Gewinnung und Test großer Primzahlen

Martin Heinzerling

16. Mai 2007

Zusammenfassung

Dieser Vortrag entstand im Rahmen des Proseminars „Kryptographische Grundlagen der Datensicherheit SS-2007“ der Technischen Universität Dresden.

Neben einer minimalen Auffrischung der mathematischen Kenntnisse stellt dieser Vortrag ein breites Spektrum aus historischen und aktuellen Primzahltest vor. Auf mathematische Beweise wurde dabei weitestgehend verzichtet und der Schwerpunkt auf die praktische Verwendung und Beispiele gelegt. Einige aktuelle Informationen zu Primzahlen runden den Überblick dann ab.

Inhaltsverzeichnis

1 Einführung

1.1 Anwendung

Verwendung großer Primzahlen

- Faktorisierung wird erschwert, praktisch unmöglich mit > 1000 Binärstellen
- Verschlüsselungsverfahren
  - z.B. RSA
- Zufallsgenerator
  - z.B. BBS (Blum-Blum-Shub)

1.2 Notation und Grundlagen

1.2.1 Ordnung

Ordnung
Die Ordnung von $a \bmod r$ ist die kleinste natürliche Zahl k, so dass $a^k \equiv 1 (\bmod\ r)$.

$$ord_r(a) = k$$

1.2.2 Eulersche ϕ-Funktion

Eulersche ϕ-Funktion
Die Eulersche ϕ-Funktion gibt für jede natürliche Zahl n an, wie viele natürliche Zahlen zwischen 1 und n zu ihr teilerfremd sind.

$$\phi(n) := |\{a \mid ggT(a, n) = 1, a \in \{1, \ldots, n-1\}\}|$$

1.2.3 Kleiner Satz von Fermat

Kleiner Satz von Fermat
Für alle Primzahlen p und alle natürlichen Zahlen n, die kein Vielfaches von p sind, gilt:

$$n^{(p-1)} - 1 \text{ ist teilbar durch } p$$

bzw.

$$n^{p-1} \equiv 1 (\bmod\ p)$$

2 Primzahlgewinnung

2.1 Sieb des Eratosthenes

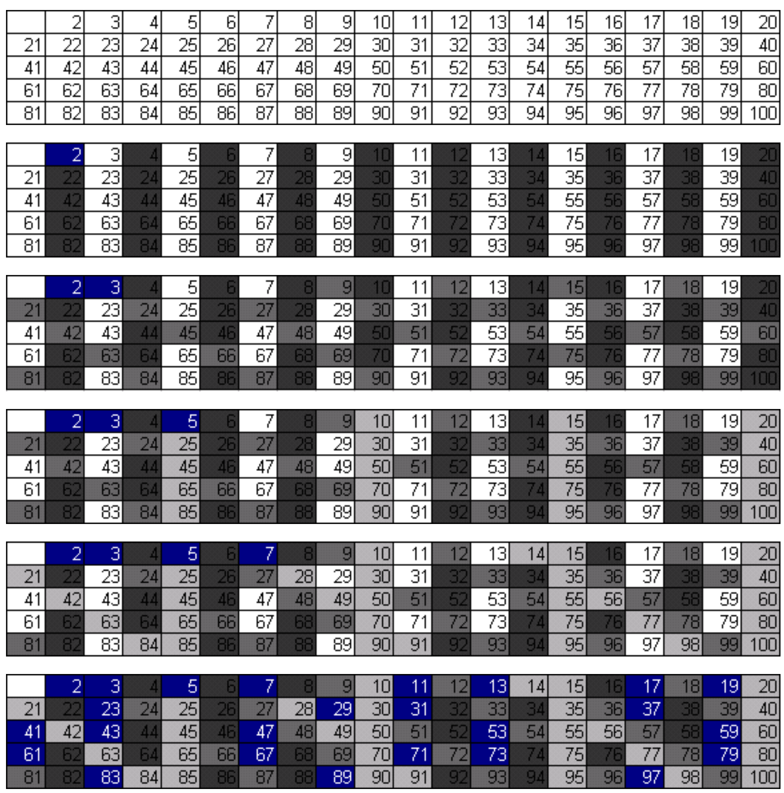
Sieb des Eratosthenes

- griechischer Mathematiker Eratosthenes
- ca. 275 - 194 v.Chr.
- in Kyrene (heutiges Libyen) geboren

Algorithmus

1. Zusammenhängende Liste von natürlichen Zahlen $2 \ldots n$
2. Erste Primzahl $p = 2$
3. Streichen aller Vielfachen von p, beginnend bei p^2
4. Wiederhole Schritt 3 mit der nächsten freien Zahl $p < \sqrt{n}$
5. Alle beim „sieben“ übrig gebliebenen Zahlen sind Primzahlen

Sieb des Eratosthenes - Beispiel $n = 100$



2.2 Formeln zur Generierung von Primzahlen

Primzahlenformeln

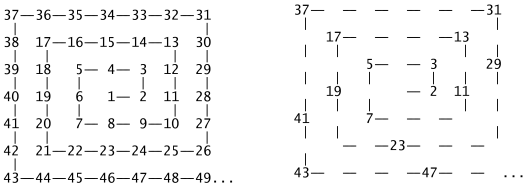
- Satz von Euklid
  - $n = 1 + \prod_{i=1}^{k} p_i$
  - n ist neue Primzahl oder
  - zusammengesetzte Zahl, aus Primzahlen die nicht am Produkt beteiligt sind
- Euler
  - $n^2 + n + 17$ für $0 < n < 16$
  - $n^2 - n + 41$ für $0 < n < 41$
  - $n^2 - 89n + 1601$ für $0 < n < 80$

2.3 Ulam-Spirale

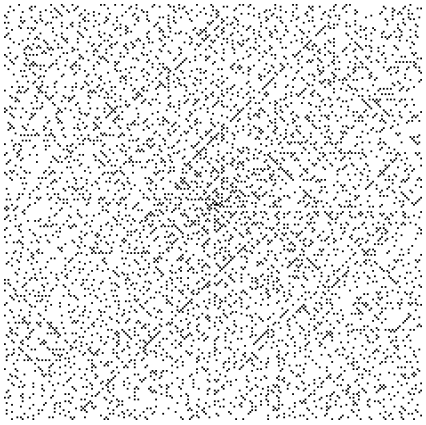
Ulam-Spirale

- polnischer Mathematiker Stanislaw Marcin Ulam
- weitere Formeln der Form $f(n) = an^2 + bn + c$ mit $a, b, c, b \in \mathbb{Z}$

Ulam-Spirale - 7×7



Ulam-Spirale - 200×200



3 Primzahlentest

3.1 Einfaches Durchtesten

Einfaches Durchtesten(Brute Force)

- n - zu testende Zahl
- Division durch alle Primzahlen $p < \sqrt{n}$
- Vorteil:
  - führt theoretisch immer zu einer eindeutigen Lösung
- Nachteil:
  - bei großen Zahlen praktisch nicht anwendbar
  - hoher Zeit- und Ressourcenaufwand
- Optimierung:
  - nur Zahlen der Form $6k-1$ oder $6k+1$ prüfen, ab $n > 3$ mit $k \in \mathbb{N}$

3.2 Fermatsche Primzahltest

3.2.1 Algorithmus

Fermatsche Primzahltest

- Anwendung des kleinen Fermat $b = a^{n-1} (\text{mod } n)$
- n - zu testende Zahl
- a - Primzahlbasis $2 \leq a < n$, $a \in \mathbb{N}$
- $b = \begin{cases} 1 & \text{Primzahlkandidat} \\ sonst & \text{keine Primzahl} \end{cases}$

Beispiel: $a = 2, 3, 5; n = 11$

$$\begin{array}{llllll} 2^{11-1} & \equiv 2^5 * 2^5 & \equiv 10 * 10 & \equiv 100 & \equiv 1 (\text{mod } 11) \\ 3^{11-1} & \equiv 9^5 & \equiv -2^5 & \equiv -32 & \equiv 1 (\text{mod } 11) \\ 5^{11-1} & \equiv 25^5 & \equiv 3^5 & \equiv 243 & \equiv 1 (\text{mod } 11) \end{array}$$

3.2.2 Fermatsche Pseudoprimzahl

Fermatsche Pseudoprimzahl

- mehr Primzahlen als Pseudoprimzahlen

Beispiel: Kleinste Pseudoprimzahlen zu einer Basis

2	$341, 561, 645, 949, \ldots$	3	$91, 121, 286, 671, \ldots$
4	$15, 85, 91, 341, \ldots$	5	$124, 217, 561, 781, \ldots$
6	$35, 185, 217, 301, \ldots$	7	$25, 325, 561, 703, \ldots$

Beispiel: Kleinste Pseudoprimzahl durch mehrere Basen

$2, 3$	1105	$2, 3, 5$	1729
$2, 3, 5, 7, 11$	29341	$2, 3, 5, 7, 11, 13$	162401

3.2.3 Carmichael-Zahl

Carmichael-Zahl

- $a^{n-1} \equiv 1 (\text{mod } n)$ für alle a mit $ggt(a, n) = 1$
- ist Produkt aus mindestens 3 Primzahlen

Beispiel: Kleinste Carmichael-Zahl $n = 561$

- $561 = 3 * 11 * 17$
- 561 wird von $a \in \{3, 11, 17, 33, 51, 187\}$ geteilt, d.h.
  - $3^{560} \equiv 375 \pmod{561}$
  - $11^{560} \equiv 154 \pmod{561}$
  - $17^{560} \equiv 34 \pmod{561}$
  - $\ldots$

3.3 Miller-Rabin-Test

Miller-Rabin-Test

- Weiterentwicklung des Fermatschen Primzahltest
- stochastische Wahl mehrerer Basen
- Monte-Carlo-Algorithmus
- zusätzlicher „Belastungszeuge“ (witness) x für n $x^2 \equiv 1 (\text{mod } n)$ mit $x \neq 1$ und $x \neq -1$

- erkennt auch Carmichael-Zahlen
- nur Primzahlen und starke Pseudoprimzahlen

Algorithmus

- n - zu testende Zahl und a - die Basis
- $t = \max(2^s | (n-1)), s \in N$
- $u = \frac{(n-1)}{t^2}$
- n ist Primzahlkanditat wenn
  - $a^u \equiv 1(\text{ mod }) n$ oder
  - $\exists s \in \{0, \ldots, t-1\}$ mit $a^{(2^s)u} \equiv -1(\text{ mod } n)$

Beispiel: $n = 561$

- $n - 1 = 561 - 1 = 1000110000_2$
- Verschiebung um $t = 4 \rightarrow u = 100011_2 = 35_{10}$
- $560 = 2^4 * 35$
- Fermattest mit a^u mod n und anschließen $(t-1) - mal$ quadrieren.
  $a = 2\ 2^{35} \equiv 34.359.738.368 \equiv 263 \neq (-)1\ 263^2 \equiv 69.169 \equiv 166\ 166^2 \equiv 27.556 \equiv 67\ 67^2 \equiv 4.489 \equiv 1 \neq -1(\text{mod } 561)$
  $\Rightarrow n$ ist keine Primzahl

Beispiel: $n = 73$

- $n - 1 = 73 - 1 = 1001000_2$
- Verschiebung um $t = 3 \rightarrow u = 1001_2 = 9_{10}$
- $72 = 2^3 * 9$
- Fermattest mit a^u mod n und anschließen $(t-1) - mal$ quadrieren.
  $a = 68$
  $68^9 \equiv 63 \neq (-)1\ 63^2 \equiv 27 \neq 72\ 27^2 \equiv 72 \equiv -1(\text{mod } 73)$
  $\Rightarrow n$ ist Primzahl(kandidat)

Fehlerrate

- in $\{1, \ldots, n-1\}$ existieren höchstens $\frac{n-1}{4}$ Zahlen die keine Zeugen sind
- d.h. $p(a) = \frac{1}{4} = 25\%$ mit a beliebig
- $p(a_1) * p(a_2) * p(a_3) * p(a_4) = 0,39\%$
- $p(a_i)^{10} = 0,0001\%$

3.4 AKS-Primzahltest

AKS-Primzahltest

- Agrawal-Kayal-Saxena-Primzahltest
- August 2002: PRIMES in P

Grundidee(1999)
n ist Primzahl gdw. $(x+a)^n \equiv x^n + a(\mod n)$ für ein $a \in Z$ mit $ggT(a,n) = 1$.

Erweiterung(2001/2002)
$(x+a)^n \equiv x^n + a(\mod x^r - 1, n)$ mit kleinstem r für das gilt $ord_r(n) > log^2 n \in \mathbb{N}$ und $ggT(r,n) = 1$

Algorithmus
Eingabe: $n \in N, n \geq 2$

1. If $n = a^b$ für $a, b > 1 \in N$, return COMPOSITE
2. Finde das kleinste r, so dass $ord_r(n) > log^2 n$
3. If $1 < ggT(a,n) < n$ für ein $a \leq r$, return COMPOSITE
4. If $n \leq r$, return PRIME
5. For $a = 1$ to $\left\lfloor \sqrt{\phi(r)} log n \right\rfloor$ do If $(x+a)^n \neq x^n + a(\mod x^{r-1}, n)$ return COMPOSITE
6. Return PRIME

3.5 Lucas-Lehmer-Test

Lucas-Lehmer-Test

- Mersenne-Zahlen $M_p = 2^p - 1$

Algorithmus

- $S(1) = 4$
- $S(k+1) = S(k)^2 - 2(\mod M_p)$
- $S(p-1) = 0 \Rightarrow M_p$ ist prim

Beispiel: $M_{19} = 524287$

$$
\begin{array}{rcrlr}
S(1) & = & 4 & & \\
S(2) & = & (4^2 - 2) & \mod 524287 = & 14 \\
S(3) & = & (14^2 - 2) & \mod 524287 = & 194 \\
S(4) & = & (194^2 - 2) & \mod 524287 = & 37634 \\
S(5) & = & (37634^2 - 2) & \mod 524287 = & 218767 \\
S(6) & = & (218767^2 - 2) & \mod 524287 = & 510066 \\
S(7) & = & (510066^2 - 2) & \mod 524287 = & 386344 \\
\ldots & & & & \\
S(14) & = & (307417^2 - 2) & \mod 524287 = & 382989 \\
S(15) & = & (382989^2 - 2) & \mod 524287 = & 275842 \\
S(16) & = & (275842^2 - 2) & \mod 524287 = & 85226 \\
S(17) & = & (85226^2 - 2) & \mod 524287 = & 523263 \\
S(18) & = & (523263^2 - 2) & \mod 524287 = & 0
\end{array}
$$

4 Aktuelles

4.1 Top Primzahlen

- 44. und größte Mersenne-Zahl
  - September 2006
  - $2^{32.582.657} - 1$
  - 9.808.358 Dezimalstellen
- Größte Zwillingsprimzahl
  - Januar 2007
  - $2.003.663.613 * 2^{195000} - 1 \pm 1$
  - 58.711 Dezimalstellen
- Größte Palindromprimzahl

  - Oktober 2006
  - $10^{170006} + 3880883 * 10^{85000} + 1$
  - 170.007 Dezimalstellen
- Größte Nicht-Mersenne-Zahl (Platz 7)
  - 10. Mai 2007
  - $19249 * 2^{13018586} + 1$
  - 2.759.677 Dezimalstellen

5 Appendix

5.1 Quellen

1. Artikel *Carmichael-Zahl*.
   In: Wikipedia, Die freie Enzyklopädie.
   Bearbeitungsstand: 18. April 2007, 01:07 UTC.
   http://de.wikipedia.org/w/index.php?title=Carmichael-Zahl&oldid=30660787

2. Artikel *Kleiner fermatscher Satz*.
   In: Wikipedia, Die freie Enzyklopädie.
   Bearbeitungsstand: 10. April 2007, 16:46 UTC.
   http://de.wikipedia.org/w/index.php?title=Kleiner_fermatscher_Satz&oldid=30338090

3. Artikel *Mersenne-Primzahl*. In: Wikipedia, Die freie Enzyklopädie.
   Bearbeitungsstand: 9. April 2007, 16:59 UTC.
   http://de.wikipedia.org/w/index.php?title=Mersenne-Primzahl&oldid=30296253

4. Artikel *Primzahl*.
   In: Wikipedia, Die freie Enzyklopädie.
   Bearbeitungsstand: 29. April 2007, 09:30 UTC.
   http://de.wikipedia.org/w/index.php?title=Primzahl&oldid=31122544

5. Artikel *Primzahltest*.
   In: Wikipedia, Die freie Enzyklopädie.
   Bearbeitungsstand: 12. April 2007, 11:02 UTC.
   http://de.wikipedia.org/w/index.php?title=Primzahltest&oldid=30412766

6. Artikel *Ulam-Spirale*.
   In: Wikipedia, Die freie Enzyklopädie.
   Bearbeitungsstand: 13. Dezember 2006, 19:30 UTC
   http://de.wikipedia.org/w/index.php?title=Ulam-Spirale&oldid=25090435

7. Website *Arndt Brünners Mathematik-Seiten*.
Autor: Arndt Brünner Bearbeitungsstand: 23. März 2007 http://www.arndt-bruenner.de/mathe

8. Artikel *Miller-Rabin Primzahltest*
Autor: F. Riehhardt Bearbeitungsstand: 2002
http://www.bitnuts.de/rienhardt/docs/miller_rabin.pdf

9. Artikel *Primes is in P*
Autor: Manindra Agrawal, Neeraj Kayal, Nitin Saxena
Bearbeitungsstand: 2004
http://www.cse.iitk.ac.in/users/manindra/algebra/primality.pdf

10. Artikel *Primzahltest*
Autor: Joris Bayer
Bearbeitungsstand: 18. Januar 2006
http://www.finanz.math.tugraz.at/~ziegler/proseminar/Bayer/Primzahltests.pdf

11. Website *Primzahltest*
Autor: H.W. Lang
Bearbeitungsstand: 03. Januar 2006
http://www.inf.fh-flensburg.de/lang/krypto/algo/primtest.htm

12. Artikel *Primes ist in P - Der AKS-Primzahltest*
Autor: Hans-Gert Gräbe
Bearbeitungsstand: 10. Oktober 2003
http://www.informatik.uni-leipzig.de/~graebe/MCAT/mcat6/graebe-folien.pdf

13. Artikel *Der AKS-Primzahltest*
Autor: Marian Claus
Bearbeitungsstand: 04. Dezember 2006
http://www.mi.uni-erlangen.de/~ruppert/WS0607/Seminar/Claus/Der_AKS-Primzahltest.pdf

14. Website *Mersenne Prime Search*
Bearbeitungsstand: 11. September 2006
http://www.mersenne.org

15. Website *primzahlen.de*
Bearbeitungsstand: 23. März 2007
http://www.primzahlen.de

16. Artikel *Miller/Rabin Primzahltest*
Autor: Bernd Borchert
Bearbeitungsstand: 14. Februar 2006
http://www-fs.informatik.uni-tuebingen.de/lehre/ws05-06/randomalg/Java/Primzahl/

17. Artikel *Primzahltests*
Autor: Christoph Spallek
Bearbeitungsstand: 13. Juni 2006
http://dud.inf.tu-dresden.de/~mb41/proseminar/2006/Primzahltest.pdf

18. Artikel *Primzahlformeln*
Bearbeitungsstand: Unversioniert
http://library.thinkquest.org/C005660/de/users/lessons/prime2.html

19. Website *The Top Twenty*
Autor: Chris Caldwell
Bearbeitungsstand: 2007
http://primes.utm.edu/top20

20. Wikibook *Pseudoprimzahlen*
Bearbeitungstand: 31. Juli 2006
http://de.wikibooks.org/w/index.php?title=
Pseudoprimzahlen:_Die_fermatsche_Pseudoprimzahl_im_allgemeinen&oldid=175241

5.2 Abbildungsverzeichnis

- **Ulam-Spirale 50_1** http://de.wikipedia.org/wiki/Bild:Ulam-Spirale1.png
- **Ulam-Spirale 50_2** http://de.wikipedia.org/wiki/Bild:Ulam-Spirale2.png
- **Ulam-Spirale 200** http://de.wikipedia.org/wiki/Bild:Ulps000-1.png

5.3 Download

Download der Präsentation und der Ausarbeitung in Textform unter:

http://tud.bashcomp.de