On Prime Generating Sequences

Gottfried Wilhelm Leibniz University Hanover
Faculty of Mathematics and Physics
Institute of Algebra, Number Theory and Discrete Mathematics

Abstract

In this paper, we consider different kinds of sequences that generate prime numbers. We will have a closer look at some "natural" prime generating recurrences according to Eric Rowland's sequence $g(n) := a(n) - a(n-1)$ where $a(n) := \gcd(n, a(n-1))$ with $a(1) = 7$. This sequence has the interesting property that it takes on only 1's and primes. Following Rowland's proof, we will examine similar examples provided by Benoit Cloitre and Aldrich Stevens.

Author	Markus Schepke
Address	Goetheplatz 2, 30169 Hannover, Germany
Telephone	+49(0)511/10532040
eMail	markus.schepke@stud.uni-hannover.de
Adviser	Stefan Wewers

Contents

1 Introduction

We call a sequence f prime generating, if it takes on only primes, i. e. $f : \mathbb{N} \to \mathbb{P}$. But why does one want to study such sequences? Primes in general have been drawing the interest of mathematicians for hundreds of years, since they are in a certain sense the "atoms" of our number system and bear important insights.

Unfortunately, the task of testing a given number for primality is extremely difficult; generally, their distribution appears to be entirely random. In fact, one can construct arbitrarily long prime gaps; one has only to regard the consecutive integers

$$(n+1)! + 2, \ldots, (n+1)! + (n+1),$$

which are divisible by $2, \ldots, n+1$ and thus not prime. On the other hand,

there are presumably infinitely many prime twins, that are gaps of the (minimal) length of 1. (We will return to this topic in section 3.2.2.) In other words: Once you know a prime number p_n, it is almost impossible to predict, how the next prime p_{n+1} looks like.

These thoughts make clear, why the prime counting function $\pi(x)$ is that challenging and worth studying at all. First of all let

$$\mathbb{P} := \{2, 3, 5, 7, 11, 13, 17, \ldots\} = \{p_1, p_2, p_3, \ldots\}$$

denote the set of prime numbers. It is known since Euclid that it is infinite. With this, we define the function

$$\pi : \mathbb{R} \longrightarrow \mathbb{N}, \quad x \longmapsto \pi(x) := \sum_{\substack{p \in \mathbb{P} \\ p \leq x}} 1 = \#\{p \in \mathbb{P} : p \leq x\},$$

i. e. a function counting the prime numbers below a given border. The most famous result concerning $\pi(x)$ is the following one, known as the *prime number theorem*, where log as usual denotes the natural logarithm to the base e:

$$\boxed{\pi(x) \sim \frac{x}{\log x}} \qquad \left(\Leftrightarrow \lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1\right). \tag{1}$$

Carl Friedrich Gauss and Adrien-Marie Legendre conjectured this independently in 1793 respectively 1798. Pafnuti Tschebyschow made important progress in 1851; the prime number theorem was finally proven by Jacques Hadamard and Charles-Jean de La Vallée Poussin in 1896. They used the means of function theory heavily (in particular a weak version of the Riemann hypothesis); a proof with more "elementary" methods was published by Atle Selberg [Sel49] and Paul Erdős [Erd49] in 1949. (For the history of the prime number theorem see [dS06, p. 64–78, 133–136, 210–217].)

This leads to the question: *Are there any explicit formulae or sequences easily calculated that deliever prime numbers?*

An example of such a formula was provided by Leonhard Euler: The polynomial

$$p(x) := x^2 - x + 41 \tag{2}$$

generates primes by the first 40 integer values, that is $p(n) \in \mathbb{P}$ for $n \in \{1, \ldots, 40\}$. However, it is clear that $p(41) = 41^2$ and generally $p(n) \notin \mathbb{P}$ for infinitely many integers n. Thus, polynomials are not suitable for prime generating sequences as we will see in theorem 2.3. Euler's polynomial will reappear in section 3.3; for the moment we will consider more common mappings. The next section deals with the possible shapes of such functions.

2 Various kinds of prime generating sequences

In his book [Rib06, Kap. 3] PAULO RIBENBOIM provides three classes of functions $f(n)$ representing primes:

(*i*) $f(n) = p_n$ for all integers n.

(*ii*) $f(n)$ takes on distinct primes.

(*iii*) The set of positive values of $f(n)$ equals the set of primes.

We will see examples for all three classes which are virtually of no use to generate new prime numbers, but they are nevertheless interesting from a theoretically point of view.

2.1 Formulae for the nth prime p_n

Regarding the random distribution of the prime numbers it may be suprising that there are explicit formulae for the nth prime number p_n at all. Still, they use only some well-known properties of primes, such as the sieve of ERATOSTHENES or MÖBIUS's μ-function. Usually the formulae we receive are quite complicated and improper for calculations.

2.1.1 Formulae depending on n

First of all we want to repeat a criterion for prime numbers that will help to construct a formula for p_n.

Theorem 2.1 (Wilson's Theorem)
Let $n \geq 2$ be an integer. Then:

$$\boxed{(n-1)! \equiv -1 \mod n \quad \Longleftrightarrow \quad n \in \mathbb{P}}$$

In first sight this theorem seems to be quite satisfying for it delivers a necessary and adequite criterion for primality. Of course it is useless for concrete examinations as the expression $(p-1)!$ rises beyond the possibilty of computations for primes in the scale of today's primes. (The largest known prime has more than 10^7 digits.) However, Wilson's theorem applies in a wide theoretical range, some of which we look at now.

Oddly enough, this theorem named after JOHN WILSON has been neither discovered nor proven by him. It was first mentioned by the Arabic mathematician IBN AL-HAYTHAM (ca. 965–1040); EDWARD WARING published it in 1770 and ascribed it to his student Wilson. The first proof was finally given by JOSEPH LOUIS LAGRANGE in 1773 [Bun02, p. 102–103].

Using Wilson's theorem it follows that $((j-1)!+1)/j$ with $j \geq 2$ is an integer, if and only if j is prime; in the composite case the term is fractional. With that we are able to give an explicit formula for $\pi(n)$. The decisive step is the construction of a term for the characteric function (???) of the prime numbers, i. e.

$$\chi_{\mathbb{P}}(n) = \begin{cases} 1 & \text{for } n \in \mathbb{P}, \\ 0 & \text{for } n \notin \mathbb{P}. \end{cases}$$

We give three examples here; two origin from C. P. WILLANS [Wil64], the last one comes from JÁN MINÁČ, first published in Ribenboim's book [Rib06, p. 136–137]:

Proposition 2.2
Let $n \geq 2$ be an integer. Then:[1]

$$\chi_{\mathbb{P}}(n) = \begin{cases} F(n) & := & \left\lfloor \cos^2 \pi \frac{(n-1)!+1}{n} \right\rfloor, \\ H(n) & := & \frac{\sin^2 \pi \frac{((n-1)!)^2}{n}}{\sin^2 \frac{\pi}{n}}, \\ M(n) & := & \left\lfloor \frac{(n-1)!+1}{n} - \left\lfloor \frac{(n-1)!}{n} \right\rfloor \right\rfloor, \end{cases}$$

where $\lfloor \cdot \rfloor$ denotes the Gauß bracket (???)[2]*, i. e. the largest integer below a given float (???) number.*

BEWEIS: Die erste Identität $F(n) = \chi_{\mathbb{P}}(n)$ folgt unmittelbar aus den oben genannten Folgerungen aus dem Satz von Wilson, zusammen mit der Eigenschaft der Kosinusfunktion, welche für ganzzahlige Vielfache von π die Werte 1 bzw. -1 annimmt und ansonsten dazwischen verläuft. Ähnlich argumentiert man bei H; für die Details verweise ich auf den Artikel von Willans [Wil64].

Für M überlegt man sich zunächst, dass $(n-1)!$ für ein zusammengesetztes $n > 4$ immer durch n teilbar ist: Entweder n lässt sich in zwei verschiedene

[1] In this place the symbol π means both the circle number (???) and the prime counting function. Nevertheless, there is no danger in mixing them up as the circle number is always used without parameter.

[2] As there will be both floor and ceil functions in this paper, I will use the more intuitive $\lfloor \cdot \rfloor$ instead of the more common notation $[\cdot]$ for the Gauß bracket.

Faktoren a und b zerlegen, d. h. $n = ab$ mit $1 < a < b < n$, und beide Faktoren $a,\ b$ tauchen in $(n-1)!$ auf, oder $n = p^2$ für eine Primzahl $p > 2$. Dann ist $2p \leq p^2 - 1 = n - 1$. Damit tauchen die Faktoren p und $2p$ in $(n-1)!$ auf, weshalb $n = p^2 \mid 2p^2$ und $2p^2 \mid (n-1)!$ gilt. Insgesamt folgt für ein zusammengesetztes $n > 4$:

$$\begin{aligned} M(n) &= \left\lfloor \frac{(n-1)!+1}{n} - \left\lfloor \frac{(n-1)!}{n} \right\rfloor \right\rfloor \\ &\overset{2.1}{=} \left\lfloor \frac{(n-1)!+1}{n} - \frac{(n-1)!}{n} \right\rfloor = \left\lfloor \frac{1}{n} \right\rfloor = 0. \end{aligned}$$

Es bleibt der Fall $n = 4$: $M(4) = \lfloor 7/4 - \lfloor 6/4 \rfloor \rfloor = \lfloor 3/4 \rfloor = 0$.

Ist andererseits n eine Primzahl, so gibt es nach dem Satz von Wilson eine ganze Zahl k mit $(n-1)! + 1 = kn$. Somit folgt:

$$\begin{aligned} M(n) &= \left\lfloor \frac{(n-1)!+1}{n} - \left\lfloor \frac{(n-1)!}{n} \right\rfloor \right\rfloor \overset{2.1}{=} \left\lfloor \frac{kn}{n} - \left\lfloor \frac{kn-1}{n} \right\rfloor \right\rfloor \\ &= \left\lfloor k - \left\lfloor k - \frac{1}{n} \right\rfloor \right\rfloor = \lfloor k - (k-1) \rfloor = 1. \end{aligned}$$

Damit sind alle Formeln bewiesen. □

Es folgt unmittelbar

$$\boxed{\pi(n) = \sum_{j=2}^{n} F(j) = \sum_{j=2}^{n} H(j) = \sum_{j=2}^{n} M(j),} \tag{3}$$

da die Summen dieselben wie in der Definition der π-Funktion sind. Insgesamt haben wir nun drei Formeln für $\pi(n)$ zur Verfügung. Da die Primzahlen damit exakt gezählt werden, sind beim Übergang von p_n zu $\pi(n)$ keine Informationen verloren gegangen. Deswegen ist es leicht einzusehen, dass sich aus einer Formel für die Primzahlfunktion auch eine für die n-te Primzahl konstruieren lässt.

Dafür bemerkt Willans zunächst, dass für $a \in \mathbb{N}_0$ und $n \in \mathbb{N}$ gilt:

$$A_n(a) := \left\lfloor \sqrt[n]{\frac{n}{1+a}} \right\rfloor = \begin{cases} 1 & \text{für } a < n, \\ 0 & \text{für } a \geq n. \end{cases}$$

Setzt man nun $a = \pi(m)$, so liefert der Ausdruck $A_n(\pi(m))$ solange 1, wie $\pi(m)$ kleiner als n ist. Offensichtlich ist $\pi(p_n) = n$, also ist $A_n(\pi(m)) = 0$ für

$m \geq p_n$. Summiert man über alle Zahlen bis p_n auf, erhält man die Formel

$$\boxed{p_n = 1 + \sum_{m=1}^{2^n} \left\lfloor \sqrt[n]{\frac{n}{1+\pi(m)}} \right\rfloor}, \tag{4}$$

wobei als obere Grenze 2^n gewählt wurde, da stets $p_n \leq 2^n$ gilt. Dies ist eine leichte Folgerung aus Bertrands Postulat[3]: Demnach gilt

$$p_n \leq 2 \cdot p_{n-1} \leq 2^2 \cdot p_{n-2} \leq \ldots \leq 2^{n-1} \cdot p_1 = 2^n.$$

Freilich ist diese Schranke im Allgemeinen sehr schlecht; bessere Abschätzungen ergeben sich aus dem Primzahlsatz (1).

Sicherlich wäre es leichter, einfach mithilfe der konstruierten Formeln sukzessive die Werte $\chi_{\mathbb{P}}(n)$ für $n = 1, 2, 3 \ldots$ auszurechnen, jedoch erfüllt dieses Vorgehen natürlich nicht die Forderung nach einer geschlossenen Formel für p_n.

Godfrey Harold Hardy und Edward Maitland Wright liefern in ihrem Buch [HW79, p. 414] einen anderen Ausdruck, der dasselbe leistet wie A_n. Dazu sei B_n für $n \neq a$ durch

$$B_n(a) := \frac{1}{2}\left(1 + \frac{n-a}{|n-a|}\right)$$

und für $n = a$ durch $B_n(n) = 0$ definiert. Dieser Term kommt zwar ohne Wurzeln und Gaußklammern aus, hat dafür aber den Nachteil der stückweisen Definition.

Einen gänzlich anderen Zugang [HW79, p. 344–345] wählen diese beiden Mathematiker durch die Definition der Konstante

$$\alpha := \sum_{m=1}^{\infty} p_m 10^{-2^m} = 0{,}020300050000000700000000000000011000\ldots$$

Es ist leicht einzusehen, dass damit die Formel

$$\boxed{p_n = \left\lfloor 10^{2^n} \alpha \right\rfloor - 10^{2^{n-1}} \left\lfloor 10^{2^{n-1}} \alpha \right\rfloor} \tag{5}$$

für die n-te Primzahl folgt. Solange jedoch keine effiziente Berechnung für α bekannt ist, erhält man aus diesem Ausdruck nur die Informationen zurück, die man vorher hineingesteckt hat.

[3] Joseph Bertrand behauptete 1845, dass es zu jeder natürlichen Zahl $n \geq 1$ eine Primzahl p mit $n < p \leq 2n$ gibt. Er konnte keinen Beweis dafür erbringen; diesen lieferte Tschebyschow 1850 nach [AZ04, p. 7–13]. Obwohl die Aussage damit zu einem gültigen Satz wurde, ist sie nach wie vor als *Bertrands Postulat* bekannt.

2.1.2 Formeln in Abhängigkeit von p_i

Neben der Frage nach einem Ausdruck für die n-te Primzahl p_n suchten Hardy und Wright [HW79, p. 5–7] eine weitere Formel, die aus $p_1, \ldots, p_n$ die nächste Primzahl p_{n+1} berechnet. Auch dafür liefert Willans eine Antwort, sogar unter der schwächeren Voraussetzung, dass nur p_n bekannt ist. Zunächst gilt für $n \geq 2$:

$$1 - \chi_{\mathbb{P}}(n) = \chi_{\mathbb{N}\setminus\mathbb{P}}(n) = \begin{cases} 0 & \text{für } n \in \mathbb{P}, \\ 1 & \text{für } n \notin \mathbb{P}. \end{cases}$$

Kennt man jetzt eine Primzahl p_n, muss man so lange weiterzählen, bis man auf die nächste Primzahl p_{n+1} trifft. Dies löste Willans so:

$$\boxed{p_{n+1} = 1 + p_n + \sum_{i=1}^{p_n} \left(\prod_{j=1}^{i} \left(1 - \chi_{\mathbb{P}}(p_n + i)\right) \right),} \tag{6}$$

wobei als obere Grenze der Summe p_n gewählt wurde, weil nach Bertrands Postulat $p_n < p_{n+1} < 2p_n$ gelten muss. Für $\chi_{\mathbb{P}}$ kann jetzt natürlich eine der Formeln F, H oder M verwendet werden, die wir oben betrachtet haben.

Doch wie funktioniert diese Formel? Für jede unmittelbar auf p_n folgende zusammengesetzte Zahl $p_n + i < p_{n+1}$ ergibt das Produkt 1, nach der ersten Primzahl hingegen sind alle Summanden 0. Somit zählt dieser Ausdruck genau bis p_{n+1}. Allerdings wäre es ebenso wie in den obigen Fällen einfacher, dies direkt zu tun, ohne die Summe zu bemühen.

Mit noch weniger Voraussetzungen kommt die Formel von Reijo Ernvall [Ern75] aus, welche die nächste Primzahl liefert, die unmittelbar auf eine *beliebige* natürliche Zahl $m \geq 2$ folgt. Dafür definiert man zunächst die Ausdrücke

$$\begin{aligned} d &:= \gcd\left((m!)^{m!} - 1, (2m)!\right) \quad \text{und} \\ t &:= \frac{d^d}{\gcd(d^d, d!)}. \end{aligned}$$

Bezeichnet man jetzt mit a diejenige Zahl, sodass $d^a \mid t$, aber $d^{a+1} \nmid t$ gilt, ist die kleinste Primzahl $p > m$ gegeben durch

$$\boxed{p = \frac{d}{\gcd(t/d^a, d)}.} \tag{7}$$

Die Ausdrücke $(m!)^{m!}$ und d^d sind schon für kleine Werte von m unmöglich auszurechnen, daher ist diese Formel, so reizvoll ihr Anspruch auch ist, nur von theoretischem Interesse.

Einen anderen Weg, der neben den Primzahlen $p_1, \ldots, p_{n-1}$ auch die Eigenschaften der μ-Funktion ausnutzt, beschritt J. M. Gandhi [Gan71]. Dabei ist die Möbiusfunktion für $n \in \mathbb{N}$ definiert als

$$\mu(n) = \begin{cases} 1, & \text{für } n = 1, \\ (-1)^r, & \text{für } n = p_{i_1} \cdots p_{i_r} \text{ quadratfrei}, \\ 0, & \text{für } n \text{ nicht quadratfrei.} \end{cases}$$

Mit der Bezeichnungsweise $P_{n-1} = p_1 \cdot p_2 \cdots p_{n-1}$ gilt dann:

$$\boxed{p_n = \left\lfloor 1 - \log_2 \left(-\frac{1}{2} + \sum_{d \mid P_{n-1}} \frac{\mu(d)}{2^d - 1} \right) \right\rfloor .} \tag{8}$$

Vereinfachte Beweise wurden in der Folge von Charles Vanden Eynden [VE72] und Solomon Golomb [Gol74] vorgelegt, die zugleich auch neue Einsichten in diese Formel boten. Jedoch ist die μ-Funktion im Allgemeinen nur mithilfe der Primfaktorzerlegung einer Zahl zu berechnen, daher ist auch dieser Ausdruck sehr schwer zu handhaben.

Wegen der großen Fakultäten bzw. der Gaußklammern sind all diese Ausdrücke ohnehin für praktische Berechnungen ungeeignet, doch eine "'elementare"' geschlossene Formel für p_n ist nicht in Sicht und wegen der Unregelmäßigkeiten innerhalb der Primzahlen auch nicht zu erwarten. Daher muss man sich darauf beschränken, andersartige Folgen zu finden, die möglichst viele Primzahlen enthalten.

2.2 Folgen, die in jedem Schritt eine Primzahl liefern

Wie bereits in der Einleitung angeführt, kann man mithilfe von Polynomen lange Reihen von Primzahlen erzeugen, jedoch niemals *ausschließlich*. Genauer gilt das folgende Resultat von Christian Goldbach [Rib06, p. 142–143]:

Lemma 2.3
Sei $f \in \mathbb{Z}[x]$ ein nichtkonstantes Polynom. Dann nimmt $|f(n)|$ für unendlich viele Argumente $n \in \mathbb{Z}$ zusammengesetzte Werte an.

BEWEIS: Sei zunächst $f = a_m x^m + \ldots + a_0 \in \mathbb{Z}[x]$ ein nichtkonstantes Polynom. O. B. d. A. gebe es ein $n_0 > 0$ mit $f(n_0) = p \in \mathbb{P}$. (Sonst sind wir bereits fertig.) Wegen $\lim_{n\to\infty} |f(n)| = \infty$ gibt es ein $n_1 > n_0$, sodass $|f(n)| > p = f(n_0)$ für alle $n \geq n_1$. Wählt man jetzt also ein h mit $n_0 + ph \geq n_1$, so folgt mit dem binomischen Lehrsatz:

$$\begin{aligned} f(n_0 + ph) &= a_m(n_0 + ph)^m + \ldots + a_1(n_0 + ph) + a_0 \\ &= a_m \sum_{k=0}^{m} \binom{m}{k} n_0^k (ph)^{m-k} + \ldots + a_1 n_0 + a_1 ph + a_0 \\ &= f(n_0) + \left(\sum_{k=0}^{m-1} \binom{m}{k} n_0^k (ph)^{m-k} + \ldots + a_1 ph \right) \\ &= f(n_0) + jp = p + jp = (1 + j)p \end{aligned}$$

für ein geeignetes $j \in \mathbb{Z}$. Somit gilt $p \mid f(n_0 + ph)$ mit $f(n_0 + ph) > p$, also ist $f(n_0 + ph)$ für unendlich viele Werte von h zusammengesetzt. □

Will man also Funktionen konstruieren, die Ribenboims zweiter Bedingung genügen, kommt man mit Polynomen nicht weiter. Die Beispiele sind dünn gesät; interessant ist jedoch folgendes Resultat von WILLIAM MILLS [Mil47].

Theorem 2.4
Es gibt eine reelle Zahl $\vartheta \in \mathbb{R}$, sodass $\left\lfloor \vartheta^{3^n} \right\rfloor$ für alle $n \in \mathbb{N}$ eine Primzahl ist.

BEWEIS: Es ist nicht sehr schwer, die Aussage zu beweisen; die Argumentation benutzt jedoch das folgende Resultat von ALBERT EDWARD INGHAM [Ing37]: Es gibt eine positive Konstante $C \in \mathbb{R}$ mit

$$p_{n+1} < p_n + C \cdot p_n^{5/8} \quad \text{für alle } n \in \mathbb{N}. \tag{9}$$

Sei nun $N > C^8$ eine natürliche Zahl. Da N^3 keine Primzahl sein kann, gibt es Primzahlen p_n und p_{n+1} mit $p_n < N^3 < p_{n+1}$. Dann gilt:

$$N^3 < p_{n+1} \overset{(9)}{<} p_n + C p_n^{5/8} < N^3 + C(N^3)^{5/8} < N^3 + N^{1/8} N^{15/8} < (N+1)^3 - 1.$$

Somit folgt unmittelbar, dass es eine Primzahl p geben muss mit

$$N^3 < p < (N+1)^3 - 1. \tag{10}$$

Wählt man jetzt eine Primzahl P_0 mit $P_0 > C^8$, so kann man durch wiederholte Anwendung der Ungleichung (10) eine Folge P_j mit $P_n^3 < P_{n+1} <$

$(P_n+1)^3-1$ konstruieren. Seien nun $u_n := P_n^{3^{-n}}$ und $v_n := (P_n+1)^{3^{-n}}$. Dann gilt:

$$v_n > u_n, \tag{11}$$
$$u_{n+1} = P_{n+1}^{3^{-n-1}} > (P_n^3)^{3^{-n-1}} = P_n^{3^{-n}} = u_n, \tag{12}$$
$$v_{n+1} = (P_{n+1}+1)^{3^{-n-1}} < ((P_n+1)^3)^{3^{-n-1}} = (P_n+1)^{3^{-n}} = v_n, \tag{13}$$

also insgesamt $u_0 < u_n < u_{n+1} < v_{n+1} < v_n < v_0$. Somit ist klar, dass u_n eine monoton wachsende (12) und beschränkte (11 und 13) Folge ist und deswegen gegen $\vartheta := \lim_{n\to\infty} u_n \in \mathbb{R}$ konvergiert. Insbesondere gilt mit den obigen Ungleichungen $u_n < \vartheta < v_n$ bzw. $P_n = u_n^{3^n} < \vartheta^{3^n} < v_n^{3^n} = P_n + 1$, woraus $\left\lfloor \vartheta^{3^n} \right\rfloor = P_n \in \mathbb{P}$ folgt. □

So überraschend das Ergebnis auf den ersten Blick sein mag, zeigt der Beweis doch, dass für die Konstruktion von ϑ zunächst die Kenntnis der Primzahlen P_j nötig ist, die wir dann aus der Formel erhalten. Dennoch hat Mills' Idee viele weitere Resultate nach sich gezogen [Dud69]. Aber verglichen mit dem sehr eleganten Beweis ist die Abschätzung (9) von Ingham alles andere als elementar. Jedoch kann sie durch Bertrands Postulat ersetzt werden. Damit bewies Wright [Wri51] die folgende Variante von Mills' Folge:

Theorem 2.5
Es gibt eine positive Zahl $\omega \in \mathbb{R}$, sodass $\lfloor w_n \rfloor$ mit $w_0 = \omega$ und $w_n = 2^{w_{n-1}}$ für alle $n \in \mathbb{N}$ eine Primzahl ist.

Abschließend sei noch erwähnt, dass es unter der Annahme der Riemann'schen Vermutung möglich ist, den kleinstmöglichen Wert für ϑ bestimmen. Er liegt bei $\vartheta \approx 1{,}3063778838\ldots$ und wird *Mills' Konstante* genannt.

2.3 Folgen, deren positiver Wertebereich mit den Primzahlen übereinstimmt

Überraschenderweise gibt es "'einfache"' Funktionen der dritten Bauart, also Funktionen, die ohne Gaußklammern, Fakultäten und riesige Exponenten auskommen. Man muss auch gar nicht allzu tief in der Mathematik suchen, denn es genügen bereits Polynome, allerdings in mehreren Veränderlichen. Dies ist umso erstaunlicher, wenn man bedenkt, dass man Goldbachs Aussage aus Lemma 2.3 über die Primzahlwerte von Polynomen in einer Veränderlichen in ähnlicher Weise für Polynome mit komplexen Koeffizienten in mehreren Variablen formulieren kann. Lässt man jedoch die Forderung fallen,

dass alle Funktionswerte dem Betrage nach Primzahlen sind, und betrachtet nur den positiven Wertebereich, kann man tatsächlich Primzahlpolynome finden. Dies besagt das folgende Resultat von Martin Davis, Yuri Matijasevič, Hilary Putnam und Julia Robinson [DPR61, Mat70, Put60]:

Theorem 2.6
Es gibt ein Polynom in $\mathbb{Z}[x_1, \ldots, x_n]$, dessen positiver Wertebereich mit den Primzahlen zusammenfällt.

Dabei nehmen die Polynome auch negative Werte an, aber dies ist kein Widerspruch zu den geforderten Eigenschaften. Die Größenordnung der Anzahl n der Variablen und des Grades d des Polynoms kann dabei sehr unterschiedlich sein. Es gibt Beweise über Polynome mit $n = 42,\ d = 5$, aber auch mit $n = 10,\ d \approx 1{,}6 \cdot 10^{45}$ [Mat77]. Vielfach gibt es nur Aussagen über die Existenz solcher Polynome, für $n = 26,\ d = 25$ möchte ich dem geneigten Leser aber ein explizites Beispiel nicht vorenthalten, das von James Jones, Daihachiro Sato, Hideo Wada und Douglas Wiens [JSWW76] vorgelegt wurde:

$$
\begin{aligned}
&(k+2)(1-(wz+h+j-q)^2-((gk+2g+k+1)(h+j)+h-z)^2\\
&-(2n+p+q+z-e)^2-(16(k+1)^3(k+2)(n+1)^2+1-f^2)^2\\
&-(e^3(e+2)(a+1)^2+1-o^2)^2-((a^2-1)y^2+1-x^2)^2\\
&-(16r^2y^4(a^2-1)+1-u^2)^2\\
&-(((a+u^2(u^2-a))^2-1)(n+4dy)^2+1-(x+cu)^2)^2\\
&-(n+l+v-y)^2-((a^2-1)l^2+1-m^2)^2-(ai+k+1-l-i)^2\\
&-(p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m)^2\\
&-(q+y(a-p-1)+s(2ap+sa-p^2-2p-2)-x)^2\\
&-(z+pl(a-p)+t(2ap-p^2-1)-pm)^2).
\end{aligned}
$$

Bemerkenswert ist noch, dass diese Resultate durch David Hilberts zehntes Problem[4] motiviert wurden, das nach der Existenz eines Algorithmus fragt, der entscheiden kann, ob eine gegebene diophantische Gleichung (also polynomiale Ausdrücke in mehreren ganzzahligen Variablen) eine Lösung besitzt oder nicht. Robinson und Matijasevič konnten schließlich zeigen, dass solch ein Algorithmus nicht existiert. Diese Resultate konnten letztlich dazu genutzt werden, um die oben genannte Aussage über Primzahlen zu gewinnen [dS06, p. 240–251]. Allerdings sind diese Polynome nichts weiter als

[4] In seinem berühmten Vortrag anlässlich des Internationalen Mathematikerkongresses 1900 in Paris formulierte Hilbert eine Liste der (seiner Meinung nach) 23 wichtigsten ungelösten Probleme der Mathematik, welche die mathematische Forschung des 20. Jahrhunderts nachhaltig beeinflusste [Hil00].

Primzahltests, die in die Sprache der Polynome übersetzt wurden; die Berechnung neuer Primzahlen mithilfe solcher Ausdrücke ist also nicht leichter als mit klassischen Methoden.

2.4 Zusammenfassung

Betrachtet man die hier besprochenen Beispiele, macht sich eine gewisse Ernüchterung breit. Allen Formeln ist gemein, dass sie zu dem Zwecke konstruiert wurden, Primzahlen zu erzeugen. Daher sind sie in der Regel extrem schwer zu berechnen; teilweise musste man zudem die zu berechnenden Primzahlen bereits in die Konstruktion der Formel hineinstecken. Will man also größere Primzahlen gewinnen, ist es leichter, auf das Sieb des Eratosthenes zurückzugreifen.

Es drängt sich die Frage auf: Gibt es eine "'natürliche"' Bildungsvorschrift, die nicht dazu konstruiert wurde, Primzahlen zu erzeugen, es aber trotzdem tut? Tatsächlich wurden in jüngster Zeit einige Formeln entdeckt, die das Gewünschte leisten und dennoch einfach zu berechnen sind. Einige Beispiele für solche Folgen sollen im nächsten Abschnitt untersucht werden.

3 Beispiele für natürliche primzahlerzeugende Folgen

Eines der ältesten Erkenntnisse über ganze Zahlen ist der Euklidische Algorithmus. Dieser liefert ein effizientes Verfahren zur Bestimmung des größten gemeinsamen Teilers (gcd) zweier Zahlen, das ohne Faktorisierung auskommt und dennoch etwas über die Primfaktorzerlegung der beteiligten Zahlen aussagt. Daher ist der Versuch, primzahlerzeugende Folgen mithilfe des gcd zu konstruieren, durchaus vielversprechend – umso mehr mag es überraschen, dass dieser Versuch bislang nicht unternommen wurde (mit Ausnahme von Ernvalls Formel (7), die den Nachteil astronomisch großer Zahlen hat).

In den letzten Jahren wurden jedoch einige bemerkenswerte Eigenschaften solcher Folgen entdeckt, die in diesem Abschnitt zusammengetragen werden sollen.

Sequence 3.1 Die ersten Werte von $g(n)$ mit der Startbedingung $a(1) = 7$ (A132199 in OEIS).

1, 1, 1, 5, 3, 1, 1, 1, 1, 11, 3, 1, 1, 1, 1, 1, 1, 1, 1, 1, 23, 3, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 47, 3, 1, 5, 3, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 101, 3, 1, 1, 7,
1, 1, 1, 1, 11, 3, 1, 1, 1, 1, 1, 13, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 233, 3, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 467, 3, 1, 5, 3, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, ...

3.1 Rowlands Primzahlfolge

Den Anfang macht die Folge $a(n)$ von Eric Rowland, die rekursiv durch

$$\boxed{a(n) := a(n-1) + \gcd(n, a(n-1))} \tag{14}$$

definiert ist. Folgen dieser Art hat Rowland in seinem Artikel [Row08] untersucht und dabei bewiesen, dass die Folge der Differenzen

$$g(n) := a(n) - a(n-1) = \gcd(n, a(n-1)) \tag{15}$$

für den Startwert $a(1) = 7$ nur aus Einsen und Primzahlen besteht (vgl. Folge 3.1). Obwohl wegen des gcd bereits Faktorisierung in der Definition enthalten ist, scheint zunächst keineswegs klar, warum $g(n)$ keine zusammengesetzten Werte annehmen soll.

Die Folge, die wir enthalten, genügt in gewissem Sinne der Bedingung (ii) aus Abschnitt 2. Zwar enthält sie lange Abschnitte mit Einsen, doch deren Länge ist determiniert und kann daher von vorneherein übersprungen werden. Allerdings geschieht dies im Wesentlichen durch Faktorisierung, also zum Preis einer wesentlich schwereren Berechnung. Darüber hinaus sind die Primzahlen, die wir durch diese verkürzte Folge erhalten, nicht alle verschieden. Zudem verlangt die Berechnung großer Werte von $a(n)$ auch viel Rechnerarbeit (jeder Primzahl p gehen $\frac{p-3}{2}$ Folgenglieder mit Wert 1 voraus, wie wir in Lemma 3.1 sehen werden), sodass auch diese Folge nicht dazu geeignet ist, schnell zu großen Primzahlen zu gelangen. Dennoch lohnt sich das Studium dieser Rekursion, zumal die Beweisführung recht elementar ist

– unser wichtigstes Hilfsmittel wird sein, dass ein gemeinsamer Teiler von zwei Zahlen auch jede Linearkombination dieser Zahlen teilt.

3.1.1 Die Struktur der Rekursion

Zunächst wollen wir ein Lemma beweisen, aus dem dann unmittelbar die Behauptung folgt.

Lemma 3.1
Seien $r \in \{2, 3\}$, $n_1 \geq \frac{3}{r-1}$ *und* $a(n_1) = rn_1$. *Die Folge* $a(n)$ *genüge der Rekursion (14) für* $n > n_1$ *und* n_2 *sei der kleinste Index größer* n_1 *mit* $g(n_2) \neq 1$. *Sei ferner* p *der kleinste Primteiler von*

$$a(n_1) - (n_1 + 1) = rn_1 - n_1 - 1 = (r-1)n_1 - 1,$$

dann gilt:

(i) $a(n) = rn_1 + n - n_1$ *für* $n_1 \leq n < n_2$,

(ii) $n_2 = n_1 + \frac{p-1}{r-1}$,

(iii) $g(n_2) = p$,

(iv) $a(n_2) = rn_2$.

Beweis: Im Folgenden sei $k := n_2 - n_1$. Zunächst ist $\frac{p-1}{r-1}$ eine natürliche Zahl: Für $r = 2$ ist dies klar, für $r = 3$ ist $(r-1)n_1 - 1$ ungerade, also auch der kleinste Primfaktor, weshalb $p-1$ gerade ist. Insbesondere versichert die Bedingung $n_1 \geq \frac{3}{r-1}$ die Existenz eines Primteilers p von

$$(r-1)n_1 - 1 \geq (r-1)\frac{3}{r-1} - 1 = 2.$$

Dass wiederum ein Index $n_2 > n_1$ mit $g(n_2) > 1$ existiert, wird durch diese Bedingung, zusammen mit $a(n_1) = rn_1$, gesichert. Dies schließt nämlich den Fall $a(n_1) = n_1 + 2$ aus, für den dann gelten würde:

$$a(n_1+1) = a(n_1) + \gcd(n_1+1, a(n_1)) = n_1 + 2 + \gcd(n_1+1, n_1+2) = n_1 + 3.$$

Das würde $g(n) = 1$ für alle $n > n_1$ bedeuten, was aber auch kein Widerspruch zu unserem angestrebten Resultat (Satz 3.2) wäre.

(*i*) Für $n = n_1$ ist mit der Voraussetzung $a(n_1) = rn_1$ die Darstellung

$$a(n_1) = rn_1 + n_1 - n_1$$

klar. Für $n_1 < n < n_2$ ist nach Voraussetzung $g(n) = 1$, also gilt:

$$\begin{aligned} a(n) &= a(n-1) + g(n) = a(n-2) + g(n-1) + g(n) \\ &= \ldots = a(n_1) + \sum_{i=n_1+1}^{n} g(i) \\ &= a(n_1) + n - (n_1 + 1) + 1 = rn_1 + n - n_1. \end{aligned}$$

(*ii*) Für $1 \leq i \leq k$ gilt:

$$g(n_1 + i) = \gcd(n_1 + i, a(n_1 + i - 1)) = \gcd(n_1 + i, rn_1 + i - 1).$$

Daher muss $g(n_1+i)$ sowohl n_1+i als auch rn_1+i-1 teilen, also auch jede Linearkombination dieser beiden Ausdrücke. Damit folgt:

$$g(n_1 + i) \mid ((rn_1 + i - 1) - (n_1 + i)) = (r-1)n_1 - 1, \quad (16)$$
$$g(n_1 + i) \mid (r \cdot (n_1 + i) - (rn_1 + i - 1)) = (r-1)i + 1. \quad (17)$$

Damit können wir jetzt zeigen, dass $k = \frac{p-1}{r-1}$ gilt. Zunächst gilt mit $i = k$ in (16):

$$g(n_2) = g(n_1 + k) \mid ((r-1)n_1 - 1).$$

Nach Voraussetzung ist $g(n_2) \neq 1$ und p der kleinste Primteiler von $(r-1)n_1 - 1$, also ist $g(n_2) \geq p$. Ferner gilt mit (17)

$$g(n_2) = g(n_1 + k) \mid (r-1)k + 1,$$

also ist $p \leq g(n_2) \leq (r-1)k + 1$ bzw. $k \geq \frac{p-1}{r-1}$.

Andererseits wissen wir, dass $g(n_1 + i) = 1$ für $1 \leq i < \frac{p-1}{r-1} \leq k$. Es bleibt also zu zeigen, dass $g\left(n_1 + \frac{p-1}{r-1}\right) \neq 1$:

$$\begin{aligned} g\left(n_1 + \frac{p-1}{r-1}\right) &= \gcd\left(n_1 + \frac{p-1}{r-1}, a\left(n_1 + \frac{p-1}{r-1} - 1\right)\right) \\ &= \gcd\left(n_1 + \frac{p-1}{r-1}, rn_1 + n_1 + \frac{p-1}{r-1} - 1 - n_1\right) \\ &= \gcd\left(\frac{((r-1)n_1 - 1) + p}{r-1}, \frac{r((r-1)n_1 - 1) + p}{r-1}\right) \end{aligned}$$

Nach Definition gilt $p \mid ((r-1)n_1 - 1)$ und $p \nmid (r-1) \in \{1, 2\}$. Somit teilt p beide Nenner, aber nicht die Zähler, also

$$g\left(n_1 + \frac{p-1}{r-1}\right) \geq p > 1.$$

Da n_2 der kleinste Index größer n_1 mit $g(n_2) \neq 1$ war, gilt $n_1 + \frac{p-1}{r-1} \geq n_2$ bzw. $k = n_2 - n_1 \leq \frac{p-1}{r-1}$. Insgesamt folgt also $k = \frac{p-1}{r-1}$.

(*iii*) Mit $i = \frac{p-1}{r-1}$ in (17) folgt:

$$g(n_2) = g(n_1 + k) = g\left(n_1 + \frac{p-1}{r-1}\right) \mid \left((r-1)\frac{p-1}{r-1} + 1\right) = p.$$

Zusammen mit $g(n_2) \geq p$ ist also $g(n_2) = p$.

(*iv*) Aus $g(n_2) = p = (r-1)k + 1$ berechnet man:

$$\begin{aligned} a(n_2) &= a(n_2 - 1) + g(n_2) = (rn_1 + n_2 - 1 - n_1) + p \\ &= rn_1 + k - 1 + (r-1)k + 1 = r(n_1 + k) = rn_2. \end{aligned}$$

Damit ist alles bewiesen. □

Entscheidend für den Beweis war das Verständnis der Struktur der Rekursion. Insbesondere scheint die Wahl von p alles andere als intuitiv zu sein. In der Tat erklärt Rowland zu Beginn seines Artikels ausführlich die experimentellen Schritte, die seinem Beweis vorangingen. Zum Erfolg führte dann das Studium der Folge

$$\Delta(n) := a(n-1) - n.$$

Wie wir im Beweis gesehen haben, ist der auf n_1 folgende, nichttriviale gcd $g(n_2)$ dann durch den kleinsten Primteiler von

$$\Delta(n_1 + 1) = a(n_1) - n_1 - 1 = rn_1 - n_1 - 1 = (r-1)n_1 - 1$$

gegeben. Aus dem Wissen der nächsten Primzahl folgt dann wiederum die genaue Kenntnis der Lücke mit Einsen. Mit diesen Einsichten in die Struktur der Folge ist der Beweis dann nicht mehr schwer.

Mithilfe dieses Lemmas sind wir jetzt in der Lage, die Behauptung vom Anfang dieses Abschnitts zu beweisen.

Theorem 3.2
Für die Rekursionsfolge (14) mit Anfangsbedingung $a(1) = 7$ ist die Folge der Differenzen $g(n) = a(n) - a(n-1)$ immer 1 oder eine Primzahl.

BEWEIS: Man rechnet leicht nach:

$$\begin{aligned} a(2) &= a(1) + \gcd(2, a(1)) = 7 + 1 = 8, \\ a(3) &= a(2) + \gcd(3, a(2)) = 8 + 1 = 9. \end{aligned}$$

Mit $r := 3$ und $n_1 := 3 > \frac{3}{3-1}$ ist $a(n_1) = rn_1$, d. h. die Bedingungen von Lemma 3.1 sind erfüllt. Wir haben

$$(r-1)n_1 - 1 = 2 \cdot 3 - 1 = 5 \quad \text{und} \quad n_2 = n_1 + \frac{p-1}{r-1} = 3 + \frac{5-1}{3-1} - 1 = 5,$$

also folgt auf eine 1 bei $n_2 = 5$ die Primzahl 5. Wegen $a(n_2) = 15$ sind wir wiederum in der Situation des Lemmas und können dies induktiv weiter anwenden, da Lemma 3.1 (iv) versichert, dass stets $a(n_i) = rn_i$ gilt. □

Der Beweis ist konstruktiv in dem Sinne, dass aus dem Wissen von n_1 und $a(n_1)$ bereits die nächste Stelle n_2 mit $g(n_2) = p > 1$ berechnet werden kann: p ist der kleinste Primfaktor von $(r-1)n_1 - 1$ und $n_2 = n_1 + \frac{p-1}{2}$. Will man jedoch diese "'Abkürzung"' nutzen, welche lange Reihen von Einsen überspringen kann, benötigt man einen externen Primzahltest, um p zu bestimmen. Somit hat man gegenüber klassischen Verfahren zur Ermittlung neuer Primzahlen nichts gewonnen.

3.1.2 Das Verhalten der Rekursion

Im Beweis haben wir gesehen, dass der Fall $a(n)/n = 3$ eine besondere Rolle spielt. Dies legt nahe, den Quotienten $a(n)/n$ genauer zu untersuchen. Im Folgenden wollen wir daher eine obere und eine untere Abschätzung beweisen.

Proposition 3.3
Sei $n_1 \geq 1$ und $a(n)$ rekursiv durch (14) definiert mit Anfangsbedingung $a(n_1) \geq 1$. Dann gilt

$$\frac{a(n)}{n} \leq \left\lceil \frac{a(n_1)}{n_1} \right\rceil \quad \textit{für alle } n \geq n_1,$$

wobei $\lceil \cdot \rceil$ die Aufrundungsfunktion bezeichnet, also die kleinste ganze Zahl größergleich einer gegebenen reellen Zahl.

Beweis: Sei $r := \lceil a(n_1)/n_1 \rceil$. Der Beweis nutzt Induktion über n. Der Induktionsanfang $n = n_1$ ist klar. Als Induktionsvoraussetzung sei angenommen, dass die Behauptung für $n - 1 \geq n_1$ stimmt. Die Ungleichung

$$\frac{a(n-1)}{n-1} \leq r$$

umgestellt liefert dann

$$rn - a(n-1) \geq r \geq 1.$$

Wegen $g(n) = \gcd(n, a(n-1))$ teilt $g(n)$ die Linearkombination $r \cdot n - a(n-1)$, also ist insbesondere $g(n) \leq rn - a(n-1)$. Somit folgt

$$a(n) = a(n-1) + g(n) \leq rn$$

und daraus die Behauptung. □

Für den Fall $a(1) = 7$ ist $a(3) = 9$, also folgt mit dem eben Bewiesenen, dass $a(n)/n \leq 3$ für alle $n \geq 3$ gilt. Andererseits haben wir bereits gesehen, dass der Fall $a(n) = 3n$ immer wieder auftritt (nämlich genau für $g(n) \neq 1$), also muss $a(n)/n > 2$ für alle $n \in \mathbb{N}$ gelten. Dass dies allgemein so gilt, ist die Aussage der folgenden Proposition.

Proposition 3.4
Sei $n_1 \geq 1$ und $a(n)$ rekursiv durch (14) definiert mit Anfangsbedingung $a(n_1) > 2n_1 + 1$. Dann gilt:

$$\frac{a(n)}{n} > 2 \quad \textit{für alle } n \geq n_1.$$

Beweis: Gemäß Voraussetzung ist $a(n_1)/n_1 > 2$. Angenommen, es gäbe ein Folgenglied mit $a(n)/n \leq 2$. Dann gibt es einen Index n mit

$$\frac{a(n)}{n} > 2 \geq \frac{a(n+1)}{n+1}.$$

Es folgt

$$2 \geq \frac{a(n+1)}{n+1} = \frac{a(n) + \gcd(n+1, a(n))}{n+1} \geq \frac{a(n)+1}{n+1},$$

also $a(n) \leq 2n+1$. Andererseits hatten wir bereits $a(n) > 2n$, somit kann der Quotient nur für $a(n) = 2n + 1$ die 2 unterschreiten. Wir zeigen jetzt, dass dieser Fall nicht auftreten kann; dafür müssen wir zwei Fälle unterscheiden.

(*i*) Sei $g(n) = 1$, d. h. $a(n-1) = a(n) - 1 = 2n$. Dann gilt:

$$2n + 1 = a(n) = a(n-1) + \gcd(n, a(n-1)) = 2n + \gcd(n, 2n) = 3n.$$

Es folgt $n = 1$, also die Anfangsbedingung $a(1) = 3$, welche aber laut Voraussetzung ausgeschlossen ist.

(*ii*) Sei jetzt $g(n) = j > 1$, also $a(n-1) = 2n - j$. Dann:

$$2n + 1 = a(n) = a(n-1) + \gcd(n, a(n-1)) = 2n - j + \gcd(n, 2n - j).$$

Somit ist $j + 1 = \gcd(n, 2n - j)$, also muss $j + 1$ die Linearkombination $2 \cdot n - (2n - j) = j$ teilen, was ein Widerspruch ist.

Dies zeigt, dass unter den gegebenen Voraussetzungen der Fall $a(n) = 2n + 1$ niemals eintritt. □

3.1.3 Verallgemeinerungen

Dass wir uns bisher genau wie Rowland in seinem Artikel auf die Startbedingung $a(1) = 7$ beschränkt haben, liegt nicht an einer besonderen Rolle dieses Wertes. Die Folge mit $a(1) = 7$ war schlicht die erste dieser Art, die untersucht und schließlich in die OEIS aufgenommen wurde. Tatsächlich ist mit Lemma 3.1 und den beiden Propositionen 3.3 und 3.4 leicht einzusehen, dass man für eine gewisse Anfangsbedingung $a(n_1) \in \mathbb{N}$ lediglich zeigen muss, dass sich der Zustand $a(N) = 3N$ irgendwann einstellt. Danach versichert das Lemma, dass die Differenz $g(n)$ nur 1 oder eine Primzahl sein kann. Bevor sich jedoch der Zustand $a(n) = 3N$ einstellt, kann $g(n)$ auch zusammengesetzte Werte annehmen. So ist $g(18) = 9$ für $a(1) = 532$ und $g(21) = 21$ für $a(1) = 800$. Empirische Untersuchungen rechtfertigen die folgende Vermutung aus Rowlands Artikel.

Conjecture 3.5
Für jede Startbedingung $n_1 \geq 1$ mit $a(n_1) \geq 1$ in der Rekursion (14) gibt es einen Index $N \in \mathbb{N}$, sodass $g(n) = a(n) - a(n-1)$ für alle $n > N$ eine 1 oder eine Primzahl ist.

Die Daten legen nahe, dass sich Lemma 3.1 für $n_1 = 1$ und $a(1) \geq 4$ immer ab einem Index N in Abhängigkeit von $a(1)$ anwenden lässt. Im Folgenden bezeichne $N(s)$ den kleinsten Index mit $a(N(s)) = 3N(s)$ bei Startbedingung $a(1) = s \in \mathbb{N}$. Tatsächlich scheint dieses N immer eine Primzahl in der Nähe von s zu sein; es gilt sogar $g(N) = N$ (vgl. Folge 3.2). Auffällig ist auch, dass häufig gleiche N in einer Reihe für aufeinanderfolgende Startbedingungen $a(1)$ auftauchen. Insbesondere gilt für $n \geq 3$:

$$N(2n) = N(2n+1).$$

Dies ist leicht einzusehen: Für $a(1) = 2n$ ist

$$a(2) = a(1) + \gcd(2, a(1)) = 2n + \gcd(2, 2n) = 2n + 2.$$

Genauso ist aber für $a(1) = 2n + 1$ ebenfalls

$$a(2) = (2n+1) + \gcd(2, 2n+1) = (2n+1) + 1 = 2n + 2,$$

d. h. bereits ab dem zweiten Glied verlaufen beide Folgen gleich.

Um uns der Vermutung zu nähern, wollen wir jetzt das Resultat aus Lemma 3.1 über die Länge der Lücken mit $g(n) = 1$ verallgemeinern. Mit der Bezeichnungsweise $\mathrm{mod}_j(a, b)$ für die Zahl x mit $x \equiv a \mod b$ und $j \leq x < j + b$ gilt das folgende Resultat.

Sequence 3.2 Die kleinsten Indizes N mit $a(N)/N = 3$.

$a(1)$	$N(a(1))$	$g(N)$	$a(1)$	$N(a(1))$	$g(N)$
4	2	2	34	41	41
5	3	3	35	41	41
6	5	5	36	41	41
7	5	5	37	41	41
8	7	7	38	37	37
9	7	7	39	37	37
10	11	11	40	41	41
11	11	11	41	41	41
12	11	11	42	41	41
13	11	11	43	41	41
14	13	13	44	43	43
15	13	13	45	43	43
16	17	17	46	47	47
17	17	17	47	47	47
18	17	17	48	47	47
19	17	17	49	47	47
20	19	19	50	59	59
21	19	19	51	59	59
22	23	23	52	53	53
23	23	23	53	53	53
24	23	23	54	53	53
25	23	23	55	53	53
26	29	29	56	59	59
27	29	29	57	59	59
28	29	29	58	59	59
29	29	29	59	59	59
30	29	29	60	59	59
31	29	29	61	59	59
32	31	31	62	61	61
33	31	31	63	61	61

Proposition 3.6
Seien $n \geq 0$, $d \geq 2$ und $j \in \mathbb{Z}$. Sei $k \geq j$ die kleinste Zahl mit $\gcd(n+k, n+d+k) \neq 1$. *Dann gilt:*

$$k = \min\left\{\mathrm{mod}_j(-n, p) : p \text{ ist Primteiler von } d\right\}.$$

Beweis: Sei $g := \gcd(n+k, n+d+k) > 1$. Da g jede Linearkombination der beiden Komponenten teilt, gilt

$$g \mid (n+d+k-(n+k)) = d.$$

Wir unterscheiden nun zwei Fälle:

(i) Sei zunächst $d = p$ eine Primzahl. Wegen $g \mid d = p$ muss $g = p$ gelten; insbesondere wird das Minimum nur über ein Element gebildet. Mit $p \mid (n + k)$ gilt

$$k \equiv -n \mod p.$$

Da k die kleinste Zahl größergleich j mit dieser Eigenschaft sein soll, folgt $k = \mathrm{mod}_j(-n, p)$ und damit die Behauptung.

(ii) Sei nun $d \geq 2$ beliebig. Wir betrachten zunächst die Zwischenbehauptung

$$I := \{i \in \mathbb{Z} : \gcd(n + i, n + d + i) \neq 1\} = \bigcup_{p|d} (-n + p\mathbb{Z}) =: J, \quad (18)$$

wobei die Vereinigung über alle Primteiler von d gebildet wird. Zum Beweis der Zwischenbehauptung sei zunächst $i \in I$, d. h.

$$i \in \mathbb{Z} \quad \text{mit} \quad \gcd(n + i, n + d + i) \neq 1$$

und $p \mid \gcd(n+i, n+d+i)$ ein Primteiler. Somit gilt $p \mid d$ und $p \mid (n+i)$ also

$$i \equiv -n \mod p \quad \text{bzw.} \quad i \in (-n + p\mathbb{Z})$$

und damit $i \in J$.

Sei jetzt umgekehrt $i \in J$, d. h. es gebe einen Primteiler $p \mid d$ mit $i \equiv -n \mod p$. Dann gilt

$$p \mid (n + i) \quad \text{und} \quad p \mid (n + d + i),$$

also $1 < p \mid \gcd(n + i, n + d + i)$ und somit $i \in I$. Insgesamt ist (18) damit bewiesen.

Damit muss jetzt analog zum Fall $d = p$ aus den betrachteten Äquivalenzklassen nur noch das richtige k ausgewählt werden, also jenes mit $k \geq j$ und $k \equiv -n \mod p$:

$$\begin{aligned} k &= \min\{i \in I : i \geq j\} \overset{(18)}{=} \min\{-n + pl \geq j : l \in \mathbb{Z},\ p \mid d\} \\ &= \min\{\mathrm{mod}_j(-n, p) : p \mid d\}. \end{aligned}$$

Damit sind alle Fälle abgedeckt und die Behauptung ist bewiesen. □

Mit dieser Proposition können wir nun die Lücken mit $g(n) = 1$ mit deutlich geringeren Einschränkungen an die Anfangsbedingung berechnen.

Corollary 3.7
Sei $a(n)$ rekursiv durch (14) definiert mit Startbedingung $n_1 \geq 1$ und $a(n_1) = n_1 + d$, wobei $d \geq 3$. Sei n_2 der kleinste Index größer n_1 mit $g(n_2) \neq 1$. Dann gilt:

$$n_2 = n_1 + \min\{\mathrm{mod}_1(-n_1, p) : p \text{ ist Primteiler von } d-1\}.$$

BEWEIS: Sei $k := n_2 - n_1$. Für $1 \leq i < k$ gilt

$$a(n_1 + i) = a(n_1) + i = n_1 + d + i.$$

Damit folgt unter Benutzung von Proposition 3.6

$$\begin{aligned} k &= \min\{i \in \mathbb{N} : g(n_1+i) \neq 1\} \\ &= \min\{i \in \mathbb{N} : \gcd(n_1+i, a(n_1+i-1)) \neq 1\} \\ &= \min\{i \in \mathbb{N} : \gcd(n_1+i, n_1+i+d-1) \neq 1\} \\ &\overset{3.6}{=} \min\{\mathrm{mod}_1(-n_1, p) : p \mid (d-1)\} \end{aligned}$$

und somit die gewünschte Identität. □

Wie man bemerkt, ist die Aussage aus Lemma 3.1 ein Spezialfall dieses Korollars für $d = (r-1)n_1$. Wir wollen nun die Funktionsweise der Formel anhand eines Beispiels untersuchen.

Example 3.8
Wie bereits erwähnt, nimmt $g(n)$ für $n_1 = 1$ und $a(n_1) = 533 = n_1 + 532$ auch zusammengesetzte Werte an. Trotzdem funktioniert die gerade bewiesene Formel, wie wir jetzt nachrechnen wollen:

(*i*) $n_1 = 1,\ a(n_1) = 533,\ d = 532$

$$\begin{aligned} n_2 &= 1 + \min\{\mathrm{mod}_1(-1, p) : p \mid 531\} \\ &= 1 + \min\{\mathrm{mod}_1(-1, 3), \mathrm{mod}_1(-1, 59)\} = 1 + 2 = 3 \end{aligned}$$

(*ii*) $n_2 = 3,\ a(n_2) = 537,\ d = 534$

$$\begin{aligned} n_3 &= 3 + \min\{\mathrm{mod}_1(-3, p) : p \mid 533\} \\ &= 3 + \min\{\mathrm{mod}_1(-3, 13), \mathrm{mod}_1(-3, 41)\} = 3 + 10 = 13 \end{aligned}$$

(*iii*) $n_3 = 13,\ a(n_3) = 559,\ d = 546$

$$\begin{aligned} n_4 &= 13 + \min\{\mathrm{mod}_1(-13, p) : p \mid 545\} \\ &= 13 + \min\{\mathrm{mod}_1(-13, 5), \mathrm{mod}_1(-13, 109)\} = 13 + 2 = 15 \end{aligned}$$

(iv) $n_4 = 15,\ a(n_4) = 565,\ d = 550$

$$\begin{aligned} n_5 &= 15 + \min\{\mathrm{mod}_1(-15, p) : p \mid 549\} \\ &= 15 + \min\{\mathrm{mod}_1(-15, 3), \mathrm{mod}_1(-15, 61)\} = 15 + 3 = 18 \end{aligned}$$

(v) $n_5 = 18,\ a(n_5) = 576,\ d = 558$

$$\begin{aligned} n_6 &= 18 + \min\{\mathrm{mod}_1(-18, p) : p \mid 557\} \\ &= 18 + \min\{\mathrm{mod}_1(-18, 557)\} = 18 + 539 = 557 \end{aligned}$$

Wegen $a(557) = 3 \cdot 557$ (mit $g(557) = 557$) lässt sich nun Lemma 3.1 anwenden; die Lücken können also mit der dort gegebenen Formel berechnet werden. □

Im Zusammenhang mit den Primzahlen, die in der Folge der $g(n)$ auftreten, äußert Rowland die Vermutung, dass die Folge mit dem Startwert $a(1) = 7$ den Wert jeder ungeraden Primzahl annimmt. Die Datenlage ist jedoch noch relativ dünn: Betrachtet man die ersten 10000 Primzahlen in der Folge der $g(n)$ mit der Startbedingung $a(1) = 7$, ist die kleinste ungerade Primzahl, die nicht auftaucht, die 587. Da Rowland auch keine heuristischen Gründe für diese Vermutung nennt, scheint diese Behauptung derzeit eher von dem Wunsch nach einer Folge, die alle Primzahlen darstellt, geleitet zu sein. Andererseits dürfte es sehr schwer sein, ein Gegenbeispiel zu finden, denn dafür wäre der Beweis über eine Primzahl p nötig, die in der unendlichen Folge der $g(n)$ nicht auftaucht.

In seinem Artikel nennt Rowland die Rekursion eine "'natürliche"' primzahlerzeugende Folge. Sicherlich ist die Folge nicht natürlich in dem Sinne, dass sie auf selbstverständliche Weise in einem Teilgebiet der Mathematik auftaucht. Dennoch beansprucht sie diesen Namen zurecht, denn im Gegensatz zu allen bisher bekannten Beispielen ist sie nicht künstlich und auf äußerst umständliche Art konstruiert, sondern durch eine einfache Bildungsvorschrift definiert. Sollte sich zudem Rowlands zweite Vermutung tatsächlich bewahrheiten, würde sie auch Ribenboims dritte Anforderung erfüllen und hätte sich die Bezeichnung als *natürliche* primzahlerzeugende Folge wahrlich verdient.

Sequence 3.3 Die ersten Werte von $q_1(n)$ mit der Startbedingung $b_1(1) = 1$ (A135506 in OEIS).

2, 1, 2, 5, 1, 7, 1, 1, 5, 11, 1, 13, 1, 5, 1, 17, 1, 19, 1, 1, 11, 23, 1, 5, 13, 1, 1, 29, 1, 31, 1, 11, 17, 1, 1, 37, 1, 13, 1, 41, 1, 43, 1, 1, 23, 47, 1, 1, 1, 17, 13, 53, 1, 1, 1, 1, 29, 59, 1, 61, 1, 1, 1, 13, 1, 67, 1, 23, 1, 71, 1, 73, 1, 1, 1, 1, 13, 79, 1, 1, 41, 83, 1, 1, 43, 29, 1, 89, 1, 13, 23, 1, 47, 1, 1, 97, 1, 1, 1, 101, 1, 103, 1, 1, 53, 107, 1, 109, 1, 1, 1, 113, 1, 23, 29, 1, 59, 1, 1, 1, 61, 41, 1, 1, 1, 127, 1, 43, 1, 131, 1, 1, 67, 1, 1, 137, 1, 139, 1, 47, 71, 1, 1, 29, 73, 1, 1, 149, 1, 151, 1, 1, 1, 1, 1, 157, 1, 53, 1, 1, 1, 163, 1, 1, 83, 167, 1, 13, 1, 1, 43, 173, 1, 1, 1, 59, 89, 179, 1, 181, 1, 61, 1, 1, 1, 1, 47, 1, 1, 191, 1, 193, 1, 1, 1, 197, 1, 199, 1, 67, 101, 1, 1, 1, 103, 1, 1, 1, 1, 211, 1, 71, 107, 43, 1, 1, 109, 73, 1, 1, 1, 223, 1, 1, 113, 227, 1, 229, 1, 1, 1, 233, 1, 47, 59, 1, 1, 239, 1, 241, 1, 1, 61, 1, 1, 1, 1, 83, 1, 251, 1, 1, 127, 1, 1, 257, 1, 1, 1, 1, 131, 263, 1, 1, 1, 89, 67, 269, 1, 271, 1, 1, 137, 1, 1, 277, 1, 1, 1, 281, 1, 283, 1, 1, 1, 1, 1, 1, 1, 73, 293, 1, 59, 1, 1, 149, 1, 1, ...

3.2 Cloitres Primzahlfolgen

3.2.1 Eine Folge mit dem kleinsten gemeinsamen Vielfachen

Durch Rowlands Formel angeregt fand Benoit Cloitre [Clo08] weitere Folgen, die Primzahlen liefern, jedoch auf Eigenschaften des kleinsten gemeinsamen Vielfachen (lcm) aufbauen. Dazu untersuchte er die Rekursion

$$\boxed{b_1(n) := b_1(n-1) + \operatorname{lcm}(n, b_1(n-1))} \qquad \text{für } n \geq 2. \tag{19}$$

Mit der Startbedingung $b_1(1) = 1$ nimmt die Folge $q_1(n)$ der Quotienten

$$q_1(n) := \frac{b_1(n)}{b_1(n-1)} - 1 \tag{20}$$

nur Einsen oder Primzahlwerte an (vgl. Folge 3.3).

Da für diese Vermutung bislang noch kein Beweis veröffentlicht wurde, möchte ich an dieser Stelle zumindest zeigen, dass die Folge $q_1(n)$ alle Primzahlen (mit Ausnahme der 3) annimmt. Ferner soll ein möglicher Beweisansatz für die Vermutung, dass $q_1(n)$ keine zusammengesetzten Werte annimmt, diskutiert werden.

Nutzt man zunächst die Beziehung

$$a \cdot b = \gcd(a, b) \cdot \operatorname{lcm}(a, b) \tag{21}$$

aus, die für alle natürlichen Zahlen $a,\ b > 0$ gilt, erhält man:

$$\begin{aligned} q_1(n) &= \frac{b_1(n)}{b_1(n-1)} - 1 \\ &= \frac{b_1(n-1) + \operatorname{lcm}(n, b_1(n-1))}{b_1(n-1)} - 1 \\ &= \frac{\operatorname{lcm}(n, b_1(n-1))}{b_1(n-1)} \\ &\overset{(21)}{=} \frac{n}{\gcd(n, b_1(n-1))}. \end{aligned}$$

Dies wiederum in (19) eingesetzt liefert

$$\begin{aligned} b_1(n) &= b_1(n-1) + \operatorname{lcm}(n, b_1(n-1)) \\ &\overset{(21)}{=} b_1(n-1) + \frac{n \cdot b_1(n-1)}{\gcd(n, b_1(n-1))} \\ &= b_1(n-1) \cdot \left(1 + \frac{n}{\gcd(n, b_1(n-1))}\right) \\ &= b_1(n-1) \cdot (1 + q_1(n)) \\ &= b_1(n-2) \cdot (1 + q_1(n-1)) \cdot (1 + q_1(n)) \\ &= \ldots \quad = b_1(1) \cdot \prod_{i=2}^{n} (1 + q_1(i)) = \prod_{i=2}^{n} (1 + q_1(i)). \end{aligned}$$

Mithilfe dieser Überlegungen wollen wir jetzt ein Lemma formulieren, das erste Hinweise auf die Struktur der Folge liefert. Dabei bezeichne $\nu_p(n)$ für eine Primzahl p die Vielfachheit dieser Primzahl in der Faktorisierung von n, also

$$\nu_p(n) := \max\left\{k \in \mathbb{N}_0 : p^k \mid n\right\}.$$

Damit folgt dann die kanonische Primfaktorzerlegung:

$$n = \prod_{i \in \mathbb{N}} p_i^{\nu_{p_i}(n)}.$$

Lemma 3.9
Seien die Folgen b_1 und q_1 durch (19) bzw. (20) definiert und $n > 3$. Mit der Startbedingung $b_1(1) = 1$ gilt dann:

(i) $\nu_2(b_1(n+1)) > \nu_2(b_1(n))$, *d. h. in jedem Schritt kommt ein Faktor 2 hinzu.*

(ii) $q_1(n+1)$ *ist ungerade.*

(iii) $b_1(n) > 2^n$.

(iv) *Sei p der größte Primteiler von $b_1(n)$. Dann ist $p < n$.*

BEWEIS: Zunächst berechnet man die nächsten Folgenglieder:

$$\begin{aligned}
b_1(2) &= b_1(1) + \operatorname{lcm}(2, b_1(1)) = 1 + 2 = 3,\\
b_1(3) &= b_1(2) + \operatorname{lcm}(3, b_1(2)) = 3 + 3 = 6 = 2 \cdot 3,\\
b_1(4) &= b_1(3) + \operatorname{lcm}(4, b_1(3)) = 6 + 12 = 18 = 2 \cdot 3^2,\\
b_1(5) &= b_1(4) + \operatorname{lcm}(5, b_1(4)) = 18 + 90 = 108 = 2^2 \cdot 3^3,\\
b_1(6) &= b_1(5) + \operatorname{lcm}(6, b_1(5)) = 108 + 108 = 216 = 2^3 \cdot 3^3.
\end{aligned}$$

(i) Der Beweis verläuft durch Induktion. Für den Induktionsanfang rechnet man nach:

$$\nu_2(b_1(6)) = 3 > \nu_2(b_1(5)) = 2 > \nu_2(b_1(4)) = 1.$$

Als Induktionsvoraussetzung gelte also die Behauptung für ein $n > 5$. Im Induktionsschluss von n nach $n+1$ unterscheiden wir zwei Fälle:

(a) Sei zunächst $n+1$ ungerade. Damit ist klar, dass auch der Quotient $(n+1)/\gcd(n+1, b_1(n))$ ungerade ist, d. h. es gilt

$$b_1(n+1) = b_1(n) \cdot \left(1 + \frac{n+1}{\gcd(n+1, b_1(n))}\right) = b_1(n) \cdot 2 \cdot m$$

für ein geeignetes $m \in \mathbb{N}$ und somit $\nu_2(b_1(n+1)) \geq \nu_2(b_1(n)) + 1$.

(b) Sei jetzt $n+1$ gerade. Es ist wiederum nachzuweisen, dass der Quotient $(n+1)/\gcd(n+1, b_1(n))$ ungerade ist. Dazu vergleicht man die Vielfachheiten $\nu_2(n+1)$ und $\nu_2(b_1(n))$. Offensichtlich gilt die Ungleichung

$$2^{\nu_2(n+1)} \leq n+1 \quad \text{bzw.} \quad \nu_2(n+1) \leq \log_2(n+1).$$

Andererseits gilt gemäß Induktionsvoraussetzung

$$\nu_2(b_1(n)) \geq \nu_2(b_1(n-1)) + 1 \geq \ldots \geq \nu_2(b_1(4)) + n - 4 = n - 3.$$

Wegen $n > 5$ gilt zudem die Abschätzung $\log_2(n+1) \leq n-3$. Insgesamt folgt damit

$$\nu_2(n+1) \leq \log_2(n+1) \leq n-3 \leq \nu_2(b_1(n)).$$

Somit gilt $2^{\nu_2(n+1)} \mid b_1(n)$ bzw. $2^{\nu_2(n+1)} \mid \gcd(n+1, b_1(n))$. Dies impliziert, dass der Quotient ungerade ist, da er keinen Faktor 2 in seiner Primfaktorzerlegung enthält. Daraus folgt die Behauptung wie oben.

Insbesondere gilt mit $b_1(3) = 6$, dass $b_1(n)$ für $n \geq 3$ gerade ist.

(*ii*) Aus der Darstellung

$$b_1(n+1) = b_1(n) \cdot (1 + q_1(n+1))$$

folgt, dass der Faktor $(1 + q_1(n+1))$ gerade, also $q_1(n+1)$ ungerade sein muss.

(*iii*) Mit der Abschätzung $b_1(4) = 18 > 16 = 2^4$ und dem gerade Bewiesenen folgt

$$b_1(n) \geq 2 \cdot b_1(n-1) \geq 2^2 \cdot b_1(n-1) \geq \ldots \geq 2^{n-4} \cdot b_1(4) > 2^{n-4} \cdot 2^4 = 2^n.$$

Insbesondere gilt damit die wesentlich schwächere Abschätzung $b_1(n) > n+1$, die noch zum Beweis von Teilerfremdheit nützlich sein wird.

(*iv*) Wir gehen wiederum induktiv vor, mit dem Induktionsanfang $b_1(4) = 18 = 2 \cdot 3^2$, also $p = 3 < 4$. Die Behauptung gelte für ein $n > 4$. Für den Induktionsschluss benutzen wir die Darstellung

$$b_1(n+1) = b_1(n) \cdot (1 + q_1(n+1)) \,.$$

Nach Induktionsvoraussetzung hat $b_1(n)$ nur Primteiler, die kleiner als n sind. Andererseits gilt die Abschätzung

$$q_1(n+1) = \frac{n+1}{\gcd(n+1, b_1(n))} \leq n+1 \quad \text{bzw.} \quad 1 + q_1(n+1) \leq n+2.$$

Da $q_1(n+1)$ ungerade ist, muss $(1+q_1(n+1))$ gerade sein, d. h. $b_1(n+1) = b_1(n) \cdot 2 \cdot m$ für ein geeignetes $m \in \mathbb{N}$. Es folgt die Abschätzung

$$m = \frac{1 + q_1(n+1)}{2} \leq \frac{n+2}{2} \leq n,$$

da $n > 4$ vorausgesetzt wurde. Somit haben wir $b_1(n+1)$ in Faktoren zerlegt, deren Primfaktoren allesamt echt kleiner als $n+1$ sind.

Damit ist dieses Lemma bewiesen. □

Mit diesen Hilfsmitteln können wir nun den angekündigten Satz beweisen.

Theorem 3.10
Seien die Folgen b_1 und q_1 durch (19) bzw. (20) definiert und $p > 3$ eine Primzahl. Mit der Startbedingung $b_1(1) = 1$ gilt dann:

$$q_1(p) = p.$$

Insbesondere wird jede Primzahl außer der 3 in der Folge angenommen.

Sequence 3.4 Die ersten Werte von $w(n)$ (A053989 in OEIS).

3, 2, 1, 1, 4, 1, 2, 1, 2, 2, 4, 1, 8, 1, 2, 2, 4, 1, 2, 1, 2, 2, 6, 1, 6, 4, 2, 3, 6, 1, 2, 1, 4, 2, 4, 2, 2, 1, 6, 2, 4, 1, 6, 1, 2, 3, 6, 1, 2, 3, 2, 2, 4, 1, 2, 3, 2, 3, 6, 1, 8, 1, 4, 2, 6, 2, 6, 1, 2, 2, 4, 1, 14, 1, 2, 2, 4, 3, 2, 1, 8, 2, 4, 1, 6, 3, 2, 3, 16, 1, 2, 4, 6, 3, 4, 2, 2, 1, 2, 2, 10, 1, 6, 1, 4, 2, 6, 1, 6, 1, 4, 2, 6, 1, 2, 3, 2, 3, 12, 2, 2, 4, 4, 5, 4, 2, 6, 1, 2, 3, 4, 1, 6, 3, 2, 2, 4, 1, 2, 1, 2, 2, 4, 3, 14, 7, 2, 3, 10, 1, 12, 1, 8, 2, 4, 2, 2, 1, 2, 3, 4, 4, 6, 1, 4, 2, 10, 1, 2, 3, 4, 5, 4, 1, 2, 7, 2, 8, 10, 1, 8, 1, 6, 2, 4, 3, 2, 3, 8, 2, 22, 1, 8, 1, 2, 3, 4, 1, 2, 1, 2, 5, 4, 5, 2, 3, 4, 5, 10, 2, 2, 1, 6, 3, 4, 2, 2, 3, 22, 2, 4, 2, 8, 1, 2, 3, 4, 1, 2, 1, 2, 2, 16, 1, 6, 13, 4, 6, 6, 1, 14, 1, 4, 2, 12, 2, 6, 3, 6, 2, 12, 1, 14, 3, 2, 5, 12, 1, 6, 4, 2, 2, 4, 1, 14, 3, 6, 6, 6, 1, 2, 1, 4, 2, 10, 3, 12, 1, 2, 3, 4, 1, 6, 1, 2, 2, 6, 3, 2, 7, 4, 5, 4, 1, 12, 3, 2, 5, 16, 2, ...

Beweis: Sei $p > 3$ eine Primzahl. Aus Lemma 3.9 folgt, dass der größte Primteiler von $b_1(p-1)$ kleiner als $p-1$ ist. Somit gilt $\gcd(p, b_1(p-1)) = 1$ und damit

$$q_1(p) = \frac{p}{\gcd(p, b_1(p-1))} = \frac{p}{1} = p.$$

Ferner wird die 2 zweimal angenommen ($q_1(2) = q_1(4) = 2$, alle größeren Folgenglieder von $q_1(n)$ sind ungerade), die 3 hingegen nie ($q_1(3) = 1$). Damit ist auch die zusätzliche Bemerkung bewiesen. □

Verglichen mit der unsicheren Situation bei Rowlands Folge ist dies eine recht erfreuliche Aussage. Wegen der offensichtlichen Abschätzung

$$q_1(n) = \frac{n}{\gcd(n, b_1(n-1))} \leq n,$$

die wir schon früher benutzt haben, kann jede Primzahl p jedoch erst an der p-ten Stelle auftauchen. Um große Primzahlen auszurechnen, muss man also sehr viele Folgenglieder bestimmen. Somit ist auch diese Folge sicher nicht dazu geeignet, schnell große Primzahlen zu generieren.

Satz 3.10 macht noch keine Aussagen über das Verhalten von $q_1(n)$ für zusammengesetzte Indizes. Um unsere Resultate zu verallgemeinern, betrachten wir jetzt die Folge $w(n)$, die durch

$$w(n) := \min\{k \in \mathbb{N} : kn - 1 \in \mathbb{P}\} \tag{22}$$

definiert ist, d. h. $w(n)n - 1$ ist eine Primzahl und $kn - 1 \notin \mathbb{P}$ für alle $k < w(n)$ (vgl. Folge 3.4). Die Menge, über die das Minimum gebildet wird, ist nicht leer; genauer besagt der Dirichlet'sche Primzahlsatz, dass es für jede natürliche Zahl $n \geq 2$ unendlich viele Primzahlen gibt, die kongruent zu -1 modulo n sind [Bun02, p. 138–140].

Damit können wir ein Lemma formulieren, das uns einen wichtigen Schritt in Richtung einer analogen Behauptung zu Rowlands Folge weiterbringt.

Lemma 3.11
Seien die Folgen b_1, q_1 und w wie oben definiert, $n > 1$ und $p > 3$ eine Primzahl. Mit der Startbedingung $b_1(1) = 1$ gilt dann:

(i) $q_1(n) = 1$ *gilt genau für* $n \mid b_1(n-1)$.

(ii) $b_1(p) = (p+1) \cdot b_1(p-1)$.

(iii) $q_1(w(p)p) = 1$.

Beweis:

(*i*) Mit der Darstellung $q_1(n) = n/\gcd(n, b_1(n-1))$ folgt unmittelbar, dass $q_1(n) = 1$ genau für $n = \gcd(n, b_1(n-1))$ gilt. Wegen $b_1(n-1) > n$ ist dies äquivalent zu $n \mid b_1(n-1)$.

(*ii*) Lemma 3.9 impliziert, dass p und $b_1(p-1)$ teilerfremd sind, da der größte Primteiler von $b_1(p-1)$ kleiner als $p-1$ ist. Somit folgt:

$$b_1(p) = b_1(p-1) \cdot \left(1 + \frac{p}{\gcd(p, b_1(p-1))}\right) = (p+1) \cdot b_1(p-1).$$

(*iii*) Nach Konstruktion ist $w(p)p - 1$ eine Primzahl. Mit dem gerade Bewiesenen folgt somit

$$\begin{aligned} b_1(w(p)p-1) &= ((w(p)p-1)+1) \cdot b_1((w(p)p-1)-1) \\ &= w(p) \cdot p \cdot b_1(w(p)p-2). \end{aligned}$$

Insbesondere gilt damit $p \mid b_1(w(p)p-1)$. Für den Quotienten folgt dann

$$\begin{aligned} q_1(w(p)p) &= \frac{w(p)p}{\gcd(w(p)p, b_1(w(p)p-1))} \\ &= \frac{w(p)p}{\gcd\big(w(p)p, w(p)p \cdot b_1(w(p)p-2)\big)} = 1. \end{aligned}$$

Damit ist das Lemma bewiesen. □

Im Anschluss an diese Betrachtungen wollen wir jetzt eine Vermutung über das Verhalten von $q_1(n)$ formulieren, die wir jedoch mit den bisher gezeigten Hilfsmitteln nicht beweisen können.

Conjecture 3.12
Seien die Folgen b_1, q_1 und w wie oben definiert und p eine Primzahl. Mit der Startbedingung $b_1(1) = 1$ gilt dann:

(i) *Für* $1 \leq n < w(p)p - 1$ *gilt* $p \nmid b_1(n)$, *d. h. der Primfaktor* p *tritt zuerst im Folgenglied* $b_1(w(p)p - 1)$ *auf.*

(ii) *Für* $1 \leq k \leq w(p) - 1$ *gilt* $k \mid b_1(kp - 1)$.

(iii) *Für* $1 \leq k \leq w(p) - 1$ *gilt* $q_1(kp) = p$.

Beweisidee: Sei $1 \leq n < w(p)p - 1$ für eine Primzahl $p > 3$. Wegen

$$b_1(n) = \prod_{i=2}^{n} (q_1(i) + 1)$$

genügt es zu zeigen, dass p keinen der Faktoren $(q_1(i) + 1)$ für $2 \leq i \leq n < w(p)p - 1$ teilt.

Angenommen, es gäbe ein i mit $p \mid (q_1(i) + 1)$. Dann gibt es ein $l \in \mathbb{N}$ mit $q_1(i) = lp - 1$. Wegen

$$lp - 1 = q_1(i) \leq i \leq n < w(p)p - 1$$

ist $lp - 1$ nach Konstruktion keine Primzahl. Aus $q_1(i) = lp - 1 > 1$ folgt jetzt $i \nmid b_1(i - 1)$, also insbesondere $\gcd(i, b_1(i - 1)) = 1$. Somit gilt:

$$lp - 1 = q_1(i) = \frac{i}{\gcd(i, b_1(i - 1))} = i.$$

Dies impliziert, dass $p \mid (q_1(i) + 1)$ nur für $i = lp - 1$ möglich ist; es genügt also das Studium von $(q_1(lp - 1) + 1)$ mit $1 \leq l \leq w(p) - 1$.

An dieser Stelle ist also für $1 \leq k \leq w(p) - 1$ zu zeigen, dass $p \nmid b_1(kp - 1)$ und $k \mid b_1(kp - 1)$ gilt. Hat man dies bewiesen, folgt die letzte Aussage unmittelbar. Sei dafür zunächst $p > 3$. Dann gilt die Darstellung

$$q_1(kp) = \frac{kp}{\gcd(kp, b_1(kp - 1))}.$$

Aus (i) und (ii) würde $\gcd(kp, b_1(kp - 1)) = k$ folgen. Insgesamt gilt dann

$$q_1(kp) = \frac{kp}{k} = p.$$

In den verbleibenden Fällen $p = 2$ und $p = 3$ gilt $w(2) = 2$ bzw. $w(3) = 1$, d. h. wir müssen lediglich $q_1(2) = 2$ nachrechnen und hätten damit die Aussage bewiesen. □

Auch wenn die Lücke in diesem Gedankengang geschlossen werden kann, ist damit noch keine Aussage über die Folgenglieder, die den Wert 1 annehmen,

getroffen. Zwar liegt die Vermutung nahe, dass $q_1(kp) = 1$ für $k \geq w(p)$ gilt, doch die Gegenbeispiele $q_1(2^2) = 2$, $q_1(5^2) = 5$ und $q_1(13^2) = 13$ widersprechen dieser allgemeinen Aussage. Solange man diese Gegenbeispiele nicht kontrollieren oder zumindest begründen kann, wäre eine Aussage über die Einsen in der Folge $q_1(n)$ reine Spekulation. Dennoch lohnen einige Überlegungen über ein möglichen Beweisversuch.

Zunächst muss man sich Gedanken über die Wohldefiniertheit der Darstellung $n = kp$ für eine Primzahl p und $1 \leq k < w(p)$ machen. Setzt man für p den größten Primteiler von n an, würde die Eindeutigkeit der Darstellung aus einer Abschätzung $w(p) \leq p$ folgen. Wie wir gesehen haben, hängt die Folge $w(n)$ mit dem Dirichlet'schen Primzahlsatz zusammen; dessen Beweis wiederum markierte den Anfang der analytischen Zahlentheorie. Daher ist ein Beweis der Abschätzung $w(p) \leq p$ mit elementaren Methoden kaum zu erwarten.

Hat man das Problem der Wohldefiniertheit gelöst, muss man noch einmal auf die Faktoren von $b_1(n)$ schauen. Die Behauptung 3.12 (i) besagt gerade, dass das erste Folgenglied von $b_1(n)$, in dem eine Primzahl p auftaucht, an der $(w(p)p - 1)$-ten Stelle steht. Somit folgt $p \mid b_1(n)$ für $n \geq w(p)p - 1$. Blicken wir auf die Darstellung

$$q_1(kp) = \frac{kp}{\gcd(kp, b_1(kp-1))},$$

wird klar, dass wir die Fälle $\gcd(kp, b_1(kp-1)) \in \{k, p, jp\}$ mit $1 < j < k$ unterscheiden müssen. Vermutung 3.12 (iii) setzt gerade voraus, dass $\gcd(kp, b_1(kp-1)) = k$ für $1 \leq k \leq w(p) - 1$ ist; ferner wissen wir bereits aus Lemma 3.11 (iii), dass $\gcd(kp, b_1(kp-1)) = kp$ für $k = w(p)$ gilt. Es ist klar: Für die Fälle mit $k \mid b_1(kp-1)$ ist $\gcd(kp, b_1(kp-1)) = kp$ und somit $q_1(kp) = 1$. Andererseits gibt es auch Folgenglieder mit $k \nmid b_1(kp-1)$, z. B. $26 \nmid b_1(26 \cdot 2 - 1)$, daher gilt $\gcd(26 \cdot 2, b_1(26 \cdot 2 - 1)) = 4$ und somit $q_1(52) = 52/4 = 13$. Dies liegt natürlich an $w(13) = 8$, weshalb nach Vermutung 3.12 (iii) auch unmittelbar $q_1(4 \cdot 13) = 13$ folgen würde. Dennoch macht dieses Beispiel klar, dass das Verhalten von $b_1(kp-1)$ nur sehr schwer zu kontrollieren ist und noch einiges an weiterer Forschung nötig ist, bis die Behauptung 3.12 (ii) bewiesen und verallgemeinert werden kann.

3.2.2 Primzahlfolgen und Primzahlzwillinge

Trotz dieser ungeklärten Fragen lohnt sich auch das Studium weitergehender Rekursionen. So besitzt die durch

$$\boxed{b_2(n) := 2 \cdot b_2(n-1) + \operatorname{lcm}(n, b_2(n-1))} \tag{23}$$

definierte Folge interessante Eigenschaften. Betrachtet man wieder die Folge der Quotienten

$$q_2(n) := \frac{b_2(n)}{b_2(n-1)} - 2 = \frac{\operatorname{lcm}(n, b_2(n-1))}{b_2(n-1)} = \frac{n}{\gcd(n, b_2(n-1))} \tag{24}$$

mit der Startbedingung $b_2(1) = 1$, so besteht diese ebenfalls nur aus Einsen und Primzahlen (vgl. Folge 3.5). Noch interessanter jedoch ist die Tatsache, dass diese Folge Verbindungen zu Primzahlzwillingen zu haben scheint. Damit bezeichnet man Paare von Primzahlen derart, dass sowohl p als auch $p + 2$ Primzahlen sind.

Die Folge der $q_2(n)$ verhält sich in vielen Belangen ähnlich wie $q_1(n)$; insbesondere gelten die gleichen Darstellungen für die Folge, wie man in (24) sieht. Entsprechend gilt auch, dass $q_2(n)$ ein Teiler von n sein muss. Bezeichnet man jetzt mit p eine Primzahl, so kann diese nur an ganzzahligen Vielfachen der Primzahl auftauchen, d. h. man sucht ein $k \in \mathbb{N}$ mit $q_2(kp) = p$. Wie die Beispiele $q_1(5^2) = 5$ und $q_1(13^2) = 13$ bereits gezeigt haben, ist nicht völlig ausgeschlossen, dass eine Primzahl p mit $q_2(p) = 1$ später in der Folge auftaucht. Hingegen legen experimentelle Untersuchungen nahe, dass die Primzahlen

$$5, 13, 19, 31, 43, 61, 73, 103, 109, 139, 151, 181, 193, 199, 229, 241, 271, 283, \ldots$$

nicht in q_2 enthalten sind. Man erkennt, dass dies genau die größeren Werte der Primzahlzwillinge größer 7 sind.

Sollte diese Folge tatsächlich in enger Verbindung mit den Primzahlzwillingen stehen, wäre sie ein mögliches Hilfsmittel zum Beweis eines der größten ungelösten Probleme der Zahlentheorie – aufgrund der Datenlage vermutet man nämlich, dass es unendlich viele Primzahlzwillinge gibt. Bislang konnte dies weder bewiesen noch widerlegt werden; wenn aber alle größeren Werte eines Primzahlzwillings in der Folge q_2 fehlen, wäre die Vermutung äquivalent zu der Annahme, dass in der Folge q_2 unendlich viele Primzahlen fehlen. Eingedenk der langen Tradition der Primzahlzwillingsvermutung kann man wohl annehmen, dass auch dieser Beweis sehr schwer wäre. Jedoch bleibt die vielleicht überraschende Einsicht, dass auch eine solche, zunächst unscheinbare Folge neue Hinweise auf sehr alte Probleme liefern kann.

Sequence 3.5 Die ersten Werte von $q_2(n)$ mit der Startbedingung $b_2(1) = 1$ (A135508 in OEIS).

2, 3, 1, 1, 1, 7, 2, 1, 1, 11, 1, 1, 7, 1, 1, 17, 1, 1, 1, 7, 11, 23, 1, 1, 1, 1, 7, 29, 1, 1, 2, 11, 17, 7, 1, 37, 1, 1, 1, 41, 7, 1, 11, 1, 23, 47, 1, 1, 1, 17, 1, 53, 1, 1, 1, 1, 29, 59, 1, 1, 1, 1, 1, 1, 1, 67, 17, 1, 1, 71, 1, 1, 37, 1, 1, 1, 1, 79, 1, 1, 41, 83, 1, 1, 1, 29, 1, 89, 1, 1, 1, 1, 47, 1, 1, 97, 1, 1, 1, 101, 1, 1, 1, 1, 53, 107, 1, 1, 1, 37, 1, 113, 1, 1, 29, 1, 59, 1, 1, 1, 1, 41, 1, 1, 1, 127, 2, 1, 1, 131, 1, 1, 67, 1, 1, 137, 1, 1, 1, 47, 71, 1, 1, 29, 1, 1, 37, 149, 1, 1, 1, 1, 1, 1, 1, 157, 79, 1, 1, 1, 1, 163, 41, 1, 83, 167, 1, 1, 1, 1, 1, 173, 29, 1, 1, 59, 89, 179, 1, 1, 1, 1, 1, 37, 1, 1, 47, 1, 1, 191, 1, 1, 97, 1, 1, 197, 1, 1, 1, 67, 101, 29, 1, 41, 1, 1, 1, 1, 1, 211, 1, 1, 107, 1, 1, 1, 1, 1, 1, 1, 37, 223, 1, 1, 113, 227, 1, 1, 1, 1, 29, 233, 1, 1, 59, 79, 1, 239, 1, 1, 1, 1, 1, 1, 41, 1, 1, 83, 1, 251, 1, 1, 127, 1, 1, 257, 1, 1, 1, 29, 131, 263, 1, 1, 1, 89, 67, 269, 1, 1, 1, 1, 137, 1, 1, 277, 1, 1, 1, 281, 1, 1, 1, 1, 1, 41, 1, 1, 29, 97, 1, 293, 1, 1, 1, 1, 149, 1, 1, ...

3.2.3 Verallgemeinerungen

Es ist nur natürlich, nach einer Verallgemeinerung dieser Rekursion zu fragen. So kann man für ein $k \in \mathbb{N}$ die Folge

$$\boxed{b_k(n) := k \cdot b_k(n-1) + \operatorname{lcm}(n, b_k(n-1))} \tag{25}$$

definieren. Die Quotienten ergeben sich dann zu

$$q_k(n) := \frac{b_k(n)}{b_k(n-1)} - k = \frac{\operatorname{lcm}(n, b_k(n-1))}{b_k(n-1)}. \tag{26}$$

Wie für die verallgemeinerte Startbedingung in Rowlands Folge ist auch für ein allgemeines q_k die Aussage, dass die Folge nur Einsen und Primzahlen annimmt, nicht richtig. So gilt z. B. $q_6(25) = 25$. Dennoch ist es wahrscheinlich, dass es analog zu Rowlands Folge einen Index N gibt, sodass $q_k(n)$ für $n \geq N$ nie zusammengesetzt ist. Jedoch scheint diese Vermutung noch genauso weit von einem Beweis wie Rowlands Vermutung 3.5 entfernt zu sein.

Ebenso haben wir uns bisher auf die Startbedingungen $b_1(1) = b_2(1) = 1$ beschränkt. Dies hat die Untersuchungen an manchen Stellen vereinfacht, war jedoch nicht wesentlich, denn die Anfangsbedingungen gingen in die Argumentation nur als Faktoren bzw. bei Induktionsanfängen ein. Tatsächlich stellt man fest, dass die erhaltenen Folgen im Wesentlichen dieselben sind, was die Beschränkung auf $b_1(1) = b_2(1) = 1$ rechtfertigt.

3.3 Stevens' Primzahlfolge

In Anlehnung an Rowlands Rekursion hat Aldrich Stevens [Ste08] eine Primzahlfolge gefunden, welche die Eigenschaften des gcd mit Eulers Poly-

Sequence 3.6 Die ersten Werte von $e(n)$ mit Parameter $a = 3$.

1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 167, 1, 1, 1, 1, 1, 1, 1, 1, 47, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 227, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 71, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 359,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 113, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 563, 1, 1, 1, …

nom verbindet. Dazu definiert man wie in (2)

$$p(n) := n^2 - n + 41.$$

Setzt man jetzt als Startbedingungen $k = 1$ und $a = 3$, so ist e durch den folgenden Iterationsprozess für $n \in \mathbb{N}$ definiert:

$$\boxed{e(n) := \gcd(p(n), p(n-1) - a \cdot k).} \tag{27}$$

Trifft man auf einen nichttrivialen gcd, muss k um 1 erhöht werden, d. h. für $e(n) > 1$ sei $k := k + 1$. Dann nimmt $e(n)$ wiederum nur Einsen und Primzahlen an (vgl. Folge 3.6).

Da schon die Definition recht kompliziert und keineswegs intuitiv ist, scheint diese Vermutung ein sehr schweres Problem zu sein. Aus dieser Sicht ist ein Beweis nicht in naher Zukunft zu erwarten. Jedoch bietet diese Folge genügend Parameter, die man variieren kann. So ist die Wahl von Eulers Polynom wohl eher historisch bedingt. Andere Polynome können problemlos eingesetzt werden; insbesondere scheinen primzahlreiche Polynome geeignet, wie Ribenboim sie in seinem Buch beschreibt [Rib06, p. 142–156]. Ebenso können die Werte von a (wenn auch nicht beliebig) verändert werden, ohne dass die Aussage falsch wird.

Es bleibt zu konstatieren, dass es tatsächlich "'einfache"' primzahlerzeugende Folgen gibt. Alle Funktionen, die wir in Abschnitt 2 diskutiert haben, sind im Hinblick auf Primzahlen konstruiert worden; entsprechend kompliziert sind ihre Definitionen und Berechnungen. Hat man jedoch die Konstruktion verstanden, ist die Beweisführung in aller Regel kein Problem mehr. Die Folgen aus diesem Abschnitt hingegen wurden nicht als Primzahlfolgen konstruiert, daher sind sie einfach definiert und nicht sehr schwer zu berechnen. Dafür sind die Beweise teilweise trickreich und keineswegs immer leicht einsichtig.

Wie man sieht, gibt es noch reichlich Forschungsstoff über Primzahlen im Allgemeinen und über Folgen von Primzahlen im Besonderen. Solange die

Primzahlen also nicht ihr letztes Geheimnis preisgegeben haben, darf man auch auf neuartige Folgen hoffen, die noch andere Richtungen einschlagen als die von Rowland, Cloitre und Stevens.

4 Danksagungen

Besonderer Dank gebührt Eric Rowland, Benoit Cloitre und Aldrich Stevens, die mich freundlicherweise mit Material über ihre Folgen versorgt haben, sowie den vielen fleißigen Korrekturlesern.

References

[AZ04] Aigner, Martin and Günter M. Ziegler: *Das BUCH der Beweise*. Springer, Berlin, Heidelberg, New York, 2nd edition, 2004.

[Bun02] Bundschuh, Peter: *Einführung in die Zahlentheorie*. Springer, Berlin, Heidelberg, New York, 5th edition, 2002.

[Clo08] Cloitre, Benoit: *On sequences related to primes*. Persönliche Mitteilung, February 2008.

[DPR61] Davis, Martin, Hilary Putnam, and Julia Robinson: *The decision problem for exponential Diophantine equations*. Annals of Mathematics, 74:425–436, 1961.

[dS06] Sautoy, Marcus du: *Die Musik der Primzahlen. Auf den Spuren des größten Rätsels der Mathematik*. Deutscher Taschenbuch Verlag, München, 2006.

[Dud69] Dudley, Underwood: *History of a formula for primes*. American Mathematical Monthly, 76:23–28, 1969.

[Erd49] Erdős, Paul: *On a new method in elementary number theory which leads to an elementary proof of the prime number theorem*. Proceedings of the National Academy of Sciences of the United States of America, 35:374–384, 1949.

[Ern75] Ernvall, Reijo: *A formula for the least prime greater than a given integer*. Elemente der Mathematik, 30:13–14, 1975.

[Gan71] Gandhi, J. M.: *Formulae for the nth prime.* In *Proc. Washington State University Conference on Number Theory*, pages 96–107, Pullman, WA, 1971. Washington State University.

[Gol74] Golomb, Solomon: *A direct interpretation of Gandhi's formula.* American Mathematical Monthly, 81:752–754, 1974.

[Hil00] Hilbert, David: *Mathematische probleme. vortrag, gehalten auf dem internationalen mathematiker-kongreß zu paris 1900.* Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse, pages 253–297, 1900.

[HW79] Hardy, Godfrey Harold and Edward Maitland Wright: *An Introduction to the Theory of Numbers.* Oxford University Press, 5th edition, 1979.

[Ing37] Ingham, Albert Edward: *On the difference between consecutive primes.* The Quarterly Journal of Mathematics, 8:255–266, 1937.

[JSWW76] Jones, James, Daihachiro Sato, Hideo Wada, and Douglas Wiens: *Diophantine representation of the set of prime numbers.* American Mathematical Monthly, 83:449–464, 1976.

[Mat70] Matijasevič, Yuri: *Enumerable sets are Diophantine.* Doklady Akademii Nauk SSSR, 191:279–282, 1970.

[Mat77] Matijasevič, Yuri: *Primes are nonnegative values of a polynomial in 10 variables.* Zapiski Sem. Leningrad Mat. Inst. Steklov, 68:62–82, 1977.

[Mil47] Mills, William: *A prime-representing function.* Bulletin of the American Mathematical Society, 53:604, 1947.

[Put60] Putnam, Hilary: *An unsolvable problem in number theory.* Journal of Symbolic Logic, 25:220–232, 1960.

[Rib06] Ribenboim, Paulo: *Die Welt der Primzahlen. Geheimnisse und Rekorde.* Springer, Berlin, Heidelberg, New York, 2006.

[Row08] Rowland, Eric: *A natural prime-generating recurrence.* Journal of Integer Sequences, 11:08.2.8, 2008.

[Sel49] Selberg, Atle: *An elementary proof of the prime-number theorem.* Annals of Mathematics, 50:305–313, 1949.

[Slo] Sloane, Neil: *The on-line encyclopedia of integer sequences.* `http://www.research.att.com/~njas/sequences`.

[Ste08] Stevens, Aldrich: *Prime number generators.* Persönliche Mitteilung, September 2008.

[VE72] Vanden Eynden, Charles: *A proof of Gandhi's formula for the nth prime.* American Mathematical Monthly, 79:625, 1972.

[Wil64] Willans, C. P.: *On formulae for the nth prime number.* Mathematical Gazette, 48:413–415, 1964.

[Wri51] Wright, Edward Maitland: *A prime-representing function.* American Mathematical Monthly, 58:616–618, 1951.

List of Sequences