

Gewinnung und Test großer Primzahlen

Martin Heinzerling

TU Dresden, Fakultät Informatik

16. Mai 2007

1 Einführung

2 Primzahlgewinnung

3 Primzahlentest

4 Aktuelles

5 Appendix

1 Einführung

- Anwendung
- Notation und Grundlagen
 - Ordnung
 - Eulersche ϕ -Funktion
 - Kleiner Satz von Fermat

Verwendung großer Primzahlen

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

Ordnung

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

$$\text{ord}_r(a) = k$$

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.

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

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.

$$n^{p-1} \equiv 1 \pmod{p}$$

2 Primzahlgewinnung

- Sieb des Eratosthenes
- Formeln zur Generierung von Primzahlen
- Ulam-Spirale

Sieb des Eratosthenes

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

Algorithmus

- 1 Zusammenhängende Liste von natürlichen Zahlen $2 \dots n$
- 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	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

Sieb des Eratosthenes - Beispiel $n = 100$

	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

	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

Sieb des Eratosthenes - Beispiel $n = 100$

	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

	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

Sieb des Eratosthenes - Beispiel $n = 100$

	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

	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

Sieb des Eratosthenes - Beispiel $n = 100$

	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

	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

Sieb des Eratosthenes - Beispiel $n = 100$

	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

	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

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 $0 < n < 80$

Ulam-Spirale

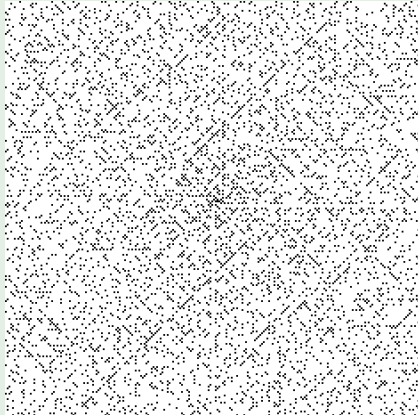
- polnischer Mathematiker Stanislaw Marcin Ulam
- weitere Formeln der Form $f(n) = an^2 + bn + c$ mit $a, b, c, b \in \mathbb{Z}$

Ulam-Spirale - 7×7

37	36	35	34	33	32	31
38	17	16	15	14	13	30
39	18	5	4	3	12	29
40	19	6	1	2	11	28
41	20	7	8	9	10	27
42	21	22	23	24	25	26
43	44	45	46	47	48	49...

37						31
	17				13	
		5		3		29
	19			2	11	
41		7				
			23			
43			47			...

Ulam-Spirale - 200×200



3 Primzahlentest

- Einfaches Durchtesten
- Fermatsche Primzahltest
 - Algorithmus
 - Fermatsche Pseudoprimzahl
 - Carmichael-Zahl
- Miller-Rabin-Test
- AKS-Primzahltest
- Lucas-Lehmer-Test

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 $k \in \mathbb{N}$

Fermatsche Primzahltest

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

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

$$2^{11-1} \equiv 2^5 * 2^5 \equiv 10 * 10 \equiv 100 \equiv 1 \pmod{11}$$

$$3^{11-1} \equiv 9^5 \equiv -2^5 \equiv -32 \equiv 1 \pmod{11}$$

$$5^{11-1} \equiv 25^5 \equiv 3^5 \equiv 243 \equiv 1 \pmod{11}$$

Fermatsche Pseudoprimzahl

- mehr Primzahlen als Pseudoprimzahlen

Beispiel: Kleinste Pseudoprimzahlen zu einer Basis

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

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

Carmichael-Zahl

- $a^{n-1} \equiv 1 \pmod{n}$ für alle a mit $\text{ggT}(a, n) = 1$
- 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.
 - $3^{560} \equiv 375 \pmod{561}$
 - $11^{560} \equiv 154 \pmod{561}$
 - $17^{560} \equiv 34 \pmod{561}$
 - ...

Miller-Rabin-Test

- Weiterentwicklung des Fermatschen Primzahltest
- stochastische Wahl mehrerer Basen
- Monte-Carlo-Algorithmus
- zusätzlicher „Belastungszeuge“ (witness) x für n
 $x^2 \equiv 1 \pmod{n}$ 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
- $t = \max(2^s | (n-1)), s \in \mathbb{N}$
- $u = \frac{(n-1)}{t^2}$
- n ist Primzahlkandidat wenn
 - $a^u \equiv 1 \pmod{n}$ oder
 - $\exists s \in \{0, \dots, t-1\}$ mit $a^{(2^s)u} \equiv -1 \pmod{n}$

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 $a^u \bmod n$ und anschließend $(t - 1) - mal$ quadrieren.

$$a = 2$$

$$2^{35} \equiv 34.359.738.368 \equiv 263 \neq (-)1$$

$$263^2 \equiv 69.169 \equiv 166$$

$$166^2 \equiv 27.556 \equiv 67$$

$$67^2 \equiv 4.489 \equiv 1 \neq -1 \pmod{561}$$

$\Rightarrow n$ 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 $a^u \bmod n$ und anschließend $(t - 1) - mal$ quadrieren.
 - $a = 68$
 - $68^9 \equiv 63 \neq (-)1$
 - $63^2 \equiv 27 \neq 72$
 - $27^2 \equiv 72 \equiv -1 \pmod{73}$
 - $\Rightarrow n$ ist Primzahl(kandidat)

Fehlerrate

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

AKS-Primzahltest

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

Grundidee(1999)

n ist Primzahl gdw. $(x + a)^n \equiv x^n + a \pmod{n}$ für ein $a \in \mathbb{Z}$ mit $\text{ggT}(a, n) = 1$.

Erweiterung(2001/2002)

$(x + a)^n \equiv x^n + a \pmod{x^r - 1, n}$ mit kleinstem r für das gilt $\text{ord}_r(n) > \log^2 n \in \mathbb{N}$ und $\text{ggT}(r, n) = 1$

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 $\text{ord}_r(n) > \log^2 n$
- 3 If $1 < \text{ggT}(a, n) < n$ 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 $(x + a)^n \not\equiv x^n + a \pmod{x^{r-1}, n}$ return COMPOSITE
- 6 Return PRIME

Lucas-Lehmer-Test

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

Algorithmus

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

Beispiel: $M_{19} = 524287$

$$S(1) = 4$$

$$S(2) = (4^2 - 2) \bmod 524287 = 14$$

$$S(3) = (14^2 - 2) \bmod 524287 = 194$$

$$S(4) = (194^2 - 2) \bmod 524287 = 37634$$

$$S(5) = (37634^2 - 2) \bmod 524287 = 218767$$

$$S(6) = (218767^2 - 2) \bmod 524287 = 510066$$

$$S(7) = (510066^2 - 2) \bmod 524287 = 386344$$

...

$$S(14) = (307417^2 - 2) \bmod 524287 = 382989$$

$$S(15) = (382989^2 - 2) \bmod 524287 = 275842$$

$$S(16) = (275842^2 - 2) \bmod 524287 = 85226$$

$$S(17) = (85226^2 - 2) \bmod 524287 = 523263$$

$$S(18) = (523263^2 - 2) \bmod 524287 = 0$$

4 Aktuelles

■ Top Primzahlen

■ 44. und größte Mersenne-Zahl

- September 2006

- $2^{32.582.657} - 1$

- 9.808.358 Dezimalstellen

■ Größte Zwillingssprimzahl

- 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

- Quellen
- Abbildungsverzeichnis
- Download

Artikel Carmichael-Zahl. In: Wikipedia, Die freie Enzyklopädie.

<http://de.wikipedia.org/w/index.php?title=Carmichael-Zahl&oldid=30660787>

Artikel Kleiner fermatscher Satz. In: Wikipedia, Die freie Enzyklopädie.

http://de.wikipedia.org/w/index.php?title=Kleiner_fermatscher_Satz&oldid=30338090

Artikel Mersenne-Primzahl. In: Wikipedia, Die freie Enzyklopädie.

<http://de.wikipedia.org/w/index.php?title=Mersenne-Primzahl&oldid=30296253>

Artikel Primzahl. In: Wikipedia, Die freie Enzyklopädie.

<http://de.wikipedia.org/w/index.php?title=Primzahl&oldid=31122544>

Artikel Primzahltest. In: Wikipedia, Die freie Enzyklopädie.

<http://de.wikipedia.org/w/index.php?title=Primzahltest&oldid=30412766>

Artikel Ulam-Spirale. In: Wikipedia, Die freie Enzyklopädie.

<http://de.wikipedia.org/w/index.php?title=Ulam-Spirale&oldid=25090435>

Quellen

<http://www.arndt-bruenner.de/mathe>

http://www.bitnuts.de/rienhardt/docs/miller_rabin.pdf

<http://www.cse.iitk.ac.in/users/manindra/algebra/primality.pdf>

<http://www.finanz.math.tugraz.at/~ziegler/proseminar/Bayer/Primzahltests.pdf>

<http://www.inf.fh-flensburg.de/lang/krypto/algo/primtest.htm>

<http://www.informatik.uni-leipzig.de/~graebe/MCAT/mcat6/graebe-folien.pdf>

http://www.mi.uni-erlangen.de/~ruppert/WS0607/Seminar/Claus/Der_AKS-Primzahltest.pdf

<http://www.mersenne.org>

<http://www.primzahlen.de>

<http://www-fs.informatik.uni-tuebingen.de/lehre/ws05-06/randomalg/Java/Primzahl/>

<http://dud.inf.tu-dresden.de/~mb41/proseminar/2006/Primzahltest.pdf>

<http://library.thinkquest.org/C005660/de/users/lessons/prime2.html>

<http://primes.utm.edu/top20>

http://de.wikibooks.org/w/index.php?title=Pseudoprimzahlen:_Die_fermatsche_Pseudoprimzahl_im_allgemeinen&oldid=175241

■ 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:Ulp000-1.png>

Download der Präsentation und der Ausarbeitung in Textform
unter:

<http://tud.bashcomp.de>