht Schultz geht der Frage nach weiteren derartigen quadratischen Polynomen nach, die "Inseln der Ordnung unter den Primzahlen" beschreiben. Es ergeben sich überraschende Bezüge zur Zahlentheorie; reizvolle graphische Interpretationen der Resultate runden den Beitrag ab. *ust*

geometrisch sichtbar, und zwar als mehr oder weniger lange Zweige, die aus dem Zentrum sprießen und sich oft noch um das Zentrum winden. Damit lassen sich auch schöne Regelmäßigkeiten in *unterbrochenen* Primzahlserien herausstellen.

An einigen Stellen des vorliegenden Textes wird auf die verwendeten Rechen- und Grafikprogramme hingewiesen. Diese sind in QBASIC geschrieben und können gegen einen Unkostenbeitrag vom Autor bezogen werden.

1 Das Eulersche Polynom

Bekanntlich gibt es kein Polynom $f(n) = a_k n^k + a_{k-1} n^{k-1} + \dots + a_1 n + a_0$ mit ganzzahligen Koeffizienten a_i und $k \geq 1$, das für alle ganzen oder erst für alle hinreichend großen ganzen Zahlen Primzahlwerte liefert. Man weiß auch nicht, ob irgendein Polynom von höherem Grad als 1 unendlich viele Primzahlwerte annimmt. Es gibt aber solche, deren Wertemenge überraschend dicht von Primzahlen besetzt ist, und es gibt eine Vielzahl von Polynomen, die lange ununterbrochene Primzahlserien liefern. Das bekannteste ist das "Eulersche Polynom" $n^2 + n + 41$, es liefert von $n = 0$ bis $n = 39$ eine Serie von vierzig verschiedenen Primzahlen. Leonhard Euler erwähnte es 1772 in einem Brief an Joh. Bernoulli. Zusammen mit dem Eulerschen wird oft das Polynom $2n^2 + 29$ erwähnt; dieses bringt es von $n = 0$ bis 28 zu einer ebenfalls stattlichen Serie, und offensichtlich hat diese ein Spiegelbild von $n = 0$ bis $n = -28$. Die Serie des Eulerschen Polynoms ist aber auch doppelt: Der Scheitel der Parabel $y = x^2 + x + 41$ hat die x -Koordinate $x_S = -\frac{1}{2}$, und die Achsensymmetrie der Parabel drückt sich in der Gleichung $f(x) = f(-x-1)$ aus. Folglich sind die Werte von $n^2 + n + 41$ für die *achtzig aufeinanderfolgenden ganzen Zahlen* $n = -40, -39, \dots, 38, 39$ Primzahlen. Dieselbe Symmetrie liegt bei allen Polynomen der Form $f(n) = an^2 + an + c$ vor: Hier gilt immer $f(n) = f(-n-1)$, alle Parabeln mit der Gleichung $y = ax^2 + ax + c$ sind zur Achse $x = -0.5$ symmetrisch.

Es lohnt sich, das Phänomen der Primzahlserien von einer höheren Warte aus zu betrachten, dann ergeben sich Informationen und Anstöße für die Suche nach neuen Serien. Zunächst soll gezeigt werden, daß zwischen der Diskriminante eines quadratischen Polynoms und den Primteilern von Polynomgliedern ein direkter Zusammenhang besteht: p_0 sei eine Primzahl, und die Diskriminante $D = b^2 - 4ac$ des Polynoms $an^2 + bn + c$ sei quadratischer Nichtrest modulo p_0 . Dann gibt es kein x mit $D \equiv x^2 \pmod{p_0}$, insbesondere gilt auch nicht $D \equiv (2an + b)^2 \pmod{p_0}$ mit irgendeinem ganzen n . Man hat also

$$\begin{aligned} (2an + b)^2 - D &\not\equiv 0 \pmod{p_0} \\ 4a^2 n^2 + 4abn + 4ac &\not\equiv 0 \pmod{p_0} \\ an^2 + bn + c &\not\equiv 0 \pmod{p_0} \quad , \end{aligned}$$

d.h. p_0 ist von keinem Polynomglied $an^2 + bn + c$ ein Teiler. Die besonders eindrucksvolle Serie im Eulerschen Polynom ist dem Umstand zu verdanken, daß alle Polynomglieder ungerade sind und *die Diskriminante* $1 - 4 \cdot 41 = -163$ *quadratischer Nichtrest modulo jeder ungeraden Primzahl unter 41 ist*: dann können in keinem Polynomglied Primteiler stecken, die kleiner als 41 sind; demnach wäre $41 \cdot 41$ ab $n = 0$ die erste mögliche Zerlegung eines Polynomgliedes, das ist aber gerade $f(40)$, und die vierzig voneinander

verschiedenen Vorgänger $f(0), f(1), \dots, f(39)$ müssen prim sein; die nächstmögliche Zerlegung eines Polynomgliedes ist $41 \cdot 43$, und das ist schon $f(41)$. Bei größeren n entfallen für die Polynomglieder beträchtliche Möglichkeiten zusammengesetzt zu sein, deshalb darf man annehmen, daß das Eulersche Polynom allgemein zahlreiche Primzahlwerte hat. In der Tat liefert es von $n = 0$ bis 1000 582 Primzahlen; darunter gibt es außer der bekannten Serie noch etliche kleinere.

In den Polynomen $f_q(n) = n^2 + n + q$ können mit $n = 0$ beginnende Primzahlserien höchstens bis $n = q-2$ reichen, denn für $n = q-1$ ergibt sich der Wert q^2 . Der "Freiraum" von $n = -(q-1)$ bis $q-2$ wird in der großen Serie des Eulerschen Polynoms voll ausgeschöpft, aber darin steht es nicht allein: Auch in den Polynomen mit $q = 17, 11, 5, 3, 2$ sind die Diskriminanten $-67, -43, -19, -11, -7$ quadratische Nichtreste modulo jeder ungeraden Primzahl unter q (soweit diese existieren), und es gibt dort von $n = 0$ bis $q-2$ jeweils 16, 10, 4, 2, 1 aufeinanderfolgende Primzahlen. Nebenbei sei bemerkt, daß die Quadrate, die jeweils die Serienenden markieren, die einzigen in den Wertefolgen dieser Polynome sind; denn für $n > q$ gilt $f_q(n-1) < n^2 < f_q(n)$, die Quadratzahlen liegen also immer *zwischen* aufeinanderfolgenden Polynomgliedern.

Nun sei aber davor gewarnt, nach einem "stärkeren" q als im Eulerschen Polynom zu suchen; der folgende Satz zerstört in dieser Hinsicht alle Illusionen:

$q = 41$ ist die größte Zahl, die in einem Polynom $n^2 + n + q$ eine Primzahlserie von $n = 0$ bis $n = q - 2$ hervorruft.

Der Weg zu dieser Erkenntnis war weit; so einfach sich das Phänomen der Primzahlserien in den Polynomen $n^2 + n + q$ auch darstellen mag – es steht in enger Verbindung mit dem sehr schwierigen "Klassenzahlproblem", das C. F. Gauß in den "Disquisitiones Arithmeticae" 1801 aufgeworfen hatte, und für das er die Antwort nur vermuten konnte. Dabei geht es um die Frage, für welche negative ganze Zahlen d die imaginär-quadratischen Körper $\mathcal{Q}(\sqrt{d})$ die Klassenzahl 1 haben. Anders formuliert: Für welche negative ganze d ist in den Zahlensystemen $\{a + b \cdot \sqrt{d}\}$ mit rationalen Koeffizienten a und b die Primfaktorzerlegung eindeutig? Die vollständige Lösung des Klassenzahlproblems bedurfte einer langen Entwicklung, die bis in die zweite Hälfte unseres Jahrhunderts hineinreichte. Heute steht fest: Außer mit $d = -1, -2$ und -3 ergibt sich die Klassenzahl 1 nur noch mit den Zahlen $-7, -11, -19, -43, -67, -163$, und das sind gerade die Diskriminanten des Eulerschen Polynoms und seiner Verwandten. Damit ist auch erwiesen, daß kein Polynom $n^2 + n + q$ das Eulersche übertrumpfen kann, denn die Primzahlserie von $n = 0$ bis $q-2$ und die Klassenzahl 1 des imaginär-quadratischen Körpers $\mathcal{Q}(\sqrt{1-4q})$ bedingen sich gegenseitig (Kap. 3 in [2], Kap. 3 in [4], Kap. 3 in [5], detailliert in [3]).

2 Grundpolynome – Definition und Formeln

2.1 Welche Polynome können zusammenhängende Primzahlserien liefern?

Die Suche nach anderen "Erfolgspolynomen" mit langen Primzahlserien darf nicht blindlings erfolgen. Man sieht schnell ein, daß ein Polynom $an^2 + bn + c$ nur dann zusammenhängende Primzahlserien liefern kann, wenn a und b entweder beide gerade oder beide ungerade sind, und wenn c ungerade ist; andernfalls wären die Polynomglieder entweder immer gerade oder abwechselnd gerade und ungerade.

$f(n) = an^2 + bn + c$ kann also nur dann Primzahlserien liefern, wenn $a + b$ gerade und c ungerade ist; außerdem dürfen a, b, c keine gemeinsamen Teiler haben, und das Polynom darf nicht in Linearfaktoren $\alpha n + \beta$ und $\gamma n + \delta$ zerfallen ($\alpha, \beta, \gamma, \delta$ ganzzahlig).

Ich beschränke mich zunächst auf Polynome mit positiven Koeffizienten a .

2.2 Klassen äquivalenter Polynome

Es muß auch bedacht werden, daß verschiedene Polynome dieselbe Wertemenge haben können. Ausgehend von einem gegebenen Polynom zweiten Grades erhält man "äquivalente" Polynome, indem man dessen Parabel um ganze Beträge parallel zur x -Achse verschiebt und die neuen Gleichungen aufstellt.

Eine kleine Rechnung führt zu den allgemeinen Translationsformeln:

$a_0 n^2 + b_0 n + c_0$ liefere Primzahlen von $n = n_A$ bis $n = n_E$. In einem neuen Polynom $a_k n^2 + b_k n + c_k$ soll dieselbe Serie von $n_A - k$ bis $n_E - k$ vorkommen:

$$\begin{aligned} a_0 n^2 + b_0 n + c_0 &= a_k (n - k)^2 + b_k (n - k) + c_k \\ &= a_k n^2 + (b_k - 2a_k k) n + (a_k k^2 - b_k k + c_k) \quad . \end{aligned}$$

Durch Koeffizientenvergleich erhält man

$$\begin{aligned} a_k &= a_0 \\ b_k &= 2a_0 k + b_0 \\ c_k &= a_0 k^2 + b_0 k + c_0 \quad . \end{aligned} \tag{1}$$

Dabei ist $|k|$ die Länge des Verschiebungspfeiles.

Anwendungsbeispiele:

- $8n^2 + 2n + 61$ liefert von $n = -9$ bis $n = 5$ nur Primzahlen; $a_0 = 8, b_0 = 2, c_0 = 61$.
- **k=1:** $8n^2 + 18n + 71$ liefert dieselben Primzahlen von $n = -10$ bis $n = 4$,
- **k=-2:** $8n^2 - 30n + 89$ liefert dieselben Primzahlen von $n = -7$ bis $n = 7$.

Die Parabel mit der Gleichung $f(x) = ax^2 + bx + c$ hat ihren Scheitel an der Stelle $x_S = -b/2a$. Die Translationsformeln (1) ermöglichen es, sich auf solche Parabeln zu beschränken, deren erste Scheitelkoordinate x_S im Intervall von -1 bis 0 liegt, die Parabeln anderer äquivalenter Polynome lassen sich wie beschrieben auf diese abbilden. Es soll also gelten

$$-1 < -\frac{b}{2a} \leq 0 \quad \text{oder} \quad 0 \leq b < 2a \quad . \tag{2}$$

Die Variationsbreite der Koeffizienten b kann noch weiter eingeschränkt werden, denn die Wertefolgen von Polynomen bleiben nicht nur bezüglich der Translationen invariant: Eine Parabel $f(x) = ax^2 + bx + c$, deren Scheitelstelle etwa in der linken Hälfte des Intervalls $] -1; 0]$ liegt, kann an der Achse $x = -\frac{1}{2}$ in die andere Intervallhälfte hinübergespiegelt werden; dabei verwandeln sich die Werte auf dem linken Parabelast zu denen des rechten Astes der Bildparabel und umgekehrt. Die Gleichung des zu $f(n)$ äquivalenten Polynoms lautet $f^*(n) = f(-n-1) = an^2 + (2a-b)n + (a-b+c)$. Das Grundintervall (2) für die x -Koordinaten der Parabelscheitel muß also halbiert werden:

$$-\frac{1}{2} \leq -\frac{b}{2a} \leq 0 \quad \text{oder} \quad 0 \leq b \leq a \quad .$$

Zusammengefaßt: Unter den Polynomen $an^2 + bn + c$ mit $a \in \mathbb{N}$, $b \in \{0, 1, \dots, a\}$, $c \in \mathbb{Z}$ befinden sich keine Paare mit identischen Wertefolgen. Sie seien deshalb mit dem Prädikat "Grundpolynome" versehen. Jedes dieser Polynome ist Repräsentant einer Klasse äquivalenter Polynome. Andere Elemente einer solchen Polynomklasse erhält man über die Translationsformeln (1) oder die erwähnte Spiegelung.

Wie in 2.1 bemerkt können nur solche Polynome $an^2 + bn + c$ Primzahlserien liefern, deren Koeffizienten a und b entweder beide gerade oder beide ungerade sind. Für die Untersuchung auf Primzahlserien kommen deshalb nur die folgenden "Blöcke" von Grundpolynomen in Betracht:

$$\begin{array}{cccccc} n^2 + n + c & 2n^2 + c & 3n^2 + n + c & 4n^2 + c & 5n^2 + n + c & \\ & 2n^2 + 2n + c & 3n^2 + 3n + c & 4n^2 + 2n + c & 5n^2 + 3n + c & \\ & & & 4n^2 + 4n + c & 5n^2 + 5n + c & \dots \end{array}$$

Dabei ist c immer eine ungerade positive oder negative Zahl.

Es muß betont werden, daß die Polynome einer bestimmten Klasse dieselben Werte in einer feststehenden Reihenfolge (vor- oder rückwärts) annehmen. Wären beliebige Reihenfolgen zugelassen, so gäbe es Überschneidungen. Im folgenden wird das erläutert:

In Abschnitt 1 wurde schon die Symmetrie im Polynom $f(n) = an^2 + an + c$ erwähnt, dort gilt $f(n) = f(-n-1)$, also auch $f(2n) = f(-2n-1)$, $n \in \mathbb{Z}$. Das heißt aber: Wenn man in einem solchen Polynom nur die geraden Nummern (positive wie negative n) herausgreift, so hat man auch die Werte der ungeraden Nummern (negative wie positive n) erfaßt. Wir ersetzen also im Polynom $an^2 + an + c$ die Variable n durch $2n$ und erhalten das Polynom $4an^2 + 2an + c$ mit derselben Wertemenge.

Man vergleiche etwa die Primzahlserien, die von den Polynomen $n^2 + n + 11$ und $4n^2 + 2n + 11$ (n durch $2n$ oder $-2n-1$ ersetzt) geliefert werden (Tab. 1):

n	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7	8	9
$n^2 + n + 11$	41	31	23	17	13	11	11	13	17	23	31	41	53	67	83	101
$4n^2 + 2n + 11$.	101	67	41	23	13	11	17	31	53	83

Tabelle 1 Grundpolynome mit gleichen Wertemengen

Dieselben Primzahlen, die im ersten Polynom vorkommen, tauchen auch im zweiten auf, nur sind sie dort anders verteilt und erscheinen nicht mehr doppelt; das neue Polynom hat die gleiche Wertemenge und liefert die eine Hälfte der ursprünglichen Primzahlserie für negative, die andere für positive n einschließlich 0.

Bei der Suche nach Primzahlserien ist also zu berücksichtigen, daß die Polynome $an^2 + an + c$ und $4an^2 + 2an + c$ ($a \in \mathbb{N}$, $c \in \mathbb{Z}$) bis auf die Reihenfolge gleiche Werte haben.

Im Polynom $4n^2 + 2n + 41$, dem verwandelten Eulerschen, erstreckt sich von $n = -20$ bis $n = 19$ die große Primzahlserie neu geordnet wieder.

3 Untersuchung von quadratischen Grundpolynomen auf Primzahlserien

Im folgenden werden nur solche Polynome auf zusammenhängende Primzahlserien untersucht, deren Diskriminanten quadratische Nichtreste bezüglich einer Reihe möglichst vieler kleiner Primzahlen sind, erst dann ist die Suche aussichtsreich. Der Zusammenhang sei noch einmal dargestellt:

Es gebe eine Primzahl p_0 , so daß die Diskriminante $D = b^2 - 4ac$ des Grundpolynoms $an^2 + bn + c$ quadratischer Nichtrest modulo p für alle ungeraden Primzahlen $p < p_0$ ist. Nach Abschnitt 1 ist dann p_0 der kleinste mögliche Primteiler für alle Polynomglieder. Solche, die kleiner als p_0^2 sind, *müssen* prim sein, die Länge einer möglichen Serie hängt von diesem p_0 ab. Ob eine Diskriminante quadratischer Nichtrest modulo einer gegebenen Primzahl ist, wird durch Berechnung des Jacobi-Symbols, einer Verallgemeinerung des Legendre-Symbols entschieden (z.B. [1], S. 210); der entsprechende Algorithmus beruht auf dem quadratischen Reziprozitätsgesetz und den zugehörigen Ergänzungssätzen (Programm "JACOBI").

Beispiel: Für das Polynom $16n^2 + 2n + 89$ ist die Diskriminante -5692 quadratischer Nichtrest modulo jeder ungeraden Primzahl unterhalb 23; kleinere Primteiler als 23 kann es demnach nicht geben. Für $n = 9$ ergibt sich die erste zusammengesetzte Zahl (1403) mit den Komponenten 23 und 61. Nach unten ist die Serie durch $f(-12)$ begrenzt, $f(-12) = 2369 = 23 \cdot 103$ ist "lokal" die letzte zusammengesetzte Zahl (siehe Tab. 2).

Bei positivem c bleiben die Polynomglieder nur in der Umgebung von $n = 0$ so klein, daß sich das Fehlen der ersten Primteiler günstig auswirken kann; sind die Koeffizienten a , b , c klein, so begünstigt schon das Fehlen weniger kleiner Primteiler beträchtliche Serien. c sollte übrigens prim sein, sonst ergeben die Einsetzungen der Null und der Teiler von c von vornherein keine Primzahlen.

Im einzelnen läuft der Suchprozeß folgendermaßen ab: Ein geeignetes Programm ("NIREDISK") gibt Diskriminanten aus, die quadratische Nichtreste bezüglich aller (oder fast aller) Primzahlen von 3 bis zu einer gewählten Mindestgrenze sind, und ein zweites ("DISKRIMI") ermittelt zugehörige Grundpolynome. Ob diese Polynome den Erwartungen entsprechen, wird mit einem letzten Programm ("P-SERIE") getestet: Wenn in einer Umgebung von $n = 0$ eine zusammenhängende Serie mit einem festgelegten Mindestumfang entsteht, wird diese Serie nach dem Abreißen ausgegeben.

Diskr. D	quadr. Nichtrest mod p, p von	Polynom $f(n)$	erstes und letztes Glied der Serie	Anz. der Serien- mitglieder
-163	3 bis 37	$n^2 + n + 41$	$f(0) = 41, \dots, f(39) = 1601$	40
-163		$179n^2 + 175n + 43$	$f(-13) = 28019, \dots, f(8) = 12899$	22
-163		$199n^2 + 193n + 47$	$f(-8) = 11239, \dots, f(9) = 17903$	18
-148	3 bis 17	$2n^2 + 2n + 19$	$f(0) = 19, \dots, f(17) = 631$	18
-232	3 bis 23	$2n^2 + 0n + 29$	$f(0) = 29, \dots, f(28) = 1597$	29
-267	5 bis 19	$3n^2 + 3n + 23$	$f(0) = 23, \dots, f(21) = 1409$	22
-403	3 bis 29 außer 11, 13	$11n^2 + 9n + 11$	$f(-10) = 1021, \dots, f(10) = 1201$	21
-708	5 bis 53 außer 31, 43	$6n^2 + 6n + 31$	$f(0) = 31, \dots, f(28) = 4903$	29
-760	3 bis 41 außer 5, 19, 29	$10n^2 + 0n + 19$	$f(0) = 19, \dots, f(18) = 3259$	19
-2608	3 bis 37	$4n^2 + 0n + 163$	$f(0) = 163, \dots, f(19) = 1607$	20
-2608		$16n^2 + 4n + 41$	$f(-21) = 7013, \dots, f(9) = 1373$	31
-2608		$16n^2 + 12n + 43$	$f(-20) = 6203, \dots, f(9) = 1447$	30
-5692	3 bis 43 außer 23	$16n^2 + 2n + 89$	$f(-11) = 2003, \dots, f(8) = 1129$	20
-5692		$32n^2 + 18n + 47$	$f(-10) = 3067, \dots, f(9) = 2801$	20
-5692		$64n^2 + 14n + 23$	$f(-9) = 5081, \dots, f(10) = 6563$	20
-6372	5 bis 41 außer 31	$54n^2 + 18n + 31$	$f(-9) = 4243, \dots, f(9) = 4567$	19
-6372		$18n^2 + 6n + 89$	$f(-9) = 1493, \dots, f(19) = 6701$	29
-10432	3 bis 37	$4n^2 + 4n + 653$	$f(0) = 653, \dots, f(17) = 1877$	18
-10432		$64n^2 + 40n + 47$	$f(-13) = 10343, \dots, f(9) = 5591$	23
-22768	3 bis 43 außer 23	$32n^2 + 12n + 179$	$f(-13) = 5431, \dots, f(5) = 1039$	19
-77683	3 bis 43	$47n^2 + 33n + 419$	$f(-6) = 1913, \dots, f(12) = 7583$	19
-77683		$59n^2 + 43n + 337$	$f(-10) = 5807, \dots, f(9) = 5503$	20
-77683		$67n^2 + 29n + 293$	$f(-8) = 4349, \dots, f(12) = 10289$	21
-77683		$101n^2 + 17n + 193$	$f(-9) = 8221, \dots, f(11) = 12601$	21
-111763	3 bis 43	$83n^2 + 11n + 337$	$f(-7) = 4327, \dots, f(12) = 12421$	20
-121972	3 bis 61	$134n^2 + 54n + 233$	$f(-10) = 13093, \dots, f(8) = 9241$	19
-121972		$142n^2 + 90n + 229$	$f(-6) = 4801, \dots, f(12) = 21757$	19
-121972		$202n^2 + 6n + 151$	$f(-5) = 5171, \dots, f(15) = 45691$	21
-189352	3 bis 47	$274n^2 + 16n + 173$	$f(-4) = 4493, \dots, f(14) = 54101$	19
-245848	3 bis 43	$166n^2 + 92n + 383$	$f(-11) = 19457, \dots, f(13) = 29633$	25
-245848		$398n^2 + 64n + 157$	$f(-5) = 9787, \dots, f(12) = 58237$	18
-289963	3 bis 43	$71n^2 + n + 1021$	$f(-11) = 9601, \dots, f(9) = 6781$	21
-332872	3 bis 59	$226n^2 + 192n + 409$	$f(-14) = 42017, \dots, f(6) = 9697$	21
-424708	3 bis 71	$146n^2 + 58n + 733$	$f(-12) = 21061, \dots, f(7) = 8293$	20
-424708		$166n^2 + 70n + 647$	$f(-11) = 19963, \dots, f(6) = 7043$	18
-447052	3 bis 43	$188n^2 + 70n + 601$	$f(-10) = 18701, \dots, f(7) = 10303$	18
-539092	3 bis 73 außer 53	$106n^2 + 70n + 1283$	$f(-9) = 9293, \dots, f(15) = 26183$	25
-539092		$158n^2 + 2n + 853$	$f(-16) = 41269, \dots, f(7) = 8609$	24
-604948	3 bis 43	$134n^2 + 14n + 1129$	$f(-6) = 5869, \dots, f(13) = 23957$	20
-1154008	3 bis 61	$146n^2 + 80n + 1987$	$f(-17) = 42821, \dots, f(6) = 7723$	24
-1154008		$194n^2 + 96n + 1499$	$f(-9) = 16349, \dots, f(11) = 26029$	21
-1154008		$206n^2 + 204n + 1451$	$f(-6) = 7643, \dots, f(14) = 44683$	21
-1154008		$226n^2 + 20n + 1277$	$f(-12) = 33581, \dots, f(12) = 34061$	25
-1698832	3 bis 71	$292n^2 + 176n + 1481$	$f(-7) = 14557, \dots, f(13) = 53117$	21
-2404147	3 bis 59	$97n^2 + 17n + 6197$	$f(-17) = 33941, \dots, f(15) = 28277$	33
-2404147		$103n^2 + 39n + 5839$	$f(-2) = 6173, \dots, f(17) = 36269$	20
	63683 bis 83 außer 37, 43, 71	$8n^2 - 199$	$f(28) = 6073, \dots, f(46) = 16729$	19
	6368	$8n^2 + 8n - 197$	$f(5) = 43, \dots, f(30) = 7243$	26
	254723 bis 83 außer 37, 43, 71	$32n^2 - 199$	$f(9) = 2393, \dots, f(26) = 21433$	18
	259668	$36n^2 + 18n - 1801$	$f(-33) = 36809, \dots, f(-8) = 359$	26
1398053	3 bis 79 außer 59	$103n^2 + 31n - 3391$	$f(-23) = 50383, \dots, f(-6) = 131$	18
1398053		$137n^2 + 67n - 2543$	$f(5) = 1217, \dots, f(24) = 77977$	20
1398053		$-59n^2 - 15n + 5923$	$f(-10) = 173, \dots, f(9) = 1009$	20
2004917	3 bis 61	$67n^2 + 3n - 7481$	$f(11) = 659, \dots, f(29) = 48953$	19
4174568	3 bis 73 außer 47	$-94n^2 - 60n + 11093$	$f(-11) = 379, \dots, f(10) = 1093$	22

Tabelle 2 Polynome mit Primzahlserien

5. Die Diskriminanten $b^2 - 4ac$ sind einer Vorzeichenänderung in a und c zugleich "resistent". Damit öffnet sich die Sicht auf bisher ausgegrenzte Polynome der Form $-an^2 - bn + c$ ($a, b, c \in \mathbb{N}$, $0 \leq b \leq a$); auch diese sind Grundpolynome im Sinn von 2.2, die zugehörigen Parabeln sind "umgestülpt" und die x -Koordinaten ihrer Scheitel liegen im Intervall $[-\frac{1}{2}, 0]$. Die positiven Glieder treten also in der Umgebung von $n = 0$ auf und haben vergleichsweise kleine Beträge. Aber sie können nicht besonders zahlreich werden und man erhält selten lange Primzahlserien. Zwei Polynome der geringen Ausbeute sind am Tabellenende aufgeführt. Sie sind insofern bemerkenswert, als ihre Serien von maximaler Länge sind; *alle* positiven Polynomglieder sind prim.

4 Primzahlreiche Polynome

Mit einem geeigneten Programm ("MULTIPRI") werden die Primzahlen gezählt, die ein gewähltes Polynom innerhalb vorgegebener Grenzen für n liefert. Das Zählintervall umfaßt jeweils 1000 Zahlen und beginnt mit $n = 0$ bzw. dort, wo der erste Wert positiv ist. (Für $n = 0$ nehmen Grundpolynome ihren tiefsten Wert an, und keine Primzahl soll doppelt gezählt werden.) Damit ist es möglich, Vergleiche über den Primzahlreichtum verschiedener Polynome anzustellen. Beispiele findet man in Tabelle 3.

Diskr. D	quadr. Nichtrest mod p, p von	Polynom	Zähl- Intervall	Anz. der Primz. im Zählintervall
-539092	3 bis 73 außer 53	$2n^2 + 2n + 67387$	0 bis 1000	635
-424708	3 bis 71	$2n^2 + 2n + 53089$	0 bis 1000	634
-1154008	3 bis 61	$2n^2 + 144251$	0 bis 1000	631
-289963	3 bis 43	$n^2 + n + 72491$	0 bis 1000	611
1398053	3 bis 79 außer 59	$n^2 + n - 349513$	591 bis 1591	611
2004917	3 bis 61	$n^2 + n - 501229$	708 bis 1708	606
-332872	3 bis 59	$2n^2 + 41609$	0 bis 1000	602
-447052	3 bis 43	$n^2 + n + 27941$	0 bis 1000	600
-2156368	3 bis 73 außer 53	$4n^2 + 134773$	0 bis 1000	595
-1698832	3 bis 71	$4n^2 + 106177$	0 bis 1000	595
1592	3 bis 67 außer 37, 43	$2n^2 - 199$	11 bis 1011	592
-1391812	3 bis 53	$2n^2 + 2n + 173977$	0 bis 1000	592
-189352	3 bis 47	$2n^2 + 23669$	0 bis 1000	585
3285992	3 bis 97 außer 59	$2n^2 - 410749$	454 bis 1454	584
-163	3 bis 37	$n^2 + n + 41$	0 bis 1000	582
-121972	3 bis 61	$2n^2 + 2n + 15247$	0 bis 1000	564
1720088	3 bis 61	$2n^2 - 215011$	328 bis 1328	562
-77683	3 bis 43	$n^2 + n + 19421$	0 bis 1000	558

Tabelle 3 Primzahlreiche Polynome

Anmerkungen zu Tabelle 3:

- Das hier angeführte Polynom $2n^2 - 410749$ ($D = 3285992$) geht durch eine Verschiebung mit $k = -450$ (siehe 2.2) in $2n^2 - 1800n - 5749$ über. In [2], S. 133 wird erwähnt, daß dieses Polynom im Intervall von 0 bis 1000 eine Höchstleistung von 686 Primzahlen erbringt. Analog zu dem Rekord, der in den Anmerkungen zu

Tab. 2 erwähnt ist, werden nur die *Beträge* der Polynomglieder beachtet, bei sehr vielen negativen Werten wird das Vorzeichen umgedreht.

- Das Eulersche Polynom bleibt in dieser Liste weit abgeschlagen, und das muß nicht überraschen: Die Diskriminanten der überlegenen Polynome sind quadratische Nichtreste bezüglich einer größeren Anzahl unter den ersten Primzahlen. Zwar liegen die Werte dieser Polynome in der Umgebung von $n = 0$ i.a. um Größenordnungen über denen des Eulerschen Polynoms, für größere n ergibt sich aber Annäherung, sodaß sich der zusätzliche Primteiler mangel deutlich auswirken kann. Dagegen sind Serien dieser Polynome, die man ja nur bei kleineren n erwarten kann, viel weniger beeindruckend als die des Eulerschen Polynoms. In Tabelle 4 ist ein Überholvorgang am Eulerschen Polynom dargestellt.

Intervall: n von	Anzahl der Primzahlen im Polynom	
	$n^2 + n + 41$	$n^2 + n + 72\,491$
0 bis 100	87	69
0 bis 200	157	139
0 bis 500	326	328
0 bis 1000	582	611
0 bis 5000	2262	2453

Tabelle 4 Ein Überholvorgang

5 Graphische Untersuchungen

Ein Zahlenstrahl wird wie im ersten Bild der Abbildung 1 zu einer quadratischen Spirale geknickt. Wenn jetzt noch die Primzahlen markiert werden, so bilden die Serien gewisser Polynome zweiten Grades ein bizarres Strichmuster (Abb. 2). Dieser Primzahlteppich ist unter dem Namen "Ulam's Spirale" bekannt [6].

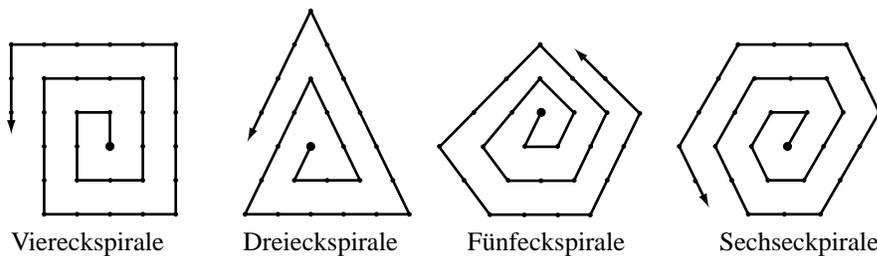


Abb. 1

Mit einem neuen Ansatz sollen übersichtlichere Strukturen erzielt werden: Das Programm "SPIRALE" gestaltet verschiedene Spiralenmuster gemäß Abbildung 1, in denen die Primzahlstränge gezielt herausmodelliert werden können; gibt man die Koeffizienten eines zu untersuchenden Polynoms $f(n) = an^2 + bn + c$ ein, so wird das Zentrum von der Zahl c eingenommen, und die Polynomglieder werden in der Spirale hervorgehoben (Kreise); unter diesen sind die Primzahlen noch besonders gekennzeichnet (ausgefüllte

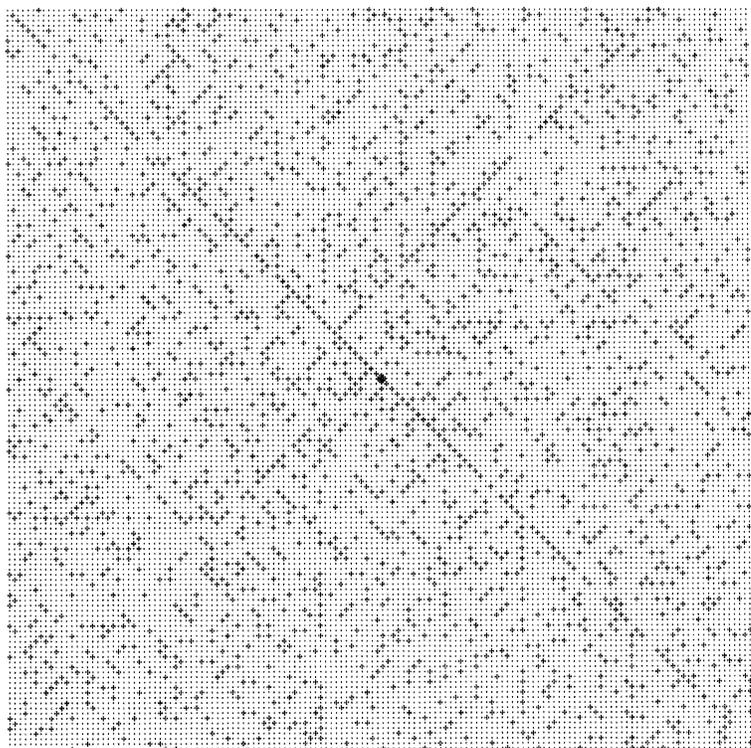


Abb. 2 Ulam's Spirale. Zentrum der Spirale: 41. Letzte Zahl in der Spirale: 20921.

Kreise). Startet man das Programm mit der Sechseckspirale und mit den Koeffizienten des Polynoms $3n^2 + n + 79$, so bilden die Polynomglieder einen Strahl, der vom Zentrum diagonal nach außen wächst (Abb. 3).

Wie es dazu kommt, ist leicht einzusehen: In der Folge der Polynomwerte 79, 83, 93, 109, 131, ... wachsen die Differenzen von einem Glied zum nächsten um jeweils 6. Andererseits erhöht sich in der Sechseckspirale die Differenz zweier aufeinanderfolgender Diagonalzahlen auch jeweils um 6 (zuerst vier Schritte bis zum Erreichen des ersten Diagonalenpunktes, dann zehn bis zum Erreichen des nächsten, dann sechzehn ...).

Solche gerade Strecken in Spiralen ergeben sich offensichtlich immer, wenn das Fortschreiten der Zahlenwerte pro Umdrehung in Resonanz mit dem Anwachsen der Polynomwerte ist. Um mehr herauszufinden, sind einige grundsätzliche Überlegungen vonnöten:

Die Glieder p_n eines Polynoms $an^2 + bn + c$ können als "arithmetische Folge zweiter Ordnung" angesehen werden; ihre "erste Differenzenfolge" Δp_n ist eine "arithmetische Folge erster Ordnung":

$$\Delta p_n = an^2 + bn + c - [a(n-1)^2 + b(n-1) + c] = 2an - a + b \quad .$$

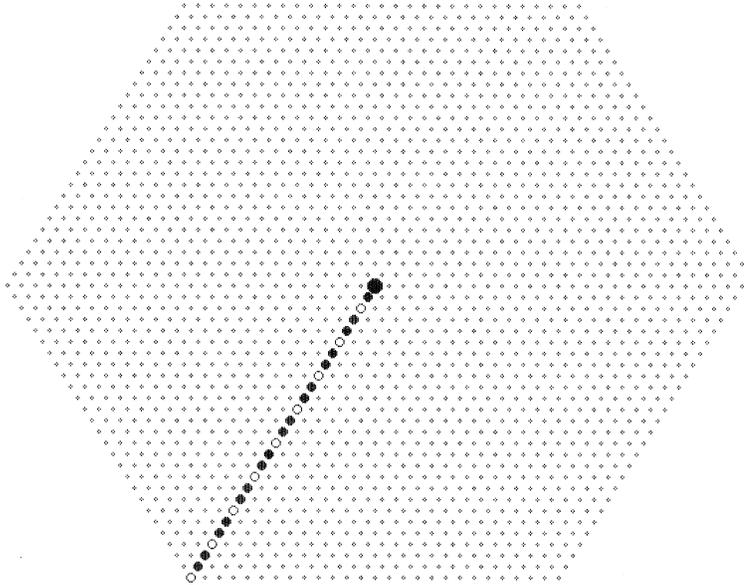


Abb. 3 $3n^2 + n + 79$, letzte Zahl in der Spirale: 2212.

Deren Differenzenfolge, die “zweite Differenzenfolge” der ursprünglichen Folge ist konstant:

$$\Delta p_n - \Delta p_{n-1} = 2an - a + b - [(2a(n-1) - a + b)] = 2a \quad .$$

Das Umgekehrte ist auch richtig: Wenn für irgendeine Folge die zweite Differenzenfolge eine Konstante $d \neq 0$ ist, so handelt es sich stets um eine arithmetische Folge zweiter Ordnung, und der Koeffizient des quadratischen Termes ist $d/2$. (Der Beweis dafür ist sehr einfach.)

In den vorgestellten Spiralen erhöht sich die Differenz der Zahlenwerte von Umlauf zu Umlauf jeweils um eine Konstante, diese beträgt in der Dreieckspirale $d_D = 9$, in der Viereckspirale $d_V = 8$, in der Fünfeckspirale $d_F = 5$ und in der Sechseckspirale $d_S = 6$.¹⁾ Wir sehen diese Zahlen jeweils als konstante zweite Differenzenfolge der Folge der Zahlenwerte z_n nach n vollen Umdrehungen an, dann müssen arithmetische Folgen vorliegen, deren Glieder die Form $z_n = An^2 + Bn + C$ haben, wobei A jeweils festliegt ($A = d_D/2 = 4.5$ bzw. $d_R/2 = 4$, $d_F/2 = 2.5$, $d_S/2 = 3$); C bildet immer das Zentrum, und B bestimmt die Stelle, an der die Zahl z_1 erscheint; dann liegt z_2 exakt eine Umdrehung weiter außen, und so fort. Die oben erwähnte Bedingung für “einfache Resonanz” lautet $p_n = z_n$ und kann nur in der Viereckspirale mit Grundpolynomen $4n^2 + bn + c$ und in der Sechseckspirale mit $3n^2 + bn + c$ exakt erfüllt werden. Der Koeffizient b bestimmt die Strahlrichtung, längs derer sich die Polynomglieder anordnen.

1) Der Hintergrund ist folgender: Die Gitterpunkte jeder Spirale bilden jeweils eine Schachtelung regelmäßiger Drei- bzw. Vier-, Fünf- und Sechsecke mit gemeinsamem Zentrum und gleichmäßig anwachsenden Seitenlängen. Z. B. erhält man in der Viereckspirale konzentrische Quadrate mit den Umfängen 8, 16, 24 usw., s. Abb. 1. Der konstante Umfangszuwachs ist gleich d_D bzw. d_V , d_F , d_S .

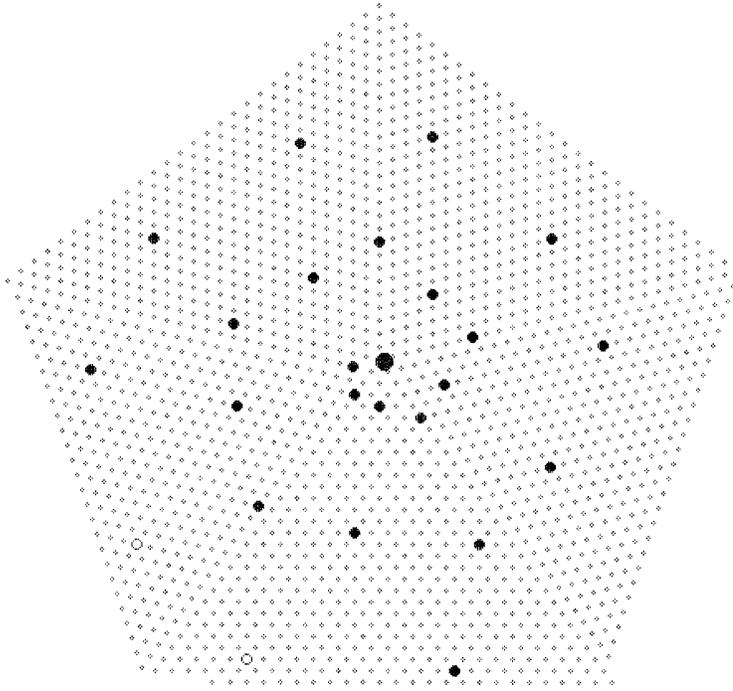


Abb. 4 $3n^2 + 3n + 23$, letzte Zahl in der Spirale: 1969.

Die Resonanzen müssen aber nicht scharf sein, wie das folgende Beispiel zeigt: In der Fünfeckspirale ist d um eins kleiner als die Zuwachsrates $2a$ in einem Polynom $3n^2 + bn + c$ beträgt, und das Vorseilen der Polynomglieder bewirkt, daß sich ihre Bildpunkte in einer Linksdrehung um das Zentrum winden (Abb. 4). Solche Resonanzen sind insofern einfach, als in jeder Spiralenwindung genau ein Polynomglied erfaßt wird. In anderen Fällen ereignet sich das erst nach einer gleichbleibenden Anzahl mehrerer Umläufe, oder jeweils nach einer gebrochenen Zahl von Umläufen auf mehreren vom Zentrum ausgehenden Linien. Diese weniger einfachen Resonanzen lassen sich verstehen und voraussagen, wenn man die folgende Regel anwendet:

Jedesmal nach r Umläufen in einer der vier Spiralen verlängert sich der zugehörige Zahlenstrang um $r^2 \cdot d$ Zahlen. Dabei ist r eine rationale Zahl und d ist die entsprechende "Spiralenkonstante" ($d = 9$ bzw. 8, 5, 6).

Beweis: $An^2 + Bn + C$ sei die nach n vollen Umdrehungen erreichte Zahl.

$$An^2 + Bn + C - [A(n-r)^2 + B(n-r) + C] = 2Arn - Ar^2 + Br$$

(erste Differenzenfolge bezüglich r zusätzlicher Umdrehungen)

$$2Arn - Ar^2 + Br - [2Ar(n-r) - Ar^2 + Br] = 2Ar^2 = d \cdot r^2$$

(konstante zweite Differenzenfolge bezüglich r zusätzlicher Umdrehungen)

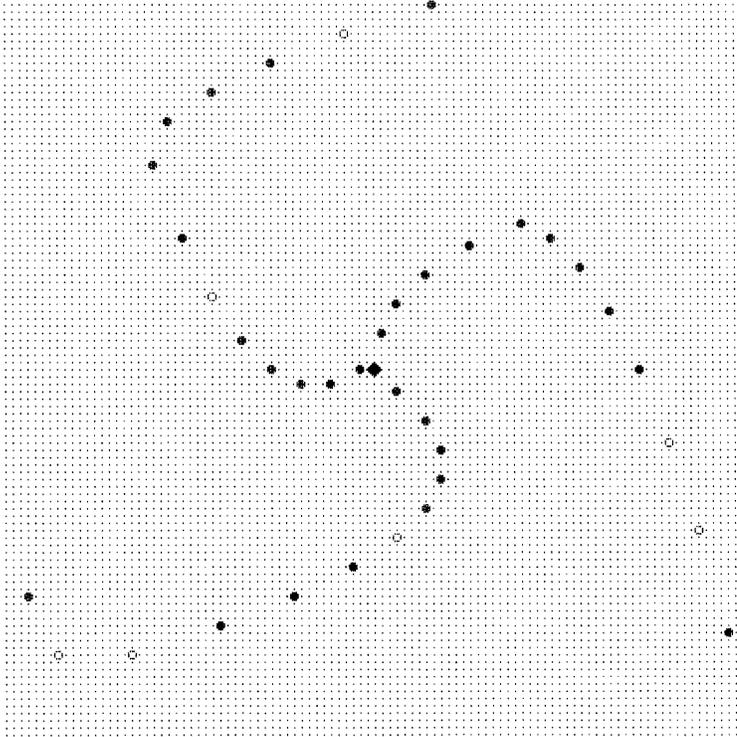


Abb. 5 $7n^2 + 7n + 17$, letzte Zahl in der Spirale: 10117.

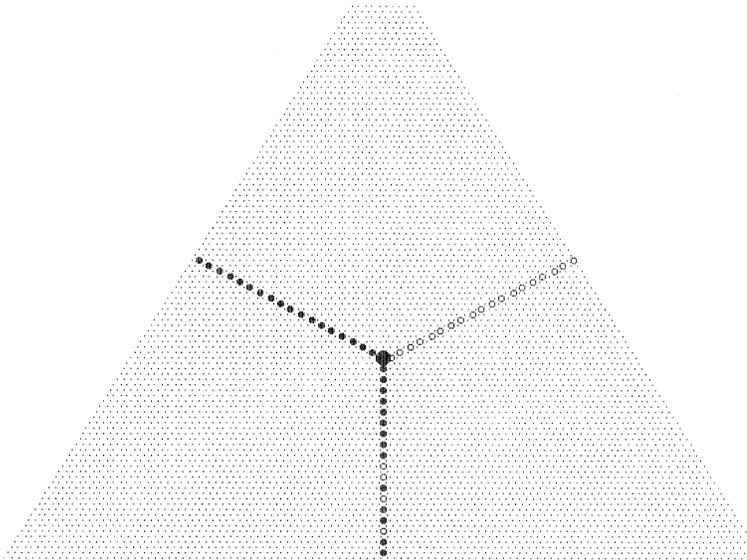


Abb. 6 $2n^2 + 2n + 89$, letzte Zahl in der Spirale: 6417.

Dazu einige Beispiele:

In der Dreieckspirale erhöht sich die Zahlendifferenz nach jeweils zwei Umdrehungen um $2^2 \cdot 9 = 36$, also liegen die Glieder der Polynome $18n^2 + bn + c$ auf einem vom Zentrum ausgehenden Strahl, der bei jedem zweiten Umlauf besetzt wird. In der Viereckspirale verlängert sich der Zahlenstrang nach jeweils $\frac{4}{3}$ Umdrehungen um $(\frac{4}{3})^2 \cdot 8 \approx 14.2$; das ist geringfügig mehr als der Zuwachs $2a$ von Glied zu Glied in einem Polynom $7n^2 + bn + c$. Deshalb werden der Reihe nach und ständig wiederholt (nach $\frac{4}{3}, \frac{8}{3}, 4, 4\frac{4}{3}, \dots$ Umdrehungen) drei Rechtsbögen mit den Gliedern des Polynoms besetzt (Abb. 5). Das Eulersche Polynom läßt sich besonders gut in der Viereckspirale darstellen: dort wird $r^2 \cdot d = 2$, wenn $r = \frac{1}{2}$ ist; deshalb verteilt ein Polynom $n^2 + bn + c$ seine Glieder abwechselnd auf zwei gerade Arme, die um 180° versetzt aus dem Zentrum wachsen, und die große Primzahlserie des Eulerschen Polynoms besetzt in einer solchen Spirale ein langes Diagonalenstück (siehe auch die Abb. 2).

Zusammengefaßt: r sei eine rationale Zahl, und in einem Grundpolynom $an^2 + bn + c$ sei $2a \approx r^2 \cdot d$, wobei d eine der vier Spiralkonstanten ist; dann liegen die Polynomglieder auf Ästen, die aus dem betreffenden Spiralenzentrum herauswachsen. Die Zahl der Äste ist gleich dem Nenner q , wenn r als gekürzter Bruch p/q geschrieben wird. Mehr oder weniger genaue Resonanzen lassen sich damit *beliebig* erzeugen, und für jedes quadratische Polynom mit ganzzahligen Koeffizienten läßt sich unter den vier Spiralen eine oder mehrere passende finden. Für das Zustandekommen typischer Muster in einer gegebenen Spirale ist nur der Koeffizient a des quadratischen Terms bestimmend; die Koeffizienten b des linearen Terms bewirken lediglich Drehungen des Grundmusters innerhalb der Spirale, und die Konstante c ist die Anfangszahl der Spirale.

Dieses graphische Verfahren eignet sich also *auch* zur Suche nach Primzahlserien, es kann das Programm "P-SERIE" ersetzen. In *einer* Spirale lassen sich allerdings nur streng monotone Folgen darstellen. Der eigentliche Nutzen des "Spiralenprogramms" liegt aber in folgendem: Besondere Ordnungen in unterbrochenen Serien kommen deutlich zum Vorschein, regelmäßige Verteilungen springen sofort ins Auge. Das wurde schon im Muster für $3n^2 + n + 79$ in der Sechseckspirale deutlich (Abb. 3): zwei Primzahlen – Lücke – zwei Primzahlen – Lücke – ... von $n = 0$ bis $n = 28$; indem man n von 0 an rückwärts laufen läßt (das ist in den Programmen möglich), bestätigt man, daß sich dieses Muster bis $n = -22$ fortsetzt! Auch die Polynome $n^2 + n + 67$ und $2n^2 + 2n + 89$ bilden solche "Primzahlwillinge". Das Bild des letzteren in der Dreieckspirale besteht aus drei Armen, und entsprechend dem Rhythmus der Primzahlfolge sind nur zwei dieser Arme von Primzahlen besetzt, der dritte "geht leer aus" (Abb. 6). Ein "Negativ" zu Abb. 3 ergibt sich in der Viereckspirale mit $4n^2 + 2n + 171$ (Primzahl – zwei Lücken – Primzahl – zwei Lücken – ..., von $n = -17$ bis $n = 18$). Der Vielfalt an geordneten bunten Ketten sind wohl keine Grenzen gesetzt.

Selbstverständlich soll auch hier der Sucherfolg nicht dem Zufall überlassen bleiben. Damit ein Polynom eine unterbrochene Serie nach den Mustern der Abbildungen 3 und 6 abgibt, muß z. B. verlangt werden, daß sich jedes dritte Polynomglied durch 3 teilen

läßt²⁾ und daß die Diskriminante quadratischer Nichtrest modulo vieler kleiner Primzahlen $abn = 5$ ist – beide Voraussetzungen werden von den betreffenden Polynomen erfüllt. Noch einfacher wird es, wenn innerhalb einer längeren Kette jeweils ein primes auf ein zusammengesetztes Polynomglied folgen soll. Dann kann nach Polynomen gesucht werden, die abwechselnd ungerade und gerade Werte annehmen und deren Diskriminanten quadratische Nichtreste modulo vieler kleiner Primzahlen ab 3 sind. Das Polynom $n^2 + 163$ mit der Diskriminante $D = -4 \cdot 163$ erfüllt diese Bedingung und liefert das entsprechende Muster von $n = -39$ bis $n = 39$.

Für Untersuchungen dieser Art können Programme wie “NIREDISK” und “DISKRIMI” (s. Abschnitt 3) nach leichten Abänderungen die nötige Vorauswahl unter Polynomen zweiten Grades besorgen.

Dank: Ich danke Herrn Dipl. Phys. Dr. Eric Maiser für das Korrekturlesen und für die technische Erstellung des Manuskriptes in LaTeX.

Literatur

- [1] H. Scheid: Zahlentheorie. 2.Aufl. – Mannheim: BI Wiss.-Verlag 1993.
- [2] P. Ribenboim: Nombres premiers: mystères et records. – Paris: Presses Universitaires de France 1994.
- [3] P. Ribenboim: Euler’s famous prime generating polynomial and the class number of imaginary quadratic fields. – L’enseignement Mathématique **34** (1988) 23–42.
- [4] P. Ribenboim: The Book of Prime Number Records. 2. Aufl. S. 141 f. – New York, Berlin, Heidelberg: Springer-Verlag 1989.
- [5] K. Devlin: Sternstunden der modernen Mathematik. – Basel: Birkhäuser 1990.
- [6] M. Gardner: Mathematisches Labyrinth. S. 82 f. – Braunschweig: Vieweg 1979.

Albrecht Schultz
 Im Alten Kloster
 D-76857 Eußerthal

2) Dafür muß im Polynom $an^2 + bn + c$ die Substitution von n durch $3k$ oder $3k + 1$ oder $3k + 2$ zu einem durch 3 teilbaren Term führen; eine kleine Rechnung ergibt: c oder $a + b + c$ oder $4a + 2b + c$ muß durch 3 teilbar sein.