2. **Primzahlen**

2.1 Definition, Eigenschaften

Definition:
Eine natürliche Zahl p heisst Primzahl, wenn p genau zwei Teiler hat.

Die Folge der Primzahlen: 2, 3, 5, 7, 11 ,13, 17, 19, 23, 29, ...

Die Suche nach immer grösseren Primzahlen geschieht nicht nur zum Vergnügen der Mathematiker, denn die Theorie der Primzahlen ist bei der Verschlüsselung von geheimen Daten von grosser praktischer Bedeutung. Eine moderne Methode beruht darauf, dass es zwar einfach ist, zwei Primzahlen zu multiplizieren, aber algorithmisch schwierig eine gegebene (grosse) Zahl in Primfaktoren zu zerlegen.

Satz:
Es gibt unendlich viele Primzahlen 2.1.1

Bereits Euklid hat diesen Satz bewiesen und zwar indirekt. Er zeigt, dass die Annahme es gebe endlich viele Primzahlen p_1, p_2, p_3, p_4, ... p_n auf einen Widerspruch führt.

Illustration der Idee an einigen Beispielen:

$a_1 = 2 + 1 = 3$
$a_2 = 2 \cdot 3 + 1 = 7$
$a_3 = 2 \cdot 3 \cdot 5 + 1 = 31$
$a_4 = 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$
$a_5 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$
$a_6 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$
$a_7 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13\ 17 + 1 = 510511 = 19 \cdot 97 \cdot 277$

Beweis:
Die Annahme, es gibt endlich viele Primzahlen führt auf einen Widerspruch:
Bilde $a = p_1 \cdot p_2 \cdot p_3 \cdot \ldots\ldots, \cdot p_n + 1$. a ist durch keine dieser Primzahlen teilbar, denn bei jeder Division durch eine der n Primzahlen tritt der Rest 1 auf.
Fall 1: a ist eine (neue) Primzahl im Widerspruch zur Annahme
Fall 2: a ist keine Primzahl. Dann lässt sich a in Primfaktoren zerlegen. Da a durch keine der Primzahlen p_1, p_2, ... p_n teilbar ist, muss es mindestens eine weitere Primzahl geben, im Widerspruch zur Annahme.

Von **Eratosthenes von Kyrene** (ca. 275 bis 194 v. Chr.) stammt die folgende Idee, Primzahlen auszusieben.

Das Sieb des Eratosthenes

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

Es werden alle natürlichen Zahlen von 1 bis zu einer beliebig gewählten Zahl n aufgeschrieben, wobei die Zahl 1 durchgestrichen wird.
2 wird als Primzahl vorgemerkt (Hintergrund grün), anschliessend werden alle geraden Zahlen(grün) "ausgesiebt".
Die nächste gefärbte Zahl wird als Primzahl gekennzeichnet (Hintergrund braun), anschliessend die Vielfachen von 3 gestrichen (braun gefärbt). Anschliessend fährt man mit der bisher nicht gefärbten 5 analog fort, usw.
Es genügt, das Sieb bis zu den Vielfachen von $\sqrt{n}$ anzuwenden. Ist nämlich eine Zahl a durch keine Primzahl p mit $p^2 \le a$ teilbar, dann ist a eine Primzahl.
Im Beispiel genügt es die Vielfachen bis 7 auszusieben. Die verbleibenden schwarz und fett dargestellten Zahlen sind ebenfalls Primzahlen, insgesamt $\pi(100) = 25$

Obwohl es unendlich viele Primzahlen gibt, hat es in ihrer Folge grosse **Lücken**:
Unter den m aufeinanderfolgenden Zahlen
(m+ 1)! + 2, (m+ 1)! + 3, (m+ 1)! + 4, ... (m+ 1)! + (m + 1)
ist keine Primzahl, denn die 1. Zahl ist durch 2, die 2. durch 3, ... , die letzte durch (m + 1) teilbar.

Bemerkung:
Eine Lücke der Länge 34 liegt schon zwischen 1327 und 1361.

Andrerseits gibt es Primzahlen p und p + 2 von minimalem Abstand 2. Beispiele solcher **Primzahlzwillinge** sind (3,5), (5,7), (11,13), (17,19), (29, 31), …

Alle Primzahlzwillinge ausser (3,5) haben die Form (6n - 1, 6n + 1).
Ob die Anzahl der Zwillingspaare unendlich ist oder nicht, ist bis heute unbekannt. Hingegen weiss man, dass sie immer seltener auftreten. Es gilt nämlich:

$$\frac{Anzahl\ der\ Zwillinge \le n}{Anzahl\ der\ Primzahlen \le n} \to 0 \quad für\ n \to \infty$$

Es ist zurzeit nicht bekannt, ob es endlich oder unendlich viele Primzahlzwillinge gibt.

Häufigkeit der Primzahlen
Die Primzahlen p_n weisen mit wachsendem n immer grössere Abstände auf, sie werden also immer seltener.

Sei $\pi(x)$ die Anzahl der Primzahlen, die kleiner oder gleich x sind.

Beispiel: $\pi(10) = 4$ {2, 3, 5, 7}

Der sogenannte Primzahlsatz macht eine asymptotische Aussage über $\pi(x)$, nämlich

Primzahlsatz von Hadamard und De la Vallée-Poussin:
Für grosse x nähert sich $\pi(x)$ immer mehr $\frac{x}{\ln x}$

Beispiele zum Primzahlsatz

x	$\pi(x)$	$\frac{x}{\ln x}$	$\frac{\pi(x) \cdot \ln x}{x}$
1.E+01	4	4	0.921034
1.E+02	25	22	1.151293
1.E+03	168	145	1.160503
1.E+04	1229	1086	1.131951
1.E+05	9592	8686	1.104320
1.E+06	78498	72382	1.084490
1.E+07	664579	620421	1.071175
1.E+08	5761455	5428681	1.061299
1.E+09	50847534	48254942	1.053727
1.E+10	455052511	434294482	1.047797

Ergänzungen siehe https://de.wikipedia.org/wiki/Primzahlsatz

Schon Euklid hat den folgenden Fundamentalsatz der Arithmetik bewiesen, der eine Aussage über das Zerlegen von natürlichen Zahlen in Primzahlen macht:

Fundamentalsatz der Arithmetik
Jede ganze Zahl grösser 1 kann nur auf eine einzige Art als Produkt von Primzahlen geschrieben werden (von der Reihenfolge der Faktoren abgesehen).

Beispiele:
Zerlegung einer Primzahl: $p = p \cdot 1$
Zerlegung einer Nicht-Primzahl: $24 = 2 \cdot 12 = 3 \cdot 8 = 4 \cdot 6 = 2 \cdot 2 \cdot 2 \cdot 3$

Auch mit den leistungsfähigsten Computern ist das Faktorisieren grosser Zahlen ausserordentlich schwierig.

2.2 Primzahlformeln, Spezielle Primzahlen:

Die Formel **$f(n) = n^2 - n + 41$** ergibt für n = 0, 1, 2, 3, ..., 40 Primzahlen.
$f(41) = 41^2$ ist aber keine Primzahl.
Gilt eine Aussage für noch so viele natürliche Zahlen, so bedeutet dies bekanntlich nicht, dass sie allgemeingültig ist.
Eine weitere Formel: **$f(n) = n^2 - 79n + 1601$**
$f(80) = 41^2$

Eine Primzahlformel

1976 wurde von einer Gruppe von Autoren eine Primzahlformel gefunden, sie ist aber wegen ihrer komplizierten Form keine Hilfe bei der Suche nach grossen Primzahlen.

Eine Primzahlformel

Rezept: Man wähle anstelle der 26 Buchstaben *a, b, c, . . . z* beliebige natürliche Zahlen inklusive der Null. Liefert dann der folgende Ausdruck eine *positive* Zahl, so ist diese Zahl automatisch eine Primzahl; umgekehrt lässt sich *jede* Primzahl auf diese Weise produzieren:

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

Diese Formel wurde 1976 in Gemeinschaftsarbeit von mehreren Autoren gefunden. Entscheidend dabei waren Vorarbeiten, die vor allem von *Y. V. Matijasevič* geleistet wurden.

Fermat-Primzahlen

Pierre de Fermat (1601-1665), Zeit-, Streitgenosse von René Descartes, glaubte, eine Formel gefunden zu haben, die lauter Primzahlen liefert.

Fermat-Primzahlen $F(n) = 2^{2^n} + 1 \quad n \in N_0$.

F(0) = 3
F(1) = 5
F(2) = 17
F(3) = 257
F(4) = 65537

Tatsächlich ergeben sich für n = 0, 1, 2, 3, 4 Primzahlen. Erst Leonhard Euler gelang 1732 der Nachweis, dass F(5) zusammengesetzt ist:

F(5) = 4 294 967 297 = 641·6700417

Bis 1998 sind die Fermatzahlen F(n) für n = 5, 6, ..., 21 und 83 weitere als zusammengesetzt erkannt worden. Die Fermatzahl F(3 329 780) ist zusammengesetzt und hat mehr als $10^{1\,002\,363}$ Stellen (Stand 2014).

Die besondere Bedeutung der Fermat-Primzahlen zeigt sich z.B. im folgenden

Satz von Gauss
Ein reguläres n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn
$n = 2^k \cdot p_1 \cdot p_2 \cdot ... \cdot p_r \quad k, r \in N$
gilt, wobei $p_1, p_2, .. , p_r$ paarweise verschiedene Fermatsche Primzahlen sind.

Ergänzungen siehe auch https://de.wikipedia.org/wiki/Fermat-Zahl

Mersenne-Primzahlen

Der Franziskanermönch und Mitschüler von Descartes Marin Mersenne (1588 - 1648) interessierte sich, für welche Primzahlen p der Ausdruck $M(p) = 2^{p-1}$ eine Primzahl liefert. Man nennt diese Zahlen deshalb Mersenne-Zahlen. Man erhält für p = 2, 3, 5, 7 Primzahlen, hingegen ist M(11) = 2047 = 23·89 zusammengesetzt.
Mersenne-Zahlen spielen bei der Jagd nach grossen Primzahlen eine Rolle.

Nähere Informationen siehe
https://de.wikipedia.org/wiki/Great_Internet_Mersenne_Prime_Search

Die Primzahleigenschaften kann bei so grossen Zahlen nicht durch Probedividieren nachgewiesen werden. Der folgende von E. Lucas und D.H. Lehmer entwickelte Primzahltest für Mersenne-Zahlen wurde 1951 erstmals mit Hilfe eines Computers durchgeführt.

Lucas-Lehmer-Test

1. Definiere u(1) = 4
2. Bestimme u(i) für i = 2, 3, 4, ...p - 1 rekursiv durch $\left[u\left(i-1\right)\right]^2 - 2 \bmod M_p$

M_p ist genau dann Primzahl, wenn u(p - 1) = 0.

Beispiel:
p = 5, $M_p = 2^5 - 1 = 31$
u(1) = 4
$u(2) = 4^2 - 2 = 14$ also u(2) = 14
$u(3) = 14^2 - 2 = 194 \equiv 8 \bmod 31$,
$u(4) = 8^2 - 2 = 62 \equiv 0 \bmod 31$
$u(4) \equiv 0 \bmod 31$ in Übereinstimmung mit der Tatsache, dass 31 prim ist.

Übungsaufgabe:
p = 11, $M_{11} = 2^{11} - 1 = 2047 = 29 \cdot 83$

Lösung:
Der Test ergibt $u(10) = 1736 \bmod 2047$, also ist M_{11} zusammengesetzt.

2.3 Zahlentheoretische Sätze und Vermutungen

Vollkommene Zahlen

Definition:
Eine Zahl n heisst vollkommen, wenn die Summe aller ihrer echten Teiler gleich der Zahl selber ist.

Beispiele:

p	n	Teiler	als Dreieckszahl
2	6	1, 2, 3	$6 = 1 + 2 + 3 = \frac{3 \cdot 4}{2}$
3	28	1, 2, 4, 7, 14	$28 = 1 + 2 + 3 + 4 + 5 + 6 + 7 = \frac{7 \cdot 8}{2}$
31	496	1, 2, 4, 8, 16, 31, 62, 124, 248	$496 = 1 + 2 + .. + 31 = \frac{32 \cdot 31}{2}$

…
Der Zusammenhang mit den Mersenne-Zahlen ergibt sich im folgenden, von Euklid stammenden

> Satz:
> Ist $2^p - 1$ eine Primzahl, dann ist $n = 2^{p-1}\left(2^p - 1\right)$ vollkommen.
> Umgekehrt kann jede vollkommene gerade Zahl in dieser Form dargestellt werden.

Mersenne bemerkte dazu: "Aus dieser Tatsache ist klar erkenntlich, dass die perfekten Zahlen sehr selten sind und dass wir durchaus berechtigt sind, sie mit vollkommenen Männern zu vergleichen“(!?)
Bis heute ist keine ungerade vollkommene Zahl bekannt. Man vermutet, dass es keine dieser Art gibt. Offen ist auch, ob es unendlich viele vollkommene Zahlen gibt.

Goldbachsche Vermutung

Christian Goldbach (1690- 1764) tätig ab 1725 an der Petersburger Akademie und als russischer Staatsminister tätig, stellte 1742 in einem Brief an Euler folgende Vermutung auf:

Jede gerade Zahl grösser als 2 kann als Summe zweier Primzahlen dargestellt werden.

Diese sogenannte Goldbachsche Vermutung ist unbewiesen.

Beispiele:

```
 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
```

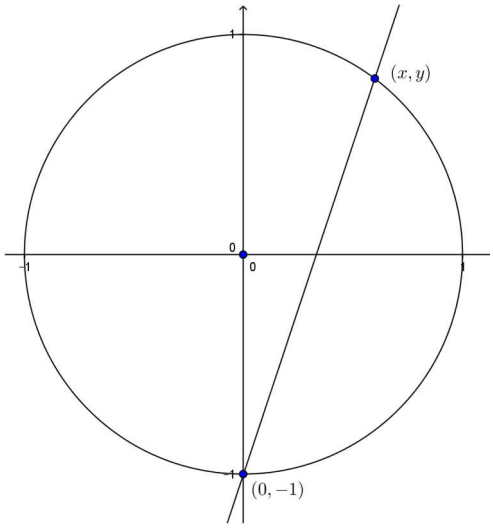
Eine Vermutung von Fermat: Der Zweiquadratesatz

Jede Primzahl p der Form 4n + 1 ist in eindeutiger Weise als Summe zweier Quadrate darstellbar:

In einem Brief vom 12.4.1749 an Goldbach kann Euler mitteilen:
„nunmehro habe ich endlich einen bündigen beweis gefunden, dass ein jeglicher numerus primus von dieser Form 4n + 1 eine summa duorum quadratorum ist.“

Pythagoreische Tripel

Für welche rechtwinkligen Dreiecke sind die Seitenlängen ganzzahlig? Schon bei Euklid (Elemente X, §§ 28-29) ist die vollständige Darstellung für ein pythagoreisches Zahlentripel zu finden. Die folgende Herleitung verbindet die Zahlentheorie mit der Geometrie.



Das Problem ist gleichbedeutend mit der Aufgabe, auf dem Einheitskreis im 1. Quadranten Punkte mit rationalen Koordinaten (x, y) zu finden.
In der Abbildung ist etwa der Punkt ($^3/_5$, $^4/_5$) dargestellt. Wegen

$$\left(\frac{3}{5}\right)^2 + \left(\frac{4}{5}\right)^2 = 1^2$$

ergibt sich daraus das Pythagoräische Tripel

$$3^2 + 4^2 = 5^2$$

Für die Schnittpunkte der Geraden durch (0, -1) mit der Steigung k > 1 und dem Einheitskreis gilt:

$$x^2 + (kx - 1)^2 = 1 \text{ oder}$$

$$x^2 + k^2x^2 - 2kx = x\big((1 + k^2)x - 2k\big) = 0$$

Die Koordinaten der 2. Lösung sind damit

$x = \frac{2k}{k^2+1}$ und $y = \frac{k^2-1}{k^2+1}$ mit $k \in Q$ und k > 1

Die rationale Zahl k kann in der Form $k = \frac{m}{n}$ mit m > n dargestellt werden, woraus folgt

$$x = \frac{2k}{k^2 + 1} = \frac{2\frac{m}{n}}{\left(\frac{m}{n}\right)^2 + 1} = \frac{2mn}{m^2 + n^2}$$

$$y = \frac{k^2 - 1}{k^2 + 1} = \frac{\left(\frac{m}{n}\right)^2 - 1}{\left(\frac{m}{n}\right)^2 + 1} = \frac{m^2 - n^2}{m^2 + n^2}$$

Damit gilt der
Satz:
Jedes pythagoräische Tripel (a, b, c) kann in der Form
$a = 2mn \quad b = m^2 - n^2 \quad c = m^2 + n^2$ mit m > n und ggT(m, n) = 1
dargestellt werden.

Beweis nach Elem. Math. 58 (2003))

Beispiele:

wähle m > n, m, n teilerfremd m - n ungerade.

m	n	a	b	c
2	1	4	3	5
3	2	12	5	13
4	3	24	7	25
4	1	8	15	17

Fermat's letzter Satz

Schon Fermat vermutete, dass die entsprechende Gleichung für Exponenten grösser als 2 nicht lösbar ist und vermerkte in einer Randnotiz, dass der Beweis etwas mehr Platz braucht als der Seitenrand zur Verfügung stellt.

Erst 1995 ist es dem Mathematiker Wiles gelungen, den folgenden Satz zu beweisen.

Fermat's letzter Satz
Die Gleichung
$a^2 + b^n = c^n$
ist für n > 2 nicht in natürlichen Zahlen lösbar.

Der Beweis, ist deutlich länger als von Fermat erwartet.

vgl. dazu die Artikel im Spektrum 12/1978 bzw. 1/1998