6.4. Eine Primzahl-Fabrik?

In der Menge alle natürlichen Zahlen finden wir sehr regelmäßige Strukturen, die durch die Teilbarkeit bestimmt werden: Man denke etwa an die Muster, die beim Sieb des Eratosthenes auftreten. Andererseits gewinnt man den Eindruck, dass gerade dieses regelmäßige Muster eine Menge mit abwirft, die sich sehr erratisch verhält: Die Menge der Primzahlen, von der wir manches wissen, viele nahe liegende Fragen aber noch nicht beantwortet haben (und das vielleicht auch nie können).

Wir haben die Primzahlen negativ definiert: Eine natürliche Zahl $n > 1$ heißt prim, wenn sie keine Teiler außer 1 und n hat.

Vielleicht könnte man die Schwierigkeiten mit der Theorie der Primzahlen ja leicht ausräumen, wenn man eine positive Definition hätte, oder gar eine Konstruktionsvorschrift, die alle Primzahlen (und nur solche) liefert? Also eine Vorschrift f, die uns zu jeder natürlichen Zahl n eine Primzahl $f(n)$ erzeugt — am liebsten noch so, dass verschiedene n auch verschiedene Primzahlen liefern, oder gar so, dass $f(n)$ genau die Primzahl p_n mit der Nummer n ist?

Eine solche Vorschrift wäre nur dann wirklich hilfreich, wenn man aus n den Wert $f(n)$ tatsächlich ohne große Schwierigkeit berechnen (oder von einer Maschine bestimmen lassen) kann. Zu den Vorschriften, die sich leicht mechanisch realisieren lassen, gehören die Polynome: Hier werden gewisse Vielfache von Potenzen aufsummiert.

Wir beginnen mit einer überraschenden Beobachtung von Leonhard Euler (1707–1783), die einen leichtsinnigen Beobachter (der nur testet, solange man bequem rechnen kann) auf eine „Primzahl-Fabrik“ hoffen lässt:

Das Polynom $f(X) = X^2 + X + 41$ liefert eine Primzahl, wenn man für X eine der Zahlen

$$\begin{array}{rrrrrrrrrr} 0, & 1, & 2, & 3, & 4, & 5, & 6, & 7, & 8, & 9, \\ 10, & 11, & 12, & 13, & 14, & 15, & 16, & 17, & 18, & 19, \\ 20, & 21, & 22, & 23, & 24, & 25, & 26, & 27, & 28, & 29, \\ 30, & 31, & 32, & 33, & 34, & 35, & 36, & 37, & 38, & 39 \end{array}$$

einsetzt, aber nicht mehr für 40, auch nicht für 41.

In der Tat ergibt sich
$f(0) = 41$, $f(1) = 43$, $f(2) = 47$, $f(3) = 53$, $f(4) = 61$, $f(5) = 71$, $f(6) = 83$, $f(7) = 97$, $f(8) = 113$, $f(9) = 131$, $f(10) = 151$, $f(11) = 173$, $f(12) = 197$, $f(13) = 223$, $f(14) = 251$, $f(15) = 281$, $f(16) = 313$, $f(17) = 347$, $f(18) = 383$, $f(19) = 421$, $f(20) = 461$, $f(21) = 503$, $f(22) = 547$, $f(23) = 593$, $f(24) = 641$, $f(25) = 691$, $f(26) = 743$, $f(27) = 797$, $f(28) = 853$, $f(29) = 911$, $f(30) = 971$, $f(31) = 1033$, $f(32) = 1097$, $f(33) = 1163$, $f(34) = 1231$, $f(35) = 1301$, $f(36) = 1373$, $f(37) = 1447$, $f(38) = 1523$, $f(39) = 1601$.

Alle diese Werte treten in unserer Liste von Primzahlen im Kapitel 1 auf — was natürlich nur als Beweis akzeptiert werden kann, wenn man auch diese Liste gewissenhaft kontrolliert hat!

Viele der Primzahlen aus der Liste werden allerdings übersprungen. Wir erreichen nach 40 Schritten bereits die Primzahl $p_{252} = 1601$.

Dass $f(41)$ nicht prim ist, sieht man sofort (und ohne Rechnung):
Es ist ja $f(41) = 41^2 + 41 + 41$ durch 41 teilbar.

Der Wert an der vorhergehenden Stelle ist $f(40) = 40^2 + 40 + 41 = 40(40 + 1) + 41 = 41^2$.

Auch für viele weitere natürliche Zahlen n wird $f(n)$ prim: So sind zum Beispiel

$f(42) = 1847$, $f(43) = 1933$, $f(45) = 2111$, $f(46) = 2203$, $f(47) = 2297$, $f(48) = 2393$, $f(50) = 2591$, $f(51) = 2693$, $f(52) = 2797$, $f(53) = 2903$, $f(54) = 3011$, $f(55) = 3121$, $f(57) = 3347$, $f(58) = 3463$, $f(59) = 3581$ und $f(60) = 3701$ prim,

nicht aber $f(44) = 2021 = 43 \cdot 47$, $f(49) = 2491 = 47 \cdot 53$ und $f(56) = 3233 = 53 \cdot 61$.

Die Hoffnung auf eine polynomiale Vorschrift, die für jede natürliche Zahl eine neue Primzahl auswirft (ganz zu schweigen davon, dass man auf diese Weise alle Primzahlen erreichen könnte) hat sich endgültig zerschlagen. Es gilt nämlich:

Für jedes nicht konstante ganzzahlige Polynom $f(X)$ gibt es unendliche viele natürliche Zahlen n derart, dass $f(n)$ nicht prim ist.

Auch die Hoffnung, man könne Eulers Beispiel immer wieder verbessern, um mehr Primzahlen zu produzieren, geht in die Irre:

Liefert ein Polynom $F(X) = X^2 + X + q$ für jede natürliche Zahl n kleiner als $q - 1$ eine Primzahl $F(n)$, so gehört q zu den Zahlen 2, 3, 5, 11, 17, 41.

Dass für jede dieser Zahlen das Polynom F tatsächlich q viele Primzahlen nacheinander liefert, hat bereits Euler 1772 erkannt.

Die umgekehrte Aussage (die uns hier interessiert) wurde erst 1966 etabliert, ihr Beweis würde uns aber viel zu tief in die Mathematik führen. Details und Literatur-Referenzen für die Beweise findet man bei Ribenboim 1991 p.103ff.

Dort werden auch Hinweise auf kompliziertere Funktionen gegeben, die tatsächlich aus jeder natürlichen Zahl eine Primzahl erzeugen — keine dieser Funktionen ist allerdings für den Alltag brauchbar.