Von Primzahlen und Pseudoprimzahlen

Holger Stephan

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

23. Tag der Mathematik
21. April 2018, Technische Universität Berlin

Warum sind Primzahlen interessant?

- Definition: Primzahlen sind natürliche Zahlen größer 1, die nur durch 1 und sich selbst teilbar sind.
- Die ersten Primzahlen: $\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, \ldots\}$
- Es gibt unendlich viele Primzahlen (Beweis von Euklid)
- Eindeutige Faktorisierung: $n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}$

Anwendungen für Primzahlen

- Public-Key-Verschlüsselungsverfahren
- Zwei große Primzahlen p und q.
- Berechnung von $n = p \cdot q$ ist einfach
  Zerlegung (Faktorisierung) von n ist schwer.
- Information bleibt erhalten, ist aber schwer zugänglich.
- Im Gegensatz zur Addition zweier Zahlen.

- Ziel: Berechne schnell viele große Primzahlen.
- Was ist viel? Am besten alle Primzahlen der Reihe nach.
- Was ist groß? 256 Binärstellen $\sim$ 80 Dezimalstellen.
- Was ist schnell? Hunderte pro Sekunde.

Interessante Fragen zu Primzahlen

- Berechnung (schnell) aller Primzahlen der Reihe nach. (Finde eine “Primzahlformel”.) hoffnungslos !
- Berechnung von unendlich vielen großen Primzahlen, möglicherweise mit Lücken.
- Berechnung (schnell) aller Primzahlen der Reihe nach, möglicherweise aber noch weitere Nicht-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 $2^p - 1 \in \mathcal{M}$ *(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	7.816230	1622441	2005
43	30402457	9.152052	1881339	2005
44	32582657	9.808358	2007537	2006
45	37156667	11.185272	2270720	2008
46	42643801	12.837064	2584328	2009
47	43112609	12.978189	2610944	2008
48?	57885161	17.425170	3443958	2013
49?	74207281	22.338618		2016
50?	77232917	23.249425		12.2017

Es gibt immer eine aktuell größte bekannte Primzahl, eine Mersennsche.

Fermatsche Primzahlen

Pierre de Fermat (1607 – 1665)
Primzahlen der Form $F_k = 2^{2^k} + 1, k = 0, 1, 2, \ldots.$

$$
\begin{aligned}
F_0 &= 2^{2^0} + 1 = 3,\ F_1 = 2^{2^1} + 1 = 5 \\
F_2 &= 2^{2^2} + 1 = 17,\ F_3 = 2^{2^3} + 1 = 257 \\
F_4 &= 2^{2^4} + 1 = 65537 \qquad \text{Fermat: ``}2^{2^k} + 1 \text{ ist stets Primzahl.''} \\
F_5 &= 2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417 \text{ (L. Euler 1732)} \\
F_5 &\cdots F_{11} \quad \text{vollständig faktorisiert} \\
F_{33} &= 2^{2^{33}} + 1 = \ldots \text{ prim ???} \\
F_{3329780} &= 2^{2^{3329780}} + 1 = \ldots = (193 \cdot 2^{3329782} + 1) \cdots \text{ (Juli 2014)}
\end{aligned}
$$

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

Was sind Pseudoprimzahlen?

Berechne alle Primzahlen mit ($\Longleftrightarrow$Theorem)?

- Satz (Def.): $n \in \mathbb{P} \iff \forall k \in \mathbb{P}, k < \sqrt{n} : \; k \nmid n$
- Satz von Wilson: $n \in \mathbb{P} \iff n | 1 \cdot 2 \cdot 3 \cdots (n-1) + 1$
- Theorem: $n \in \mathbb{P} \iff n | \binom{n}{k} \; \forall k = 1, \ldots, n-1$

Berechne alle Primzahlen mit ($\Longrightarrow$Theorem)?

- $p \in \mathbb{P} \implies p$ erfüllt Eigenschaft $A(p)$
- n erfüllt Eigenschaft $A(n) \;\not\Longrightarrow\; n \in \mathbb{P}$

Solche $n \notin \mathbb{P}$, die die Eigenschaft $A(n)$ haben heißen Pseudoprimzahlen bezüglich der Eigenschaft $A(n)$.

Ziel: Bei einfacher Berechnung möglichst wenig Pseudoprimzahlen.

Eine Eigenschaft von Binomialkoeffizienten

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

Satz: Falls $p \in \mathbb{P}$, dann $p \mid \binom{p}{k}$ für $k = 1, ..., p-1$.

Beweis: $p \mid \binom{p}{k} \cdot k! = p(p-1)\cdots(p-k+1)$

Lemma: Falls $p \in \mathbb{P}$: $p \mid a \cdot b$, dann $p \mid a$ oder $p \mid b$.

Also: p teilt $\binom{p}{k}$ oder $k!$. Wegen $k < p$ folgt $p \mid \binom{p}{k}$. $\square$

Das Pascalsche Dreieck

Binomialkoeffizient

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

1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
1 5 10 10 5 1
1 6 15 20 15 6 1
1 7 21 35 35 21 7 1
1 8 28 56 70 56 28 8 1
1 9 36 84 126 126 84 36 9 1
1 10 45 120 210 252 210 120 45 10 1
1 11 55 165 330 462 462 330 165 55 11 1
1 12 66 220 495 792 924 792 495 220 66 12 1
1 13 78 286 715 1287 1716 1716 1287 715 286 78 13 1

Binomischer Satz

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

$$f_n = (a+b)^n - a^n - b^n = \binom{n}{1}a^{n-1}b + \ldots + \binom{n}{n-1}ab^{n-1}$$

Satz: Falls $p \in \mathbb{P}$, dann $p | f_p$

Kleiner Satz von Fermat

$$f_n = (a+b)^n - a^n - b^n = \binom{n}{1} a^{n-1} b + \ldots + \binom{n}{n-1} a b^{n-1}$$

Satz: Falls $p \in \mathbb{P}$, dann $p|f_p$

Beispiel: $a = b = 1 \quad \Longrightarrow \quad f_n = 2^n - 2$

Folgerung: Falls $p \in \mathbb{P}$, dann $p|2^p - 2$

Kleiner Satz von Fermat: $p \in \mathbb{P}$ dann $p|a^p - a$ für alle $a \in \mathbb{N}$.

Gibt es Zahlen, die die Umkehrung nicht erfüllen?
Wenn ja, dann hoffentlich nur wenige!

D.h. $n|2^n - 2$ aber $n \notin \mathbb{P}$?

Solche Zahlen heißen Fermatsche Pseudoprimzahlen zur Basis $a = 2$

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.

Anzahl der PP pro Basis bis $n = 100000$

Basis a	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	Carmichael-Zahl	Primfaktoren
561	$3 \cdot 11 \cdot 17$	15841	$7 \cdot 31 \cdot 73$
1105	$5 \cdot 13 \cdot 17$	29341	$13 \cdot 37 \cdot 61$
1729	$7 \cdot 13 \cdot 19$	41041	$7 \cdot 11 \cdot 13 \cdot 41$
2465	$5 \cdot 17 \cdot 29$	46657	$13 \cdot 37 \cdot 97$
2821	$7 \cdot 13 \cdot 31$	52633	$7 \cdot 73 \cdot 103$
6601	$7 \cdot 23 \cdot 41$	62745	$3 \cdot 5 \cdot 47 \cdot 89$
8911	$7 \cdot 19 \cdot 67$	63973	$7 \cdot 13 \cdot 19 \cdot 37$
10585	$5 \cdot 29 \cdot 73$	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).

Aber $(a^p + b^p) - (a+b)^p$ sollte eine ganze Zahl sein.

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

Wenn $p \in \mathbb{P}$, 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!

$$(a+b)^n \quad \Longrightarrow \quad (a+b+c)^n$$

$$(a+b+c)^n \quad = \quad a^n + b^n + c^n + \sum_{i+j+k=n} \frac{(i+j+k)!}{i!\, j!\, k!}\, a^i b^j c^k$$

Trinomische Formel.
Trinomial-/Multinomial-Koeffizienten stehen im/in der Pascalschen Tetraeder/Pyramide.

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

Es seien a, b, c

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

Die Perrin-Folge

a, b, c seien

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

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

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

Einfaches rekursives Bildungsgesetz: $P_n = P_{n-2} + P_{n-3}$

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 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	=	$22027 \cdot 44053$

1702 Perrin-Pseudoprimzahlen bis 10^{14}

$$
\begin{array}{rcl}
271441 & = & 521 \cdot 521 \\
904631 & = & 7 \cdot 13 \cdot 9941 \\
16532714 & = & 2 \cdot 11 \cdot 11 \cdot 53 \cdot 1289 \\
24658561 & = & 19 \cdot 271 \cdot 4789 \\
27422714 & = & 2 \cdot 11 \cdot 11 \cdot 47 \cdot 2411 \\
& \ldots & \\
99121845868033 & = & 5748097 \cdot 17244289 \\
99222369111361 & = & 7043521 \cdot 14087041 \\
99298644118081 & = & 5753221 \cdot 17259661 \\
99607901521441 & = & 5762173 \cdot 17286517
\end{array}
$$

$P_{99607901521441}$ hat 12.164.524.642.561 Dezimalstellen.
Das sind etwa 5 TByte für eine Zahl.

Was muß noch geklärt werden?

- Wann klappt der Trick auch bei reellen oder komplexen Zahlen?
- Warum sind die P_n ganzzahlig?
- Warum kann man die P_n rekursiv berechnen?
- Wie testet man schnell eine Perrin-Zahl?

Beweisidee I

Wann ist $f_n = a^n + b^n + c^n - (a+b+c)^n$ ganzzahlig?

Wenn a, b, c Nullstellen eines Polynoms $G(x)$ mit ganzzahligen Koeffizienten sind.

$$\begin{aligned} G(x) &= (x-a)(x-b)(x-c) \\ &= x^3 - (a+b+c)x^2 + (ab+bc+ca)x - abc \\ &= x^3 - K_2x^2 - K_1x - K_0 \end{aligned}$$

(Satz von Vieta!)

Weil: Dann kann man f_n als Funktion der K_0, K_1, K_2 darstellen.

Stichwort: Elementarsymmetrische Polynome.

Beweisidee II

Warum ist $f_p = a^p + b^p + c^p - (a+b+c)^p$ durch p teilbar, wenn p Primzahl ist?

$$f_n = (a+b+c)^n - (a^n + b^n + c^n) = \sum_{i+j+k=n} \frac{(i+j+k)!}{i!\ j!\ k!}\ a^i b^j c^k$$

Von den Multinomialkoeffizienten sind viele gleich (entspricht der Spiegelsymmetrie im Pascalschen Dreieck). Faßt man die zusammen, z.B. für $i = 2$, $j = 4$, $k = 5$ (das ergibt $p = i + j + k = 11$) ist

$$\frac{11!}{2!\ 4!\ 5!} = 6930 = 11 \cdot 630$$

Das ergibt

$$6930(a^2b^4c^5 + b^2c^4a^5 + c^2a^4b^5 + a^2c^4b^5 + b^2a^4c^5 + c^2b^4a^5)$$

Das kann man wieder als Funktion der K_0, K_1, K_2 darstellen.

Stichwort: Symmetrische Polynome.

Beweiside III

Warum kan man die f_n rekursiv berechnen?

Sind a, b, c Nullstellen des Polynoms $x^3 - K_2 x^2 - K_1 x - K_0$, dann läßt sich $f_n = a^n + b^n + c^n$ (mit geeigneten Anfangswerten) rekursiv als

$$f_{n+3} = K_2\, f_{n+2} + K_1\, f_{n+1} + K_0\, f_n$$

berechnen.

Das sieht man, wenn man hier $f_n = x^n$ setzt.

Die geeigneten Anfangswerte der Folge f_n sind

$$\begin{aligned}
f_0 &= a^0 + b^0 + c^0 - (a+b+c)^0 = 2 \\
f_1 &= a^1 + b^1 + c^1 - (a+b+c)^1 = 0 \\
f_2 &= a^2 + b^2 + c^2 - (a+b+c)^2 = -2(ab+bc+ca) = -K_2
\end{aligned}$$

Die größte Perrin-Pseudoprimzahl

Die größte bekannte PPP (bis jetzt) ist (20-stellig)

$$18446724258335155361 = 2479699193 \cdot 7439097577$$

Die größte bekannte PPP (ab jetzt) ist (255-stellig)

Zusammenfassung

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

Oder “Stephan WIAS” googeln.

“Für mathematisch interessierte Schüler”

Da gibt es eine Listen von Perrin-Pseudoprimzahlen.

Da gibt es eine Liste aller Primzahlen bis 37813.