

## Mersennesche Zahlen

- Antike bis Mittelalter: Für jede Primzahl  $p$  ist  $2^p - 1$  eine Primzahl.
- 1456: unbekannter Mathematiker:  $2^{13} - 1$  ist prim
- 1536: Hudalricus Regius:  $2^{11} - 1 = 2047 = 23 \cdot 89$
- 1603: Pietro Cataldi:  $2^{17} - 1$  und  $2^{19} - 1$  sind prim  
Behauptung:  $2^{23} - 1; 2^{29} - 1; 2^{31} - 1; 2^{37} - 1$  sind prim
- 1640: Pierre Fermat:  $2^{23} - 1$  und  $2^{37} - 1$  zusammengesetzt
- 1738: Leonhard Euler:  $2^{29} - 1$  zusammengesetzt
- 1750: Leonhard Euler:  $2^{31} - 1$  prim
- 1876: Lucas:  $2^{127} - 1$  ist prim
- **1644: Marin Mersenne (franz. Mönch 1588 - 1648):**

Behauptung: **Für alle Primzahlen bis 257 liefern nur die Fälle**

$$\mathbf{p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257}$$

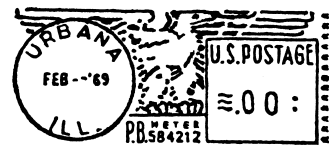
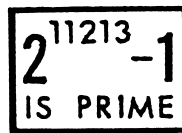
### **Primzahlen.**

- 1883: Pervouchine:  $p = 61$  übersehen
- 1911: Powers:  $p = 89$  übersehen
- 1914: Powers:  $p = 107$  übersehen
- 1947: endgültige Überprüfung bis  $p = 257$  abgeschlossen

$\Rightarrow M_p = 2^p - 1$  **sind Primzahlen für**

$$\mathbf{p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127}$$

- 1963: Gillies:  $2^{11213} - 1$  ist prim

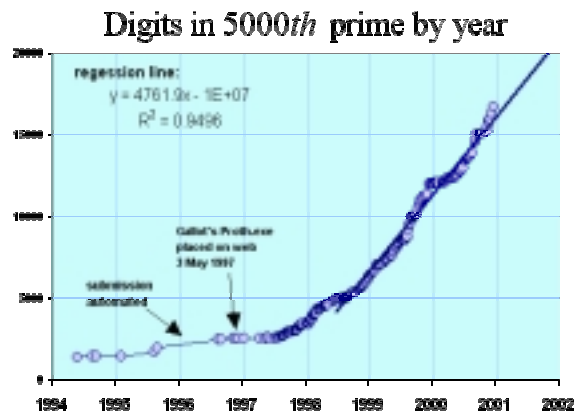


**Primfaktoren der zusammengesetzten Mersenneschen Zahlen bis  $M_{20}$**

Primfaktorzerlegung von $M_n$
$M_4 = 15 = 3 \cdot 5$
$M_6 = 63 = 3 \cdot 3 \cdot 7$
$M_8 = 255 = 3 \cdot 5 \cdot 17$
$M_9 = 511 = 7 \cdot 73$
$M_{10} = 1023 = 3 \cdot 11 \cdot 31$
$M_{11} = 2047 = 23 \cdot 89$
$M_{12} = 4095 = 3 \cdot 3 \cdot 5 \cdot 7 \cdot 13$
$M_{14} = 16383 = 3 \cdot 43 \cdot 127$
$M_{15} = 32767 = 7 \cdot 31 \cdot 151$
$M_{16} = 65535 = 3 \cdot 5 \cdot 17 \cdot 257$
$M_{18} = 262143 = 3 \cdot 3 \cdot 3 \cdot 7 \cdot 19 \cdot 73$
$M_{20} = 1048575 = 3 \cdot 5 \cdot 5 \cdot 11 \cdot 31 \cdot 41$

**Primzahlentdeckungen, bevor es Computer gab:**  
[http://www.utm.edu/research/primes/notes/by\\_year.html#1](http://www.utm.edu/research/primes/notes/by_year.html#1)

**Größte bekannte Primzahlen:**  
<http://www.utm.edu/research/primes/largest.html>



**PrimeNet**

- Koordination von
  - mehr als 21500 Rechnern
  - mehr als 12600 Internetbenutzern
  - 720 Billionen Berechnungen pro Sekunde
- Preisgeld: **\$100000** für erste Primzahl mit mehr als 10Mio Stellen (nicht viel schwerer als Berechnung der Primzahl mit 2Mio Stellen)
- Internetadresse: Links zu Primzahlen siehe [www.bernheiden.de](http://www.bernheiden.de)

**Größte bekannte Primzahl:  $2^{6972593} - 1$**  (30.06.1999)

<http://www.utm.edu/research/primes/notes/6972593/>

- erste bekannte Primzahl mit über 1Mio Stellen (2098960 Stellen)
- Computer: 350 MHz IBM Aptiva
  - Testdauer: 111 Tage (ohne Unterbrechung: 3 Wochen)
  - Testdauer mit einem besseren Testprogramm: 2 Wochen (500 MHz Alpha workstation)
- \$50000 für Entdeckung
- ausgeschrieben im Textfile: 2MB
- Länge der Primzahl: <http://www.utm.edu/research/primes/cgi/HowLong.cgi/6972593/>