6

Heuristische und probabilistische Betrachtungen

Das Wort „heuristisch“ bedeutet: auf Erfahrungen beruhend oder mit Erfahrungen verbunden sein. Heuristische Ergebnisse entstehen aus der Beobachtung numerischer Daten, die in Tabellen vorliegen oder durch umfangreiche Berechnungen gewonnen wurden. Manchmal folgen die Ergebnisse aus einer statistischen Analyse der Daten.

Es gibt auch probabilistische (wahrscheinlichkeitstheoretische) Methoden. Die Idee ist in dem Artikel von Cramér (1937), der schon in Kapitel 4 erwähnt wurde, recht gut erklärt:

> Bei Untersuchungen über die asymptotischen Eigenschaften von arithmetischen Funktionen ist es häufig möglich, probabilistische Methoden in interessanter Weise zu nutzen. Wenn wir uns zum Beispiel für die Verteilung einer gegebenen Folge S ganzer Zahlen interessieren, betrachten wir S als Element einer unendlichen Klasse C von Folgen, was man sich konkret als Realisierung eines Glücksspiels vorstellen könnte. Es ist dann in vielen Fällen möglich zu beweisen, dass *mit einer Wahrscheinlichkeit von* 1 eine bestimmte Relation R in C gilt, d.h., dass in einer festgelegten mathematischen Bedeutung „fast alle“ Folgen von C die Relation R erfüllen. Natürlich kann man im Allgemeinen nicht schließen, dass R auch für die spezielle Folge S

P. Ribenboim, *Die Welt der Primzahlen*, 2. Aufl., Springer-Lehrbuch,
DOI 10.1007/978-3-642-18079-8_6, © Springer-Verlag Berlin Heidelberg 2011

gilt. Aber Ergebnisse, die man auf diese Weise gewonnen hat, können danach vielleicht mit Hilfe anderer Methoden streng bewiesen werden.

Wenn man heuristische und probabilistische Methoden nicht mit Vorsicht und auf intelligente Weise benutzt, können sie zu einer Art „Traum-Mathematik“ ohne jeden Bezug zur Realität führen. Hastig formulierte Vermutungen und Fehlinterpretation numerischer Indizien müssen vermieden werden.

Ich werde vorsichtig sein und mich nur auf wenige der zuverlässigen Beiträge beschränken. Ich denke an Hardy & Littlewood und ihre berühmten Vermutungen aus *Partitio Numerorum* sowie an die faszinierenden Hypothesen von Dickson, Bunjakowski, Schinzel und Sierpiński.

I Primzahlwerte linearer Polynome

Der Ausgangspunkt ist wiederum Dirichlets Satz über Primzahlen in arithmetischen Folgen. Er besagt, dass wenn $f(X) = bX+a$ mit ganzen Zahlen a, b und $a \neq 0$, $b \geq 1$, $\mathrm{ggT}(a, b) = 1$, dann existieren unendlich viele $m \geq 0$ derart, dass $f(m)$ eine Primzahl ist.

Im Jahre 1904 äußerte Dickson die folgende Vermutung über gleichzeitig angenommene Werte mehrerer linearer Polynome:

(D) *Es sei* $s \geq 1$, $f_i(X) = b_iX + a_i$ *mit ganzen Zahlen* a_i, b_i *und* $b_i \geq 1$ (*für* $i = 1, \ldots, s$). *Angenommen, die folgende Bedingung ist erfüllt*:

(*) *Es gibt keine Zahl* $n > 1$, *die das Produkt* $f_1(k)f_2(k)\cdots f_s(k)$ *für alle ganzen Zahlen* k *teilt.*

Dann existieren unendlich viele natürlichen Zahlen m *derart, dass alle Zahlen* $f_1(m)$, $f_2(m), \ldots, f_s(m)$ *prim sind.*

Die folgende Aussage scheint schwächer als (D) zu sein:

(D_0) *Unter denselben Voraussetzungen für* $f_1(X), \ldots, f_s(X)$ *existiert eine natürliche Zahl* m *derart, dass die Zahlen* $f_1(m), \ldots, f_s(m)$ *Primzahlen sind.*

Während man zunächst die Gültigkeit von (D) anzweifeln könnte, würde man Aussage (D_0) eher akzeptieren, da sie anscheinend viel weniger verlangt. Tatsächlich aber sind (D) und (D_0) äquivalent.

Denn wenn (D_0) wahr ist, gibt es $m_1 \geq 0$ derart, dass $f_1(m_1), \ldots, f_s(m_1)$ Primzahlen sind. Sei $g_i(X) = f_i(X + 1 + m_1)$ für $i = 1, \ldots, s$. Dann ist (*) von $g_1(X), \ldots, g_s(X)$ erfüllt, daher gibt es nach (D_0) ein $k_1 \geq 0$ derart, dass $g_1(k_1), \ldots, g_s(k_1)$ prim sind; sei $m_2 = k_1 + 1 + m_1 > m_1$, so dass $f_1(m_2), \ldots, f_s(m_2)$ Primzahlen sind. Das Argument lässt sich fortführen und zeigt schließlich, dass (D) aus (D_0) folgt.

Dickson erforschte die Konsequenzen seiner Vermutung nicht. Dies war Gegenstand eines Artikels von Schinzel & Sierpiński (1958), den ich so interessant finde, dass ich ihm einen größeren Teil von Kapitel 6 widmen werde.

In der Tat hatte Schinzel eine viel umfassendere Vermutung vorgeschlagen (Hypothese (H)), die Polynome behandelt, die nicht notwendigerweise linear sein müssen. Bevor ich aber Hypothese (H) und Folgerungen daraus diskutiere, werde ich auf die vielen interessanten Ergebnisse eingehen, die Schinzel & Sierpiński unter der Voraussetzung der Gültigkeit von Vermutung (D) bewiesen.

Die eindrucksvollen Konsequenzen aus Hypothese (D), die unten aufgelistet sind, sollten jeden davon überzeugen, dass der Beweis von (D) in weiter Ferne liegt, falls er überhaupt möglich ist.

(D_1) *Es seien* $s \geq 1$ *und* $a_1 < a_2 < \cdots < a_s$ *ganze Zahlen ungleich* 0. *Angenommen, dass* $f_1(X) = X + a_1, \ldots, f_s(X) = X + a_s$ *der Bedingung* (*) *in* (D) *genügen. Dann gibt es unendlich viele Zahlen* $m \geq 1$ *derart, dass* $m+a_1, m+a_2, \ldots, m+a_s$ *aufeinander folgende Primzahlen sind.*

Die Vermutung von Polignac (1849), die in Kapitel 4 in den Abschnitten II und III besprochen wurde, folgt aus (D_1):

(D_2) *Für jede gerade Zahl* $2k \geq 2$ *existieren unendlich viele Paare aufeinander folgender Primzahlen mit Differenz* $2k$. *Insbesondere gibt es unendlich viele Paare von Primzahlzwillingen.*

Hier eine interessante Konsequenz, welche die Häufigkeit der Primzahlzwillinge betrifft:

(D_3) *Für jede Zahl* $m \geq 1$ *gibt es* $2m$ *aufeinander folgende Primzahlen, die* m *Paare von Primzahlzwillingen bilden.*

Eine weitere, ziemlich unerwartete Folgerung bezieht sich auf Primzahlen in arithmetischen Folgen. In Kapitel 4, Abschnitt IV habe ich

gezeigt, dass wenn a, $a+d, \ldots, a+(n-1)d$ mit $1 < n < a$ Primzahlen sind, dann ist d Vielfaches von $\prod_{p \le n} p$.

Aus (D_1) folgt:

(D_4) *Es sei $n > 2$ und d ein Vielfaches von $\prod_{p \le n} p$. Dann gibt es unendlich viele Primzahlen p derart, dass p, $p+d$, $p+2d$, …, $p+(n-1)d$ aufeinander folgende Primzahlen sind.*

Der Leser sollte diese sehr starke Aussage mit dem vergleichen, was unabhängig von irgendeiner Vermutung in Kapitel 4, Abschnitt IV gesagt wurde.

Was Sophie-Germain-Primzahlen angeht, so lässt sich aus (D) ableiten:

(D_5) *Für jedes $m \ge 3$ existieren unendlich viele arithmetische Folgen, die sich aus m Sophie-Germain-Primzahlen zusammensetzen.*

Insbesondere impliziert (D) die Existenz unendlich vieler Sophie-Germain-Primzahlen, was nie bewiesen werden konnte, ohne auf die Gültigkeit einer Vermutung zurückzugreifen. Ich werde gleich auf eine quantitative Aussage über die Verteilung von Sophie-Germain-Primzahlen zurückkommen.

Vermutung (D) ist so gewaltig, dass sie sogar zur Folge hat:

(D_6) *Es gibt unendlich viele zerlegbare Mersenne-Zahlen.*

Ich erinnere daran (siehe Kapitel 2, Abschnitt IV), dass es bisher niemand geschafft hat zu beweisen (ohne Vermutung (D) vorauszusetzen), dass es unendlich viele zerlegbare Mersenne-Zahlen gibt. Es ist jedoch leicht, dies für andere Folgen zu zeigen, die der Folge der Mersenne-Zahlen ähneln. Das folgende Resultat war 1982 von Powell als Problem gestellt worden (eine Lösung von Israel wurde 1983 veröffentlicht):

Wenn m, n Zahlen sind, für die $m > 1$, $mn > 2$ gilt (wodurch der Fall $m = 2$, $n = 1$ ausgeschlossen ist), dann gibt es unendlich viele zerlegbare Zahlen der Form $m^p - n$, wobei p eine Primzahl ist.

Beweis. Es sei q ein Primteiler von $mn - 1$, also $q \nmid m$. Falls p eine Primzahl ist, für die $p \equiv q-2 \pmod{q-1}$ gilt, dann ist $m(m^p - n) \equiv m(m^{q-2} - n) \equiv 1 - mn \equiv 0 \pmod{q}$ und somit q Teiler von $m^p - n$. Nach dem Satz von Dirichlet über Primzahlen in arithmetischen Folgen gibt es unendlich viele Primzahlen p, die $p \equiv q-2 \pmod{q-1}$ erfüllen

und somit auch unendlich viele zerlegbare Zahlen $m^p - n$, wobei p eine Primzahl ist. □

Ein weiterer Beweis der Stärke von Vermutung (D) ist die folgende Vermutung:

(D_7) *Es gibt unendlich viele Carmichael-Zahlen, die aus drei verschiedenen Primfaktoren zusammengesetzt sind.*

Ich möchte daran erinnern, dass Alford, Granville & Pomerance (1994) die Unendlichkeit der Anzahl der Carmichael-Zahlen auch ohne den Rückgriff auf Vermutung (D) beweisen konnten. Es ist jedoch noch nie gezeigt worden, dass es auch unendlich viele Carmichael-Zahlen gibt, die das Produkt von genau drei verschiedenen Primzahlen sind.

Eine andere, noch beachtlichere Konsequenz aus (D) ist die berühmte Vermutung von Artin:

(A) *Es sei a eine von 0 und -1 verschiedene Zahl, die kein Quadrat ist. Dann gibt es unendlich viele Primzahlen p, für die a eine Primitivwurzel modulo p ist.*

Obwohl noch kein Beweis für Artins Vermutung gefunden werden konnte, gab es in dieser Richtung substantielle Fortschritte. Zunächst den bahnbrechenden Artikel von Gupta & Ram Murty (1984), dann das krönende Resultat von Heath-Brown (1986), der bewies: Es gibt höchstens zwei Primzahlen und höchstens drei positive quadratfreie Zahlen, die im Widerspruch zu Artins Vermutung stehen.

II Primzahlwerte von Polynomen beliebigen Grades

Ich wende mich nun Polynomen zu, die auch nichtlinear sein können. Die diesbezüglich erste Vermutung stammt von Bunjakowski aus dem Jahre 1857 und bezieht sich auf ein Polynom, das mindestens den Grad 2 hat:

(B) *Es sei $f(X)$ ein irreduzibles Polynom mit ganzzahligen Koeffizienten, einem positiven Leitkoeffizienten und einem Grad von mindestens 2. Angenommen, die folgende Bedingung ist erfüllt:*

(*) *Es gibt kein $n > 1$, das $f(k)$ für alle ganzen Zahlen k teilt.*

Dann gibt es unendlich viele natürliche Zahlen m, für die $f(m)$ eine Primzahl ist.

Der Leser sollte wissen, dass genau wie bei den Vermutungen (D) und (D_0) an dieser Stelle (B) äquivalent zu einer Vermutung (B_0) ist, die sich ähnlich formulieren lässt.

Bevor ich näher auf Vermutung (B) eingehe, sei gesagt, dass es tatsächlich sehr wenige Resultate über prime Werte von Polynomen gibt. So ist beispielsweise noch kein Polynom $f(X)$ eines Grades höher als 1 bekannt, das im Betrag $|f(n)|$ für unendlich viele natürliche Zahlen n Primzahlwerte annimmt.

Andererseits zeigte Sierpiński 1964, dass es für jedes $k \geq 1$ eine ganze Zahl b derart gibt, dass $n^2 + b$ für mindestens k natürliche Zahlen n prim ist.

Mit $f(X)$ vom Grad $d \geq 2$ und ganzzahligen Koeffizienten bezeichne für jedes $x \geq 1$

$$\pi_{f(X)}(x) = \#\{n \geq 1 \mid |f(n)| \leq x \text{ und } |f(n)| \text{ ist eine Primzahl}\}.$$

Nagell zeigte 1922, dass $\lim_{x\to\infty} \pi_{f(X)}(x)/x = 0$, es gibt also sehr wenige Primzahlwerte. Heilbronn bewies 1931 die präzisere Aussage:

Es existiert eine positive Konstante C (abhängig von $f(X)$) derart, dass

$$\pi_{f(X)}(x) \leq C\frac{x^{1/d}}{\log x}, \quad \text{für jedes } x \geq 1.$$

Im Falle beliebiger Polynome scheint nicht viel mehr bekannt zu sein. Es gibt jedoch interessante Vermutungen über spezielle Typen von Polynomen und umfangreiche Berechnungen hierzu. Ich werde darauf an späterer Stelle detaillierter eingehen.

Die Frage nach der Existenz unendlich vieler Primzahlen p, die zu primen $f(p)$ führen, ist sogar noch schwieriger. Insbesondere ist es, wie bereits erwähnt, unbekannt, ob es unendlich viele Primzahlen gibt, für die die Polynome $f(X) = X + 2$ beziehungsweise $f(X) = 2X + 1$ prime Werte annehmen (Existenz unendlich vieler Primzahlzwillinge oder unendlich vieler Sophie-Germain-Primzahlen). Wenn man allerdings mit Fastprimzahlen zufrieden ist, dann werden einem die Siebmethoden und das unvermeidliche Buch von Halberstam & Richert wieder einmal gute Gründe liefern, um glücklich zu werden.

Zur Erinnerung die Definition von „Fastprimzahl“. Zu gegebenem $k \geq 1$ heißt eine natürliche Zahl $n = p_1p_2 \cdots p_r$, geschrieben als Produkt seiner nicht notwendigerweise verschiedenen Primfaktoren, eine *k-Fastprimzahl*, falls $r \leq k$. Die Menge aller k-Fastprimzahlen wird mit P_k bezeichnet. Richert (1969) bewies:

Es sei $f(X)$ ein von X verschiedenes Polynom mit ganzzahligen Koeffizienten, positivem Leitkoeffizienten und einem Grad $d \geq 1$. Angenommen, dass für jede Primzahl p die Anzahl $\rho(p)$ der Lösungen von $f(X) \equiv 0 \pmod{p}$ kleiner als p ist und darüber hinaus $\rho(p) < p-1$ gilt, falls $p \leq d+1$ und p kein Teiler von $f(0)$ ist. Dann gibt es unendlich viele Primzahlen p derart, dass $f(p)$ eine $(2d+1)$-Fastprimzahl ist.

Den folgenden Spezialfall bewies Rieger (1969): Es gibt unendlich viele Primzahlen p, für die $p^2 - 2 \in P_5$.

Nun zurück zu Bunjakowskis Hypothese! Bunjakowski zog keine Schlussfolgerungen aus seiner Vermutung. Es waren wieder einmal Schinzel und Sierpiński, die ein Jahrhundert später eine allgemeinere, unabhängig formulierte Hypothese untersuchten.

Der folgende, unbewiesene Satz folgt unmittelbar aus der Richtigkeit von Vermutung (B):

(B_1) *Es seien a, b, c teilerfremde Zahlen derart, dass $a \geq 1$ und $a+b$ und c nicht gleichzeitig gerade sind. Falls $b^2 - 4ac$ kein Quadrat ist, gibt es unendlich viele natürliche Zahlen m, für die $am^2 + bm + c$ eine Primzahl ist.*

Aus Satz (B_1) wiederum folgt:

(B_2) *Wenn k eine ganze Zahl ist und $-k$ kein Quadrat, dann gibt es unendlich viele natürliche Zahlen m derart, dass $m^2 + k$ eine Primzahl ist.*

Insbesondere impliziert (B), dass es unendlich viele Primzahlen der Form $m^2 + 1$ gibt.

Das „Spiel der Primzahlen der Form $m^2 + 1$“ ist nicht so harmlos, wie man vielleicht zunächst versehentlich denken mag. Es hängt stark mit der Klassenzahl reell-quadratischer Zahlkörper zusammen.

Das Polynom $X^2 + 1$ ist das einfachste quadratische Polynom mit negativer Diskriminante. Ein Beweis, dass dieses Polynom unendlich viele Primzahlwerte annimmt, würde einen gigantischen Fortschritt bedeuten. Aber das Problem scheint – oder ist bestimmt – zu schwierig. Man vergleiche nur mit dem wahrlich bemerkenswerten Satz, den Friedlander & Iwaniec erst vor kürzerer Zeit (1998) bewiesen:

Es gibt unendlich viele Primzahlen, die die Summe eines Quadrats und einer vierten Potenz sind.

Der Beweis erforderte unter anderem tiefliegende Siebmethoden. Wie weit ist das Resultat von „$m^2 + 1$ unendlich oft prim“ entfernt?

Letzteres würde nicht nur den Satz von Friedlander und Iwaniec umfassen, sondern auch, dass es für jedes $k \geq 1$ unendlich viele Primzahlen gibt, die die Summe eines Quadrats und einer 2^k-ten Potenz sind.

Die folgende Aussage ist eine weitere Vermutung von Hardy & Littlewood aus dem Jahr 1923; sie ist unter Annahme der Richtigkeit von Vermutung (B) beweisbar.

(B_3) *Es sei d eine ungerade Zahl mit $d > 1$ und k eine Zahl, die für keinen Faktor $e > 1$ von d eine e-te Potenz ist. Dann gibt es unendlich viele natürliche Zahlen m derart, dass $m^d + k$ eine Primzahl ist.*

In seinem gemeinsamen Artikel mit Sierpiński stellte Schinzel die folgenden Vermutungen auf:

(H) *Es seien $s \geq 1$ und $f_1(X), \ldots, f_s(X)$ irreduzible Polynome mit ganzzahligen Koeffizienten und positivem Leitkoeffizienten. Angenommen, die folgende Bedingung sei erfüllt:*

(*) *Es gibt keine Zahl $n > 1$, die das Produkt $f_1(k)f_2(k)\cdots f_s(k)$ für alle ganzen Zahlen k teilt.*

Dann existieren unendlich viele natürliche Zahlen m derart, dass $f_1(m), f_2(m), \ldots, f_s(m)$ alle prim sind.

(H_0) *Unter denselben Voraussetzungen für $f_1(X), \ldots, f_s(X)$ existiert eine natürliche Zahl m derart, dass $f_1(m), \ldots, f_s(m)$ sämtlich Primzahlen sind.*

Wieder sind (H) und (H_0) äquivalent. Im Falle, dass alle Polynome $f_1(X), \ldots, f_s(X)$ den Grad 1 haben, fallen diese Vermutungen mit Dicksons (D) und (D_0) zusammen. Für $s = 1$ sind sie mit Bunjakowskis Vermutungen (B) und (B_0) identisch.

Ich werde hier nicht alle Konsequenzen aus dieser Hypothese aufzählen, die die Autoren bewiesen haben. Allerdings möchte ich ein Resultat von Schinzel erwähnen, das mit Carmichaels Vermutung über die Valenz von Eulers Funktion in Verbindung steht. Man erinnere sich an die folgende Bezeichnung aus Kapitel 2, Abschnitt II, F: Für jedes $m \geq 1$ sei

$$V_\varphi(m) = \#\{n \geq 1 \mid \varphi(n) = m\}.$$

Schinzel bewies 1961, dass aus Vermutung (H) folgt:

(H_1) *Für jedes $s > 1$ gibt es unendlich viele ganze Zahlen $m > 1$ derart, dass $V_\varphi(m) = s$.*

Man beachte, dass $s \neq 1$, so dass Aussage (H_1) Carmichaels Vermutung nicht enthält.

Für meine Leser, die pythagoreische Dreiecke mögen: Sie haben vielleicht festgestellt, dass es viele pythagoreische Tripel (a, b, c) mit geradem b und Primzahlen a, c gibt, so zum Beispiel $(3, 4, 5)$, $(5, 12, 13)$ und viele mehr. Ich bin sicher, dass Sie sich gefragt haben, ob es unendlich viele davon gibt. Vielleicht haben Sie sogar versucht, dies zu beweisen und irgendwann frustriert aufgegeben. Doch es gibt keinen Grund dafür, denn tatsächlich weiß niemand, wie man es beweisen kann – es sei denn, man setzt Hypothese (H) voraus.

Dieser Weg ist im Artikel von Schinzel & Sierpiński beschrieben, und ich möchte ihn hier der Einfachheit halber für Sie wiedergeben. Es ist zunächst notwendig, das Folgende herzuleiten:

(H_2) *Es seien a, b, c, d ganze Zahlen mit $a > 0$, $d > 0$ und nichtquadratischem $b^2 - 4ac$. Zudem sei angenommen, dass es ganze Zahlen x_0, y_0 derart gibt, dass* $\mathrm{ggT}(x_0y_0, 6ad) = 1$ *und $ax_0^2 + bx_0 + c = dy_0$. Dann existieren unendlich viele Primzahlen p, q, die der Gleichung $ap^2 + bp + c = dq$ genügen.*

Beweis, dass (H_2) **aus** (H) **folgt.** Es seien $f_1(X) = dX + x_0$, $f_2(X) = adX^2 + (2ax_0 + b)X + y_0$. Da $(2ax_0 + b)^2 - 4ady_0 = (2ax_0 + b)^2 - 4a(ax_0^2 + bx_0 + c) = b^2 - 4ac$ kein Quadrat ist, folgt, dass das Polynom $f_2(X)$ irreduzibel ist, dasselbe gilt für $f_1(X)$.

Ich verifiziere Bedingung (*). Sei $g(X) = f_1(X)f_2(X)$; dieses Polynom hat den Grad 3 mit Leitkoeffizient ad^2. Wenn es eine Primzahl p gibt, die $g(m)$ für jede ganze Zahl m teilt, dann ist p auch Teiler von $g(m) - g(m-1) = \Delta g(m)$, $g(m-1) - g(m-2) = \Delta g(m-1)$, $g(m-2) - g(m-3) = \Delta g(m-2)$, der ersten Differenzen von $g(X)$ an den Stellen m, $m-1$, $m-2$. Auf die gleiche Weise teilt p auch $\Delta^2 g(m) = \Delta g(m) - \Delta g(m-1)$, $\Delta^2 g(m-1) = \Delta g(m-1) - \Delta g(m-2)$ und p ist auch Teiler von $\Delta^3 g(m) = \Delta^2 g(m) - \Delta^2 g(m-1)$. Es ist aber $\Delta^3 g(X) = 6ad^2$. Wenn p auch $g(0) = x_0y_0$ teilte, dann würde p auch $\mathrm{ggT}(6ad, x_0y_0) = 1$ teilen, was nicht sein kann. Dies zeigt, dass Bedingung (*) erfüllt ist. Nach (H) gibt es nun unendlich viele natürliche Zahlen m derart, dass $f_1(X) = p$ und $f_2(X) = q$ Primzahlen sind. Und wegen $af_1(X)^2 + bf_1(X) + c = df_2(X)$ ist $ap^2 + bp + c = dq$. □

Aus obiger Aussage (H_2) folgt:

(H_3) *Jede rationale Zahl $r > 1$ lässt sich auf unendlich viele Weisen in der Form $r = (p^2-1)/(q-1)$ schreiben, wobei p und q Primzahlen sind.*

Beweis, dass (H_3) **aus** (H_2) **folgt.** Es sei $r = d/a$ mit $d > a > 0$. Wähle nun in (H_2) $b = 0$ und $c = d - a$. Wegen $b^2 - 4ac = -4a(d - a) < 0$ kann $b^2 - 4ac$ kein Quadrat sein. Seien $x_0 = y_0 = 1$, dann sind die Annahmen von (H_2) erfüllt; somit existieren unendlich viele Primzahlen p und q derart, dass $ap^2 + d - a = dq$, daher

$$\frac{d}{a} = \frac{d}{a}\,q - p^2 + 1, \quad \text{daher} \quad r = \frac{p^2-1}{q-1}. \qquad \square$$

Und nun zum angekündigten Satz

(H_4) *Es gibt unendlich viele Tripel (a, b, c) positiver ganzer Zahlen derart, dass $a^2 + b^2 = c^2$ und a und c Primzahlen sind.*

Beweis, dass (H_4) **aus** (H_3) **folgt.** Sei $r = 2$. Nun gibt es unendlich viele Primzahlen p und q mit $2 = (p^2 - 1)/(q - 1)$, daher $p^2 = 2q - 1$ und somit $p^2 + (q - 1)^2 = q^2$. $\square$

Die Tripel $(3, 4, 5)$ und $(5, 12, 13)$ sind pythagoreische Tripel mit zwei Primzahlen, im obigen Sinne, die durch die Primzahl 5 verbunden sind. Die folgende Frage wurde von Dubner untersucht, der mir seine Ergebnisse 1999 mitteilte.

Ich führe den Begriff einer *Dubner-Kette* pythagoreischer Tripel ein. Es handelt sich dabei um eine endliche (oder unendliche) Folge T_1, T_2, T_3, ... von pythagoreischen Dreiecken mit zwei Primzahlen, die in folgender Weise miteinander verbunden sind: Die Hypotenuse jeden Dreiecks ist die Kathete der nächsten. Soweit ich weiß, ist nicht bewiesen, dass Hypothese (H) die Existenz beliebig langer Dubner-Ketten zur Folge hat.

Da $a^2 + b^2 = c^2$ mit primem a, muss (a, b, c) ein primitives pythagoreisches Tripel sein, also $a = u^2 - v^2$, $b = 2uv$, $c = u^2 + v^2$. Damit a eine Primzahl sein kann, ist es notwendig, dass $u - v = 1$. Daraus folgt $b = 2v^2 + 2v$, $c = 2v^2 + 2v + 1$ und somit $c = b + 1$, analog zum Beweis, der zu (H_4) führte.

Daher werden die Dreiecke in einer Dubner-Kette mit wachsendem a immer dünner. Zudem ist $a^2 = (u+v)^2 = c+b = 2c-1$, so dass es notwendig ist, Primzahlen a derart zu finden, dass $c = (a^2+1)/2$ auch eine Primzahl ist.

Für $k = 2, 3, 4, 5$ und 6 bestimmte Dubner die kleinste Primzahl a, die zu einer Kette mit k Dreiecken führt:

k	Kleinstes a für k Dreiecke
2	3
3	271
4	169219
5	356498179
6	2500282512131

Es ist alles andere als einfach, lange Ketten von Dreiecken zu erzeugen, von denen man nachweisen kann, dass zwei Seiten wirklich Primzahlen sind. Dubner & Forbes (2001) konstruierten eine Dubner-Kette, die aus 7 Dreiecken besteht, wobei $a = 2185103796349763249$ und die Länge der letzten Hypotenuse eine Primzahl mit 2310 Stellen ist.

Die folgende Konsequenz aus (H_3) wurde mir von P.T. Mielke mitgeteilt. Sie betrifft Dreiecke mit ganzzahligen Seiten, aber nicht notwendigerweise rechtem Winkel.

(H_5) *Es gibt unendlich viele Dreiecke mit ganzzahligen Seiten a, p, q, wobei p, q Primzahlen sind und der Winkel zwischen den Seiten der Längen a, p im Bogenmaß $\pi/3$ (beziehungsweise $2\pi/3$) beträgt.*

Beweis, dass (H_5) **aus** (H_3) **folgt.** Nach (H_3) gibt es unendlich viele Primzahlpaare (p, q) derart, dass $4 = (p^2-1)/(q-1)$. Für jedes solche Paar ist $p > 2$ und $q = (p^2+3)/4$. Es sei $a = ((p-1)(p+3))/4$, so dass a eine ganze Zahl ist. Dann ist $a - p = ((p+1)(p-3))/4$ und

$$p^2 + a^2 - ap = p^2 + a(a-p) = p^2 + \frac{(p^2-1)(p^2-q)}{16} = \left(\frac{p^2+3}{4}\right)^2 = q^2.$$

Aus dem Kosinussatz folgt, dass der Winkel zwischen den Seiten mit den Längen a und p gleich $\pi/3$ ist. Der Beweis für den Winkel $2\pi/3$ verläuft ähnlich, hier nimmt man $a = ((p+1)(p-3))/4$. □

Immer noch im selben Artikel von 1958 stellte Sierpiński die folgende Vermutung auf:

(S) *Für jede ganze Zahl $n > 1$ seien die n^2 Zahlen $1, 2, \ldots, n^2$ auf folgende Weise wie in einer $n \times n$-Matrix aufgeschrieben:*

$$\begin{array}{cccc} 1 & 2 & \cdots & n \\ n+1 & n+2 & \cdots & 2n \\ 2n+1 & 2n+2 & \cdots & 3n \\ \vdots & \vdots & \vdots & \vdots \\ (n-1)n+1 & (n-1)n+2 & \cdots & n^2. \end{array}$$

Dann gibt es in jeder Zeile eine Primzahl.

In der ersten Zeile befindet sich auf jeden Fall die 2. Nach dem Satz von Bertrand und Tschebyscheff gibt es auch in der zweiten Zeile eine Primzahl.

Mit Hilfe einer stärkeren Form des Satzes von Bertrand und Tschebyscheff lässt sich auch für einige der folgenden Zeilen etwas aussagen. Beispielsweise zeigte Breusch 1932, dass für $n \geq 48$ zwischen n und $(9/8)n$ eine Primzahl existiert. Für $0 < k \leq 7$ und $n \geq 9$ gibt es daher eine Primzahl p mit $kn + 1 \leq p \leq (9/8)(kn + 1) \leq (k + 1)n$, was die Existenz einer Primzahl in jeder der ersten 8 Zeilen sichert.

Nach dem Primzahlsatz gibt es für jedes $h \geq 1$ ein $n_0 = n_0(h) > h$ mit der Eigenschaft, dass für $n \geq n_0$ eine Primzahl p mit $n < p < (1 + 1/h)n$ existiert. Und daraus folgt, dass es für $n \geq n_0$ in jeder der ersten h Zeilen des Feldes eine Primzahl gibt.

Wie bei den vorangegangenen Vermutungen zieht auch (S) einige interessante Konsequenzen nach sich.

(S_1) *Für jedes $n \geq 1$ gibt es mindestens zwei Primzahlen p und p' mit $n^2 < p < p' < (n + 1)^2$.*

(S_2) *Für jedes $n \geq 1$ gibt es mindestens vier Primzahlen p, p', p'', p''' mit $n^3 < p < p' < p'' < p''' < (n + 1)^3$.*

Beachtenswerterweise konnte bisher keine der Aussagen (S_1) und (S_2) ohne Zuhilfenahme von Vermutung (S) bewiesen werden. Es ist jedoch leicht zu zeigen, dass es für jedes genügend große n zwischen n^3 und $(n + 1)^3$ eine Primzahl p gibt; dies lässt sich durch Inghams Satz bewerkstelligen, der aussagt, dass $d_n = p_{n+1} - p_n = O\big(p_n^{(5/8)+\varepsilon}\big)$ für jedes $\varepsilon > 0$ gilt.

Schinzel stellte die folgende, „transponierte“ Form von Sierpińskis Vermutung auf:

(S′) *Für jede Zahl* $n > 1$ *seien die* n^2 *Zahlen* $1, 2, \ldots, n^2$ *in einem Feld mit* n *Zeilen und* n *Spalten angeordnet (genau wie in* (S)*). Wenn* $1 \leq k \leq n$ *und* $\mathrm{ggT}(k, n) = 1$*, dann enthält die* k*-te Spalte mindestens eine Primzahl.*

Diesmal zogen Schinzel & Sierpiński keine Schlüsse aus Vermutung (S′). Ich nehme an, es war Sonntagabend und sie waren müde. Wie auch immer, Kanold stellte 1963 die Vermutung ein zweites Mal auf.

Ich schließe mit der Übersetzung des folgenden Kommentars aus Schinzel & Sierpińskis Artikel:

> Wir kennen zwar das Schicksal unserer Vermutungen nicht, denken aber, dass selbst wenn sie widerlegt werden sollten, dies nicht ohne Nutzen für die Zahlentheorie geschieht.

III Polynome mit großen Bereichen zerlegbarer Werte

Ich möchte nun über einige Resultate von McCurley berichten, die ich sehr interessant fand. Gemäß Bunjakowskis Vermutung gibt es für ein irreduzibles Polynom $f(X)$ mit ganzzahligen Koeffizienten, das Bedingung (*) genügt, eine kleinste ganze Zahl $m \geq 1$ derart, dass $f(m)$ eine Primzahl ist. Diese sei mit $p(f)$ bezeichnet.

Wenn $f(X) = dX + a$ mit $d \geq 2$, $1 \leq a \leq d - 1$ und $\mathrm{ggT}(a, d) = 1$, dann existiert natürlich $p(f)$. Mit der Bezeichnung aus Kapitel 4, Abschnitt IV:

$$p(dX + a) = \frac{p(d, a) - a}{d}\,.$$

Man erinnere sich daran, dass Prachar und Schinzel untere Schranken für $p(d, a)$ angaben.

Die Arbeit von McCurley stellt eine Erweiterung der obigen Resultate für Polynome $f(X)$ beliebigen Grades dar. Ein wesentliches Werkzeug für McCurley war das folgende Ergebnis von Odlyzko (das in dem Artikel von Adleman, Pomerance & Rumely (1983), der in Kapitel 2 zitiert wurde, enthalten ist).

Es gibt eine absolute Konstante $C > 0$ und unendlich viele ganze Zahlen $d > 1$, die mindestens $e^{C \log d/(\log\log d)}$ Faktoren der Form $p-1$ haben, wobei p eine ungerade Primzahl ist.

Für jedes d wie oben seien $p_1, p_2, \ldots, p_r$ diejenigen ungeraden Primzahlen, für die $p_i - 1$ die Zahl d teilt. Sei $k = p_1 p_2 \cdots p_r - 1$ oder $k = 3p_1 p_2 \cdots p_r - 1$, so dass $k \equiv 1 \pmod 4$. Sei $f(X) = X^d + k$, dann ist $f(X)$ irreduzibel und erfüllt Bedingung (*). McCurley bewies 1984:

Es gibt eine Konstante $C' > 0$ derart, dass wenn m der Ungleichung $|m| < e^{C' \log d/(\log\log d)}$ genügt, $f(m)$ zerlegbar ist.

Im Beweis selbst wurde kein Polynom explizit angegeben. Allerdings entdeckte man durch Computersuche die folgenden Polynome (das erste Beispiel stammt von Shanks, 1971):

Tabelle 27. Polynome mit vielen initialen zerlegbaren Werten

$f(X)$	$f(m)$ ist zerlegbar für alle m bis
$X^6 + 1091$	3905
$X^6 + 82991$	7979
$X^{12} + 4094$	170624
$X^{12} + 488669$	616979

Der kleinste prime Wert des letzten Polynoms hat nicht weniger als 70 Stellen.

Mit Hilfe einer anderen Methode zeigte McCurley 1986:

Für jedes $d \geq 1$ gibt es ein irreduzibles Polynom $f(X)$ vom Grad d derart, dass die Bedingung (*) erfüllt ist und der Wert $|f(m)|$ für alle m mit

$$|m| < e^{C\sqrt{L(f)/(\log L(f))}},$$

zerlegbar ist.

In obiger Aussage bezeichnet $L(f)$ die Länge von $f(X) = \sum_{k=0}^{d} a_k X^k$, die durch $L(f) = \sum_{k=0}^{d} \|a_k\|$ definiert ist. Dabei ist $\|a_k\|$ die Anzahl der Stellen von $|a_k|$ in Binärdarstellung, wobei $\|0\| = 1$. Man beachte, dass dieses letzte Resultat sich auf Polynome beliebigen Grades anwenden lässt, der Beweis lieferte zudem explizit Polynome mit der gewünschten Eigenschaft.

McCurley bestimmte $p(X^d + k)$ für verschiedene Polynome. Aus seinen Tabellen notiere ich:

Tabelle 28. Polynome $X^d + k$ mit vielen initialen zerlegbaren Werten

d	m	$\max\{p(X^d + k) \mid k \leq m\}$
2	10^6	$p(X^2 + 576239) = 402$
3	10^6	$p(X^3 + 382108) = 297$
4	150000	$p(X^4 + 72254) = 2505$
5	10^5	$p(X^5 + 89750) = 339$

S.M. Williams untersuchte quadratische Polynome mit einem Leitkoeffizienten verschieden von 1 und teilte mir die Ergebnisse seiner Berechnungen von 1992 mit:

$$p(8X^2 + X + 564135) = 482$$
$$p(4X^2 + X + 530985) = 472$$
$$p(2X^2 + X + 931650) = 443$$
$$p(73X^2 + 7613) = 420.$$

IV Partitio Numerorum

Es ist sehr lehrreich, einmal durch die Arbeit *Partitio Numerorum*, III: *On the expression of a number as a sum of primes* von Hardy & Littlewood (1923) zu blättern. Darin findet sich ein in einem solchen Umfang erstmaliger Versuch, auf systematische Weise heuristische Formeln für die Verteilung von Primzahlen abzuleiten, die verschiedenen speziellen Bedingungen genügen.

Ich werde hier eine Auswahl der probabilistischen Vermutungen aus Hardy & Littlewoods Artikel unter Verwendung ihrer klassischen Bezeichnungen vorstellen. Die erste Vermutung bezieht sich auf Goldbachs Problem:

Vermutung A. *Jede genügend große gerade Zahl* $2n$ *ist die Summe von zwei Primzahlen. Die asymptotische Formel für die Anzahl der Darstellungen ist*

$$r_2(2n) \sim 2C_2 \frac{2n}{(\log 2n)^2} \prod_{\substack{p>2 \\ p|n}} \frac{p-1}{p-2} \ ,$$

mit

$$C_2 = \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right) = 0{,}66016\ldots .$$

Man beachte, dass C_2 gleich der Primzahlzwillingskonstanten aus Kapitel 4, Abschnitt III ist.

Die folgende Vermutung handelt von (nicht notwendigerweise aufeinander folgenden) Primzahlen mit einer gegebenen Differenz von $2k$, insbesondere von Primzahlzwillingen:

Vermutung B. *Für jede gerade Zahl $2k \geq 2$ gibt es unendlich viele Primzahlen p derart, dass auch $p + 2k$ prim ist. Für $x \geq 1$ sei*

$$\pi_{X,\,X+2k}(x) = \#\{p \text{ prim} \mid p + 2k \text{ ist prim und } p + 2k \leq x\}.$$

Dann gilt

$$\pi_{X,\,X+2k}(x) \sim 2C_2 \frac{x}{(\log x)^2} \prod_{\substack{p>2 \\ p|k}} \frac{p-1}{p-2}\,,$$

wobei C_2 die Primzahlzwillingskonstante ist.

Insbesondere ergibt sich für $2k = 2$ eine asymptotische Abschätzung für die Primzahlzwillingsfunktion aus Kapitel 4, Abschnitt III.

Vermutung E betrifft Primzahlen der Form $m^2 + 1$:

Vermutung E. *Es gibt unendlich viele Primzahlen der Form $m^2 + 1$. Für $x > 1$ sei*

$$\pi_{X^2+1}(x) = \#\{p \text{ prim} \mid p \leq x \text{ und } p \text{ hat die Form } p = m^2 + 1\}.$$

Dann gilt

$$\pi_{X^2+1}(x) \sim C \frac{\sqrt{x}}{\log x}\,,$$

wobei

$$C = \prod_{p\geq 3} \left(1 - \frac{(-1 \mid p)}{p-1}\right) = 1{,}3728134628\ldots$$

und $(-1 \mid p) = (-1)^{(p-1)/2}$ das Legendre-Symbol bezeichnet.

Die durch die Vermutung vorhergesagten Werte stimmen mit den tatsächlichen Werten von $\pi_{X^2+1}(x)$ im Wesentlichen überein, wie aus Tabelle 29 ersichtlich ist:

Tabelle 29. Primzahlen der Form m^2+1

x	$\pi_{X^2+1}(x)$	$C\sqrt{x}/\log x$	Verhältnis
10^6	112	99	0,8839
10^8	841	745	0,8858
10^{10}	6656	5962	0,8957
10^{12}	54110	49684	0,9182
10^{14}	456362	425861	0,9332
10^{16}	3954181	3726283	0,9424
10^{18}	34900213	33122517	0,9491
10^{20}	312357934	298102656	0,9544
10^{22}	2826683630	2710024144	0,9587

Die Tabellenwerte bis $x = 10^{14}$ wurden von Wunderlich bereits 1973 bestimmt. Die letzten vier Einträge wurden 2006 von H. Dubner und W. Keller errechnet.

Hier sei noch das folgende Resultat von Iwaniec (1978) erwähnt: Es gibt unendlich viele Zahlen m^2+1, die 2-Fastprimzahlen sind.

Und noch eine weitere Vermutung:

Vermutung F. *Es seien $a > 0$, b, c ganze Zahlen mit der Eigenschaft, dass $\mathrm{ggT}(a,b,c) = 1$, b^2-4ac kein Quadrat ist und $a+b$, c nicht gleichzeitig gerade sind. Dann gibt es unendlich viele Primzahlen der Form am^2+bm+c (dies war Aussage (B_1)). Die Anzahl $\pi_{aX^2+bX+c}(x)$ der Primzahlen am^2+bm+c kleiner als x ist asymptotisch gleich*

$$x_{aX^2+bX+c}(x) \sim \frac{\varepsilon C}{\sqrt{a}} \frac{\sqrt{x}}{\log x} \prod_{\substack{p>2 \\ p \mid \mathrm{ggT}(a,b)}} \frac{p}{p-1}$$

wobei

$$\varepsilon = \begin{cases} 1 & \text{falls } a+b \text{ ungerade,} \\ 2 & \text{falls } a+b \text{ gerade,} \end{cases}$$

$$C = \prod_{\substack{p>2 \\ p \nmid a}} \left(1 - \frac{\left(\dfrac{b^2-4ac}{p}\right)}{p-1} \right)$$

und $(b^2-4ac \mid p)$ das Legendre-Symbol bezeichnet.

Die Vermutung lässt sich insbesondere auf Primzahlen der Form m^2+k mit nichtquadratischem $-k$ anwenden.

Für den Spezialfall von Polynomen $f_A(X) = X^2 + X + A$ (mit ganzem $A \geq 1$) besagt Vermutung F, dass

$$\pi_{X^2+X+A}(x) \sim C(A)\,\frac{2\sqrt{x}}{\log x},$$

wobei

$$C(A) = \prod_{p>2} \left(1 - \frac{\left(\frac{1-4A}{p}\right)}{p-1}\right).$$

Man beachte, dass für ein Polynom $f_A(X)$ die Anzahl $\pi^*_{f_A(X)}(N) = \pi^*_{X^2+X+A}(N)$ (wie in Kapitel 3 definiert) von Werten $n \leq N$, die zu primen $f_A(n)$ führen, mit dem Wert von $\pi_{f_A(X)}(x)$ für $x = N^2$ nahe verwandt ist. In diesem Fall ergibt sich die asymptotische Formel

$$\pi^*_{X^2+X+A}(N) \sim \pi_{X^2+X+A}(N^2) \sim C(A)\,\frac{N}{\log N}\,.$$

Ein höherer Wert von $C(A)$ liefert also wahrscheinlich eine höhere Anzahl $\pi^*_{X^2+X+A}(N)$ von Primzahlen.

Shanks (1975) hatte berechnet, dass sich für $A = 41$ (was zu Eulers berühmtem Polynom führt) der Wert $C(41) = 3{,}3197732$ ergibt. Im Jahre 1990 ermittelten Fung & Williams $C(A)$ und $\pi^*_{X^2+X+A}(10^6)$ für viele A-Werte. Jacobson (1995) erweiterte diese Berechnungen.

Rekord

Das bisherige Maximum $C(A) = 5{,}5338891$ wurde bei einer 70-stelligen Zahl A festgestellt, veröffentlicht von Jacobson & Williams im Jahre 2003. In seiner Dissertation von 1995 ermittelte Jacobson

$$C(517165153168577) = 5{,}0976398,$$

dies ergibt

$$\pi^*_{X^2+X+517165153168577}(10^6) = 300923.$$

Der vorherige Rekord von Fung & Williams war

$$C(132874279528931) = 5{,}0870883,$$

mit

$$\pi^*_{X^2+X+132874279528931}(10^6) = 312975.$$

Das bisher maximale $\pi^*_{X^2+X+A}(10^6)$ ist

$$\pi^*_{X^2+X+21425625701}(10^6) = 361841$$

mit

$$C(21425625701) = 4{,}7073044.$$

Zum Vergleich:

$$\pi^*_{X^2+X+41}(10^6) = 261081 \quad \text{mit} \quad C(41) = 3{,}3197732,$$

sowie für ein Polynom, das N.G.W.H. Beeger 1939 untersucht hatte,

$$\pi^*_{X^2+X+27941}(10^6) = 286129 \quad \text{mit} \quad C(27941) = 3{,}6319998.$$

Partitio Numerorum enthält viele weitere Vermutungen, von denen ich nur noch erwähnen möchte:

Vermutung N. *Es gibt unendlich viele Primzahlen p der Form $p = k^3 + l^3 + m^3$, wobei k, l, m positive, ganze Zahlen sind.*

Diese Vermutung beinhaltet auch eine asymptotische Aussage für die Anzahl von Tripeln (k, l, m) mit $p \leq x$.

In einem vor wenigen Jahren (2001) erschienenen Artikel bewies Heath-Brown den Satz:

Es gibt unendlich viele Primzahlen p der Form $p = k^3 + 2l^3$, wobei k, l positive, ganze Zahlen sind.

Insbesondere erweist sich die Existenzaussage von Vermutung N als richtig; allerdings führte die Methode des Beweises nicht zur asymptotischen Abschätzung aus der Vermutung. Die Handhabung von Kuben ist ungleich schwieriger als die von Quadraten, so dass man den Satz von Heath-Brown wohl als substantiellen Fortschritt beim Problem der Darstellung von Primzahlen durch Binärformen feiern kann.

Die Vermutungen von Hardy und Littlewood gaben Anlass zu umfangreichen Berechnungen. Diese dienten einerseits der genauen Bestimmung der in den Formeln enthaltenen Konstanten, andererseits dem Vergleich der Voraussagen mit den tatsächlich auftretenden Werten. Da die Konstanten häufig durch langsam konvergierende unendliche Produkte gegeben waren, war es dabei unbedingt erforderlich, diese zunächst so zu modifizieren, dass die entstandenen Ausdrücke leichter zu berechnen waren.