Primzahlen und Pseudoprimzahlen

Holger Stephan

Weierstraß Institut für Angewandte
Analysis und Stochastik (WIAS), Berlin

20. Tag der Mathematik
9. Mai 2015, Beuth Hochschule für Technik Berlin

Warum sind Primzahlen interessant?

Carl Friedrich Gauss (1777–1855) in
Disquisitiones Arithmeticae (1801):

Dass das Problem, die Primzahlen von den zusammengesetzten zu unterscheiden und letztere in ihre Primfaktoren zu zerlegen zu den wichtigsten und nützlichsten der ganzen Arithmetik gehört und den Fleiss und die Weisheit der Geometer der Antike und der Neuzeit beschäftigt hat, ist so bekannt, dass es überflüssig ist, viel darüber zu sagen.

Nützlich? Anwendungen:

- Verschlüsselung von Daten
  (große – z.B. 100-stellige – Primzahlen sind gesucht)
- Fouriertransformation (kleine Primzahlen reichen aus)

Euklid und die Primzahlen

Definition: Primzahlen sind natürliche Zahlen größer 1, die nur durch 1 und sich selbst teilbar sind.

Die ersten Primzahlen:

$$\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, \ldots\}$$

Euklid (3. Jahrhundert v. Chr. in Alexandria):

"Es gibt mehr Primzahlen als jede vorgegebene Anzahl von Primzahlen."

(heute sagt man: unendlich viele)

Beweis: Angenommen, es gibt nur die Primzahlen $p_1, \ldots, p_n$. Wir betrachten die Zahl $x = p_1 \cdots p_n + 1$. Diese Zahl ist durch keine der p_i teilbar aber größer als alle p_i. Also muß x selbst eine Primzahl oder durch eine größere Primzahl als p_n teilbar sein. Es gibt also wenigstens noch eine weitere Primzahl.

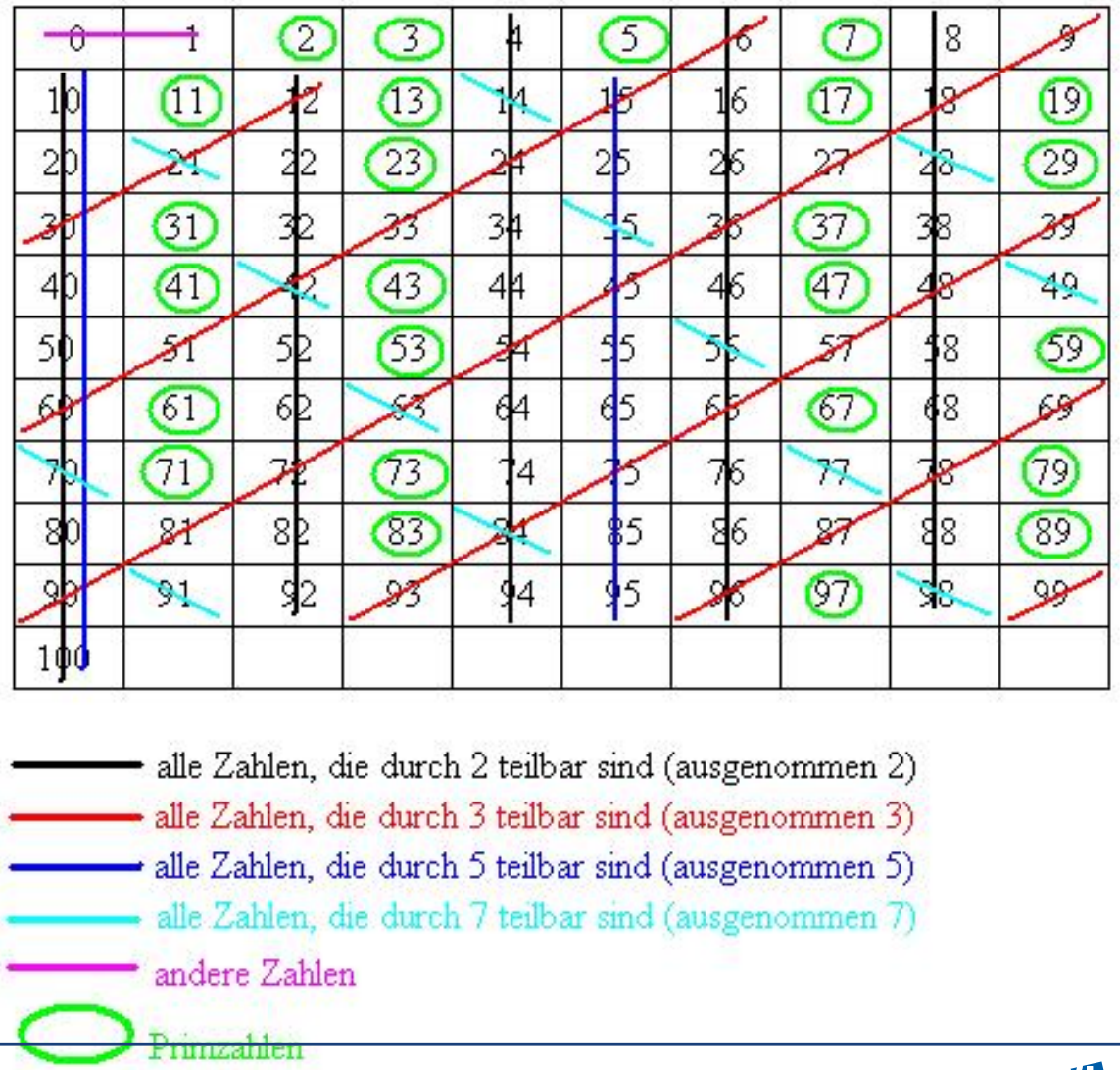
Interessante Fragen zu Primzahlen

- Einfache Berechnung aller Primzahlen der Reihe nach.
  (Finde eine “Primzahlformel”.) völlig hoffnungslos !
- Einfache Berechnung von unendlich vielen (nicht allen)
  Primzahlen. weitgehend hoffnungslos !
- (Einfache) Berechnung aller Primzahlen, möglicherweise noch
  weitere (Pseudoprimzahlen).
- Viele ungelöste Probleme warten auf junge Mathematiker.

Das Sieb des Eratosthenes

Berechnung aller Primzahlen bis 100 durch Streichung aller Vielfachen der Primzahlen bis $\sqrt{100}$.

Immer nur endlich viele Primzahlen!



Euklidische Primzahlen

$$
\begin{aligned}
p_1 \cdots p_n + 1 &= x \quad \text{ist Primzahl?} \\
2 + 1 &= 3 \\
2 \cdot 3 + 1 &= 7 \\
2 \cdot 3 \cdot 5 + 1 &= 31 \\
2 \cdot 3 \cdot 5 \cdot 7 + 1 &= 211 \\
2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 &= 2311 \\
2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 &= 30031 = 59 \cdot 509
\end{aligned}
$$

$$
\begin{aligned}
p_1 \cdots p_n - 1 &= x \quad \text{ist Primzahl?} \\
2 - 1 &= 1 \\
2 \cdot 3 - 1 &= 5 \\
2 \cdot 3 \cdot 5 - 1 &= 29 \\
2 \cdot 3 \cdot 5 \cdot 7 - 1 &= 209 = 11 \cdot 19
\end{aligned}
$$

Gibt es unter diesen Zahlen unendlich viele Primzahlen?
Das ist eins von vielen ungelösten Problemen mit Primzahlen.

Mersenne–Primzahlen

Zahlen der Form $2^p - 1$ mit $p \in \mathbb{P}$ sind einfach zu testen (Binärz.)
$2^{a \cdot b} - 1$ ist stets zusammengesetzt, z.B. $2^{2 \cdot 3} - 1 = (2^3 - 1)(2^3 + 1)$

p	Nr. von p in $\mathbb{P}$	$2^p - 1$	Faktoren	Nr. in $\mathcal{M}$
2	1	3	prim	1
3	2	7	prim	2
5	3	31	prim	3
7	4	127	prim	4
11	5	2047	$23 \cdot 89$	
13	6	8191	prim	5
17	7	131071	prim	6
19	8	524287	prim	7
23	9	8388607	$47 \cdot 178481$	
29	10	536870911	$233 \cdot 1103 \cdot 2089$	
31	11	2147483647	prim	8

Mersenne–Primzahlen ($2^p - 1$). Fortsetzung

Nr. in $\mathcal{M}$	Exp. p	Stellen von $2^p - 1$	Nr. von p in $\mathbb{P}$	Jahr
39	13466917	4053496	877615	2001
40	20996011	6320430	1329726	2003
41	24036583	7235733	1509263	2004
42	25964951	7816230	1622441	2005
43	30402457	9152052	1881339	2005
44	32582657	9808358	2007537	2006
45?	37156667	11185272	2270720	2008
46?	42643801	12837064	2584328	2009
47?	43112609	12978189	2610944	2008
48?	57885161	17425170	3443958	2013

Es gibt immer eine aktuell größte bekannte Primzahl.
GIMPS = Great Internet Mersenne Prime Search

Fermatsche Primzahlen

Pierre de Fermat (1607 – 1665)

Primzahlen der Form $F_k = 2^{2^k} + 1,\ k = 0, 1, 2, \ldots.$

$$
\begin{aligned}
F_0 &= 2^{2^0} + 1 = 3 \\
F_1 &= 2^{2^1} + 1 = 5 \\
F_2 &= 2^{2^2} + 1 = 17 \\
F_3 &= 2^{2^3} + 1 = 257 \\
F_4 &= 2^{2^4} + 1 = 65537 \qquad \text{Fermat: “} 2^{2^k} + 1 \text{ ist stets Primzahl.”} \\
F_5 &= 2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417 \text{ (Leonhard Euler 1732)} \\
F_6 &= 2^{2^6} + 1 = 18446744\ldots. = 274177 \cdot 67280421310721 \qquad (1880) \\
F_{33} &= 2^{2^{33}} + 1 = \ldots \text{ prim ???} \\
F_{2\ldots} &= 2^{2^{2478782}} + 1 = \ldots = (3 \cdot 2^{2478785} + 1) \cdots
\end{aligned}
$$

Gauß (1796): Konstruktion eines $2^{2^k} + 1$-Ecks (am Beispiel 17)

Was sind Pseudoprimzahlen?

Wir suchen Folgen, die alle Primzahlen enthalten und möglicherweise noch weitere – hoffentlich wenig.

Definition von Pseudoprimzahlen (wikipedia):

Eine Pseudoprimzahl ist eine zusammengesetzte, natürliche Zahl, die gewisse Eigenschaften mit Primzahlen gemeinsam hat, selbst aber keine Primzahl ist.

Ziel: Bei einfacher Berechnung möglichst wenig Pseudoprimzahlen.

Primzahlen bis 1000:	168 Stück
Primzahlen bis 100000:	9592 Stück

Kleiner Satz von Fermat

Satz: Wenn p Primzahl ist, dann läßt a^p bei Division durch p denselben Rest wie a.

Das schreibt man: $a^p \equiv a \pmod{p}$ oder $a^p - a \equiv 0 \pmod{p}$

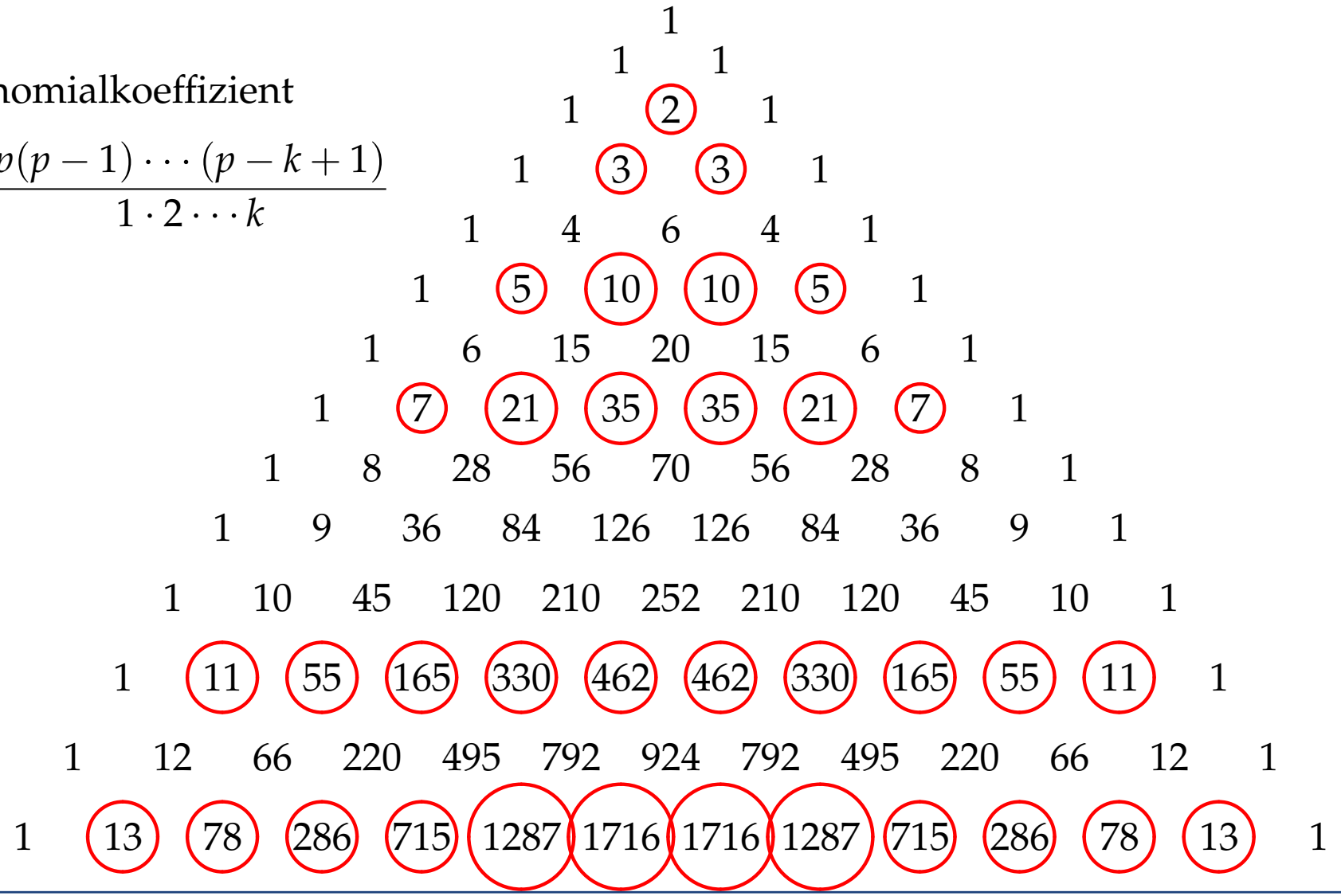
Beweis: Mit binomischem Satz:

$$
\begin{aligned}
(a+b)^1 &= a+b \\
(a+b)^2 &= a^2+2ab+b^2 \\
(a+b)^3 &= a^3+3a^2b+3ab^2+b^3 \\
(a+b)^4 &= a^4+4a^3b+6a^2b^2+4ab^3+b^4 \\
(a+b)^5 &= a^5+5a^4b+10a^3b^2+10a^2b^3+5ab^4+b^5 \\
&\cdots \\
(a+b)^n &= a^n+\binom{n}{1}a^{n-1}b+\binom{n}{2}a^{n-2}b^2+\binom{n}{3}a^{n-3}b^3+\cdots+b^n
\end{aligned}
$$

Das Pascalsche Dreieck

Binomialkoeffizient

$$\binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{1\cdot 2\cdots k}$$



Kleiner Satz von Fermat. Beweis

$$\begin{aligned}(a+1)^p &= a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots + \binom{p}{p-1}a + 1 = \\ &= a^p + 1 + \text{ (Vielfaches von } p)\end{aligned}$$

Also p teilt $(a+1)^p - a^p - 1$ oder $(a+1)^p - a^p - 1 \equiv 0 \pmod{p}$.

$$\begin{aligned}a = 1: &\quad 2^p - 2 \equiv 0 \pmod{p} \\ a = 2: &\quad 3^p - 2^p - 1 \equiv 3^p - 3 \equiv 0 \pmod{p} \\ a = 3: &\quad 4^p - 3^p - 1 \equiv 4^p - 4 \equiv 0 \pmod{p} \\ &\quad a^p - a \equiv 0 \pmod{p}\end{aligned}$$

Fermatscher Primzahltest: p teilt $a^p - a$ für beliebige Basis a.
Aber die Umkehrung gilt nicht:
Es kann Nicht-Primzahlen n geben, die $a^n - a$ teilen für gewisse a.
Hoffentlich wenige! Das sind gerade die Pseudoprimzahlen.

Die Basis $a = 2$

n	$2^n - 2$	n teilt $2^n - 2$?	n ist Primzahl?	
2	2	ja!	ja!	
3	6	ja!	ja!	
4	14	nein!	nein!	
5	30	ja!	ja!	
6	62	nein!	nein!	
7	126	ja!	ja!	
341	4479... (103 Stellen)	ja!	nein!	$341 = 11 \cdot 31$
561	7547... (169 Stellen)	ja!	nein!	$561 = 3 \cdot 11 \cdot 17$
645	1459... (195 Stellen)	ja!	nein!	$645 = 3 \cdot 5 \cdot 43$

Bis 1000 gibt es drei Pseudoprimzahlen (bei 168 Primzahlen)

Bis 100000 gibt es 78 Pseudoprimzahlen (bei 9592 Primzahlen).
Etwa jede 123-te ist falsch.

Eine andre Basis: $a = 3$

n teilt $3^n - 3$, aber n ist keine Primzahl?

n	$3^n - 3$	n teilt $3^n - 3$?	n ist Primzahl?
2	6	ja!	ja!
3	24	ja!	ja!
4	78	nein!	nein!
5	240	ja!	ja!
6	726	ja!	nein!
341	4992... (163 Stellen)	nein!	nein!
561	4624... (268 Stellen)	ja!	nein!
645	5536... (308 Stellen)	nein!	nein!

561 wird auch bei Basis $a = 3$ nicht aussortiert!

Pseudoprimzahlen pro Basis bis $n = 100000$

Basis	Anzahl
2	78
3	86
4	182
5	96
6	145
7	115
8	239
9	222
10	151
11	132
12	168
13	136
14	163
15	124

Basis	Anzahl
16	424
17	127
18	215
19	161
20	147
21	189
22	200
23	203
24	168
25	273
26	196
27	300
28	170
29	153

Basis	Anzahl
30	241
31	141
32	297
33	180
34	213
35	185
36	360
37	241
38	202
39	154
40	179
41	178
42	203
43	228

Carmichael-Zahlen

Gibt es Nicht-Primzahlen die den Test: n teilt $a^n - a$ zu allen Basen a bestehen? Ja! 561 ist die kleinste.

Bis 100000 gibt es 16 Stück.

Carmichael-Zahl	Primfaktoren
561	$3 \cdot 11 \cdot 17$
1105	$5 \cdot 13 \cdot 17$
1729	$7 \cdot 13 \cdot 19$
2465	$5 \cdot 17 \cdot 29$
2821	$7 \cdot 13 \cdot 31$
6601	$7 \cdot 23 \cdot 41$
8911	$7 \cdot 19 \cdot 67$
10585	$5 \cdot 29 \cdot 73$

Carmichael-Zahl	Primfaktoren
15841	$7 \cdot 31 \cdot 73$
29341	$13 \cdot 37 \cdot 61$
41041	$7 \cdot 11 \cdot 13 \cdot 41$
46657	$13 \cdot 37 \cdot 97$
52633	$7 \cdot 73 \cdot 103$
62745	$3 \cdot 5 \cdot 47 \cdot 89$
63973	$7 \cdot 13 \cdot 19 \cdot 37$
75361	$11 \cdot 13 \cdot 17 \cdot 31$

Heute ist bekannt: Es gibt unendlich viele Carmichael-Zahlen.

Verallgemeinerungen

Gibt es Verallgemeinerungen? Wie wissen: Wenn $p \in \mathbb{P}$, dann teilt p

$$(a+b)^p - (a^p + b^p) = \binom{p}{1} a^{p-1}b + \binom{p}{2} a^{p-2}b^2 + \binom{p}{3} a^{p-3}b^3 + \cdots$$

Wir setzen $a = \frac{1+\sqrt{5}}{2}$ und $b = \frac{1-\sqrt{5}}{2}$ (keine natürlichen Zahlen).

$(a+b)^p - (a^p + b^p)$ oder $(a^p + b^p) - (a+b)^p$ sollte natürlich sein.

$$\text{Es sei} \quad L_n = \left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n$$

Dann ist $(a^p + b^p) - (a+b)^p = L_p - 1$ teilbar durch p.

Die Lucas-Folge

Die Folge

$$L_n = \left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n$$

heißt Lucas-Folge (nach Edouard Lucas). Die ersten Werte:

$$(L_n)_{n=0}^{\infty} = 2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, 322, 521, \ldots$$

Wir stellen fest: $L_n = L_{n-1} + L_{n-2}$ (rekursives Bildungsgesetz).

Fibonacci-Folge: Auch $F_n = F_{n-1} + F_{n-2}$, aber andere F_0, F_1

$$(F_n)_{n=0}^{\infty} = 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots$$

Pseudoprimzahlen? Ja, die kleinste aber erst $n = 705 = 3 \cdot 5 \cdot 47$
$L_{705} - 1 =$ (148-stellige Zahl) ist durch 705 teilbar.

25 Lucas-Pseudoprimzahlen bis 100000

Lucas-Zahl	Primfaktoren
705	$3 \cdot 5 \cdot 47$
2465	$5 \cdot 17 \cdot 29$
2737	$7 \cdot 17 \cdot 23$
3745	$5 \cdot 7 \cdot 107$
4181	$37 \cdot 113$
5777	$53 \cdot 109$
6721	$11 \cdot 13 \cdot 47$
10877	$73 \cdot 149$
13201	$43 \cdot 307$
15251	$101 \cdot 151$
24465	$3 \cdot 5 \cdot 7 \cdot 233$
29281	$7 \cdot 47 \cdot 89$
34561	$17 \cdot 19 \cdot 107$

Lucas-Zahl	Primfaktoren
35785	$5 \cdot 17 \cdot 421$
51841	$47 \cdot 1103$
54705	$3 \cdot 5 \cdot 7 \cdot 521$
64079	$139 \cdot 461$
64681	$71 \cdot 911$
67861	$79 \cdot 859$
68251	$131 \cdot 521$
75077	$193 \cdot 389$
80189	$17 \cdot 53 \cdot 89$
90061	$113 \cdot 797$
96049	$139 \cdot 691$
97921	$181 \cdot 541$

Noch bessere Folgen? Weitere Verallgemeinerung!

$$\begin{aligned} (a+b)^n &\implies (a+b+c)^n \\ (a+b+c)^n &= a^n + b^n + c^n + \sum_{i+j+k=n} \frac{(i+j+k)!}{i!\ j!\ k!}\, a^i b^j c^k \end{aligned}$$

Trinomische Formel.
Trinomial-Koeffizienten stehen in der Pascalschen Pyramide.

$$a^p + b^p + c^p - (a+b+c)^p \equiv 0 \pmod{p}$$

Es seien a, b, c die Lösungen der Gleichung $x^3 = x + 1$.

$$\begin{aligned} a &= 1.32472... \\ b &= -0.662359... + 0.56228...\sqrt{-1} \\ c &= -0.662359... - 0.56228...\sqrt{-1} \end{aligned}$$

Die Perrin-Folge

a, b, c seien die Lösungen der Gleichung $x^3 = x + 1$.

$$\begin{aligned} a &= 1.32472... \\ b &= -0.662359... + 0.56228...\sqrt{-1} \\ c &= -0.662359... - 0.56228...\sqrt{-1} \\ \Longrightarrow &\quad a + b + c = 0 \end{aligned}$$

Die Folge $P_n = a^n + b^n + c^n - (a + b + c) = a^n + b^n + c^n$
heißt Perrin-Folge. Die ersten Werte

$$(P_n)_{n=0}^{\infty} = 3, 0, 2, 3, 2, 5, 5, 7, 10, 12, 17, 22, 29, 39, 51, 68, 90, 119, \ldots$$

Einfaches rekursives Bildungsgesetz: $P_n = P_{n-2} + P_{n-3}$
Folgt aus $\quad x^3 = x + 1 \quad \Longrightarrow \quad x^n = x^{n-2} + x^{n-3}$

Berechnung der Primzahlen

n	P_n	n teilt P_n ?	n ist Primzahl?
2	2	ja!	ja!
3	3	ja!	ja!
4	2	nein!	nein!
5	5	ja!	ja!
6	5	nein!	nein!
7	7	ja!	ja!
8	10	nein!	nein!
9	12	nein!	nein!
10	17	nein!	nein!
11	22	ja!	ja!
12	29	nein!	nein!
13	39	ja!	ja!

Unter den ersten 100000 Zahlen keine Perrin-Pseudoprimzahlen!

Gibt es überhaupt Perrin-Pseudoprimzahlen

Ja! Die kleinste ist $271441 = 521 \cdot 521$.

P_{271441} hat 33150 Dezimalstellen.

17 Perrin-Pseudoprimzahlen bis 10^9 bei 50847534 echten Primzahlen.

271441	=	$521 \cdot 521$	102690901	=	$5851 \cdot 17551$
904631	=	$7 \cdot 13 \cdot 9941$	130944133	=	$6607 \cdot 19819$
16532714	=	$2 \cdot 11 \cdot 11 \cdot 53 \cdot 1289$	196075949	=	$5717 \cdot 34297$
24658561	=	$19 \cdot 271 \cdot 4789$	214038533	=	$8447 \cdot 25339$
27422714	=	$2 \cdot 11 \cdot 11 \cdot 47 \cdot 2411$	517697641	=	$6311 \cdot 82031$
27664033	=	$3037 \cdot 9109$	545670533	=	$13487 \cdot 40459$
46672291	=	$4831 \cdot 9661$	801123451	=	$8951 \cdot 89501$
			855073301	=	$16883 \cdot 50647$
			903136901	=	$17351 \cdot 52051$
			970355431	=	$22027 \cdot 44053$

3810 Perrin-Pseudoprimzahlen bis 10^{16}

$$
\begin{aligned}
271441 &= 521 \cdot 521 \\
904631 &= 7 \cdot 13 \cdot 9941 \\
16532714 &= 2 \cdot 11 \cdot 11 \cdot 53 \cdot 1289 \\
24658561 &= 19 \cdot 271 \cdot 4789 \\
27422714 &= 2 \cdot 11 \cdot 11 \cdot 47 \cdot 2411 \\
&\dots \\
996981928470533 &= 18229847 \cdot 54689539 \\
997536207538261 &= 22333117 \cdot 44666233 \\
997661482017481 &= 12894841 \cdot 77369041 \\
999549903125233 &= 14138953 \cdot 70694761
\end{aligned}
$$

$P_{999549903125233}$ hat 122.069.125.464.094 Dezimalstellen.
Solche Zahlen passen auch auf keinen Computer mehr.

Wie berechnet man Perrin-Pseudoprimzahlen?

Man berechnet nicht P_n aus $P_n = P_{n-2} + P_{n-3}$ sondern nur $P_n \pmod n$ und benutzt eine dreidimensionale Darstellung:

$$\begin{pmatrix} P_{3m} \\ P_{3m+1} \\ P_{3m+2} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}^m \cdot \begin{pmatrix} 3 \\ 0 \\ 2 \end{pmatrix}$$

Siehe `http://www.wias-berlin.de/people/stephan/`

Oder "Stephan WIAS" googeln.

"Für mathematisch interessierte Schüler"

Da gibt es eine Liste aller Perrin-Pseudoprimzahlen bis 10^{16}.

Da gibt es eine Liste aller Primzahlen bis 37813.