KAPITEL 1

Einführung

1. Grundlegende Eigenschaften der natürlichen und ganzen Zahlen

Ausgangspunkt der Zahlentheorie ist die Frage nach Eigenschaften der natürlichen (und ganzen) Zahlen. $\mathbb{N}$ bezeichnet die Menge der natürlichen Zahlen $\{1, 2, 3, \dots\}$, $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ ist die Menge der natürlichen Zahlen mit der 0. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ steht wie üblich für die Mengen der ganzen bzw. rationalen bzw. reellen bzw. komplexen Zahlen. Die ganzen Zahlen bilden einen Ring, d.h. man kann addieren, subtrahieren und multiplizieren.
Eine wesentliche weitere Eigenschaft der ganzen Zahlen ist die

Division mit Rest: Teilt man $a \in \mathbb{N}_0$ durch $b \in \mathbb{N}$, so erhält man einen Quotienten $q \in \mathbb{N}_0$ und einen Rest $r \in \mathbb{N}_0$, also

$$a : b = q \text{ Rest } r,$$

wobei der Rest kleiner ist als b. Mathematisch kann man dies in der Form

$$a = qb + r \quad \text{mit} \quad q, r \in \mathbb{N}_0 \quad \text{und} \quad 0 \le r \le b - 1$$

schreiben. (Beispiel: $23 : 4 = 5$ Rest 3 bzw. $23 = 5 \cdot 4 + 3$)
Mit der Abrundungsfunktion

$$\lfloor\ \rfloor : \mathbb{R} \to \mathbb{Z} \text{ mit } \lfloor x \rfloor = \sup\{n \in \mathbb{Z} : n \le x\}$$

können wir die Division mit Rest auch etwas anders beschreiben:

LEMMA. *Zu $a \in \mathbb{Z}$ und $b \in \mathbb{N}$ gibt es genau eine Zahl $q \in \mathbb{Z}$ und eine Zahl $r \in \mathbb{N}_0$, sodass gilt*

$$a = qb + r \quad \textit{und} \quad 0 \le r \le b - 1,$$

nämlich

$$q = \left\lfloor \frac{a}{b} \right\rfloor \quad \textit{und} \quad r = a - \left\lfloor \frac{a}{b} \right\rfloor b.$$

(Beweis als Übung)

Python (und SAGE) berechnet den (ganzzahligen) Quotienten mit `a//b`, den Divisionsrest mit `a%b`. Für den Divisionsrest r ist auch die Bezeichnung $a \bmod b$ üblich.

Teilbarkeit: Für $a, b \in \mathbb{Z}$ definiert man

$$a \mid b \quad \Longleftrightarrow \quad \text{es gibt ein } c \in \mathbb{Z} \text{ mit } b = ac.$$

Man sagt dann, a teilt b oder a ist ein Teiler von b oder b ist ein Vielfaches von a. Ist a kein Teiler von b, so schreiben wir $a \nmid b$. Für jede ganze Zahl a hat man folgende triviale Teilbarkeitsrelationen:

$$1 \mid a, \quad -1 \mid a, \quad a \mid a, \quad -a \mid a \quad \text{und} \quad a \mid 0.$$

Datei: anazt1.tex. Version vom 14.4.2026

Ferner seien noch folgende Eigenschaften erwähnt (mit $a, b, c, d, x, y \in \mathbb{Z}$):

$$\begin{aligned} a \mid b, \quad b \mid c \quad &\Longrightarrow \quad a \mid c, \\ d \mid a, \quad d \mid b \quad &\Longrightarrow \quad d \mid ax + by, \\ a \mid b, \quad a \neq 0 \quad &\Longleftrightarrow \quad \frac{b}{a} \in \mathbb{Z} \quad \Longleftrightarrow \quad b \bmod a = 0, \\ d \mid 1 \quad &\Longleftrightarrow \quad d = \pm 1, \\ 0 \mid a \quad &\Longleftrightarrow \quad a = 0, \\ a \mid b \quad &\Longleftrightarrow \quad \pm a \mid \pm b \quad \Longleftrightarrow \quad |a| \mid |b|. \end{aligned}$$

(Die Teilbarkeit hängt nicht vom Vorzeichen ab.)
Reden wir von den Teilern einer natürlichen Zahl n, so meinen wir im Allgemeinen nur die positiven Teiler.

Will man mit Python oder SAGE die Teilbarkeit $a \mid b$ testen, so geschieht dies man einfachsten mit der Beziehung

$$a \mid b \quad \Longleftrightarrow \quad \texttt{b\%a==0}$$

ggT und kgV: Der größte gemeinsame Teiler und das kleinste gemeinsame Vielfache zweier ganzer Zahlen a und b werden definiert durch

$$\mathrm{ggT}(a,b) = \begin{cases} \max\{d \in \mathbb{N} : d \mid a \text{ und } d \mid b\} & \text{für } (a,b) \neq (0,0), \\ 0 & \text{für } (a,b) = (0,0) \end{cases}$$

und

$$\mathrm{kgV}(a,b) = \begin{cases} \min\{e \in \mathbb{N} : a \mid e \text{ und } b \mid e\} & \text{für } (a,b) \neq (0,0), \\ 0 & \text{für } (a,b) = (0,0). \end{cases}$$

Insbesondere gilt für alle $a \in \mathbb{Z}$ die Beziehung $\mathrm{ggT}(a,0) = |a|$ und $\mathrm{kgV}(a,0) = 0$.
(SAGE berechnt mit `gcd(a,b)` den ggT von a und b, mit `lcm(a,b)` das kgV von a und b.)

Kongruenzen: Wir erinnern auch an die Kongruenzschreibweise (für $a, b, m \in \mathbb{Z}$):

$$a \equiv b \bmod m \quad \Longleftrightarrow \quad m \mid a - b,$$

man sagt, a ist kongruent zu b modulo m. Für $m \in \mathbb{N}$ ist dies gleichwertig damit, dass a und b bei Division durch m den gleichen Rest liefern:

$$a \equiv b \bmod m \quad \Longleftrightarrow \quad (a \bmod m) = (b \bmod m).$$

(Hier wird mod in zwei verschiedenen Bedeutungen benutzt.) Die Kongruenz modulo m ist eine Äquivalenzrelation. Die Kongruenzklasse von a modulo m schreiben wir (hier) als

$$\overline{a}^{\bmod m}.$$

Dann gilt

$$\overline{a}^{\bmod m} = \overline{b}^{\bmod m} \quad \Longleftrightarrow \quad a \equiv b \bmod m \quad \Longleftrightarrow \quad m \mid a - b.$$

Die Menge der Äquivalenzklassen schreibt man als $\mathbb{Z}/m\mathbb{Z}$. Es ist

$$\mathbb{Z}/m\mathbb{Z} = \{\overline{0}^{\bmod m}, \overline{1}^{\bmod m}, \ldots, \overline{m-1}^{\bmod m}\}.$$

Die Äquivalenzrelation „kongruent modulo m“ ist mit Addition und Multiplikation verträglich, weswegen man durch

$$\overline{a}^{\bmod m} + \overline{b}^{\bmod m} := (a+b)^{\bmod m}$$

und

$$\overline{a}^{\bmod m} \cdot \overline{b}^{\bmod m} := (a \cdot b)^{\bmod m}$$

eine Addition und Multiplikation auf $\mathbb{Z}/m\mathbb{Z}$ erhält, die $\mathbb{Z}/m\mathbb{Z}$ zu einem kommutativen Ring macht.

Iteriert man die Divison mit Rest, so kommt man zum euklidischen Algorithmus:

Euklidischer Algorithmus: Zu vorgegebenen Zahlen $a_0, a_1 \in \mathbb{N}$ werden rekursiv Zahlen $a_i \in \mathbb{N}$ und $q_i \in \mathbb{N}_0$ durch folgende Vorschrift definiert: Man teilt a_{i-1} durch a_i und erhält q_i mit Rest a_{i+1}. Ist $a_{i+1} = 0$, so hört man auf.

$$\begin{aligned}
a_0 &= q_1 a_1 + a_2 \quad \text{mit} \quad 0 < a_2 < a_1,\\
a_1 &= q_2 a_2 + a_3 \quad \text{mit} \quad 0 < a_3 < a_2,\\
&\vdots \quad\quad \vdots\\
a_{i-1} &= q_i a_i + a_{i+1} \quad \text{mit} \quad 0 < a_{i+1} < a_i,\\
&\vdots \quad\quad \vdots\\
a_{n-2} &= q_{n-1} a_{n-1} + a_n \quad \text{mit} \quad 0 < a_n < a_{n-1},\\
a_{n-1} &= q_n a_n + 0.
\end{aligned}$$

Ist d ein Teiler von a_0 und a_1, so auch ein Teiler aller a_i, also auch von a_n. Liest man das Schema von unten nach oben, so folgt, dass a_n ein gemeinsamer Teiler von a_0 und a_1 ist. Damit ist klar, dass

$$\mathrm{ggT}(a_0, a_1) = a_n$$

gilt. Außerdem sieht man auch folgende, aus der Definition zunächst nicht offensichtliche Eigenschaft des ggT:

$$d \mid a_0, \quad d \mid a_1 \quad \Longleftrightarrow \quad d \mid \mathrm{ggT}(a_0, a_1).$$

Mit dem euklidischen Algorithmus kann man den ggT zweier Zahlen schnell berechnen.

Erweiterter euklidischer Algorithmus: Führt man den euklidischen Algorithmus für $a_0, a_1 \in \mathbb{N}$ aus, und definiert man sich dazu rekursiv ganze Zahlen x_i, y_i durch die Vorschrift

$$x_0 = 1,\, y_0 = 0, \quad x_1 = 0,\, y_1 = 1$$

und

$$x_i = x_{i-2} - q_{i-1} x_{i-1},\, y_i = y_{i-2} - q_{i-1} y_{i-1} \text{ für } i \geq 2,$$

so sieht man durch Induktion sofort, dass

$$a_i = x_i a_0 + y_i a_1$$

gilt, was insbesondere

$$\mathrm{ggT}(a_0, a_1) = a_n = x_n a_0 + y_n a_1$$

liefert. Der ggT von a_0 und a_1 ist also eine ganzzahlige Linearkombination von a_0 und a_1.

SAGE liefert mit `xgcd(a,b)` ein Tripel (g, x, y) mit $g = \mathrm{ggT}(a, b)$ und $xa + yb = \mathrm{ggT}(a, b)$.

Primzahlen: Eine natürliche Zahl $p > 1$ heißt **Primzahl**, wenn sie nur die trivialen Teiler 1 und p besitzt. Durch Ausprobieren findet man, dass die Folge der Primzahlen so beginnt:

$$2, \quad 3, \quad 5, \quad 7, \quad 11, \quad 13, \quad 17, \quad 19, \quad 23, \quad 29, \quad 31, \quad 37, \quad 41, \quad 43, \quad 47, \quad \ldots$$

p bezeichnet im Folgenden immer eine Primzahl. Eine wichtige Eigenschaft von Primzahlen ist die folgende:

$$p \mid ab \quad \Longrightarrow \quad p \mid a \text{ oder } p \mid b,$$

die wir kurz beweisen wollen: Gilt $p \mid a$, so sind wir fertig. Im Fall $p \nmid a$ gilt offensichtlich $\mathrm{ggT}(a, p) = 1$, da p nur die Teiler 1 und p hat. Also gibt es x, y in $\mathbb{Z}$ mit $1 = ax + py$. Multiplikation mit b liefert $b = abx + pby$. Wegen $p \mid ab$ gibt es c mit $ab = cp$, sodass wir schreiben können $b = abx + pby = cpx + pby = p(cx + by)$, was schließlich die Aussage $p \mid b$ beweist.
(SAGE testet mit `is_prime(n)`, ob n eine Primzahl ist.)

Zusammengesetzte Zahlen: Eine natürliche Zahl n heißt **zusammengesetzt**, wenn es $a, b \in \mathbb{N}$ gibt mit $n = ab$ und $a > 1$, $b > 1$. Äquivalent dazu ist, dass n keine Primzahl ist, und dass $n > 1$ gilt.

2. Der Fundamentalsatz der Arithmetik

Mit den erwähnten Eigenschaften natürlicher Zahlen ist es nicht schwer, den folgenden Satz zu beweisen, der von zentraler Bedeutung für die Zahlentheorie ist:

SATZ (Fundamentalsatz der Arithmetik). *Jede natürliche Zahl n ist eindeutig als Produkt von Primzahlen darstellbar:*

$$n = p_1^{e_1} \dots p_r^{e_r}$$

mit paarweise verschiedenen Primzahlen $p_1, \dots, p_r$ und $e_1, \dots, e_r \in \mathbb{N}$. (Im Fall $n = 1$ hat man auf der rechten Seite das leere Produkt mit $r = 0$.) Die Primzahlen $p_1, \dots, p_r$ werden auch als Primteiler der Zahl n bezeichnet.

Beispiel: Hier haben wir die Primfaktorzerlegung der ersten 100 natürlichen Zahlen bestimmt:

$1 = 1$	$2 = 2$	$3 = 3$	$4 = 2^2$	$5 = 5$
$6 = 2 \cdot 3$	$7 = 7$	$8 = 2^3$	$9 = 3^2$	$10 = 2 \cdot 5$
$11 = 11$	$12 = 2^2 \cdot 3$	$13 = 13$	$14 = 2 \cdot 7$	$15 = 3 \cdot 5$
$16 = 2^4$	$17 = 17$	$18 = 2 \cdot 3^2$	$19 = 19$	$20 = 2^2 \cdot 5$
$21 = 3 \cdot 7$	$22 = 2 \cdot 11$	$23 = 23$	$24 = 2^3 \cdot 3$	$25 = 5^2$
$26 = 2 \cdot 13$	$27 = 3^3$	$28 = 2^2 \cdot 7$	$29 = 29$	$30 = 2 \cdot 3 \cdot 5$
$31 = 31$	$32 = 2^5$	$33 = 3 \cdot 11$	$34 = 2 \cdot 17$	$35 = 5 \cdot 7$
$36 = 2^2 \cdot 3^2$	$37 = 37$	$38 = 2 \cdot 19$	$39 = 3 \cdot 13$	$40 = 2^3 \cdot 5$
$41 = 41$	$42 = 2 \cdot 3 \cdot 7$	$43 = 43$	$44 = 2^2 \cdot 11$	$45 = 3^2 \cdot 5$
$46 = 2 \cdot 23$	$47 = 47$	$48 = 2^4 \cdot 3$	$49 = 7^2$	$50 = 2 \cdot 5^2$
$51 = 3 \cdot 17$	$52 = 2^2 \cdot 13$	$53 = 53$	$54 = 2 \cdot 3^3$	$55 = 5 \cdot 11$
$56 = 2^3 \cdot 7$	$57 = 3 \cdot 19$	$58 = 2 \cdot 29$	$59 = 59$	$60 = 2^2 \cdot 3 \cdot 5$
$61 = 61$	$62 = 2 \cdot 31$	$63 = 3^2 \cdot 7$	$64 = 2^6$	$65 = 5 \cdot 13$
$66 = 2 \cdot 3 \cdot 11$	$67 = 67$	$68 = 2^2 \cdot 17$	$69 = 3 \cdot 23$	$70 = 2 \cdot 5 \cdot 7$
$71 = 71$	$72 = 2^3 \cdot 3^2$	$73 = 73$	$74 = 2 \cdot 37$	$75 = 3 \cdot 5^2$
$76 = 2^2 \cdot 19$	$77 = 7 \cdot 11$	$78 = 2 \cdot 3 \cdot 13$	$79 = 79$	$80 = 2^4 \cdot 5$
$81 = 3^4$	$82 = 2 \cdot 41$	$83 = 83$	$84 = 2^2 \cdot 3 \cdot 7$	$85 = 5 \cdot 17$
$86 = 2 \cdot 43$	$87 = 3 \cdot 29$	$88 = 2^3 \cdot 11$	$89 = 89$	$90 = 2 \cdot 3^2 \cdot 5$
$91 = 7 \cdot 13$	$92 = 2^2 \cdot 23$	$93 = 3 \cdot 31$	$94 = 2 \cdot 47$	$95 = 5 \cdot 19$
$96 = 2^5 \cdot 3$	$97 = 97$	$98 = 2 \cdot 7^2$	$99 = 3^2 \cdot 11$	$100 = 2^2 \cdot 5^2$

Die Bestimmung der Primfaktorzerlegung einer natürlichen Zahl ist eine wichtige und (für größere Zahlen) schwierige Aufgabe, die in den Bereich der Algorithmischen Zahlentheorie oder computational number theory gehört.
SAGE bestimmt die Primfaktorzerlegung einer natürlichen Zahl n mit dem Befehl `factor(n)`.

Beispiel: Hier sind die Primfaktorzerlegungen der 10 größten 30-stelligen Zahlen ($10^{30} - i$ für $i = 10, 9, 8, 7, 6, 5, 4, 3, 2, 1$):

$$\begin{aligned}
999999999999999999999999999990 &= 2 \cdot 3^2 \cdot 5 \cdot 3191 \cdot 16763 \cdot 43037 \cdot 62003 \cdot 77843839397 \\
999999999999999999999999999991 &= 599 \cdot 2131 \cdot 3733 \cdot 209861 \cdot 14902357 \cdot 67103479 \\
999999999999999999999999999992 &= 2^3 \cdot 7 \cdot 17 \cdot 151 \cdot 14033 \cdot 20959 \cdot 23651844848628193 \\
999999999999999999999999999993 &= 3 \cdot 19^2 \cdot 923361034164358264081255771 \\
999999999999999999999999999994 &= 2 \cdot 191 \cdot 2617801047120418848167539267 \\
999999999999999999999999999995 &= 5 \cdot 73571 \cdot 783988798759 \cdot 3467476119491 \\
999999999999999999999999999996 &= 2^2 \cdot 3 \cdot 166666666666667 \cdot 499999999999999 \\
999999999999999999999999999997 &= 24551 \cdot 1514197 \cdot 26899761675796814351 \\
999999999999999999999999999998 &= 2 \cdot 23 \cdot 47 \cdot 457 \cdot 3691153 \cdot 274199124029771599 \\
999999999999999999999999999999 &= 3^3 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 37 \cdot 41 \cdot 211 \cdot 241 \cdot 271 \cdot 2161 \cdot 9091 \cdot 2906161
\end{aligned}$$

Oft ist es sinnvoll, in der Primfaktorzerlegung einer Zahl n auch Faktoren p^0 zuzulassen. Dann hat man also

$$n = p_1^{e_1} \dots p_r^{e_r} \quad \text{mit} \quad e_1, \dots, e_r \geq 0$$

und paarweise verschiedenen Primzahlen $p_1, \dots, p_r$. Auch die Schreibweise

$$n = \prod_p p^{e_p}$$

ist gebräuchlich, wobei jetzt nur endlich viele e_p's ungleich 0 sind. Die Eindeutigkeit der Primfaktorzerlegung drückt sich dann darin aus, dass die Exponenten e_p eindeutig bestimmt sind. Man definiert die **Bewertung $v_p(n)$ von n in p** durch

$$v_p(n) = e_p.$$

Die Bewertung $v_p(n)$ zählt also, wie oft p in n aufgeht.
So gilt beispielsweise wegen $56 = 2^3 \cdot 7$

$$v_2(56) = 3, \quad v_3(56) = 0, \quad v_5(56) = 0, \quad v_7(56) = 1, \quad v_{11}(56) = 0, \quad \dots$$

Die Eindeutigkeit der Primfaktorzerlegung führt dazu, dass man sofort die Teiler einer natürlichen Zahl angeben kann, wenn man die Primfaktorzerlegung kennt:

Satz. *Für natürliche Zahlen a, b mit den Primfaktorzerlegungen $a = \prod_p p^{\alpha_p}$, $b = \prod_p p^{\beta_p}$ gilt:*

(1) *Teilbarkeit lässt sich an den Exponenten ablesen:*

$$a \mid b \quad \Longleftrightarrow \quad \alpha_p \leq \beta_p \text{ für alle } p.$$

(2) *Die Teiler und Vielfachen von a lassen sich so beschreiben:*

$$\begin{aligned}
\{d \in \mathbb{N} : d \mid a\} &= \{\prod_p p^{d_p} : 0 \leq d_p \leq \alpha_p \text{ für alle } p\}, \\
\{e \in \mathbb{N} : a \mid e\} &= \{\prod_p p^{e_p} : e_p \geq \alpha_p \text{ für alle } p, e_p \neq 0 \text{ für nur endliche viele } p\}.
\end{aligned}$$

(3) *Für den ggT und das kgV gelten die Formeln*

$$\mathrm{ggT}(a,b) = \prod_p p^{\min(\alpha_p, \beta_p)} \quad \text{und} \quad \mathrm{kgV}(a,b) = \prod_p p^{\max(\alpha_p, \beta_p)}.$$

(4) *Es ist*

$$\mathrm{ggT}(a,b) \cdot \mathrm{kgV}(a,b) = a\,b.$$

Beweis:

(1) Gilt $a \mid b$, so gibt es ein $c \in \mathbb{N}$ mit $b = ac$. Mit der Primfaktorzerlegung $c = \prod_p p^{\gamma_c}$ folgt dann

$$\prod_p p^{\beta_p} = \prod_p p^{\alpha_p+\gamma_p}, \quad \text{also} \quad \beta_p = \alpha_p + \gamma_p,$$

was wegen $\gamma_p \geq 0$ sofort $\alpha_p \leq \beta_p$ liefert. Gilt umgekehrt $\alpha_p \leq \beta_p$ für alle p, so ist $c = \prod_p p^{\beta_p-\alpha_p}$ eine natürliche Zahl, sodass aus

$$\prod_p p^{\beta_p} = \prod_p p^{\alpha_p} \cdot \prod_p p^{\beta_p-\alpha_p}$$

$b = ac$ und damit $a \mid b$ folgt.

(2) Das folgt sofort aus (1).

(3) Für $d = \prod_p p^{d_p} \in \mathbb{N}$ gilt mit (1)

$$\begin{aligned} d \mid a,\, d \mid b \quad &\iff \quad d_p \leq \alpha_p, d_p \leq \beta_p \text{ für alle } p \quad \iff \quad d_p \leq \min(\alpha_p, \beta_p) \text{ für alle } p \\ &\iff \quad d \mid \prod_p p^{\min(\alpha_p,\beta_p)}, \end{aligned}$$

sodass offensichtlich $\prod_p p^{\min(\alpha_p,\beta_p)}$ der ggT von a und b ist. Genauso erhält man mit $e = \prod_p p^{e_p}$

$$\begin{aligned} a \mid e,\, b \mid e \quad &\iff \quad \alpha_p \leq e_p,\, \beta_p \leq e_p \text{ für alle } p \quad \iff \quad \max(\alpha_p, \beta_p) \leq e_p \text{ für alle } p \\ &\iff \quad \prod_p p^{\max(\alpha_p,\beta_p)} \mid e, \end{aligned}$$

was zeigt, dass $\prod_p p^{\max(\alpha_p,\beta_p)}$ das kgV von a und b ist.

(4) $\mathrm{ggT}(a, b) \cdot \mathrm{kgV}(a, b) = ab$ folgt nun sofort aus (3), wenn man beachtet, dass

$$\min(\alpha_p, \beta_p) + \max(\alpha_p, \beta_p) = \alpha_p + \beta_p$$

gilt. ■

3. Konstruktion neuer Primzahlen aus alten Primzahlen

Der Fundamentalsatz der Arithmetik sagt noch nichts darüber aus, wieviele Primzahlen es gibt. Man kann aber sofort mit einem Argument von Euklid zeigen, dass es unendlich viele Primzahlen gibt.

LEMMA. *Sind $p_1, \ldots, p_r$ verschiedene Primzahlen, $r \geq 1$ und $e_1, \ldots, e_r \geq 1$, so kommen in der Primfaktorzerlegung von*

$$n = p_1^{e_1} \ldots p_r^{e_r} - 1$$

nur von $p_1, \ldots, p_r$ verschiedene Primzahlen vor.

Beweis: Wir schreiben die Primfaktorzerlegung von n in der Form

$$n = p_1^{e_1} \ldots p_r^{e_r} - 1 = p_1^{f_1} \ldots p_r^{f_r} p_{r+1}^{f_{r+1}} \ldots p_s^{f_s} \quad \text{mit} \quad f_i \geq 0$$

an. Wäre z.B. $f_1 \geq 1$, so hätte man

$$1 = p_1 \left(p_1^{e_1-1} p_2^{e_2} \ldots p_r^{e_r} - p_1^{f_1-1} p_2^{f_2} \ldots p_r^{f_r} p_{r+1}^{f_{r+1}} \ldots p_s^{f_2} \right),$$

was offensichtlich nicht sein kann, da auf der rechten Seite eine natürliche Zahl $\geq p_1$ stehen würde. Also folgt $f_1 = 0$ und analog $f_2 = \cdots = f_r = 0$, was die Behauptung beweist. ■

Außer im Fall $r = 1$, $p_1 = 2$, $e_1 = 1$ gilt immer $n > 1$, also erhält man tatsächlich eine neue, von $p_1, \ldots, p_r$ verschiedene Primzahl. Daher kann es nicht nur endlich viele Primzahlen geben:

SATZ (Euklid). *Es gibt unendlich viele Primzahlen.*

Das Lemma lädt auch zum Experimentieren ein. Davon findet sich etwas in den folgenden Beispielen.

Beispiel: Wir konstruieren eine Folge von Primzahlen rekursiv wie folgt: $q_1 = 2$, $q_2 = 3$ und für $r \geq 2$ sei q_{r+1} der kleinste Primteiler von $q_1 q_2 \dots q_r - 1$.

r	q_r	$q_1 \dots q_r - 1$ mit Primfaktorzerlegung	q_{r+1}
1	2	1	3
2	3	5	5
3	5	29	29
4	29	$869 = 11 \cdot 79$	11
5	11	$9569 = 7 \cdot 1367$	7
6	7	$66989 = 13 \cdot 5153$	13
7	13	$870869 = 37 \cdot 23537$	37
8	37	32222189	32222189
9	32222189	$131 \cdot 4920061 \cdot 1610899$	131
10	131	136013303998782209	136013303998782209
11	136013303998782209	$31 \cdot 41 \cdot 181 \cdot 499 \cdot 18166774231909276189 \cdot 8870749$	31
12	31	$197 \cdot 90378998357009832683040962059 7 \cdot 3221$	197
13	197	$19 \cdot 49532972059 \cdot 5835626580317 \cdot 9547427 \cdot 2154611$	19
14	19	$157 \cdot 769 \cdot 271338827 \cdot 25766771512898971353713 \cdot 2543$	157
15	157	$17 \cdot 437905041439670272831614777 17 \cdot 452704788101$	17
16	17	$8609 \cdot 232140980642201053042534 1209 \cdot 8907623 \cdot 32183$	8609
17	8609	$1831129 \cdot 705073635630813269 \cdot 395499093031447 \cdot 96593227$	1831129

Man sieht, dass die ersten Primzahlen 2, 3, 5, 7, 11, 17, 19 als Folgenglieder auftreten. So stellt sich die Frage: Kommen alle Primzahlen in der Folge q_r vor? Ich kenne die Antwort nicht[1].

Mersennesche Zahlen: Wir wählen im Lemma $r = 1$, $p_1 = 2$ und variieren e_1, d.h. wir betrachten Zahlen der Gestalt

$$M_n = 2^n - 1,$$

die auch als Mersennesche Zahlen bezeichnet werden. Die ersten Mersenneschen Zahlen haben wir mit SAGE faktorisiert:

$$\begin{array}{lcllcllcl}
2^1-1 &=& 1 & 2^{11}-1 &=& 23\cdot 89 & 2^{21}-1 &=& 7^2\cdot 127\cdot 337\\
2^2-1 &=& 3 & 2^{12}-1 &=& 3^2\cdot 5\cdot 7\cdot 13 & 2^{22}-1 &=& 3\cdot 23\cdot 89\cdot 683\\
2^3-1 &=& 7 & 2^{13}-1 &=& 8191 & 2^{23}-1 &=& 47\cdot 178481\\
2^4-1 &=& 3\cdot 5 & 2^{14}-1 &=& 3\cdot 43\cdot 127 & 2^{24}-1 &=& 3^2\cdot 5\cdot 7\cdot 13\cdot 17\cdot 241\\
2^5-1 &=& 31 & 2^{15}-1 &=& 7\cdot 31\cdot 151 & 2^{25}-1 &=& 31\cdot 601\cdot 1801\\
2^6-1 &=& 3^2\cdot 7 & 2^{16}-1 &=& 3\cdot 5\cdot 17\cdot 257 & 2^{26}-1 &=& 3\cdot 2731\cdot 8191\\
2^7-1 &=& 127 & 2^{17}-1 &=& 131071 & 2^{27}-1 &=& 7\cdot 73\cdot 262657\\
2^8-1 &=& 3\cdot 5\cdot 17 & 2^{18}-1 &=& 3^3\cdot 7\cdot 19\cdot 73 & 2^{28}-1 &=& 3\cdot 5\cdot 29\cdot 43\cdot 113\cdot 127\\
2^9-1 &=& 7\cdot 73 & 2^{19}-1 &=& 524287 & 2^{29}-1 &=& 233\cdot 1103\cdot 2089\\
2^{10}-1 &=& 3\cdot 11\cdot 31 & 2^{20}-1 &=& 3\cdot 5^2\cdot 11\cdot 31\cdot 41 & 2^{30}-1 &=& 3^2\cdot 7\cdot 11\cdot 31\cdot 151\cdot 331
\end{array}$$

Es fällt auf, dass unter diesen Zahlen $2^n - 1$ auch Primzahlen auftreten. Aus

$$2^{ab} - 1 = (2^a)^b - 1^b = (2^a - 1)((2^a)^{b-1} + (2^a)^{b-2} + \dots + 2^a + 1)$$

folgt, dass $2^n - 1$ höchstens dann eine Primzahl ist, wenn n selbst eine Primzahl ist. Eine Mersennesche Primzahl ist eine Primzahl der Gestalt

$$M_p = 2^p - 1 \quad \text{mit einer Primzahl } p.$$

[1]Weitere Folgenglieder sind bei „The On-Line Encyclopedia of Integer Sequences“ unter „https://oeis.org“ zu finden, wo die Folge die Bezeichnung A084598 trägt. Dort findet man auch, dass $q_{43} = 23$ ist.

Allerdings ist nicht für jede Primzahl p die Zahl $M_p = 2^p - 1$ prim, wie die Beispiele $M_{11} = 23 \cdot 89$, M_{23} und M_{29} zeigen. Die Mersenneschen Primzahlen $< 10^{100}$ sind

$$\begin{aligned}
2^2 - 1 &= 3 \\
2^3 - 1 &= 7 \\
2^5 - 1 &= 31 \\
2^7 - 1 &= 127 \\
2^{13} - 1 &= 8191 \\
2^{17} - 1 &= 131071 \\
2^{19} - 1 &= 524287 \\
2^{31} - 1 &= 2147483647 \\
2^{61} - 1 &= 2305843009213693951 \\
2^{89} - 1 &= 618970019642690137449562111 \\
2^{107} - 1 &= 162259276829213363391578010288127 \\
2^{127} - 1 &= 170141183460469231731687303715884105727
\end{aligned}$$

Man kann leicht Fragen stellen, die bis heute nicht beantwortet sind: Gibt es unendlich viele Mersennesche Primzahlen? Gibt es unendlich viele zusammengesetzte Zahlen M_p mit p prim?
Zur Zeit (April 2026) sind 52 Mersennesche Primzahlen bekannt, nämlich

$$\begin{aligned}
&2^2 - 1, \quad 2^3 - 1, \quad 2^5 - 1, \quad 2^7 - 1, \quad 2^{13} - 1, \quad 2^{17} - 1, \quad 2^{19} - 1, \quad 2^{31} - 1, \quad 2^{61} - 1, \quad 2^{89} - 1, \\
&2^{107} - 1, \quad 2^{127} - 1, \quad 2^{521} - 1, \quad 2^{607} - 1, \quad 2^{1279} - 1, \quad 2^{2203} - 1, \quad 2^{2281} - 1, \quad 2^{3217} - 1, \quad 2^{4253} - 1, \\
&2^{4423} - 1, \quad 2^{9689} - 1, \quad 2^{9941} - 1, \quad 2^{11213} - 1, \quad 2^{19937} - 1, \quad 2^{21701} - 1, \quad 2^{23209} - 1, \quad 2^{44497} - 1, \\
&2^{86243} - 1, \quad 2^{110503} - 1, \quad 2^{132049} - 1, \quad 2^{216091} - 1, \quad 2^{756839} - 1, \quad 2^{859433} - 1, \quad 2^{1257787} - 1, \\
&2^{1398269} - 1, \quad 2^{2976221} - 1, \quad 2^{3021377} - 1, \quad 2^{6972593} - 1, \quad 2^{13466917} - 1, \quad 2^{20996011} - 1, \\
&2^{24036583} - 1, \quad 2^{25964951} - 1, \quad 2^{30402457} - 1, \quad 2^{32582657} - 1, \quad 2^{37156667} - 1, \quad 2^{42643801} - 1, \\
&2^{43112609} - 1, \quad 2^{57885161} - 1, \quad 2^{74207281} - 1, \quad 2^{77232917} - 1, \quad 2^{82589933} - 1, \quad 2^{136279841} - 1.
\end{aligned}$$

Die größten explizit angebbaren Primzahlen sind meist Mersennesche Primzahlen. So ist heute die größte bekannte Primzahl die Mersennesche Primzahl

$$2^{136279841} - 1$$

mit 41024320 Dezimalstellen. Sie wurde im Oktober 2014 gefunden[2].

4. Die Primzahlzählfunktion $\pi(x)$

Wir definieren für eine reelle Variable x

$$\pi(x) = |\{p \leq x\}| = \sum_{p \leq x} 1,$$

d.h. $\pi(x)$ ist die Anzahl der Primzahlen $\leq x$. Ist

$$p_1 = 2, \quad p_2 = 3, \quad p_3 = 5, \quad p_4 = 7, \quad p_5 = 11, \quad p_6 = 13, \quad \ldots$$

die Folge der Primzahlen, d.h. p_n ist die n-te Primzahl, so gilt offensichtlich

$$\pi(x) = \begin{cases} 0 & \text{für } x < 2, \\ n & \text{für } p_n \leq x < p_{n+1}. \end{cases}$$

$\pi(x)$ ist also stückweise konstant. Die Funktion springt um 1 nach oben, wenn x eine Primzahl erreicht.

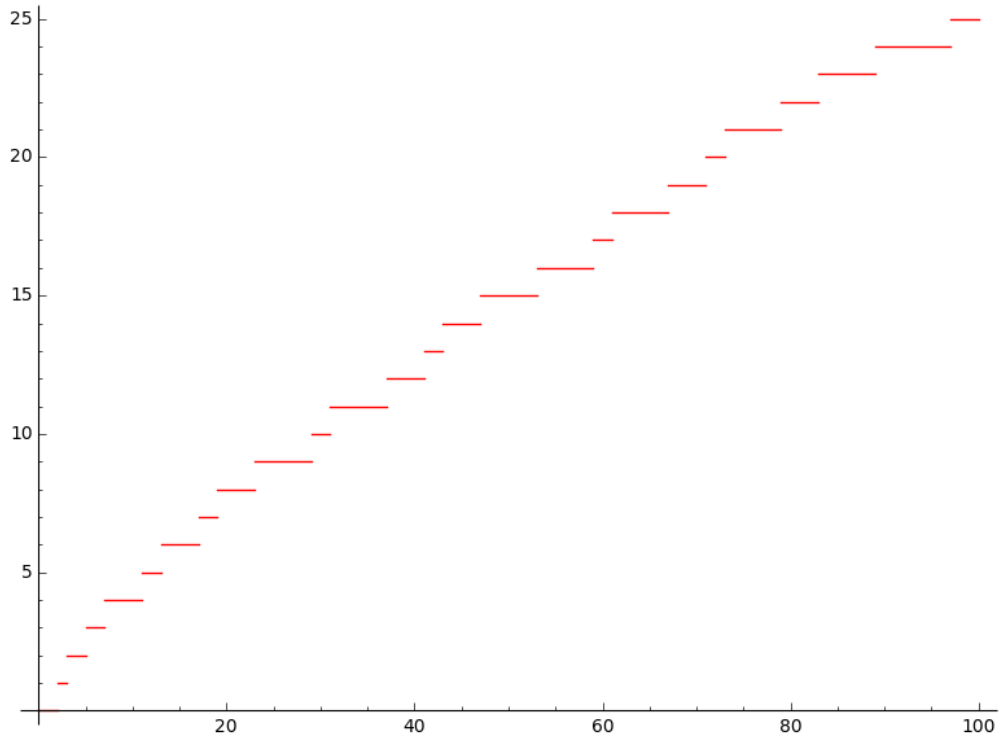
[2]Aktuelle Ergebnisse zur Suche nach Mersenneschen Primzahlen findet man bei „GIMPS - Great Internet Mersenne Prime Search“ unter „https://www.mersenne.org“.

Beispiele: Aus folgender Liste der Primzahlen < 100

$$
\begin{array}{llll}
2, & 3, & 5, & 7, \\
11, & 13, & 17, & 19, \\
23, & 29, & & \\
31, & 37, & & \\
41, & 43, & 47, & \\
53, & 59, & & \\
61, & 67, & & \\
71, & 73, & 79, & \\
83, & 89, & & \\
97, & \ldots & &
\end{array}
$$

ersieht man sofort

$$\pi(10) = 4, \quad \pi(20) = 8, \quad \pi(30) = 10, \quad \pi(40) = 12, \quad \pi(50) = 15,$$
$$\pi(60) = 17, \quad \pi(70) = 19, \quad \pi(80) = 22, \quad \pi(90) = 24, \quad \pi(100) = 25.$$



Die Abbildung zeigt $\pi(x)$ für $0 \leq x \leq 100$. Die Abbildung wurde erstellt mit dem SAGE-Befehl `plot(prime_pi,0,100,color="red",vertical_lines=False)`

Die Erstellung von Primzahltabellen und die Bestimmung von $\pi(x)$ hat eine jahrhundertelange Tradition. Unter Maple 9 sind Werte von $\pi(x)$ gespeichert, die mit `numtheory[pi](x)` abgerufen werden können, wovon der größte wohl

$$\pi(10^{21}) = 21127269486018731928$$

ist[3]. Bei SAGE lautet der Befehl `prime_pi(x)`. Für die nachfolgenden Tabellen haben wir auch auf Maple zurückgegriffen.

[3]Maple 18 scheint auch nicht mehr gespeichert zu haben.

Eine natürliche Frage ist, wie denn $\pi(x)$ mit x wächst. Hat man Primzahltabellen, so kann man $\pi(x)$ mit bekannten Funktionen vergleichen. Dies haben vor 200 Jahren bereits Legendre und Gauß getan [4].
Die folgende Tabelle vergleicht beispielhaft einige Werte von $\pi(x)$ mit bekannten Funktionen:

x	$\pi(x)$	$\frac{x}{\pi(x)}$	$\log x$	$\frac{\pi(x)\log x}{x}$	$\log x - \frac{x}{\pi(x)}$
10^1	4	2.50	2.30	0.9210	-0.1974
10^2	25	4.00	4.61	1.1513	0.6052
10^3	168	5.95	6.91	1.1605	0.9554
10^4	1229	8.14	9.21	1.1320	1.0736
10^5	9592	10.43	11.51	1.1043	1.0876
10^6	78498	12.74	13.82	1.0845	1.0763
10^7	664579	15.05	16.12	1.0712	1.0710
10^8	5761455	17.36	18.42	1.0613	1.0640
10^9	50847534	19.67	20.72	1.0537	1.0566
10^{10}	455052511	21.98	23.03	1.0478	1.0504
10^{11}	4118054813	24.28	25.33	1.0430	1.0451
10^{12}	37607912018	26.59	27.63	1.0391	1.0409
10^{13}	346065536839	28.90	29.93	1.0359	1.0373
10^{14}	3204941750802	31.20	32.24	1.0332	1.0344
10^{15}	29844570422669	33.51	34.54	1.0308	1.0318
10^{16}	279238341033925	35.81	36.84	1.0288	1.0297
10^{17}	2623557157654233	38.12	39.14	1.0270	1.0278
10^{18}	24739954287740860	40.42	41.45	1.0254	1.0261
10^{19}	234057667276344607	42.72	43.75	1.0240	1.0246
10^{20}	2220819602560918840	45.03	46.05	1.0227	1.0233
10^{21}	21127269486018731928	47.33	48.35	1.0216	1.0221

Legendre hat gemutmaßt, dass

$$\pi(x) \approx \frac{x}{\log x - B} \quad \text{mit} \quad B = 1.08366$$

gilt, was aber mit der vorangegangenen Tabelle nicht gut vereinbar ist. Etwas ungenauer könnte man vermuten, dass $\frac{x}{\pi(x)}$ wie $\log x$ wächst, dass $\frac{\pi(x)\log x}{x}$ der Zahl 1 nahe kommt. Tatsächlich gilt der folgende Satz, der auch als „Primzahlsatz“ bezeichnet wird und eine zentrale Rolle in der Analytischen Zahlentheorie spielt:

Satz (Primzahlsatz). *Es gilt*

$$\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1.$$

Ein Hauptziel dieser Vorlesung ist der Beweis dieses Satzes. Es gibt inzwischen zahlreiche Beweise, wovon allerdings keiner trivial ist. Zum ersten Mal wurde der Satz unabhängig voneinander von Hadamard und de la Vallée Poussin im Jahre 1896 bewiesen.

Der Gaußsche Ansatz war etwas anders. Er beobachtete, dass bei festem l die Anzahl der Primzahlen im Intervall $[x-l, x+l]$ mit x abnimmt. In der folgenden Tabelle findet sich die Anzahl Primzahlen im

[4] Siehe [**Riesel 1985**, S.45].

Intervall $(x-5000, x+5000]$, also $\pi(x+5000)-\pi(x-5000)$.

x	$\pi(x+5000)-\pi(x-5000)$	$\frac{10000}{\log x}$
10000	1085	1085.74
20000	1008	1009.75
30000	970	970.03
40000	943	943.70
50000	915	924.23
60000	903	908.92
70000	900	896.36
80000	884	885.76
90000	880	876.61
100000	867	868.59
110000	847	861.46
120000	863	855.05
130000	842	849.24
140000	846	843.92
150000	850	839.04
160000	821	834.52
170000	823	830.32
180000	829	826.40
190000	828	822.72
200000	808	819.26

Gauß vermutete an Hand seiner Experimente, dass

$$\frac{\#\{p : x-l < p \leq x+l\}}{2l} = \frac{\pi(x+l)-\pi(x-l)}{2l} \approx \frac{1}{\log x}$$

gilt, d.h. dass die Primzahldichte um x ungefähr $\frac{1}{\log x}$ ist. Also sollte für $a < b$ gelten

$$|\{p : a < p \leq b\}| = \pi(b)-\pi(a) \approx \int_a^b \frac{dx}{\log x}$$

und damit insbesondere

$$\pi(x) \approx \int_2^x \frac{dt}{\log t}.$$

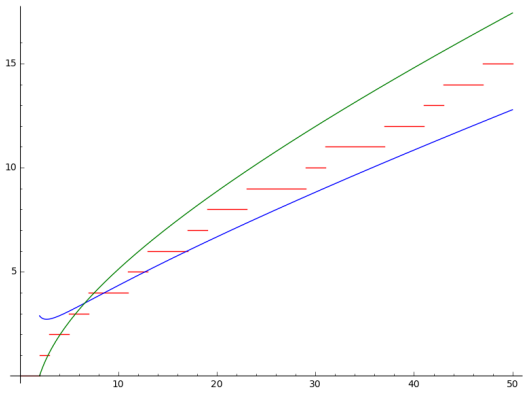
(Gauß hat aber in diesem Zusammenhang nichts bewiesen.) Das angegebenene Integral ist unter dem Namen „logarithmisches Integral“ mit der Bezeichung

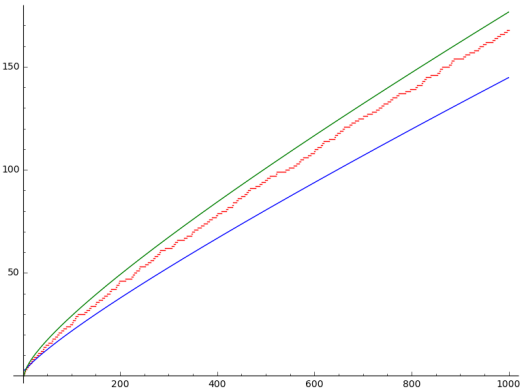
$$\mathrm{li}(x) = \int_2^x \frac{dt}{\log t}$$

zu finden [5]. (In SAGE kann man $\mathrm{li}(x)$ mit dem Befehl `log_integral(x)-log_integral(2)` berechnen.)

[5] In [**Jameson 2003**, S.3], [**Bach/Shallit 1996**, S.209] und [**Montgomery/Vaughan 2006**, S.5] wird diese Bezeichnung verwendet, oft steht $\mathrm{li}(x)$ auch für $\lim_{\varepsilon\to 0}(\int_0^{1-\varepsilon} \frac{dt}{\log t} + \int_{1+\varepsilon}^x \frac{dt}{\log t})$, beispielsweise bei [**Brüdern 1995**, S.5]. In [**Ribenboim 2006**, S.167] findet sich $\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t}$.

In den folgenden Abbildungen sind die Funktionen $\pi(x)$, $\frac{x}{\log x}$ und $\mathrm{li}(x)$ skizziert (in den Farben rot, blau und grün):





Die folgende Tabelle haben wir mit Maple erstellt:

x	$\pi(x)$	$\frac{x}{\log x}$	$\frac{\pi(x)\log x}{x}$	$\mathrm{li}(x)$	$\frac{\pi(x)}{\mathrm{li}(x)}$
10^1	4	4.34	0.921034	5.12	0.781184
10^2	25	21.71	1.151293	29.08	0.859668
10^3	168	144.76	1.160503	176.56	0.951494
10^4	1229	1085.74	1.131951	1245.09	0.987076
10^5	9592	8685.89	1.104320	9628.76	0.996182
10^6	78498	72382.41	1.084490	78626.50	0.998366
10^7	664579	620420.69	1.071175	664917.36	0.999491
10^8	5761455	5428681.02	1.061299	5762208.33	0.999869
10^9	50847534	48254942.43	1.053727	50849233.91	0.999967
10^{10}	455052511	434294481.90	1.047797	455055613.54	0.999993
10^{11}	4118054813	3948131653.67	1.043039	4118066399.58	0.999997
10^{12}	37607912018	36191206825.27	1.039145	37607950279.76	0.999999
10^{13}	346065536839	334072678387.12	1.035899	346065645809.01	1.000000
10^{14}	3204941750802	3102103442166.08	1.033151	3204942065690.91	1.000000
10^{15}	29844570422669	28952965460216.79	1.030795	29844571475286.54	1.000000
10^{16}	279238341033925	271434051189532.39	1.028752	279238344248555.75	1.000000
10^{17}	2623557157654233	2554673422960304.87	1.026964	2623557165610820.73	1.000000
10^{18}	24739954287740860	24127471216847323.76	1.025385	24739954309690413.98	1.000000
10^{19}	234057667276344607	228576043106974646.13	1.023982	234057667376222381.18	1.000000
10^{20}	2220819602560918840	2171472409516259138.26	1.022725	2220819602783663482.50	1.000000
10^{21}	21127269486018731928	20680689614440563221.48	1.021594	21127269486616126181.29	1.000000

Man sieht, dass $\mathrm{li}(x)$ die Primzahlzählfunktion $\pi(x)$ für größere x weit besser zu approximieren scheint als $\frac{x}{\log x}$. Was den möglichen Grenzwert betrifft, besteht allerdings kein Unterschied, da nach der Regel von l'Hospital gilt

$$\lim_{x\to\infty}\frac{\mathrm{li}(x)}{\frac{x}{\log x}}=\lim_{x\to\infty}\frac{\int_2^x\frac{dt}{\log t}}{\frac{x}{\log x}}=\lim_{x\to\infty}\frac{\frac{1}{\log x}}{\frac{1}{\log x}-\frac{1}{(\log x)^2}}=\lim_{x\to\infty}\frac{1}{1-\frac{1}{\log x}}=1.$$

Die Aussage des Primzahlsatzes $\lim_{x\to\infty}\frac{\pi(x)\log x}{x}=1$ ist also äquivalent zu $\lim_{x\to\infty}\frac{\pi(x)}{\mathrm{li}(x)}=1$.

Wir wollen nochmals die Approximation von $\pi(x)$ durch $\mathrm{li}(x)$ anschauen:

x	$\pi(x)$	$\mathrm{li}(x)$	$\mathrm{li}(x)-\pi(x)$	$\frac{(\mathrm{li}(x)-\pi(x))\log x}{\sqrt{x}}$
10^1	4	5.12	1.12	0.8158
10^2	25	29.08	4.08	1.8794
10^3	168	176.56	8.56	1.8708
10^4	1229	1245.09	16.09	1.4821
10^5	9592	9628.76	36.76	1.3385
10^6	78498	78626.50	128.50	1.7753
10^7	664579	664917.36	338.36	1.7246
10^8	5761455	5762208.33	753.33	1.3877
10^9	50847534	50849233.91	1699.91	1.1140
10^{10}	455052511	455055613.54	3102.54	0.7144
10^{11}	4118054813	4118066399.58	11586.58	0.9280
10^{12}	37607912018	37607950279.76	38261.76	1.0572
10^{13}	346065536839	346065645809.01	108970.01	1.0315
10^{14}	3204941750802	3204942065690.91	314888.91	1.0151
10^{15}	29844570422669	29844571475286.54	1052617.54	1.1497
10^{16}	279238341033925	279238344248555.75	3214630.75	1.1843
10^{17}	2623557157654233	2623557165610820.73	7956587.73	0.9849
10^{18}	24739954287740860	24739954309690413.98	21949553.98	0.9097
10^{19}	234057667276344607	234057667376222381.18	99877774.18	1.3818
10^{20}	2220819602560918840	2220819602783663482.50	222744642.50	1.0258
10^{21}	21127269486018731928	21127269486616126181.29	597394253.29	0.9135

Die Tabelle legt die Vermutung nahe, dass $0 < \frac{(\mathrm{li}(x)-\pi(x))\log x}{\sqrt{x}} < c$ mit einer Konstanten c für $x \geq x_c$ gilt[6], also

$$\mathrm{li}(x) - c\frac{\sqrt{x}}{\log x} < \pi(x) < \mathrm{li}(x) \quad \text{für} \quad x \geq x_c.$$

Dies ist aber falsch, wie Littlewood [7] gezeigt hat: Es gibt ein $c \in \mathbb{R}_{>0}$ und Folgen y_n und z_n mit $\lim_{n\to\infty} y_n = \infty$ und $\lim_{n\to\infty} z_n = \infty$, sodass für alle n

$$\pi(y_n) < \mathrm{li}(y_n) - c\frac{\sqrt{y_n}}{\log y_n}\log\log\log y_n \quad \text{und} \quad \mathrm{li}(z_n) + c\frac{\sqrt{z_n}}{\log z_n}\log\log\log z_n < \pi(z_n)$$

gilt. Unter Annahme der sogenannten Riemannschen Vermutung kann man aber immerhin beweisen, dass

$$|\pi(x) - \mathrm{li}(x)| \leq 3\sqrt{x}\log x \text{ für } x \geq 2$$

gilt [8].

Bemerkungen:

(1) Die Idee einer Primzahldichte $\frac{1}{\log x}$, wie von Gauß vermutet, ist natürlich verlockend. Für $a < b$ sollte man dann (unter geeigneten Voraussetzungen) haben

$$\#\{p : a \leq p \leq b\} \approx \int_a^b \frac{dt}{\log t}.$$

Dies ist allerdings problematisch, wie das folgende Beispiel zeigt.

(2) Es gilt

$$\int_{370262}^{370372} \frac{dt}{\log t} = 8.5789\ldots,$$

es gibt aber keine einzige Primzahl zwischen 370262 und 370372. (370261 und 370373 sind Primzahlen.)

---

[6] Im Anhang findet sich eine Untersuchung, wonach die Ungleichungen mit $c = 3$ im Intervall $8 \leq x \leq 10^5$ gelten.

[7] Ein Beweis findet sich bei [**Ingham 1932**, S.103].

[8] Dies ist zu finden bei [**Ruppert 2005**, Kapitel: Explizite Formeln für $\psi(x)$]

(3) Trotzdem ist die Vorstellung einer Dichte für Anwendungen manchmal sinnvoll. Wegen
$$\frac{1}{\log 10^{100}} \approx \frac{1}{230}$$
kann man sich vorstellen, dass um 10^{100} auf 230 Zahlen durchschnittlich eine Primzahl kommt. Die ersten zehn Primzahlen $> 10^{100}$ sind (wahrscheinlich)
$$10^{100}+267,\quad 10^{100}+949,\quad 10^{100}+1243,\quad 10^{100}+1293,\quad 10^{100}+1983,$$
$$10^{100}+2773,\quad 10^{100}+2809,\quad 10^{100}+2911,\quad 10^{100}+2967,\quad 10^{100}+3469.$$

5. Die Landau-Symbole

In der Analytischen Zahlentheorie versucht man häufig, komplexere Funktionen durch einfachere zu approximieren. Dabei sind die folgenden Schreibweisen nützlich.
Sei $D \subseteq \mathbb{R}$ eine Teilmenge, die ∞ als Häufungspunkt besitzt, und $f : D \to \mathbb{C}$, $\widetilde{f} : D \to \mathbb{C}$, $g : D \to \mathbb{R}$ Funktionen.

(1) Wir schreiben $f = O(g)$, wenn es eine Konstante $C \in \mathbb{R}_{>0}$ und ein $x_0 \in \mathbb{R}$ gibt mit
$$|f(x)| \le Cg(x) \quad \text{für alle } x \in D \text{ und } x \ge x_0.$$
Die Schreibweise $\widetilde{f} = f + O(g)$ meint $\widetilde{f} - f = O(g)$.

(2) Wir schreiben $f = o(g)$, wenn
$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$$
gilt. $\widetilde{f} = f + o(g)$ wird durch $\widetilde{f} - f = o(g)$ definiert.

(3) Wir schreiben $f \sim g$, wenn
$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$$
gilt, und sagen dann, dass f und g asymptotisch gleich sind.

Beispiele:

(1) Ist a_n eine Folge, so bedeutet $a_n = o(1)$, dass a_n gegen 0 konvergiert. $a_n = O(1)$ besagt, dass a_n eine beschränkte Folge ist.

(2) Der Logarithmus wächst langsamer als jede positive Potenz von x, also gilt für alle $\alpha > 0$
$$\log x = o(x^\alpha) \quad \text{und damit auch} \quad \log x = O(x^\alpha).$$

(3) Wir haben bereits gezeigt, dass $\lim_{x\to\infty} \frac{\mathrm{li}(x)}{\frac{x}{\log x}} = 1$ gilt. In der neuen Schreibweise heißt dies
$$\mathrm{li}(x) \sim \frac{x}{\log x}.$$
Die (noch unbewiesene) Aussage des Primzahlsatzes ist $\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1$, was man nun auch als
$$\pi(x) \sim \frac{x}{\log x} \sim \mathrm{li}(x)$$
schreiben kann.

Lemma. *Es gilt*
$$\frac{x}{\log x} \overset{x\ge 7}{<} \mathrm{li}(x) \overset{x\ge 2}{<} \frac{x}{\log x} + 2\frac{x}{(\log x)^2},$$
(Die linke Ungleichung gilt also für alle $x \ge 7$, die rechte für alle $x \ge 2$.) und etwas genauer
$$\frac{x}{\log x} + \frac{x}{(\log x)^2} \overset{x\ge 21}{<} \mathrm{li}(x) \overset{x\ge 2}{<} \frac{x}{\log x} + 2\frac{x}{(\log x)^2},$$
und damit
$$\mathrm{li}(x) = \frac{x}{\log x} + O(\frac{x}{(\log x)^2}).$$

Beweis:

(1) Wir definieren $f : [2, \infty) \to \mathbb{R}$ durch

$$f(x) = \int_2^x \frac{dt}{\log t} - \frac{x}{\log x}.$$

Für die Ableitung finden wir

$$f'(x) = \frac{1}{(\log x)^2},$$

also ist f streng monoton steigend. Wegen $f(6) \approx -0.17$, $f(7) \approx 0.11$ gilt $f(x) > 0$ für $x \geq 7$ und damit

$$\frac{x}{\log x} < \int_2^x \frac{dt}{\log t} \text{ für alle } x \geq 7.$$

(2) Wir definieren $g : [2, \infty) \to \mathbb{R}$ durch

$$g(x) = \frac{x}{\log x} + \frac{2x}{(\log x)^2} - \int_2^x \frac{dt}{\log t}.$$

Dann gilt für die Ableitung

$$g'(x) = \frac{1}{(\log x)^2} - \frac{4}{(\log x)^3} = \frac{\log x - 4}{(\log x)^3} = \frac{\log(\frac{x}{e^4})}{(\log x)^3}.$$

Die Funktion g hat daher ein Minimum in $x_0 = e^4 \approx 54.60$. Wegen $g(e^4) \approx 1.89$ gilt $g(x) > 0$ für alle $x \in [2, \infty)$. Es folgt

$$\mathrm{li}(x) < \frac{x}{\log x} + \frac{2x}{(\log x)^2} \quad \text{für alle} \quad x \geq 2.$$

(3) Wir definieren $h : [2, \infty) \to \mathbb{R}$ durch

$$h(x) = \int_2^x \frac{dt}{\log t} - \frac{x}{\log x} - \frac{x}{(\log x)^2}.$$

Für die Ableitung gilt

$$h'(x) = \frac{2}{(\log x)^3}.$$

Die Funktion h ist also streng monoton steigend. Mit SAGE (oder Maple) berechnet man $h(20) \approx -0.045$, $h(21) \approx 0.028$. Also ist $h(x) > 0$ für $x \geq 21$ und somit

$$\frac{x}{\log x} + \frac{x}{(\log x)^2} < \int_2^x \frac{dt}{\log t} \text{ für alle } x \geq 21.$$

(4) Für $x \geq 7$ folgt mit den gerade gezeigten Ungleichungen

$$|\mathrm{li}(x) - \frac{x}{\log x}| = \mathrm{li}(x) - \frac{x}{\log x} < 2\frac{x}{(\log x)^2},$$

was sofort $\mathrm{li}(x) = \frac{x}{\log x} + O(\frac{x}{(\log x)^2})$ beweist. ■

6. Wie groß ist die n-te Primzahl?

Die Primzahlen bilden eine Folge

$$p_1 = 2, \quad p_2 = 3, \quad p_3 = 5, \quad p_4 = 7, \quad p_5 = 11,$$

also kann man fragen, ob man etwas über die Größenordnung der n-ten Primzahl p_n sagen kann.

SATZ. *Es gilt die Äquivalenz:*

$$\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1 \quad \Longleftrightarrow \quad \lim_{n\to\infty} \frac{p_n}{n\log n} = 1,$$

was man auch in der Form

$$\pi(x) \sim \frac{x}{\log x} \quad \Longleftrightarrow \quad p_n \sim n\log n$$

schreiben kann. (Hat man also den Primzahlsatz $\pi(x) \sim \frac{x}{\log x}$ bewiesen, so folgt sofort $p_n \sim n\log n$.)

Beweis:

(1) Es gelte zunächst $\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1$. Setzen wir $x = p_n$ ein, so folgt wegen $\pi(\pi_n) = n$ die Aussage

$$\lim_{n\to\infty} \frac{n\log p_n}{p_n} = 1.$$

Logarithmieren liefert wegen der Stetigkeit von log sofort

$$\lim_{n\to\infty} (\log n + \log\log p_n - \log p_n) = 0,$$

woraus dann durch Multiplikation mit $\lim_{n\to\infty} \frac{1}{\log p_n} = 0$ die Beziehung

$$\lim_{n\to\infty} \left(\frac{\log n}{\log p_n} + \frac{\log\log p_n}{\log p_n} - 1 \right) = 0, \quad \text{also} \quad \lim_{n\to\infty} \left(\frac{\log n}{\log p_n} + \frac{\log\log p_n}{\log p_n} \right) = 1$$

folgt. Nun ist $\lim_{x\to\infty} \frac{\log x}{x} = 0$ und damit auch

$$\lim_{n\to\infty} \frac{\log\log p_n}{\log p_n} = 0,$$

sodass wir

$$\lim_{n\to\infty} \frac{\log n}{\log p_n} = 1$$

erhalten. Multiplizieren wir diese Beziehung mit $\lim_{n\to\infty} \frac{n\log p_n}{p_n} = 1$, so folgt

$$\lim_{n\to\infty} \frac{n\log n}{p_n} = 1, \quad \text{also} \quad p_n \sim n\log n,$$

wie behauptet.

(2) Es gelte nun $p_n \sim n\log n$, also $\lim_{n\to\infty} \frac{p_n}{n\log n} = 1$.

(a) Durch Logarithmieren folgt aus $\lim_{n\to\infty} \frac{p_n}{n\log n} = 1$

$$\lim_{n\to\infty} (\log p_n - \log n - \log\log n) = 0.$$

Multiplikation mit $\lim_{n\to\infty} \frac{1}{\log n} = 0$ liefert

$$\lim_{n\to\infty} \left(\frac{\log p_n}{\log n} - 1 - \frac{\log\log n}{\log n} \right) = 0.$$

Wegen $\lim_{n\to\infty} \frac{\log\log n}{\log n} = 0$ folgt

$$\lim_{n\to\infty} \frac{\log p_n}{\log n} = 1.$$

(b) Wir definieren zwei Folgen a_n und b_n durch

$$a_n = \frac{n\log p_n}{p_{n+1}} \quad \text{und} \quad a_n = \frac{n\log p_{n+1}}{p_n}.$$

Wegen

$$\begin{aligned} a_n &= \frac{n\log p_n}{p_{n+1}} = \frac{(n+1)\log(n+1)}{p_{n+1}} \cdot \frac{\log p_n}{\log n} \cdot \frac{n}{n+1} \cdot \frac{\log n}{\log(n+1)}, \\ b_n &= \frac{n\log p_{n+1}}{p_n} = \frac{n\log n}{p_n} \cdot \frac{\log p_{n+1}}{\log(n+1)} \cdot \frac{\log(n+1)}{\log n} \end{aligned}$$

folgt mit der Voraussetzung und (1) dann

$$\lim_{n\to\infty} a_n = 1 \quad \text{und} \quad \lim_{n\to\infty} b_n = 1.$$

(c) Sei nun $x \in \mathbb{R}_{\geq 2}$ und $n \in \mathbb{N}$ mit $p_n \leq x < p_{n+1}$. Dann ist $\pi(x) = n$ und damit

$$a_{\pi(x)} = a_n = \frac{n\log p_n}{p_{n+1}} < \frac{\pi(x)\log x}{x} < \frac{n\log p_{n+1}}{p_n} = b_n = b_{\pi(x)}.$$

Dies liefert sofort

$$\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1, \quad \text{also} \quad \pi(x) \sim \frac{x}{\log x},$$

wie behauptet. ■

Maple hat die Funktion `ithprime(n)`, die die n-te Primzahl angibt. Damit wurde folgende Tabelle erstellt. (In SAGE erhält man die n-te Primzahl mit `Primes().unrank(n-1)`.)

n	p_n	$n \log n$	$\frac{p_n}{n \log n}$
10	29	23.03	1.259454
20	71	59.91	1.185019
30	113	102.04	1.107453
40	173	147.56	1.172443
50	229	195.60	1.170750
60	281	245.66	1.143854
70	349	297.39	1.173525
80	409	350.56	1.166698
90	463	404.98	1.143258
100	541	460.52	1.174767
1000000	15485863	13815510.56	1.120904
2000000	32452843	29017315.48	1.118396
3000000	49979687	44742368.54	1.117055
4000000	67867967	60807219.68	1.116117
5000000	86028121	77124742.35	1.115441
6000000	104395301	93643620.16	1.114815
7000000	122949823	110329944.95	1.114383
8000000	141650939	127159616.80	1.113962
9000000	160481183	144114616.22	1.113566

7. Primzahlzwillinge

Ist p eine ungerade Primzahl, so ist $p+1$ eine gerade, also eine zusammengesetzte Zahl. $p+2$ ist wieder ungerade und damit möglicherweise eine Primzahl. Ist p und auch $p+2$ eine Primzahl, so nennt man $p, p+2$ **Primzahlzwillinge**.
In der folgenden Tabelle sind die Primzahlzwillingspaare bis 1000 aufgelistet:

$(3,5)$, $(5,7)$, $(11,13)$, $(17,19)$, $(29,31)$, $(41,43)$, $(59,61)$, $(71,73)$,
$(101,103)$, $(107,109)$, $(137,139)$, $(149,151)$, $(179,181)$, $(191,193)$, $(197,199)$,
$(227,229)$, $(239,241)$, $(269,271)$, $(281,283)$, $(311,313)$, $(347,349)$,
$(419,421)$, $(431,433)$, $(461,463)$, $(521,523)$, $(569,571)$, $(599,601)$,
$(617,619)$, $(641,643)$, $(659,661)$, $(809,811)$, $(821,823)$, $(827,829)$, $(857,859)$, $(881,883)$.

Die Anzahl der Primzahlzwillinge $\leq x$ bezeichnen wir mit $\pi_2(x)$, d.h. wir setzen

$$\pi_2(x) = |\{(p, p+2) : p, p+2 \text{ prim}, p \leq x\}|.$$

Es wird vermutet, dass es unendliche viele Primzahlzwillinge gibt, d.h. dass

$$\lim_{x \to \infty} \pi_2(x) = \infty$$

gilt, bewiesen ist dies aber bis heute nicht. Für die folgende Tabelle wurde $\pi_2(x)$ für verschiedene Werte von x mit Maple berechnet und mit anderen Funktionen verglichen:

x	$\pi_2(x)$	$\frac{\pi_2(x)\log x}{x}$	$\frac{\pi_2(x)(\log x)^2}{x}$	$\frac{\pi_2(x)(\log x)^3}{x}$	$\frac{\pi_2(x)}{\int_2^x \frac{dt}{(\log t)^2}}$
$4 = 2^2$	1	0.346574	0.480453	0.666049	0.520177
$8 = 2^3$	2	0.519860	1.081019	2.247916	0.615999
$10 = 10^1$	2	0.460517	1.060380	2.441614	0.546018
$16 = 2^4$	3	0.519860	1.441359	3.996296	0.653714
$32 = 2^5$	5	0.541521	1.876770	6.504388	0.804885
$64 = 2^6$	7	0.454878	1.891784	7.867707	0.834710
$100 = 10^2$	8	0.368414	1.696607	7.813166	0.780363
$128 = 2^7$	10	0.379065	1.839234	8.924020	0.869409
$256 = 2^8$	17	0.368234	2.041925	11.322838	1.050222
$512 = 2^9$	24	0.292421	1.824220	11.380077	1.021797
$1000 = 10^3$	35	0.241771	1.670098	11.536628	1.009080
$1024 = 2^{10}$	36	0.243685	1.689093	11.707898	1.023126
$2048 = 2^{11}$	62	0.230823	1.759941	13.418877	1.140732
$4096 = 2^{12}$	107	0.217285	1.807329	15.032941	1.239533
$8192 = 2^{13}$	177	0.194694	1.754369	15.808467	1.260035
$10000 = 10^4$	205	0.188812	1.739023	16.016990	1.263551
$16384 = 2^{14}$	290	0.171764	1.666806	16.174786	1.242698
$32768 = 2^{15}$	505	0.160235	1.666000	17.321744	1.280202
$65536 = 2^{16}$	860	0.145534	1.614022	17.900075	1.271159
$100000 = 10^5$	1224	0.140918	1.622381	18.678349	1.294198
$131072 = 2^{17}$	1526	0.137189	1.616566	19.048806	1.299211
$262144 = 2^{18}$	2679	0.127506	1.590848	19.848454	1.300319
$524288 = 2^{19}$	4750	0.119317	1.571382	20.694783	1.302879
$1000000 = 10^6$	8169	0.112859	1.559203	21.541191	1.307673
$1048576 = 2^{20}$	8535	0.112839	1.564280	21.685527	1.312956
$2097152 = 2^{21}$	15500	0.107584	1.565998	22.794814	1.328424
$4194304 = 2^{22}$	27995	0.101781	1.552090	23.668187	1.328943
$8388608 = 2^{23}$	50638	0.096237	1.534240	24.459441	1.324541
$10000000 = 10^7$	58980	0.095065	1.532259	24.697100	1.325407

Schaut man sich die vorangegangene Tabelle an, so kann man Vermutungen über das Wachstumsverhalten von $\pi_2(x)$ aufstellen. Tatsächlich gibt es heuristische Überlegungen, die die asymptotische Gleichheit

$$\pi_2(x) \sim c\frac{x}{(\log x)^2} \sim c\int_2^x \frac{dt}{(\log t)^2}$$

vermuten lassen [9]. Dabei ist

$$c = 2\prod_{p\geq 3}\left(1 - \frac{1}{(p-1)^2}\right) = 1.32032\ldots$$

(Die asymptotische Gleichheit $\frac{x}{(\log x)^2} \sim \int_2^x \frac{dt}{(\log t)^2}$ sieht man wieder mit der Regel von l'Hospital.)

Bemerkungen:

(1) Es wird auch nach großen Primzahlzwillingen gesucht. Der aktuelle Rekord (Stand: Februar 2024) ist das Paar

$$2996863034895 \cdot 2^{1290000} \pm 1,$$

das am 14. September 2016 gefunden wurde[10].

[9] Siehe [**Hardy/Wright 1979**, S.371-373].

[10] Siehe Stichwort „Twin Prime Search“ unter Wikipedia.

(2) Chen bewies, dass es unendlich viele Primzahlen p gibt, sodass $p+2$ eine Primzahl oder das Produkt zweier Primzahlen p_1p_2 ist [11].

8. Kleine Abstände zwischen Primzahlen

Sei $p_1 = 2, p_2 = 3, p_3 = 5, \ldots$ die Folge der Primzahlen. Man kann natürlich auch fragen, welche Abstände $p_{n+1} - p_n$ überhaupt auftreten und wie sie verteilt sind.
In der folgenden Tabelle wurden alle Primzahlen $\leq 10^7$ betrachtet. Für die folgende Tabelle sei $a(d)$ die Anzahl der Primzahlen $p_n \leq 10^7$ mit $d = p_{n+1} - p_n$, also

$$a(d) = |\{n : p_n \leq 10^7 \text{ und } p_{n+1} - p_n = d\}| :$$

d	$a(d)$	d	$a(d)$	d	$a(d)$
1	1	50	2048	100	36
2	58980	52	1449	102	34
4	58621	54	2403	104	21
6	99987	56	1072	106	12
8	42352	58	1052	108	26
10	54431	60	1834	110	11
12	65513	62	543	112	11
14	35394	64	559	114	11
16	25099	66	973	116	7
18	43851	68	358	118	4
20	22084	70	524	120	10
22	19451	72	468	122	3
24	27170	74	218	124	4
26	12249	76	194	126	8
28	13256	78	362	128	2
30	21741	80	165	130	1
32	6364	82	100	132	5
34	6721	84	247	134	1
36	10194	86	66	136	2
38	4498	88	71	138	2
40	5318	90	141	140	2
42	7180	92	37	146	1
44	2779	94	39	148	2
46	2326	96	65	152	1
48	3784	98	29	154	1

Die Vermutung, dass es unendlich viele Primzahlzwillinge gibt, ist gleichwertig mit

$$\liminf_{n\to\infty}(p_{n+1} - p_n) = 2.$$

Dies ist zwar noch nicht bewiesen, aber kürzlich gelang es Zhang [Zhang], die Aussage

$$\liminf_{n\to\infty}(p_{n+1} - p_n) \leq 7 \cdot 10^7$$

zu zeigen. Maynard [Maynard2013, Theorem 1.3] konnte zeigen, dass

$$\liminf_{n\to\infty}(p_{n+1} - p_n) \leq 600$$

gilt. (Es gibt zur Zeit auch Anstrengungen, die Schranke 600 noch zu verkleinern[12].)

[11] Siehe [**Crandall/Pomerance 2005**, S.16].
[12] Siehe *polymath8b* im Internet.

9. Große Abstände zwischen Primzahlen

Wir bezeichnen wieder mit p_n die Folge der Primzahlen. $d_n = p_{n+1} - p_n$ ist dann der Abstand von p_n zur nächsten Primzahl p_{n+1}. Es ist $p_2 - p_1 = 3 - 2 = 1$ und $p_{n+1} - p_n \geq 2$ für $n \geq 2$. Die Vermutung, dass es unendlich viele Primzahlzwillinge gibt, ist gleichwertig mit $\liminf(p_{n+1} - p_n) = 2$. Wir wollen jetzt anschauen, wie groß $p_{n+1} - p_n$ werden kann.

In der folgenden Tabelle ist p_n angegeben, wenn der Abstand $d_n = p_{n+1} - p_n$ größer ist als bei allen vorangegangenen Primzahlen.

p_n	$d_n = p_{n+1} - p_n$	$\frac{d_n}{p_n}$	$\frac{d_n}{\sqrt{p_n}}$	$\frac{d_n}{\log p_n}$	$\frac{d_n}{(\log p_n)^2}$
2	1	0.500000	0.707107	1.442695	2.081369
3	2	0.666667	1.154701	1.820478	1.657071
7	4	0.571429	1.511858	2.055593	1.056366
23	6	0.260870	1.251086	1.913574	0.610294
89	8	0.089888	0.847998	1.782278	0.397065
113	14	0.123894	1.317009	2.961466	0.626449
523	18	0.034417	0.787085	2.875592	0.459390
887	20	0.022548	0.671534	2.946443	0.434076
1129	22	0.019486	0.654750	3.129851	0.445271
1327	34	0.025622	0.933348	4.728345	0.657566
9551	36	0.003769	0.368365	3.928244	0.428642
15683	44	0.002806	0.351349	4.554709	0.471486
19609	52	0.002652	0.371343	5.261164	0.532305
31397	72	0.002293	0.406339	6.953520	0.671548
155921	86	0.000552	0.217794	7.192377	0.601515
360653	96	0.000266	0.159855	7.502537	0.586334
370261	112	0.000302	0.184062	8.735012	0.681254
492113	114	0.000232	0.162507	8.697998	0.663642
1349533	118	0.000087	0.101576	8.359741	0.592248
1357201	132	0.000097	0.113306	9.347823	0.661983
2010733	148	0.000074	0.104372	10.197044	0.702566
4652353	154	0.000033	0.071398	10.030689	0.653342
17051707	180	0.000011	0.043590	10.809668	0.649161
20831323	210	0.000010	0.046011	12.461452	0.739466
47326693	220	0.000005	0.031979	12.448660	0.704405
122164747	222	0.000002	0.020085	11.922100	0.640254
189695659	234	0.000001	0.016990	12.276420	0.644062
191912783	248	0.000001	0.017902	13.002980	0.681764
387096133	250	0.000001	0.012707	12.642747	0.639356
436273009	282	0.000001	0.013501	14.175286	0.712549
1294268491	288	0.000000	0.008005	13.726567	0.654231
1453168141	292	0.000000	0.007660	13.840823	0.656056
2300942549	320	0.000000	0.006671	14.844652	0.688637

Mit Hilfe des folgenden Satzes ist es nicht schwer, große Intervalle zu konstruieren, die keine Primzahl enthalten.

SATZ. *Ist $m \geq 2$, so sind alle Zahlen zwischen $m! + 2$ und $m! + m$ zusammengesetzt, d.h. das Intervall $[m! + 2, m! + m]$ enthält keine Primzahl.*

Beweis: Für $2 \leq i \leq m$ gilt $i \mid m! + i$ und $1 < i < m! + i$, sodass also i ein nichttrivialer Teiler von $m! + i$ ist. Daher ist $m! + i$ zusammengesetzt, was wir zeigen wollten. ■

Im nächsten Satz wird das letzte Argument noch etwas verfeinert.

SATZ. *Sei $k \geq 3$ und $p_1, p_2, p_3, \ldots$ die Folge der Primzahlen.*

(1) *Alle Zahlen zwischen $p_1 \ldots p_k - p_k - 1$ und $p_1 \ldots p_k - 2$ sind zusammengesetzt.*
(2) *Sei $n = n(k)$ so gewählt, dass $p_{n(k)}$ die größte Primzahl $\leq p_1 \ldots p_k - 2$ ist. Dann gilt*

$$p_{n(k)} \leq p_1 \ldots p_k - p_k - 2 \quad \text{und} \quad p_{n(k)+1} \geq p_1 \ldots p_k - 1.$$

(3) *Es ist*

$$p_{n(k)+1} - p_{n(k)} \geq p_k + 1.$$

(4) *Es gilt*

$$\frac{p_{n(k)+1} - p_{n(k)}}{\log p_{n(k)}} \geq \frac{p_k}{\log(p_1 \ldots p_k)}.$$

Beweis:

(1) Wegen $k \geq 3$ gilt $p_1 \ldots p_k - p_k - 1 = (p_1 \ldots p_{k-1} - 1)p_k - 1 \geq (2 \cdot 3 - 1) \cdot p_k - 1 \geq 5p_k - 1 > 5 \cdot 5 - 1 = 24$. Die Zahl $p_1 \ldots p_k - p_k - 1$ ist gerade, also zusammengesetzt. Wir betrachten nun die Zahlen $p_1 \ldots p_k - i$ mit $2 \leq i \leq p_k$. Die Zahl i hat dann einen Primteiler $p_j \leq p_k$, also folgt $p_j \mid p_1 \ldots p_k - i$. Nach obiger Abschätzung ist $p_1 \ldots p_k - i > p_k \geq p_j$, also ist p_j nichttrivialer Teiler, die Zahl also zusammengesetzt, was zu zeigen war.
(2) Da alle Zahlen zwischen $p_1 \ldots p_k - p_k - 1$ zusammengesetzt sind, folgt aus der Definition von p_n sofort $p_n \leq p_1 \ldots p_k - p_k - 2$. Die Abschätzung $p_{n+1} \geq p_1 \ldots p_k - 1$ ist dann trivial.
(3) Aus (2) folgt

$$p_{n(k)+1} - p_{n(k)} \geq (p_1 \ldots p_k - 1) - (p_1 \ldots p_k - p_k - 2) = p_k + 1,$$

wie behauptet.
(4) Mit (3) und $p_{n(k)} \leq p_1 \ldots p_k - p_k - 2 \leq p_1 \ldots p_k$ ergibt sich

$$\frac{p_{n(k)+1} - p_{n(k)}}{\log p_{n(k)}} \geq \frac{p_k}{\log(p_1 \ldots p_k)},$$

wie behauptet. ■

Beispiele: Die folgenden Beispiele demonstrieren die Aussage des Satzes:

k	p_k	p_n	$p_1 \ldots p_k - p_k - 2$	$p_1 \ldots p_k - 1$	p_{n+1}	$p_{n+1} - p_n$
3	5	23	23	29	29	6
4	7	199	201	209	211	12
5	11	2297	2297	2309	2309	12
6	13	30013	30015	30029	30029	16
7	17	510481	510491	510509	510529	48
8	19	9699667	9699669	9699689	9699713	46
9	23	223092827	223092845	223092869	223092907	80
10	29	6469693189	6469693199	6469693229	6469693291	102

Wegen $\lim_{k\to\infty} p_k = \infty$ folgt aus Teil (3) des letzten Satzes sofort:

SATZ. $\limsup_{n\to\infty}(p_{n+1} - p_n) = \infty$, *d.h. die Abstände zwischen benachbarten Primzahlen werden beliebig groß.*

Wie groß kann der Abstand $d_n = p_{n+1} - p_n$ im Verhältnis zu p_n werden? Wir geben ein paar Ergebnisse ohne Beweise an.

Bemerkungen:

(1) Teil (4) des vorangegangenen Satzes besagt

$$\frac{p_{n(k)+1}-p_{n(k)}}{\log p_{n(k)}} \geq \frac{p_k}{\log(p_1 \dots p_k)} \quad \text{für alle } k \geq 3.$$

Nun werden wir sehen, dass der Primzahlsatz

$$\lim_{k\to\infty} \frac{p_k}{\log(p_1 \dots p_k)} = 1$$

liefert. Daher folgt

$$\limsup_{n\to\infty} \frac{p_{n+1}-p_n}{\log p_n} \geq 1.$$

(2) Ein aktuelles Resultat von J. Maynard ist [Maynard2014]

$$\limsup_{n\to\infty} \frac{p_{n+1}-p_n}{\log p_n} \cdot \frac{(\log\log\log p_n)^2}{(\log\log p_n)(\log\log\log\log p_n)} = \infty.$$

Ein ähnliches Ergebnis findet sich bei [FordGreenKonyaginTao2014]. Vorläufer dieses Resultats stammen von Westzynthius, Erdös, Rankin, Pintz.

Wir stellen nun Aussagen zusammen, die den Abstand $d_n = p_{n+1} - p_n$ in Abhängigkeit von p_n nach oben abschätzen.

Bemerkungen:

(1) Das Bertrandsche Postulat, das wir später beweisen werden, besagt, dass für jedes $n \in \mathbb{N}$ eine Primzahl p mit $n < p \leq 2n$ existiert. Damit folgt $p_n < p_{n+1} < 2p_n$, also

$$p_{n+1} - p_n < p_n,$$

insbesondere also $p_{n+1} - p_n = O(p_n)$.

(2) Setzen wir den Primzahlsatz in der Form $p_n \sim n\log n$ voraus, so folgt mit $\lim_{n\to\infty} \frac{p_n}{n\log n} = 1$ und $\lim_{n\to\infty} \frac{n}{n+1} = \lim_{n\to\infty} \frac{\log n}{\log(n+1)} = 1$

$$\begin{aligned}\lim_{n\to\infty} \frac{p_{n+1}-p_n}{p_n} &= \lim_{n\to\infty} \frac{p_{n+1}}{p_n} - 1 = \\ &= \lim_{n\to\infty} \frac{p_{n+1}}{(n+1)\log(n+1)} \cdot \frac{n\log n}{p_n} \cdot \frac{n+1}{n} \cdot \frac{\log(n+1)}{\log n} - 1 = 1 - 1 = 0,\end{aligned}$$

also

$$p_{n+1} - p_n = o(p_n).$$

(3) Der Mittelwert der ersten n Primzahlabstände ist

$$D_n = \frac{1}{n}\sum_{k=1}^{n}(p_{k+1} - p_k) = \frac{1}{n}(p_{n+1} - 2).$$

Setzen wir wieder den Primzahlsatz voraus, so haben wir beim Beweis von $\lim_{n\to\infty} \frac{p_n}{n\log n} = 1$ gesehen, dass $\lim_{n\to\infty} \frac{\log p_n}{\log n} = 1$ gilt; außerdem haben wir in (2) die Aussage $\lim_{n\to\infty} \frac{p_{n+1}}{p_n} = 1$ hergeleitet. Damit folgt dann

$$\lim_{n\to\infty} \frac{D_n}{\log p_n} = \lim_{n\to\infty} \left(\frac{p_{n+1}}{n\log p_n} - \frac{2}{n\log p_n} \right) = \lim_{n\to\infty} \left(\frac{p_{n+1}}{p_n} \cdot \frac{p_n}{n\log n} \cdot \frac{\log n}{\log p_n} \right) = 1,$$

d.h.

$$D_n \sim \log p_n.$$

(4) Die Abschätzungen aus (1) und (2) wurden im Laufe der Zeit immer wieder verbessert [Ribenboim, S.195]. Wir erwähnen nur die Abschätzung

$$p_{n+1} - p_n = O(p_n^{0.625})$$

von Ingham aus dem Jahre 1937 und

$$p_{n+1} - p_n = O(p_n^{0.525})$$

von Baker, Harman und Pintz aus dem Jahr 2001 [BakerHarmanPintz].

(5) Setzt man die Richtigkeit der Riemannschen Vermutung voraus, so gilt [13]

$$\pi(x) = \int_2^x \frac{dt}{\log t} + R(x) \quad \text{mit} \quad |R(x)| \leq 3\sqrt{x}\log x \quad \text{für} \quad x \geq 2.$$

Sei $0 < \varepsilon < 1$ beliebig. Dann ist wegen $\pi(p_{n+1} - \varepsilon) = n = \pi(p_n)$

$$\begin{aligned}\frac{(p_{n+1}-\varepsilon)-p_n}{\log(p_{n+1}-\varepsilon)} &\leq \int_{p_n}^{p_{n+1}-\varepsilon} \frac{dt}{\log t} = \int_2^{p_{n+1}-\varepsilon} \frac{dt}{\log t} - \int_2^{p_n} \frac{dt}{\log t} = \\ &= \Big(\pi(p_{n+1}-\varepsilon) - R(p_{n+1}-\varepsilon)\Big) - \Big(\pi(p_n) - R(p_n)\Big) = \\ &= R(p_n) - R(p_{n+1}-\varepsilon) \leq 3\left(\sqrt{p_n}\log p_n + \sqrt{p_{n+1}-\varepsilon}\log(p_{n+1}-\varepsilon)\right).\end{aligned}$$

Das Bertrandsche Postulat, das im nächsten Kapitel bewiesen wird, liefert $p_{n+1} \leq 2p_n$, außerdem gilt für $x \geq 2$ die Abschätzung $\log(2x) \leq 2\log x$. Damit folgt weiter

$$\begin{aligned}p_{n+1} - p_n - \varepsilon &\leq 3\left(\sqrt{p_n}\log p_n + \sqrt{p_{n+1}-\varepsilon}\log(p_{n+1}-\varepsilon)\right)\log(p_{n+1}-\varepsilon) \leq \\ &\leq 3\left(\sqrt{p_n}\log p_n + \sqrt{2p_n}\log(2p_n)\right)\log(2p_n) \leq \\ &\leq 3\left(\sqrt{p_n}\log p_n + \sqrt{2}\sqrt{p_n}\cdot 2\log p_n\right)\cdot 2\log p_n = \\ &= 3\cdot 2\cdot(1+2\sqrt{2})\cdot\sqrt{p_n}(\log p_n)^2 \leq 23\sqrt{p_n}(\log p_n)^2.\end{aligned}$$

Da $\varepsilon > 0$ beliebig klein gewählt werden kann, folgt

$$p_{n+1} - p_n \leq 23\sqrt{p_n}(\log p_n)^2,$$

insbesondere also

$$p_{n+1} - p_n = O(p_n^{0.5}(\log p_n)^2).$$

Cramér konnte dies unter Annahme der Riemannschen Vermutung verschärfen zu[14]

$$p_{n+1} - p_n = O(p_n^{0.5}\log p_n).$$

(6) Cramér[15] vermutete, dass sogar

$$p_{n+1} - p_n = O((\log p_n)^2)$$

gilt. (Vergleiche auch die Tabelle zu Beginn des Abschnitts, speziell die Werte von $\frac{p_{n+1}-p_n}{(\log p_n)^2}$.)

10. Primzahldrillinge

Wir fragen nun nach Primzahldrillingen, d.h. nach Tripeln $(p, p+2, p+4)$, wo $p, p+2, p+4$ Primzahlen sind. Das einfachste Beispiel ist $(3, 5, 7)$. Schaut man sich weiter um, findet man nichts. Warum?

SATZ. *Sind p, $p+2$ und $p+4$ Primzahlen, so ist $(p, p+2, p+4) = (3, 5, 7)$.*

Beweis: Wir dividieren p durch 3 mit Rest und erhalten eine Darstellung

$$p = 3q + r \quad \text{mit } 0 \leq r \leq 2 \quad \text{und} \quad q \geq 1.$$

Es gibt also drei Fälle:

(1) $r = 0$. Dann ist $p = 3q$. Da p Primzahl ist, folgt $q = 1$ und damit das angegebene Beispiel.
(2) $r = 1$. Dann ist $p + 2 = (3q + 1) + 2 = 3q + 3 = 3(q + 1)$, was nicht sein kann.
(3) $r = 2$. Dann ist $p + 4 = (3q + 2) + 4 = 3q + 6 = 3(q + 2)$, was ebenso nicht sein kann.

Also gibt es tatsächlich nur die behauptete Lösung. ■

Wir wollen die Vorgehensweise nochmals anschauen und setzen jetzt $p > 3$ voraus. Wir schreiben $p = 3q+r$ mit $r \in \{1, 2\}$ und $q \geq 1$.

---

[13] Dies findet sich bei [**Ruppert 2005**, Kapitel: Explizite Formeln für $\psi(x)$].
[14] Siehe [**Cramér 1920**] oder [**Brüdern 1995**, Aufgabe 1, S.232].
[15] Siehe [**Cramér 1936**] oder [**Tenenbaum, Mendès France 2000**, S.61-66].

(1) Ist $r = 1$, also $p \equiv 1 \bmod 3$, so ist

$$p = 3q + 1, \quad p + 2 = 3q + 3 = 3(q + 1), \quad p + 4 = 3q + 5, \quad p + 6 = 3q + 7.$$

Von den Zahlen $p, p + 4, p + 6$ ist also keine durch 3 teilbar.

(2) Ist $r = 2$, also $p \equiv 2 \bmod 3$, so ist

$$p = 3q + 2, \quad p + 2 = 3q + 4, \quad p + 4 = 3q + 6 = 3(q + 2), \quad p + 6 = 3q + 8.$$

Von den Zahlen $p, p + 2, p + 6$ ist also keine durch 3 teilbar.

Die folgende Tabellen zeigen, dass es sowohl Primzahltripel $(p, p + 4, p + 6)$ als auch $(p, p + 2, p + 6)$ vorkommen.

p	$p+4$	$p+6$
7	11	13
13	17	19
37	41	43
67	71	73
97	101	103
103	107	109
193	197	199
223	227	229
277	281	283
307	311	313
457	461	463
613	617	619
823	827	829
853	857	859
877	881	883

p	$p+2$	$p+6$
5	7	11
11	13	17
17	19	23
41	43	47
101	103	107
107	109	113
191	193	197
227	229	233
311	313	317
347	349	353
461	463	467
641	643	647
821	823	827
857	859	863
881	883	887

Auch hier kann man Vermutungen anstellen, was im nächsten Abschnitt passieren wird.

11. Die Primzahl-k-Tupel-Vermutung

Gegeben seien k ganze Zahlen $a_1 < a_2 < \cdots < a_k$. Uns interessiert die Frage, ob es passieren kann, dass für unendlich viele $n \in \mathbb{N}$ das k-Tupel

$$(n + a_1, n + a_2, \ldots, n + a_k)$$

nur aus Primzahlen besteht. Wir werden zunächst eine Eigenschaft betrachten, die dafür notwendig ist.

Ein k-Tupel $(a_1, a_2, \ldots, a_k) \in \mathbb{Z}^k$ mit $a_1 < a_2 < \cdots < a_k$ heißt **zulässig**, wenn für alle Primzahlen ℓ die Bilder der a_i in $\mathbb{Z}/\ell\mathbb{Z}$ nicht ganz $\mathbb{Z}/\ell\mathbb{Z}$ sind, d.h.

$$\{\overline{a_1}^{\bmod \ell}, \ldots, \overline{a_k}^{\bmod \ell}\} \neq \mathbb{Z}/\ell\mathbb{Z} = \{\overline{0}^{\bmod \ell}, \overline{1}^{\bmod \ell}, \ldots, \overline{\ell - 1}^{\bmod \ell}\}.$$

(Wegen $\#\mathbb{Z}/\ell\mathbb{Z} = \ell$ ist dies für $\ell > k$ immer der Fall.) Alternativ kann man sagen: $(a_1, a_2, \ldots, a_k)$ ist genau dann zulässig, wenn für jede Primzahl $\ell \leq k$ eine Zahl u_ℓ existiert mit

$$a_1 \not\equiv u_\ell \bmod \ell, \quad a_2 \not\equiv u_\ell \bmod \ell, \quad \ldots \quad a_k \not\equiv u_\ell \bmod \ell.$$

(D.h. von $a_1, \ldots, a_k$ wird mindestens eine Restklasse modulo ℓ ausgelassen.)

Beispiele:

(1) $(a_1, a_2) = (0, 2)$ ist zulässig, denn $a_i \not\equiv 1 \bmod 2$ für $i = 1, 2$.
(2) $(a_1, a_2, a_3) = (0, 2, 6)$ ist zulässig, denn $a_i \not\equiv 1 \bmod 2$ und $a_i \not\equiv 1 \bmod 3$.

Bemerkung: Ist $(a_1, \ldots, a_k)$ ein zulässiges k-Tupel, so ist für alle $m \in \mathbb{Z}$ auch $(a_1 + m, \ldots, a_k + m)$ ein zulässiges k-Tupel. (Gilt $a_i \not\equiv u_\ell \bmod \ell$, so ist $a_i + m \not\equiv u_\ell + m \bmod \ell$ für alle Primzahlen $\ell \leq k$ und $i = 1, \ldots, k$.) Daher kann man praktisch auch $a_0 = 0$ wählen.

LEMMA. *Sei $(a_1, \ldots, a_k) \in \mathbb{Z}^k$ (mit $a_1 < a_2 < \cdots < a_k$) kein zulässiges k-Tupel. Dann gilt:*

(1) *Es gibt eine Primzahl* $\ell \leq k$ *mit*

$$\{\overline{a_1}^{\bmod \ell}, \ldots, \overline{a_k}^{\bmod \ell}\} = \{\overline{0}^{\bmod \ell}, \overline{1}^{\bmod \ell}, \ldots, \overline{\ell-1}^{\bmod \ell}\}.$$

(Für das Folgende sei diese Primzahl fest gewählt.)

(2) *Für jedes* $n \in \mathbb{Z}$ *gibt es einen Index* $i(n) \in \{1, \ldots, k\}$ *mit*

$$\ell \mid n + a_{i(n)}.$$

(3) *Für alle* $n \in \mathbb{Z}$ *mit* $n > k - a_1$ *ist* $n + a_{i(n)}$ *zusammengesetzt. (*$n + a_{i(n)}$ *hat den nichttrivialen Primteiler* ℓ*).*

(4) *Für alle* $n \in \mathbb{Z}$ *mit* $n > k - a_1$ *besteht das* k*-Tupel* $(n + a_1, n + a_2, \ldots, n + a_k)$ *nicht nur aus Primzahlen.*

Beweis:

(1) Wenn $(a_1, \ldots, a_k)$ nicht zulässig ist, so gibt es nach Definition eine Primzahl $\ell \leq k$ mit

$$\{\overline{a_1}^{\bmod \ell}, \ldots, \overline{a_k}^{\bmod \ell}\} = \{\overline{0}^{\bmod \ell}, \overline{1}^{\bmod \ell}, \ldots, \overline{\ell-1}^{\bmod \ell}\}.$$

(2) Zu $n \in \mathbb{Z}$ gibt es nach (1) einen Index $i(n)$ mit

$$\overline{-n}^{\bmod \ell} = \overline{a_{i(n)}}^{\bmod \ell},$$

d.h. $-n \equiv a_{i(n)} \bmod \ell$ und damit

$$\ell \mid n + a_{i(n)}.$$

(3) Ist $n \in \mathbb{Z}$ und $n > k - a_1$, so folgt

$$n + a_{i(n)} \geq n + a_1 > k \geq \ell.$$

Mit (2) sieht man, dass ℓ ein nichttrivialer Teiler von $n + a_{i(n)}$ ist.

(4) Dies folgt sofort aus (3). ■

Ist $(a_1, \ldots, a_k)$ ein k-Tupel mit $0 = a_1 < a_2 < \cdots < a_k$, sodass für unendlich viele $n \in \mathbb{N}$ das k-Tupel

$$(n + a_1, n + a_2, \ldots, n + a_k)$$

nur aus Primzahlen besteht, so muss $(a_1, \ldots, a_k)$ wegen des vorangegangenen Lemmas zulässig sein. Die Umkehrung ist eine Vermutung:

Die Primzahl-k-Tupel-Vermutung: *Ist* $(a_1, \ldots, a_k) \in \mathbb{Z}^k$ *mit* $a_1 < a_2 < \cdots < a_k$ *ein zulässiges* k*-Tupel, so gibt es unendlich viele Primzahl-*k*-Tupel der Gestalt*

$$(p_1, p_2, \ldots, p_k) = (n + a_1, n + a_2, \ldots, n + a_k).$$

Die Primzahl-k-Tupel-Vermutung ist im Fall $k \geq 2$ für kein zulässiges k-Tupel bewiesen.

Beispiele:

(1) $(a_1, a_2) = (0, 2)$ ist ein zulässiges 2-Tupel. Gilt die Primzahl-k-Tupel-Vermutung, sollte es unendlich viele Primzahlenpaare der Gestalt

$$(p_1, p_2) = (n, n + 2),$$

also Primzahlzwillinge geben.

(2) $(a_1, a_2, a_3) = (0, 2, 4)$ ist kein zulässiges 3-Tupel, da modulo 3 gilt $\overline{0} = \overline{0}$, $\overline{4} = \overline{1}$, $\overline{2} = \overline{2}$. Nach dem vorangegangenen Lemma kann es also nicht unendlich viele Primzahltripel der Gestalt

$$(p_1, p_2, p_3) = (n, n + 2, n + 4)$$

geben, was wir bereits zuvor gesehen haben.

(3) $(a_1, a_2, a_3) = (0, 2, 6)$ ist ein zulässiges 3-Tupel wegen

$$\{\overline{0}^{\bmod 2}, \overline{2}^{\bmod 2}, \overline{6}^{\bmod 2}\} = \{\overline{0}^{\bmod 2}\} \subsetneq \mathbb{Z}/2\mathbb{Z}$$

und

$$\{\overline{0}^{\bmod 3}, \overline{2}^{\bmod 3}\overline{6}^{\bmod 3}\} = \{\overline{0}^{\bmod 3}, \overline{2}^{\bmod 3}\} \subsetneq \mathbb{Z}/3\mathbb{Z},$$

was wir aber bereits gesehen haben. Gilt die Primzahl-k-Tupel-Vermutung, so sollte es unendlich viele Primzahltripel der Gestalt

$$(p_1, p_2, p_3) = (n, n+2, n+6)$$

geben. Genauso sieht man, dass $(0, 4, 6)$ ein zulässiges 3-Tupel ist.

Das folgende Lemma zeigt einen Weg, wie man an zulässige k-Tupel kommen kann:

LEMMA. *Sei $(p_1, p_2, \ldots, p_k)$ mit $p_1 < p_2 < \cdots < p_k$ ein k-Tupel aus Primzahlen. Gilt dann $p_1 > k$, so ist*

$$(p_1, p_2, \ldots, p_k)$$

ein zulässiges k-Tupel.

Beweis: Ist $\ell \leq k$ eine Primzahl, so gilt $\ell < p_i$ und damit $\ell \nmid p_i$, also $p_i \not\equiv 0 \bmod \ell$ für $i = 1, \ldots, k$. Daher ist $(p_1, \ldots, p_k)$ zulässig. ■

Dass die Voraussetzung $p_1 > k$ im Satz notwendig ist, sieht man an den nicht zulässigen Tupeln $(2, 3)$ und $(3, 5, 7)$.

12. Primzahlen als Werte von Polynomen

Beispiel: Euler bemerkte[16], dass das Polynom $x^2 - x + 41$ für $x = 1, \ldots, 40$ Primzahlen als Werte hat. (Natürlich nimmt das Polynom dann wegen $(1-x)^2 - (1-x) + 41 = x^2 - x + 41$ sogar zwischen -39 und 40 Primzahlen als Werte an.)

Es gibt aber kein nichtkonstantes Polynom, das nur Primzahlen als Werte annimmt:

SATZ. *Ist $f = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0$ ein nichtkonstantes Polynom mit $a_i \in \mathbb{Z}$ und $d \in \mathbb{N}$, so enthält die Menge*

$$\{f(n) : n \in \mathbb{N}\}$$

nicht nur Primzahlen.

Beweis: Wir nehmen das Gegenteil an. Sei $f(n) = p$. Dann folgt für $m \in \mathbb{N}$

$$f(pm + n) = \sum_{i=0}^{d} a_i (pm+n)^i \equiv \sum_{i=}^{d} a_i n^i = f(n) = p \equiv 0 \bmod p, \quad \text{also} \quad p \mid f(pm+n).$$

Da auch $f(pm+n)$ eine Primzahl sein sollte, folgt $f(pm+n) = p$, da $m \in \mathbb{Z}$ beliebig war, folgt, dass f konstant gleich p ist, ein Widerspruch zur Annahme. ■

Ist $f(x)$ ein nichtkonstantes Polynom mit ganzzahligen Koeffizienten, so kann die Menge

$$\{f(n) : n \in \mathbb{N}\}$$

also nicht nur Primzahlen enthalten. Eine Frage ist, ob die Menge unendlich viele Primzahlen enthält.

Wir werden später beweisen:

SATZ (Dirichletscher Primzahlsatz). *Ist $a \in \mathbb{N}$, $b \in \mathbb{Z}$ mit $\mathrm{ggT}(a, b) = 1$, so gibt es unendlich viele Primzahlen der Gestalt $an + b$, d.h. das Polynom $ax + b$ nimmt an ganzzahligen Stellen unendlich oft Primzahlen als Werte an.*

Auf den Spuren von Euklid zeigen wir elementar folgenden Satz:

[16] Siehe [**Ribenboim 2006**, S.143].

SATZ. (1) *Es gibt unendlich viele Primzahlen* $\equiv -1 \bmod 4$*, d.h. Primzahlen der Gestalt* $4n-1$.
(2) *Es gibt unendlich viele Primzahlen* $\equiv -1 \bmod 6$*, d.h. Primzahlen der Gestalt* $6n-1$.

Beweis: Wir konstruieren eine Folge von (paarweise verschiedenen) Primzahlen $q_n \equiv -1 \bmod 6$. Wir beginnen mit $q_1 = 5$. Seien nun $q_1, \ldots, q_n$ bereits konstruiert. Wir betrachten $N = 6q_1 \ldots q_n - 1$ und die zugehörige Primfaktorzerlegung

$$N = 6q_1 \ldots q_n - 1 = p_1^{e_1} \ldots p_r^{e_r}.$$

Was kann $p_i \bmod 6$ sein?

- $p_i \equiv 0 \bmod 6$ ist für keine Primzahl möglich.
- $p_i \equiv 2 \bmod 6$ oder $p_i \equiv 4 \bmod 6$ ist nur für $p_i = 2$ möglich, was aber hier wegen $N \equiv 1 \bmod 2$ nicht geht.
- $p_i \equiv 3 \bmod 6$ würde $p_i = 3$ implizieren, was hier aber durch $N \equiv -1 \bmod 3$ ausgeschlossen wird.

Also bleibt nur $p_i \equiv 1 \bmod 6$ oder $p_i \equiv 5 \equiv -1 \bmod 6$. Wäre $p_i \equiv 1 \bmod 6$ für alle i, so hätte man $N = \prod p_i^{e_i} \equiv 1 \bmod 6$, ein Widerspruch zu $N \equiv -1 \bmod 6$. Also gibt es mindestens einen Index i_0 mit $p_{i_0} \equiv -1 \bmod 6$. Daher können wir definieren

$$q_{n+1} = \min\{p : p \mid (6q_1 \ldots q_n - 1) \text{ und } p \equiv -1 \bmod 6\},$$

d.h. q_{n+1} ist der kleinste Primteiler von N, der $\equiv -1 \bmod 6$ ist. Wegen $q_{n+1} \mid N$ ist $q_{n+1} \neq q_i$ für $1 \leq i \leq n$. Damit haben wir mit q_{n+1} eine neue Primzahl $\equiv -1 \bmod 6$. Insbesondere muss es also unendlich viele Primzahlen $\equiv -1 \bmod 6$ geben. Genauso zeigt man, dass es unendlich viele Primzahlen $\equiv -1 \bmod 4$ gibt, wobei man hier $N = 4q_1 \ldots q_n - 1$ betrachtet. ■

Betrachtet man Polynome vom Grad ≥ 2, so ist praktisch nichts bewiesen.

Beispiel: Es ist nicht bekannt, ob es unendlich viele Primzahlen der Gestalt $n^2 + 1$ gibt.

Hindernisse: Wann kann ein nichtkonstantes Polynom $f(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0 \in \mathbb{Z}[x]$ (mit $d \in \mathbb{N}$ und $a_d \neq 0$) nicht unendlich viele Primzahlen darstellen?

(1) Gilt $f(x) = g(x)h(x)$ mit nichtkonstanten Polynomen $g(x), h(x) \in \mathbb{Z}[x]$, so ist $f(n) = g(n)h(n)$, die Zahl $f(n)$ hat also eine Faktorisierung, die im Allgemeinen nicht trivial ist, da $g(n)$ und $h(n)$ nur endlich oft ± 1 sein kann.
(2) Ist der höchste Koeffizient $a_d < 0$, so wird $f(n)$ für große n negativ, kann also keine Primzahl sein.
(3) Ist $\mathrm{ggT}(a_d, a_{d-1}, \ldots, a_0) > 1$, so kann es nur endlich viele Primzahlen der Gestalt $f(n)$ geben.
(4) Es gibt aber noch ein Hindernis, wie das Beispiel $x^2 + x + 2$ zeigt. Alle Werte sind hier gerade. Gilt

$$\mathrm{ggT}(\{f(n) : n \in \mathbb{Z}\}) > 1,$$

so kann es natürlich nicht unendlich viele Primzahlen der Gestalt $f(n)$ geben.

Vermutung von Bouniakowsky[17]**:** *Ist* $f(x) \in \mathbb{Z}[x]$ *irreduzibel mit positivem höchsten Koeffizienten und* $\mathrm{ggT}\{f(n) : n \in \mathbb{Z}\} = 1$*, so enthält die Menge*

$$\{f(n) : n \in \mathbb{N}\}$$

unendlich viele Primzahlen.

Beispiel: Nach der Vermutung von Bouniakowsky sollte es also unendlich viele Primzahlen der Gestalt $n^2 + 1$ geben. Hier sind die Primzahlen der Gestalt $n^2 + 1$ mit $1 \leq n \leq 100$:

$2 = 1^2 + 1$, $5 = 2^2 + 1$, $17 = 4^2 + 1$, $37 = 6^2 + 1$, $101 = 10^2 + 1$, $197 = 14^2 + 1$, $257 = 16^2 + 1$,
$401 = 20^2 + 1$, $577 = 24^2 + 1$, $677 = 26^2 + 1$, $1297 = 36^2 + 1$, $1601 = 40^2 + 1$, $2917 = 54^2 + 1$,
$3137 = 56^2 + 1$, $4357 = 66^2 + 1$, $5477 = 74^2 + 1$, $7057 = 84^2 + 1$, $8101 = 90^2 + 1$, $8837 = 94^2 + 1$.

Auch wenn man sich andere Beispiele anschaut, wirkt die Vermutung von Bouniakowsky experimentell recht plausibel.

[17] Siehe [**Bouniakowsky 1857**] oder [**Ribenboim 2006**, S.261]. Statt Bouniakowsky findet sich auch die Schreibweise Bunjakowski.

Die Vermutung von Bouniakowsky wurde von Schinzel[18] verallgemeinert:

Hypothese H: *Seien $f_1(x), \ldots, f_k(x) \in \mathbb{Z}[x]$ irreduzible, nichtkonstante Polynome mit höchstem Koeffizienten > 0, sodass*

$$\mathrm{ggT}(\{(\prod_{i=1}^{k} f_i)(n) : n \in \mathbb{Z}\}) = 1$$

gilt. Dann gibt es unendlich viele $n \in \mathbb{N}$, sodass alle Zahlen $f_1(n), \ldots, f_k(n)$ Primzahlen sind.

Bemerkung: Was passiert, wenn $\mathrm{ggT}(\{(\prod_{i=1}^{k} f_i)(n) : n \in \mathbb{Z}\}) > 1$ ist? Dann gibt es eine Primzahl p mit $p \mid \prod_{i=1}^{k} f_i(n)$ für alle $n \in \mathbb{Z}$. Für jedes $n \in \mathbb{Z}$ gibt es also einen Index i_n mit $p \mid f_{i_n}(n)$. Wegen $\lim_{n\to\infty} f_i(n) = \infty$ ist dann für alle hinreichend großen n die (große) Zahl $f_{i_n}(n)$ zusammengesetzt mit p als (einem kleinen) Primteiler. Will man also, dass für unendlich viele $n \in \mathbb{N}$ alle Zahlen $f_1(n), \ldots, f_k(n)$ Primzahlen sind, so ist $\mathrm{ggT}(\{(\prod_{i=1}^{k} f_i)(n) : n \in \mathbb{Z}\}) = 1$ sicher eine notwendige Bedingung.

Wir wollen die Mächtigkeit der Hypothese H an Hand einiger Beispiele zeigen:

Satz. *Sei $(a_1, \ldots, a_k) \in \mathbb{Z}^k$ ein zulässiges k-Tupel (mit $a_1 < a_2 < \cdots < a_k$). Dann gilt:*

1. *Die Polynome $x + a_1, \ldots, x + a_k$ erfüllen die Voraussetzungen der Hypothese H.*
2. *Gilt die Hypothese H, so gilt die Primzahl-k-Tupel-Vermutung, d.h. es gibt unendlich viele $n \in \mathbb{N}$, sodass das k-Tupel $(n+a_1, \ldots, n+a_k)$ nur aus Primzahlen besteht. (Es gibt also unendlich viele Primzahl-k-Tupel der Gestalt $(n + a_1, \ldots, n + a_k)$.)*

Beweis:

1. Trivialerweise sind die Polynome $x + a_i$ irreduzibel und haben positiven höchsten Koeffizienten. Angenommen, es gäbe eine Primzahl ℓ mit $\ell \mid \mathrm{ggT}(\{(\prod_{i=1}^{k} f_i)(n) : n \in \mathbb{Z}\})$. Dann würde $\ell \mid (n + a_1) \ldots (n + a_k)$ für alle $n \in \mathbb{Z}$ gelten, es gäbe also für jedes $n \in \mathbb{Z}$ einen Index $i(n)$ mit $\ell \mid n + a_{i(n)}$ und somit $-n \equiv a_{i(n)} \bmod \ell$, was zu
$$\begin{aligned} \mathbb{Z}/\ell\mathbb{Z} &= \{\overline{-0}^{\bmod \ell}, \overline{-1}^{\bmod \ell}, \ldots, \overline{-(\ell-1)}^{\bmod \ell}\} = \\ &= \{\overline{a_{i(0)}}^{\bmod \ell}, \overline{a_{i(1)}}^{\bmod \ell}, \ldots, \overline{a_{i(\ell-1)}}^{\bmod \ell}\} \subseteq \\ &\subseteq \{\overline{a_1}^{\bmod \ell}, \ldots, \overline{a_k}^{\bmod \ell}\} \subseteq \mathbb{Z}/\ell\mathbb{Z}, \end{aligned}$$
also
$$\{\overline{a_1}^{\bmod \ell}, \ldots, \overline{a_k}^{\bmod \ell}\} = \mathbb{Z}/\ell\mathbb{Z}$$
führen würde, im Widerspruch zur Voraussetzung, dass das k-Tupel $(a_1, \ldots, a_k)$ zulässig sein sollte. Also kann dieser Fall nicht eintreten und es muss gelten
$$\mathrm{ggT}(\{(n + a_1) \ldots (n + a_k) : n \in \mathbb{Z}\}) = 1.$$
Damit folgt sofort, dass die Voraussetzungen der Hypothese H erfüllt sind.
2. Dies ist eine Anwendung der Hypothese H auf die Polynome $x + a_1, \ldots, x + a_k$. ■

Da $(0, 2)$, $(0, 2, 6)$ und $(0, 4, 6)$ zulässige k-Tupel sind, folgt nun auch:

Folgerung. *Gilt die Hypothese H, so gilt auch:*

1. *Es gibt unendlich viele Primzahlzwillinge.*
2. *Es gibt unendlich viele Primzahltripel der Gestalt $p, p + 2, p + 6$.*
3. *Es gibt unendlich viele Primzahltripel der Gestalt $p, p + 4, p + 6$.*

Eine andere Anwendung liefert der folgende Satz:

Satz. *Gilt die Hypothese H, so gibt es zu jeder natürlichen Zahl m Primzahlen p und q mit*
$$m = \frac{p+1}{q+1}.$$

[18] [**Schinzel/Sierpiński 1958**]

Beweis: Sei $m \in \mathbb{N}$ fest gewählt. Wir setzen $f_1(x) = mx + m - 1$, $f_2(x) = x$. Wir haben $f_1(-1)f_2(-1) = (-1)(-1) = 1$, also ist $\mathrm{ggT}(\{f_1(n)f_2(n) : n \in \mathbb{Z}\}) = 1$, also gibt es unter Annahme der Hypothese H ein $n \in \mathbb{N}$, sodass sowohl $p = f_1(n) = mn + m - 1$ als auch $q = f_2(n) = n$ prim sind. Es folgt $p + 1 = mn + m = mq + m = m(q + 1)$, was sofort die Behauptung liefert. ■

Beispiel: Hier sind die ersten natürlichen Zahlen geschrieben in der Form[19] $n = \frac{p+1}{q+1}$:

$$1 = \frac{2+1}{2+1}, \quad 2 = \frac{5+1}{2+1}, \quad 3 = \frac{11+1}{3+1}, \quad 4 = \frac{11+1}{2+1}, \quad 5 = \frac{19+1}{3+1}, \quad 6 = \frac{17+1}{2+1}, \quad 7 = \frac{41+1}{5+1}, \quad \dots$$

Wir wollen noch eine interessante Anwendung von Schinzels Hypothese H zeigen und schicken dafür ein Lemma voraus.

Lemma. *Ist p eine ungerade Primzahl, so gilt*

$$2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \equiv \begin{cases} 1 \bmod p & \text{für } p \equiv 1, 7 \bmod 8, \\ -1 \bmod p & \text{für } p \equiv 3, 5 \bmod 8. \end{cases}$$

Beweis: Wir berechnen das Produkt der geraden Zahlen zwischen 1 und p auf zwei Weisen.

$$\begin{aligned}
\prod_{\substack{1 \le i \le p \\ i \equiv 0 \bmod 2}} i &= \prod_{\substack{1 \le i \le \frac{p-1}{2} \\ i \equiv 0 \bmod 2}} i \cdot \prod_{\substack{\frac{p+1}{2} \le i \le p-1 \\ i \equiv 0 \bmod 2}} i = \prod_{\substack{1 \le i \le \frac{p-1}{2} \\ i \equiv 0 \bmod 2}} i \cdot \prod_{\substack{1 \le i \le \frac{p-1}{2} \\ i \equiv 1 \bmod 2}} (p-i) \overset{\bmod p}{\equiv} \\
&\overset{\bmod p}{\equiv} \prod_{\substack{1 \le i \le \frac{p-1}{2} \\ i \equiv 0 \bmod 2}} i \cdot (-1)^i \cdot \prod_{\substack{1 \le i \le \frac{p-1}{2} \\ i \equiv 1 \bmod 2}} i \cdot (-1)^i = \prod_{1 \le i \le \frac{p-1}{2}} i \cdot (-1)^i = \\
&= \left(\prod_{1 \le i \le \frac{p-1}{2}} i \right) \cdot (-1)^{\sum_{1 \le i \le \frac{p-1}{2}} i} = (\frac{p-1}{2})! \cdot (-1)^{\frac{1}{2} \cdot \frac{p-1}{2} \cdot \frac{p-1}{2}} = \\
&= (\frac{p-1}{2})! \cdot (-1)^{\frac{p^2-1}{8}} \bmod p, \\
\prod_{\substack{1 \le i \le p \\ i \equiv 0 \bmod 2}} i &= \prod_{\substack{2 \le i \le p-1 \\ i \equiv 0 \bmod 2}} i = \prod_{1 \le i \le \frac{p-1}{2}} 2i = \\
&= 2^{\frac{p-1}{2}} \cdot \prod_{1 \le i \le \frac{p-1}{2}} i = (\frac{p-1}{2})! \cdot 2^{\frac{p-1}{2}}.
\end{aligned}$$

Es folgt

$$p \mid (\frac{p-1}{2})! \cdot \left(2^{\frac{p-1}{2}} - (-1)^{\frac{p^2-1}{8}} \right).$$

Da alle Teiler von $(\frac{p-1}{2})!$ kleiner als $\frac{p}{2}$ sind, folgt $p \nmid (\frac{p-1}{2})!$ und damit

$$2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \bmod p.$$

Wir schreiben nun $p = 8m + r$ mit $r \in \{1, 3, 5, 7\}$ und erhalten

$$(-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{1}{8}(64m^2+16mr+r^2-1)} = (-1)^{8m^2+2mr+\frac{r^2-1}{8}} = (-1)^{\frac{r^2-1}{8}} = \begin{cases} 1 & \text{für } r = 1, 7, \\ -1 & \text{für } r = 3, 5. \end{cases}$$

Damit ist die Behauptung bewiesen. ■

Satz. (1) *Sind für ein $n \ge 2$ die Zahlen $p = 4n - 1$ und $q = 8n - 1$ Primzahlen, so ist q ein nichttrivialer Teiler von $M_p = 2^p - 1$. Insbesondere ist dann M_p zusammengesetzt.*

(2) *Gilt Schinzels Hypothese H, so tritt der Fall (1) unendlich oft auf. Insbesondere gibt es dann unendlich viele Primzahlen p, sodass $M_p = 2^p - 1$ zusammengesetzt ist.*

[19] Stichwort „Shifted Primes“.

Beweis:

(1) Wir setzen voraus, dass $p = 4n - 1$ und $q = 8n - 1$ Primzahlen sind. Das letzte Lemma liefert dann $2^{\frac{q-1}{2}} \equiv 1 \bmod q$. Nun ist aber $\frac{q-1}{2} = \frac{8n-2}{2} = 4n - 1 = p$, sodass die Aussage $2^p \equiv 1 \bmod q$ und damit

$$q \mid 2^p - 1$$

folgt. Nun haben wir die äquivalenten Umformungen:

$$2^p - 1 > q \quad \Longleftrightarrow \quad 2^{4n-1} - 1 > 8n - 1 \quad \Longleftrightarrow \quad 2^{4n-1} > 8n \quad \Longleftrightarrow \quad 16^{n-1} > n.$$

Wir zeigen nun durch Induktion, dass $16^{n-1} > n$ für $n \geq 2$ gilt, wobei der Induktionsanfang $n = 2$ klar ist. Mit der Induktionsannahme $16^{n-1} > n$ folgt dann

$$16^{(n+1)-1} = 16 \cdot 16^{n-1} > 16n = n + 1 + (15n - 1) > n + 1,$$

sodass die Behauptung durch Induktion bewiesen ist. Für $n \geq 2$ ist daher q ein nichttrivialer Teiler von $2^p - 1$.

(2) Für die Polynome $f_1(x) = 4x - 1$, $f_2(x) = 8x - 1$ sind die Voraussetzungen von Schinzels Hypothese H erfüllt. ($f_1(0)f_2(0) = 1$.) Daher sollte es unendlich viele Zahlen n geben, sodass $p = f_1(n)$ und $q = f_2(n)$ prim sind. ■

Beispiele: Die folgenden Beispiele illustrieren den Satz.

n	p	q	$2^p - 1$
3	11	23	$23 \cdot 89$
6	23	47	$47 \cdot 178481$
21	83	167	$167 \cdot 57912614113275649087721$
33	131	263	$263 \cdot 1035079443105516238671861923746823456 9$
45	179	359	$359 \cdot 1433 \cdot 1489459109360039866456940197095433721664951999121$

Bemerkung: Gilt die Hypothese H, so kann man auch leicht zeigen, dass es unendlich viele Carmichael-Zahlen gibt, und dass die Artin-Vermutung (über Primitivwurzeln) gilt.

Bateman und Horn[20] haben eine quantitative Version von Schinzels Hypothese H angegeben:

Bateman-Horn-Vermutung: *Seien $f_1(x), \ldots, f_k(x) \in \mathbb{Z}[x]$ paarweise verschiedene, irreduzible Polynome mit höchstem Koeffizienten > 0, sodass*

$$\mathrm{ggT}(\{(\prod_{i=1}^{k} f_i)(n) : n \in \mathbb{Z}\}) = 1$$

gilt. Dann gilt für die Anzahlfunktion

$$\pi(f_1, \ldots, f_k; x) = \#\{1 \leq n \leq x : \textit{alle Zahlen } f_1(n), \ldots, f_k(n) \textit{ sind Primzahlen}\}$$

die asymptotische Gleichheit

$$\pi(f_1, \ldots, f_k; x) \sim \frac{C(f_1, \ldots, f_k)}{(\mathrm{grad} f_1) \ldots (\mathrm{grad} f_k)} \int_2^x \frac{dt}{(\log t)^k},$$

wobei $C(f_1, \ldots, f_k)$ durch

$$C(f_1, \ldots, f_k) = \prod_p \frac{1 - \frac{\omega(p)}{p}}{(1 - \frac{1}{p})^k} \quad \textit{mit} \quad \omega(p) = \#\{0 \leq n \leq p - 1 : f_1(n) \ldots f_k(n) \equiv 0 \bmod p\}$$

definiert wird.

Bemerkungen:

(1) Bateman und Horn beweisen, dass das $C(f_1, \ldots, f_k)$ definierende Produkt tatsächlich konvergiert.

[20] Siehe [**Bateman/Horn 1962**].

(2) Die Voraussetzung $\mathrm{ggT}(\{f_1(n)\dots f_k(n) : n \in \mathbb{Z}\} = 1$ ist gleichwertig damit, dass für jede Primzahl p ein $n_p \in \mathbb{Z}$ existiert mit $f_1(n_p)\dots f_k(n_p) \not\equiv 0 \bmod p$, also damit, dass $\omega(p) < p$ für alle Primzahlen p gilt.

Beispiele:

(1) Wählen wir $k = 1$ und $f_1(x) = x$, so ist $\omega(p) = 1$, $C(x) = 1$ und $\pi(x; x) = \pi(x)$. Die Bateman-Horn-Vermutung liefert also in diesem Fall einfach die Aussage des Primzahlsatzes

$$\pi(x) \sim \int_2^x \frac{dt}{\log t}.$$

(2) Wir nehmen nun die Polynome $f_1(x) = x$ und $f_2(x) = x + 2$. Es ist dann

$$\begin{aligned}\pi(x, x+2; x) &= |\{1 \le n \le x : n \text{ und } n+2 \text{ prim}\}| = \\ &= |\{(p, p+2) : p, p+2 \text{ prim}, p \le x\}| = \pi_2(x)\end{aligned}$$

die früher definierte Primzahlzwillingszählfunktion $\pi_2(x)$. Nun ist

$$\omega(p) = \#\{0 \le n \le p-1 : n(n+2) \equiv 0 \bmod p\} = \begin{cases} |\{0\}| = 1 & \text{für } p = 2, \\ |\{0, p-2\}| = 2 & \text{für } p \ge 3, \end{cases}$$

sodass

$$\begin{aligned}C(x, x+2) &= \prod_p \frac{1 - \frac{\omega(p)}{p}}{(1-\frac{1}{p})^2} = \frac{1-\frac{1}{2}}{(1-\frac{1}{2})^2} \prod_{p \ge 3} \frac{1-\frac{2}{p}}{(1-\frac{1}{p})^2} = 2 \prod_{p \ge 3} \frac{p^2 - 2p}{(p-1)^2} = \\ &= 2 \prod_{p \ge 3} \frac{(p-1)^2 - 1}{(p-1)^2} = 2 \prod_{p \ge 3} (1 - \frac{1}{(p-1)^2})\end{aligned}$$

folgt. Die Bateman-Horn-Vermutung liefert dann

$$\pi_2(x) \sim C(x, x+2) \int_2^x \frac{dt}{(\log t)^2},$$

was wir auch schon als Vermutung bei den Primzahlzwillingen angegeben hatten. Es ist

$$2 \cdot \prod_{p \le 10^6} (1 - \frac{1}{(p-1)^2}) = 1.3203237\dots$$

(3) Nun wollen wir Primzahlpaare der Form $(p, p+6)$ betrachten. Wir wählen $f_1(x) = x$ und $f_2(x) = x + 6$. Wir brauchen

$$\omega(p) = |\{0 \le n \le p-1 : n(n+6) \equiv 0 \bmod p\}| = \begin{cases} |\{0\}| = 1 & \text{für } p = 2, \\ |\{0\}| = 1 & \text{für } p = 3, \\ |\{0, 4\}| = 2 & \text{für } p = 5, \\ |\{0, p-6\}| = 2 & \text{für } p \ge 7. \end{cases}$$

Daher gilt

$$\begin{aligned}C(x, x+6) &= \prod_p \frac{1 - \frac{\omega(p)}{p}}{(1-\frac{1}{p})^2} = \frac{1-\frac{1}{2}}{(1-\frac{1}{2})^2} \cdot \frac{1-\frac{1}{3}}{(1-\frac{1}{3})^2} \cdot \prod_{p \ge 5} \frac{1-\frac{2}{p}}{(1-\frac{1}{p})^2} = \\ &= 2 \cdot \frac{3}{2} \cdot \prod_{p \ge 5} \frac{p^2 - 2p}{(p-1)^2} = 3 \cdot \prod_{p \ge 5} \frac{(p-1)^2 - 1}{(p-1)^2} = 3 \cdot \prod_{p \ge 5} (1 - \frac{1}{(p-1)^2}).\end{aligned}$$

Nun ist

$$C(x, x+2) = 2 \cdot \prod_{p \ge 3} (1 - \frac{1}{(p-1)^2}) = 2 \cdot \frac{3}{4} \cdot \prod_{p \ge 5} (1 - \frac{1}{(p-1)^2}) = \frac{3}{2} \cdot \prod_{p \ge 2} (1 - \frac{1}{(p-1)^2}).$$

Also gilt

$$C(x, x+6) = 2 \cdot C(x, x+2).$$

Gilt die Bateman-Horn-Vermutung, so folgt

$$\pi(x, x+6; x) \sim 2 \cdot \pi(x, x+2; x).$$

Es sollte also ungefähr doppelt so viele Primzahlpaare der Form $(p, p+6)$ wie Primzwillige $(p, p+2)$ geben.
Tatsächlich findet man:

- Anzahl der Primzahlpaare $(p, p+2)$ mit $p \leq 10^7$: 58980.
- Anzahl der Primzahlpaare $(p, p+6)$ mit $p \leq 10^7$: 117207. $(2 \cdot 58980 = 117960)$

13. Die Goldbachsche Vermutung

Goldbach schrieb 1742 in einem Brief an Euler eine Vermutung auf, die man heutzutage so formuliert[21]:

Goldbachsche Vermutung: Jede gerade Zahl $n \geq 4$ ist Summe zweier Primzahlen.

Beispiele: Für die geraden Zahlen $4 \leq n \leq 50$ sind hier alle Darstellungen $n = p_1 + p_2$ (mit Primzahlen $p_1 \leq p_2$) angegeben:

$$\begin{aligned}
4 &= 2+2\\
6 &= 3+3\\
8 &= 3+5\\
10 &= 3+7 = 5+5\\
12 &= 5+7\\
14 &= 3+11 = 7+7\\
16 &= 3+13 = 5+11\\
18 &= 5+13 = 7+11\\
20 &= 3+17 = 7+13\\
22 &= 3+19 = 5+17 = 11+11\\
24 &= 5+19 = 7+17 = 11+13\\
26 &= 3+23 = 7+19 = 13+13\\
28 &= 5+23 = 11+17\\
30 &= 7+23 = 11+19 = 13+17\\
32 &= 3+29 = 13+19\\
34 &= 3+31 = 5+29 = 11+23 = 17+17\\
36 &= 5+31 = 7+29 = 13+23 = 17+19\\
38 &= 7+31 = 19+19\\
40 &= 3+37 = 11+29 = 17+23\\
42 &= 5+37 = 11+31 = 13+29 = 19+23\\
44 &= 3+41 = 7+37 = 13+31\\
46 &= 3+43 = 5+41 = 17+29 = 23+23\\
48 &= 5+43 = 7+41 = 11+37 = 17+31 = 19+29\\
50 &= 3+47 = 7+43 = 13+37 = 19+31
\end{aligned}$$

Bemerkungen:

(1) Die Goldbachsche Vermutung wurde verifiziert[22] für $n \leq 3 \cdot 10^{17}$.
(2) Noch am nähesten an der unbewiesenen Goldbach-Vermutung ist ein Resultat von Chen[23]: Jede hinreichend große gerade Zahl n lässt sich schreiben als $n = p + q$ oder $n = p + q_1 q_2$ mit Primzahlen p, q, q_1, q_2.
(3) Ramaré hat gezeigt, dass sich jede gerade Zahl als Summe von höchstens 6 Primzahlen schreiben lässt [**Ramaré 1995**].

Wie kann man ungerade Zahlen als Summe von Primzahlen darstellen? Eine Darstellung als Summe zweier Primzahlen ist unrealistisch, da die eine davon dann 2 sein müsste. Die nächste Möglichkeit ist die sogenannte **Ternäre Goldbach-Vermutung**, die 2013 von Helfgott [Helfgott] bewiesen wurde:

[21] Siehe [**Ribenboim 2006**, S.217].
[22] Siehe [**Ribenboim 2006**, S.222].
[23] Siehe [**Crandall/Pomerance 2005**, S.19].

SATZ (Ternäre Goldbach-Vermutung - Helfgott). *Jede ungerade Zahl $n \geq 7$ ist Summe dreier Primzahlen.*

Beispiele: Für die ungeraden Zahlen $7 \leq n \leq 49$ sind hier alle Darstellungen $n = p_1 + p_2 + p_3$ mit Primzahlen $p_1 \leq p_2 \leq p_3$ aufgelistet:

$7 = 2+2+3$
$9 = 2+2+5 = 3+3+3$
$11 = 2+2+7 = 3+3+5$
$13 = 3+3+7$
$15 = 2+2+11 = 3+5+7 = 5+5+5$
$17 = 2+2+13 = 3+3+11 = 5+5+7$
$19 = 3+3+13 = 3+5+11$
$21 = 2+2+17 = 3+5+13 = 3+7+11 = 5+5+11 = 7+7+7$
$23 = 2+2+19 = 3+3+17 = 3+7+13 = 5+5+13 = 5+7+11$
$25 = 3+3+19 = 3+5+17 = 5+7+13 = 7+7+11$
$27 = 2+2+23 = 3+5+19 = 3+7+17 = 5+5+17 = 7+7+13$
$29 = 3+3+23 = 3+7+19 = 5+5+19 = 5+7+17$
$31 = 3+5+23 = 5+7+19 = 7+7+17$
$33 = 2+2+29 = 3+7+23 = 3+11+19 = 5+5+23 = 5+11+17 = 7+7+19 = 11+11+11$
$35 = 2+2+31 = 3+3+29 = 5+7+23 = 5+11+19 = 7+11+17 = 11+11+13$
$37 = 3+3+31 = 3+5+29 = 3+11+23 = 7+7+23 = 7+11+19$
$39 = 3+5+31 = 3+7+29 = 3+13+23 = 5+5+29 = 5+11+23 = 7+13+19 = 11+11+17 = 13+13+13$
$41 = 2+2+37 = 3+7+31 = 5+5+31 = 5+7+29 = 5+13+23 = 7+11+23 = 11+11+19 = 11+13+17$
$43 = 3+3+37 = 3+11+29 = 5+7+31 = 7+7+29 = 7+13+23 = 11+13+19 = 13+13+17$
$45 = 2+2+41 = 3+5+37 = 3+11+31 = 3+13+29 = 5+11+29 = 7+7+31 = 11+11+23 = 13+13+19$
$47 = 2+2+43 = 3+3+41 = 3+7+37 = 3+13+31 = 5+5+37 = 5+11+31 = 5+13+29 = 7+11+29 = 11+13+23$
$49 = 3+3+43 = 3+5+41 = 5+7+37 = 5+13+31 = 7+11+31 = 7+13+29 = 13+13+23$

Bemerkungen:

(1) Ist $n \geq 7$ ungerade und gilt die Goldbach-Vermutung für die gerade Zahl $n-3$ (mit $n-3 \geq 4$), so gibt es Primzahlen p, q mit $n-3 = p+q$, also $n = 3+p+q$. Dies zeigt, dass die (inzwischen bewiesene) ternäre Goldbach-Vermutung aus der Goldbach-Vermutung folgt.

(2) Man kann dieses Argument leicht verallgemeinern: Ist p eine ungerade Primzahl und $n \geq p+4$, so ist $n-p \geq 4$ und gerade. Gilt also die Goldbach-Vermutung, so gibt es Primzahlen p_1, p_2 mit $n-p = p_1+p_2$ und damit $n = p+p_1+p_2$.

14. Anhang: Numerischer Vergleich von $\mathrm{li}(x)-\pi(x)$ mit $\frac{\log x}{\sqrt{x}}$

In der Einführung wurde $\mathrm{li}(x)-\pi(x)$ mit $\frac{\sqrt{x}}{\log x}$ für einige Werte von x verglichen. Hier wollen wir überlegen, wie man dies auf Intervalle ausdehnen kann.

LEMMA. *Die für $n \in \mathbb{N}$ und $x \geq 2$ durch*

$$f_n(x) = \frac{(\mathrm{li}(x)-n)\log x}{\sqrt{x}}$$

definierte Funktion ist im Intervall $[p_n, p_{n+1})$ streng monoton steigend und es gilt

$$\begin{aligned} \inf_{x\in[p_n,p_{n+1})} \frac{(\mathrm{li}(x)-\pi(x))\log x}{\sqrt{x}} &= \frac{(\mathrm{li}(p_n)-n)\log p_n}{\sqrt{p_n}} \quad \textit{und} \\ \sup_{x\in[p_n,p_{n+1})} \frac{(\mathrm{li}(x)-\pi(x))\log x}{\sqrt{x}} &= \frac{(\mathrm{li}(p_{n+1})-n)\log p_{n+1}}{\sqrt{p_{n+1}}}. \end{aligned}$$

Beweis: Aus $f_n(x) = (\mathrm{li}(x)-n)\cdot\log x\cdot x^{-\frac{1}{2}}$ folgt

$$\begin{aligned} f_n'(x) &= \frac{1}{\log x}\cdot\log x\cdot x^{-\frac{1}{2}} + (\mathrm{li}(x)-n)\cdot\frac{1}{x}\cdot x^{-\frac{1}{2}} + (\mathrm{li}(x)-n)\cdot\log x\cdot(-\frac{1}{2}x^{-\frac{3}{2}}) = \\ &= x^{-\frac{1}{2}} + (\mathrm{li}(x)-n)\cdot x^{-\frac{3}{2}}\cdot(1-\frac{1}{2}\log x) = \frac{x+\mathrm{li}(x)(1-\frac{1}{2}\log x)-n(1-\frac{1}{2}\log x)}{x\sqrt{x}}. \end{aligned}$$

Wir betrachten den Fall $2 \leq x \leq e^2$ und $x \in [p_n, p_{n+1})$. Dann folgt mit $1-\frac{1}{2}\log x \geq 0$ und $x \geq p_n > n$

$$f_n'(x) \geq \frac{x+\mathrm{li}(x)(1-\frac{1}{2}\log x)-n(1-\frac{1}{2}\log x)}{x\sqrt{x}} \geq \frac{x-n}{x\sqrt{x}} \geq \frac{p_n-n}{x\sqrt{x}} > 0,$$

sodass $f_n(x)$ in diesem Fall streng monoton steigend ist.
Ist $x \geq e^2$, so folgt mit $\frac{1}{2}\log x - 1 \geq 0$ und der früher gezeigten Ungleichung

$$\mathrm{li}(x) \overset{x\geq 2}{<} \frac{x}{\log x} + \frac{2x}{(\log x)^2}$$

in diesem Fall

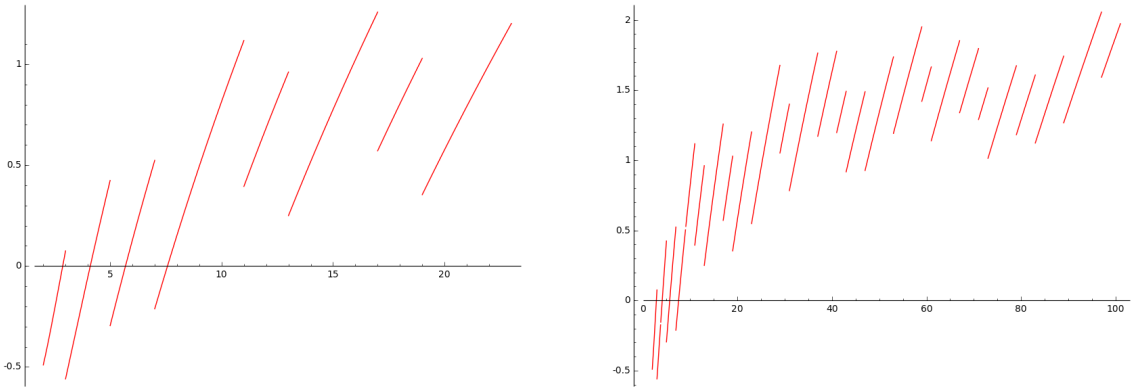
$$\begin{aligned} f_n'(x) &= \frac{x + (n - \mathrm{li}(x))(\frac{1}{2}\log x - 1)}{x\sqrt{x}} \geq \frac{x + (n - \frac{x}{\log x} - \frac{2x}{(\log x)^2})(\frac{1}{2}\log x - 1)}{x\sqrt{x}} = \\ &= \frac{x + n(\frac{1}{2}\log x - 1) - \frac{1}{2}x - \frac{x}{\log x} + \frac{x}{\log x} + \frac{2x}{(\log x)^2}}{x\sqrt{x}} = \frac{\frac{1}{2}x + n(\frac{1}{2}\log x - 1) + \frac{2x}{(\log x)^2}}{x\sqrt{x}} > 0, \end{aligned}$$

was auch hier die strenge Monotonie beweist. Wegen

$$\frac{(\mathrm{li}(x) - \pi(x))\log x}{\sqrt{x}} = f_n(x) \quad \text{für} \quad x \in [p_n, p_{n+1})$$

folgen nun sofort die Aussagen über das Infimum und das Supremum. ■

Die folgenden Abbildungen zeigen die Funktion $\frac{(\mathrm{li}(x)-\pi(x))\log x}{\sqrt{x}}$ für $2 \leq x \leq 23$ und $2 \leq x \leq 101$:



Für $f(x) = \frac{(\mathrm{li}(x)-\pi(x))\log x}{\sqrt{x}}$ haben wir für die Primzahlen zwischen 11 und $10^6 + 3$ jeweils die Werte $\inf_{x\in[p_n,p_{n+1})} f(x)$ und $\sup_{x\in[p_n,p_{n+1})} f(x)$ unter Verwendung des vorangegangenen Lemmas bestimmt. Sie wurden in die Tabelle aufgenommen, wenn sie kleiner bzw. größer als alle vorhergehenden Infima bzw. Suprema sind.

p_n	p_{n+1}	$\inf_{x\in[p_n,p_{n+1})} f(x)$	$\sup_{x\in[p_n,p_{n+1})} f(x)$
11	13	0.394642	0.961360
13	17	0.249971	1.258388
23	29		1.677023
31	37		1.764582
37	41		1.777329
53	59		1.951144
89	97		2.056482
113	127		2.059472
139	149		2.155228
211	223		2.333033
547	557		2.368327
1399	1409		2.370272
1409	1423		2.540711

Wegen $0.15 \leq f(x) \leq 1.12$ für $8 \leq x < 11$ folgt insgesamt:

$$0 < \frac{(\mathrm{li}(x) - \pi(x))\log x}{\sqrt{x}} < 3 \quad \text{für} \quad 8 \leq x \leq 10^6,$$

also

$$\mathrm{li}(x) - 3\frac{\sqrt{x}}{\log x} < \pi(x) < \mathrm{li}(x) \quad \text{für} \quad 8 \leq x \leq 10^6.$$

(Sicherheitshalber sei nochmals bemerkt, dass diese Ungleichungen für große x nicht mehr allgemein gelten.)

Literaturverzeichnis

[Alon/Spencer 2016] N. Alon, J. H. Spencer. The Probabilistic Method. Fourth Edition. Wiley, 2016.

[Apostol 1974] T. M. Apostol. Mathematical Analysis. Second Edition. Addison-Wesley Publishing Company, 1974.

[Apostol 1976] T. M. Apostol. Introduction to Analytic Number Theory. Springer-Verlag, 1976.

[Axer 1910] A. Axer. Beitrag zur Kenntnis der zahlentheoretischen Funktionen $\mu(n)$ und $\lambda(n)$. Prace Matematyczno-Fizyczne 21 (1910), 65-95.

[Bach/Shallit 1996] E. Bach, J. Shallit. Algorithmic Number Theory. Volume 1: Efficient Algorithmus. The MIT Press, 1996.

[Baker/Harman/Pintz 2001] R. C. Baker, G. Harman and J. Pintz. The difference between consecutive primes, II. Proc. London Math. Soc. (3) 83 (2001) 532-562.

[Bateman/Horn 1962] P. T. Bateman, R. A. Horn. A Heuristic Asymptotic Formula Concerning the Distribution of Prime Numbers. Math. Comp. **16** (1962), 363-367.

[Bouniakowsky 1857] V. Bouniakowsky. Nouveaux théorèmes relatifs à la distinction des nombres premiers et à la décomposition des entiers en facteurs. Mém. Acad. Sci. St. Petersbourg (6), Sci. Math. Phys. **6** (1857), 305-329.

[Brüdern 1995] J. Brüdern. Einführung in die analytische Zahlentheorie. Springer-Verlag, 1995.

[Chandrasekharan 1968] K. Chandrasekharan. Introduction to Analytic Number Theory. Springer-Verlag, 1968.

[Cohen 2007II] H. Cohen. Number Theory. Volume II: Analytic and Modern Tools. Graduate Texts in Mathematics 240. Springer-Verlag, 2007.

[Cramér 1920] H. Cramér. Some theorems concerning prime numbers. Ark. Mat. Astr. Fys. **15** (5) (1920), 1-33. Oder: Collected Works I, S.138-170.

[Cramér 1936] H. Cramér. On the order of magnitude of the difference between consecutive prime numbers. Acta Arith. **2** (1) (1936), 23-46. Oder: Collected Works II, S.871-894.

[Crandall/Pomerance 2005] R. Crandall, C. Pomerance. Prime Numbers, A Computational Perspective. Second Edition. Springer-Verlag, 2005.

[Dirichlet 1849] P. G. L. Dirichlet. Über die Bestimmung der mittleren Werthe in der Zahlentheorie. Abhandlungen der Königlich Preussischen Akademie der Wissenschaften von 1849, 69-83. Oder: Werke II, 49-66.

[Dusart 1998] P. Dusart. Sharper bounds for ψ, ϑ, π, p_k. Laboratoire d'Arithmétique, de Calcul formel et d'Optimisation. Rapport de recherche n^0 1998-06.

[Edwards 1974] H. M. Edwards. Riemann's Zeta Function. Dover Publications, Inc., 1974.

[Ellison/Ellison 1985] W. Ellison, F. Ellison. Prime Numbers. John Wiley and Sons, 1985.

[Ford/Green/Konyagin/Tao 2014] K. Ford, B. Green, S. Konyagin, T. Tao. Large gaps between consecutive prime numbers. arXiv:1408.4505v1 [math.NT].

[Hardy/Littlewood III] G. H. Hardy, J. E. Littlewood. Some problems of 'partitio numerorum'; III: On the expression of a number as a sum of primes. Acta Math. 44 (1923), pp. 1-70.

[Hardy/Riesz] G. H. Hardy, M. Riesz. The general theory of Dirichlet series. Cambridge University Press, 1915.

[Hardy/Wright 1979] G. H. Hardy, E. M. Wright. An Introduction to the Theory of Numbers. Fifth Edition. Clarendon Press, Oxford, 1979.

[Helfgott 2014] H. A. Helfgott. The ternary Goldbach conjecture is true. arXiv:1312.7748v2 [math.NT].

[Hensley/Richards 1974] D. Hensley, I. Richards. Primes in Intervals. Acta Arithmetica **25** (1974), 375-391.

[Ingham 1932] A. E. Ingham. The distribution of prime numbers. Cambridge University Press, 1932.

[Jameson 2003] G. J. O. Jameson. The Prime Number Theorem. London Mathematical Society Student Texts **53**, Cambridge University Press, 2003.

[Korevaar 1982] J. Korevaar. On Newman's Quick Way to the Prime Number Theorem. The Mathematical Intelligencer **4** (1982), 108–115.

[Landau 1909] E. Landau. Handbuch der Lehre von der Verteilung der Primzahlen. Erster Band. Second Edition. Chelsea Publishing Company, New York, 1953.

[Landau 1910] E. Landau. Über die Bedeutung einiger neuen Grenzwertsätze der Herren Hardy und Axer. Prace Matematyczno-Fizyczne 21 (1910), 97-177.

[Lang 1999] S. Lang. Complex Analysis. Fourth Edition. Graduate Texts in Mathematics **103**. Springer, 1999.

[Maynard 2013] J. Maynard. Small gaps between primes. arXiv:1311.4600v2 [math.NT].

[Maynard 2014] J. Maynard. Large gaps between primes. arXiv:1408.5110v1 [math.NT].

[Montgomery/Vaughan 2006] H. L. Montgomery, R. C. Vaughan. Multiplicative Number Theory: I. Classical Theory. Cambridge studies in advanced mathematics **97**, Cambridge University Press, 2006.

[Narkiewicz 2000] W. Narkiewicz. The Development of Prime Number Theory. Springer-Verlag, 2000.

[Nathanson 2000] M. B. Nathanson. Elementary Methods in Number Theory. Graduate Texts in Mathematics **195**. Springer-Verlag, 2000.

[Newman 1980] D. J. Newman. Simple Analytic Proof of the Prime Number Theorem. American Mathematical Monthly **87** (1980), 693–696.

[Ramaré 1995] O. Ramaré. On S'nirel'man's constant. Annali dela Scuola Superiore di Pisa, vol. 21, no. 4 (1995), pages 645-705.

[Ribenboim 2006] P. Ribenboim. Die Welt der Primzahlen. Aktualisierte Übersetzung der englischen Ausgabe 'The Little Book of Bigger Primes' (2. Auflage, Springer-Verlag, 2004). Springer-Verlag, 2006.

[Riesel 1985] H. Riesel. Prime Numbers and Computer Methods for Factorization. Birkhäuser, 1985.

[Rosser/Schoenfeld 1962] J. B. Rosser, L. Schoenfeld. Approximate Formulas for Some Functions of Prime Numbers. Illinois J. Math. **6** (1962), 64-94.

[Ruppert 2005] W. Ruppert. Analytische Zahlentheorie II. Vorlesungsskript zu einer Vorlesung im Sommersemester 2005.

[Schinzel/Sierpiński 1958] A. Schinzel, W. Sierpiński. Sur certaines hypothèses concernant les nombres premiers. Acta Arith. **4** (1958), 185-208. Erratum: **5** (1959), 259.

[Soundararajan 2007] K. Soundararajan. Small gaps between prime numbers: the work of Goldston-Pintz-Yildirim. Bull. AMS **44** (2007), 1-18.

[Tenenbaum, Mendès France 2000] G. Tenenbaum, M. Mend'es France. The Prime Numbers and Their Distribution. AMS, 2000.

[Titchmarsh 1986] E. C. Titchmarsh. The Theory of the Riemann Zeta-Function. Second Edition. Revised by D. R. Heath-Brown. Clarendon Press, Oxford, 1986.

[Zagier 1997] D. Zagier. Newman's Short Proof of the Prime Number Theorem. The American Mathematical Monthly **104** (1997), 705-708.

[Zhang 2014] Y. Zhang. Bounded gaps between primes. Annals of Mathematics. Volume 179 (2014), Issue 3, Pages 1121-1174.