Primzahlen“

10. Dezember 2009

Willi More
willi.more@uni-klu.ac.at

ALPEN-ADRIA
UNIVERSITÄT
KLAGENFURT
Institut für Mathematik

Überblick

1/ Primzahlen

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,
…, …, $2^{2^4}+1$, …, $2^{43112609}-1$, …

2/ Mersennesche Zahlen

$M_n = 2^n - 1$

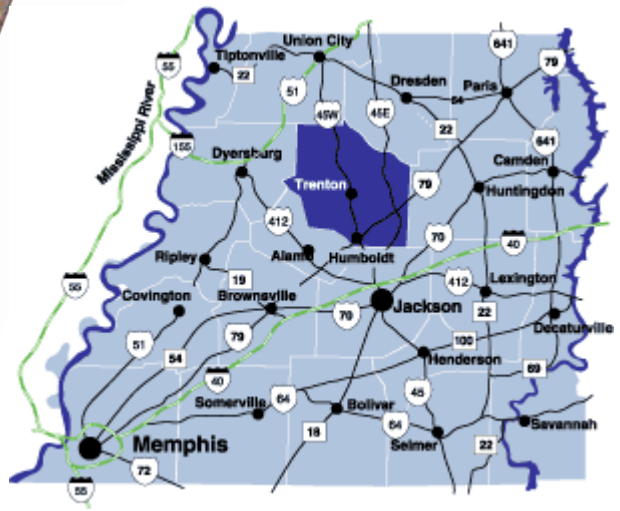
3/ Fermatsche Zahlen

$F_n = 2^{2^n} + 1$

4/ Primzahlen in Anwendungen

ISBN-10 $(a \bmod p)$, RSA $(x^e \bmod p \cdot q)$, …

Trenton, Gibson County



1/ Primzahlen

Natürliche Zahlen: 1, 2, 3, 4, …

Primzahlen sind natürliche Zahlen größer 1, welche nur durch 1 und sich selbst teilbar sind:

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,
…, $2^{2^4}+1$, …, $2^{43112609}-1$, …

Die Zahl 1 wird **Einheit** genannt. Alle natürlichen Zahlen größer 1, welche nicht Primzahlen sind, nennen wir **zusammengesetzte Zahlen**: $4 = 2\cdot 2$, $6 = 2\cdot 3$, $8 = 2\cdot 4$, $9 = 3\cdot 3$, …

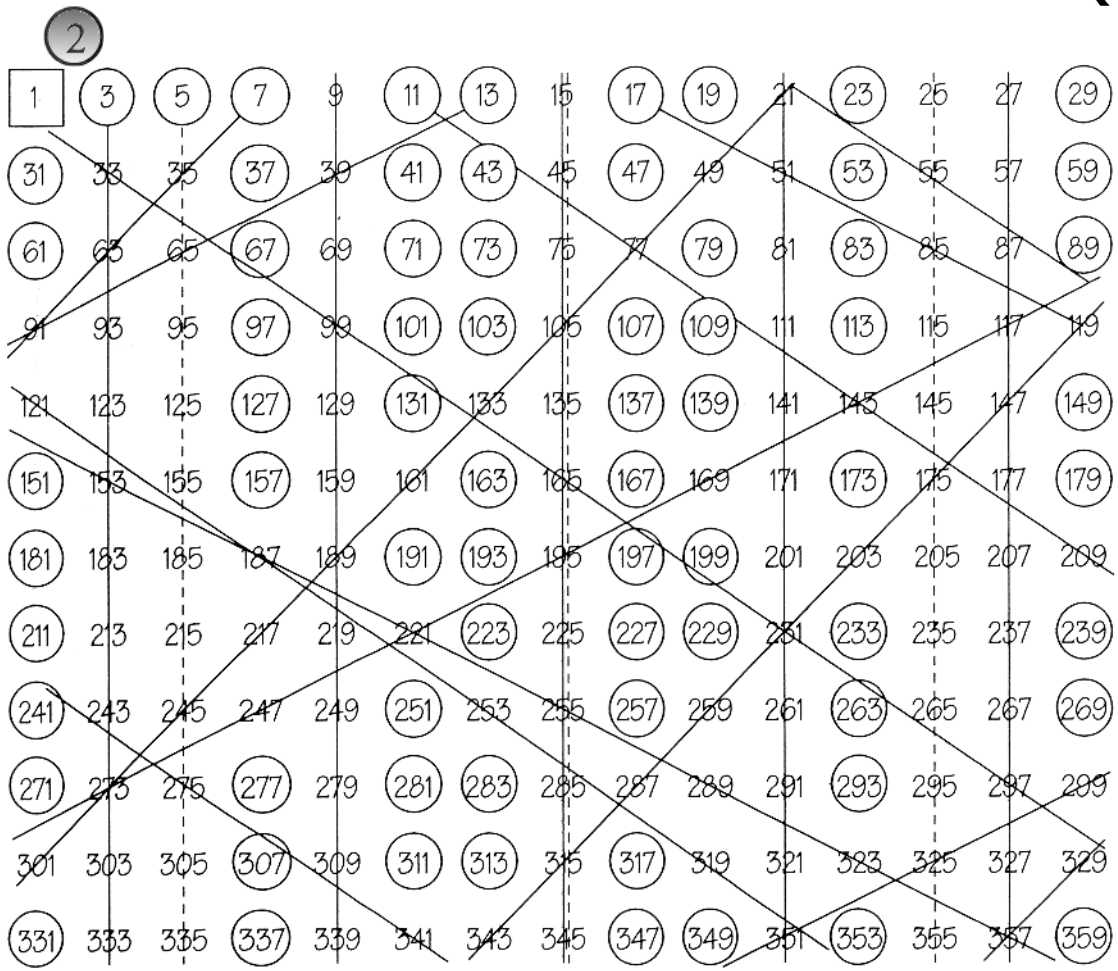
Fundamentalsatz der Arithmetik (der elementaren Zahlentheorie):
Jede natürliche Zahl größer 1 kann auf genau eine Weise in ihre Primteiler zerlegt werden.

Primzahlen sind die elementaren „multiplikativen" Bausteine der natürlichen Zahlen.

- Wie können Primzahlen erkannt werden?
- Wie viele Primzahlen gibt es?
- Wie sind die Primzahlen verteilt?
- Sind Primzahlen tatsächlich nicht zerlegbar?
- Primzahlen spezieller Bauart

The Prime Pages
prime number research, records, and resources
http://primes.utm.edu
http://primes.utm.edu/curios

1/… Primzahltabelle – Sieb des Eratosthenes (-230)



1/… Wie viele Primzahlen gibt es?

Der Abstand zwischen zwei ungeraden Primzahlen ist mindestens zwei (Primzahlzwillinge), sonst eins, kann aber beliebig groß sein: $n! = 1\cdot 2\cdot 3\cdot\ldots\cdot(n-1)\cdot n \Rightarrow 2|n!+2,\ 3|n!+3,\ \ldots,\ n|n!+n$

Aber: **Es gibt unendlich viele Primzahlen**
Beweis von Euklid von Alexandria (-3Jhdt., Elemente, Buch IX, Satz 20)

¿ **H. Lenstra**: Es gibt unendlich viele zusammengesetzte Zahlen.
Beweis: Multipliziere die ersten r Primzahlen und addiere 1 nicht. □

„Faktorisierungsproblem"

Gegeben ist eine natürliche Zahl n, gesucht ist die Primfaktorzerlegung $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$

Ähnliches, aber einfacheres Problem: Bestimme ob eine natürliche Zahl n eine Primzahl ist.

- Primzahltest, AKS [Agrawal, Kayal & Saxena 2002] $O(\ln(n)^{6+o(1)})$ $f(\ln\ln(n))$ [Lenstra/Pomerance]

Ähnliches, aber komplexitätstheoretisch fast gleich schweres Problem

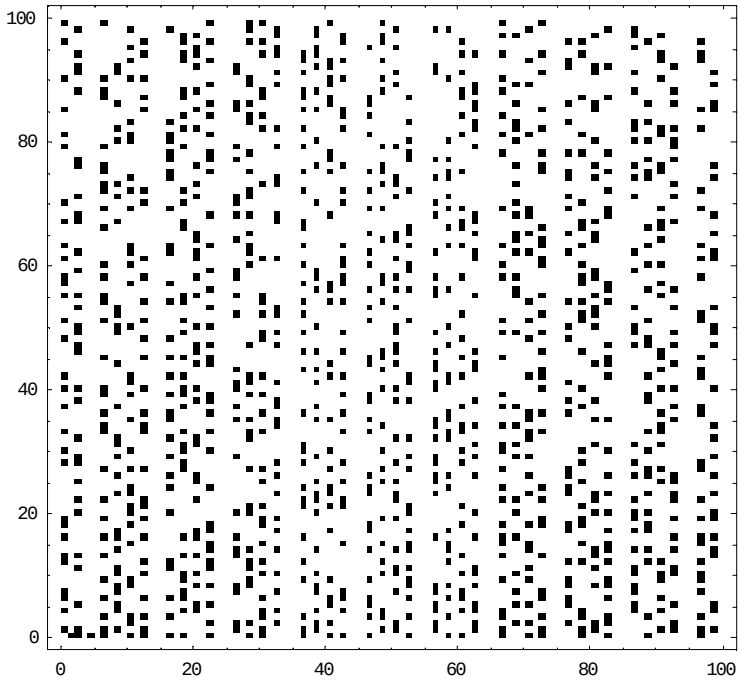
- Zerlegung von $n = a\cdot b$ mit $1 < a,b < n$

„Triviale" Algorithmen: Probedivision, Fermat-Faktorisierung 

Faktorisierungsrekord: $M_{1039} = 2^{1039}-1 = p_7 \cdot p_{80} \cdot p_{227}$ (SNFS 2007), $O(e^{(1+o(1))\sqrt[3]{\frac{32}{9}\ln(n)(\ln\ln(n))^2}})$

1/… Wie häufig sind Primzahlen?

$\pi(x) = |\{\text{Primzahlen } p \text{ mit } p \leq x\}|$



Primzahlsatz
[Gauss 1792; Beweis: Hadamard / De La Vallée-Poussin, 1896]

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln(x)} = 1$$

Der derzeitige Rekord [pi(x) project / Gourdon et.al. 2001] für $\pi(x)$ liegt bei

$$\pi(4\cdot 10^{22}) = 783964159847056303858 \cong 7.8\cdot 10^{20}$$

In diesem Bereich ist im Durchschnitt jede 26te ungerade Zahl eine Primzahl.

1/… Sind Primzahlen unzerlegbar?

Für die Primzahl 5 gilt

$$5 = (1–2i)(1+2i),$$

wobei $i^2 = –1$.

Mit Hilfe der **imaginären Einheit** i können die ganzen Zahlen zum Zahlbereich

$$\mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i] = \{a + bi \mid a,b\in\mathbb{Z}\}$$

der **Gaußschen Zahlen** erweitert werden, anschaulich: ganzzahlige Gitterpunkte.

$\mathbb{Z}[i]$ ist ein **faktorieller Ring**, d.h. jedes Element besitzt eine eindeutige Zerlegung in **Primelemente** ($p|a\cdot b \Rightarrow p|a$ oder $p|b$). Die Einheiten in $\mathbb{Z}[i]$ sind ±1, $\pm i$.

Die **Gaußsche Primzahlen** sind 2, alle Primzahlen der Form $4k+3$ (7, 11, 19, 23, …) und alle Teiler von $a^2+b^2=(a+bi)(a–bi)$ der Primzahlen der Form $4k+1$ ($5=1^2+2^2$, $13=2^2+3^2$, $17=1^2+4^2$, $29=2^2+5^2$, …).

Hinweis: Es gibt auch Zahlbereiche die keine eindeutige Zerlegung in Primelemente besitzen. Etwa gilt in $\mathbb{Z}[\sqrt{-5}] = \mathbb{Z}[i\sqrt{5}]$ mit den Einheiten ±1, dass $6 = 2\cdot3 = (1–i\sqrt{5})(1+i\sqrt{5})$, wobei alle vier Faktoren Primelemente in $\mathbb{Z}[i\sqrt{5}]$ sind.

2/... Mersennesche Zahlen

Für welche Exponenten $t \geq 1$ ist $2^t - 1$ eine Primzahl?

$2^t - 1$ kann nur dann Primzahl sein, wenn t selbst eine Primzahl ist, denn $2^u - 1 | 2^{uv} - 1$.
$M_n = 2^n - 1$ wird **Mersennesche Zahl** genannt.

Ist M_p eine Primzahl, so nennen wir sie **Mersennesche Primzahl**:

- genau 39 für p = 2, 3, 5, 7, 13, 17, 19, 31, …, 11213, …, 13466917
- weitere 8 für p = 20996011, 24036583, 25964951, 30402457
  32582657, 37156667, 42643801, 43112609

Die Mersennesche Primzahl [Smith et al 2008, GIMPS/PrimeNet]

$$2^{43112609} - 1 = 3164702693\ldots6697152511$$

ist die derzeit größte bekannte Primzahl mit rund 13 Millionen Dezimalstellen und einem Wert von US$ 100000.

- Gibt es unendlich viele Mersennesche Primzahlen?
- Gibt es unendlich viele zusammengesetzte M_n?
- Ist jede Mersennesche Zahl quadratfrei?

GIMPS
The Great Internet Mersenne Prime Search
www.mersenne.org

3/... Fermatsche Zahlen

Für welche Exponenten $t \geq 1$ ist 2^t+1 eine Primzahl?

2^t+1 Primzahlkandidat wenn t Zweierpotenz, denn für eine ungerades v gilt: $2^u+1 | 2^{uv}+1$.
$F_n = 2^{2^n}+1$ wird **Fermatsche Zahl** genannt.

Ist F_n eine Primzahl, so nennen wir sie **Fermatsche Primzahl**:
$F_0 = 2^{2^0}+1 = 3$, $F_1 = 2^{2^1}+1 = 5$, $F_2 = 2^{2^2}+1 = 17$, $F_3 = 2^{2^3}+1 = 257$, $F_4 = 2^{2^4}+1 = 65537$

Komplett faktorisiert: F_5, ..., F_{10} und [Cunnigham 1899 + Brent & Morain 1988]
$F_{11} = 319489 \cdot 974849 \cdot 167988556341760475137 \cdot 3560841906445833920513 \cdot P_{564}$
Zusammengesetzt, aber kein Faktor bekannt für $n = 14, 20, 22, 24$
Zuordnung von F_n bisher **unbekannt** für $n = 33 – 35, 40, 41, 44 – 47, \ldots$

$F_{2478782}$ [Cosgrave et al 2003] ist zusammengesetzt und hat rund 10^{746187} Dezimalstellen.

- Gibt es unendlich viele Fermatsche Primzahlen?
- Gibt es unendlich viele zusammengesetzte F_n?
- Ist jede Fermatsche Zahl quadratfrei?

www.fermatsearch.org

4/... Primzahlen in Anwendungen

Die Zahlentheorie, und mit ihr die Primzahlen, galt lange Zeit als ein Beispiel für „reinste Mathematik" ohne Anwendungsbezug und „zu nichts außer allenfalls in der Mathematik nütze". Diese Einschätzung hat sich in den letzten 30 Jahren stark verändert.

Prüfziffern

Bei der Internationale Standardbuchnummer **ISBN-10** basiert die Prüfziffernberechnung auf einer gewichteten Summe $\bmod 11$.

Beispiel: ISBN-10 3-8274-2118-7, denn $1\cdot 3+2\cdot 8+3\cdot 2+4\cdot 7+5\cdot 4+6\cdot 2+7\cdot 1+8\cdot 1+9\cdot 8 = 172 = 7 \bmod 11$.

Hinweis: Bei ISBN-13/EAN (Europäische Artikelnummer) wird für die Prüfzifferberechnung alternierend mit 1 und 3 gewichtet und $\bmod 10$ gerechnet, um das bei der ISBN-10 zusätzlich benötigte Zeichen X für 10 zu vermeiden.

Public key-Kryptographie

RSA-Kryptosystem  , ElGamal-Kryptosystem, Diffie-Hellman-Schlüsselaustausch, Elliptische Kurven über endlichen Körpern, …

Hash-Tabellen, Pseudozufallsgeneratoren, ...