Proseminar zur Linearen Algebra

Kryptographie und Codierungstheorie

Thema: Faktorisierungsalgorithmen
(nach der Fermat'schen Faktorisierungsmethode)

- Kettenbruchalgorithmus (Continued Fraction Method)
- Quadratisches Sieb
- Implementierungen

Gliederung:

0. Einleitung:

Sei N eine natürliche Zahl, dann folgt:

$$N = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_d^{e_d} \quad mit\ e_i \in \mathbb{N}\ \ und\ p_i\ Primzahlen$$

(nach Euklid (360 – 280 v. Chr.)): jede natürliche Zahl ist zerlegbar in eindeutige Primteiler)

Nächstliegende Idee: Trial Division bis $\sqrt{N}$

Sieb des Eratosthenes (276 – 194 v. Chr.):

Ermitteln aller Primzahlen bis zu einer Schranke n

Strategie zur Faktorisierung einer natürlichen Zahl N:

1. N durch 2 teilen, bis N‘ ungerade wird

2. Primteiler von N durch Trial Division und/oder der eben vorgestellten Methode abspalten

3. Methoden für kleine Primzahlen nutzen, um diese abzuspalten (Elliptische-Kurven-Methode, Pollard-Methoden, …)

4. Primzahl- und Primzahlpotenztests durchführen (Gruppe 1)

5. Faktorisierungsalgorithmen mit quadratischen Resten nach Fermats Ideen (CFM, QS, Zahlkörpersieb)

Je nach Größe des N, des benutzten Programms und der Literatur werden unterschiedliche Grenzen zwischen den einzelnen Punkten gezogen bzw. empfohlen.

Fermats Idee (1607-1665 n. Chr.):

Sei dazu $N \in \mathbb{N}$ ungerade und keine Primzahl

$\Rightarrow N = a \cdot b, \quad a, b \in \mathbb{N}$ ungerade

$$\Rightarrow N = (x+y) \cdot (x-y) = x^2 - y^2$$

$$mit\ x := \frac{a+b}{2} \quad und \quad y := \frac{a-b}{2}$$

Algorithmus :

(1) *Setze* $x := \lfloor \sqrt{N} \rfloor + 1$ *und* $f(x) := x^2 - N$

(2) *Ist nun* $f(x) = y^2$ *ein Quadrat, so haben wir die Faktorisierung von*
$N = (x+y) \cdot (x-y)$,
wenn nicht :
$x := x + 1$, $f(x+1) := f(x) + 2x + 1$ *und gehe zu* (2)

Gliederung:

1. Continued Fraction Method:

Definition:

- Als Kettenbruch definiert man Objekte der Form

$$\kappa_0 := a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \cfrac{b_3}{a_3 + \cfrac{b_4}{a_4 + \cfrac{b_5}{a_{n-1} + \cfrac{b_n}{a_n}}}}}}$$

- a_0 heißt das Anfangsglied. Die a_i und die b_i heißen Teilnenner bzw. –zähler.
- Sind alle b_i=1 und ist a_0 eine ganze Zahl so heißt der Kettenbruch regulär.

Reguläre Kettenbrüche

Nun schreiben wir eine reelle Zahl x in der Form

$$x = b_0 + \cfrac{1}{b_1 + \cfrac{1}{b_2 + \cdots}} = b_0 + \frac{1|}{|b_1} + \frac{1|}{|b_2} + \cdots,$$

wie folgt:

$$b_0 = [x], \quad x_1 = \frac{1}{x - b_0}, \qquad b_1 = [x_1], \quad x_2 = \frac{1}{x_1 - b_1},$$
$$b_2 = [x_2], \quad x_3 = \frac{1}{x_2 - b_2}, \cdots, b_n = [x_n], \quad x_{n+1} = \frac{1}{x_n - b_n} \cdots$$

wobei die b_i ganze Zahlen sind.

Beispiel 1:

- Wir erweitern die Wurzel aus 2 zu einem Kettenbruch:

$$b_0 = [\sqrt{2}] = 1, \qquad x_1 = \frac{1}{\sqrt{2}-1} = \sqrt{2}+1$$

$$b_1 = [\sqrt{2}+1] = 2, \quad x_2 = \frac{1}{\sqrt{2}+1-2} = \sqrt{2}+1.$$

- Man sieht die Entwicklung setzt sich periodisch fort.

$$\sqrt{2} = 1 + \frac{1|}{|2} + \frac{1|}{|2} + \frac{1|}{|2} + \cdots,$$

Beispiel 2:

- Kettenbruch-erweiterung von e:

$$
\begin{aligned}
b_0 &= 2, & x_1 &= 1/0.71828182\ldots = 1.39221119\ldots \\
b_1 &= 1, & x_2 &= 1/0.39221119\ldots = 2.54964677\ldots \\
b_2 &= 2, & x_3 &= 1/0.54964677\ldots = 1.81935024\ldots \\
b_3 &= 1, & x_4 &= 1/0.81935024\ldots = 1.22047928\ldots \\
b_4 &= 1, & x_5 &= 1/0.22047928\ldots = 4.53557347\ldots \\
b_5 &= 4, & x_6 &= 1/0.535573\ldots = 1.867157\ldots \\
b_6 &= 1, & x_7 &= 1/0.867157\ldots = 1.153193\ldots \\
b_7 &= 1, & x_8 &= 1/0.153193\ldots = 6.527707\ldots \\
b_8 &= 6, & x_9 &= 1/0.5277\ldots = 1.8949\ldots \\
b_9 &= 1, & x_{10} &= 1/0.8949\ldots = 1.1173\ldots \\
b_{10} &= 1, & x_{11} &= 1/0.1173\ldots = 8.5226\ldots \\
b_{11} &= 8, & \ldots
\end{aligned}
$$

- Dies führt in unserer Darstellung zu

$$e = 2 + \frac{1|}{|1} + \frac{1|}{|2} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|4} + \frac{1|}{|1} + \frac{1|}{|1} + \frac{1|}{|6} + \cdots$$

Bemerkung:

- Ein endlicher Kettenbruch stellt eine rationale Zahl dar.

- Stellt man x als Kettenbruch dar, so stellt der vorzeitig abgebrochene Kettenbruch eine Approximation an x dar.

- <u>Insbesondere</u>: Man kann x (irrational) als endlichen Kettenbruch darstellen indem man das b_n durch x_n ersetzt. (Siehe Bsp. 1)

$$\sqrt{2} = 1 + \frac{1|}{|2} + \frac{1|}{|2} + \cdots + \frac{1|}{|2} + \frac{1|}{|\sqrt{2}+1},$$

Auswertung von Kettenbrüchen

- Ziel: $2+\frac{1|}{|1}+\frac{1|}{|2}+\frac{1|}{|1}+\frac{1|}{|2}+\frac{1|}{|2}+\frac{1|}{|3}$ auszuwerten.

  Achtung: Nicht einfach drauflos rechnen!

Satz: Seien b_i ganze Zahlen und alle $b_{i>0}$ >0. Dann lässt sich der reguläre Kettenbruch

$$\frac{A_n}{B_n} = b_0 + \frac{1|}{|b_1} + \frac{1|}{|b_2} + \cdots + \frac{1|}{|b_n}$$

mit vollständig gekürzten A_s/B_s durch folgende Rekursionsformel darstellen:

$$\begin{cases} A_s = b_s A_{s-1} + A_{s-2} \\ B_s = b_s B_{s-1} + B_{s-2}. \end{cases}$$

mit A_{-1}:=1, B_{-1}:=0, A_0:=b_0 und B_0:=1.

Beispiel 3:

- Berechne: $$2+\frac{1|}{|1}+\frac{1|}{|2}+\frac{1|}{|1}+\frac{1|}{|2}+\frac{1|}{|2}+\frac{1|}{|3}$$

Schritt	0	1	2	1	2	2	3	
A_n/B_n	1/0	2/1	3/1	8/3	11/4	30/11	71/26	243/89

- Ergebnis: $$\frac{243}{89}=2+\frac{1|}{|1}+\frac{1|}{|2}+\frac{1|}{|1}+\frac{1|}{|2}+\frac{1|}{|2}+\frac{1|}{|3}$$

- Ein kleiner Satz den wir für einen Beweis benötigen:

- **Satz**: Es gilt für die A_s und B_s :

$$\mathbf{A_{s-1}B_s - A_sB_{s-1} = (-1)^s}$$

Beweis per Induktion, hier nur der Induktionsschluss:

$$A_sB_{s+1} - A_{s+1}B_s \quad = A_s(b_{s+1}B_s+B_{s-1}) - (b_{s+1}A_s+A_{s-1})B_s$$

$$= -(A_{s-1}B_s - A_sB_{s-1})$$

$$= -(-1)^s = (-1)^{s+1}$$

Kettenbrucherweiterungen von Quadratwurzeln

- Die Quadratwurzeln lassen sich leicht mit der Formel berechnen: $x_0 = \sqrt{N}, \quad b_i = [x_i], \quad x_{i+1} = 1/(x_i - b_i),$
- D.h. die Wurzel aus N lässt sich damit so schreiben

$$\sqrt{N} = b_0 + \frac{1|}{|b_1} + \frac{1|}{|b_2} + \frac{1|}{|b_3} + \cdots + \frac{1|}{|b_n} + \cdots$$

Beispiel 4:

- N=69 => b_0=8

$$x_1 = \frac{1}{\sqrt{69}-8} = \frac{\sqrt{69}+8}{5} = 3 + \frac{\sqrt{69}-7}{5}$$

$$x_2 = \frac{5}{\sqrt{69}-7} = \frac{5(\sqrt{69}+7)}{20} = \frac{\sqrt{69}+7}{4} = 3 + \frac{\sqrt{69}-5}{4}$$

$$x_3 = \frac{4}{\sqrt{69}-5} = \frac{4(\sqrt{69}+5)}{44} = \frac{\sqrt{69}+5}{11} = 1 + \frac{\sqrt{69}-6}{11}$$

$$x_4 = \frac{11}{\sqrt{69}-6} = \frac{11(\sqrt{69}+6)}{33} = \frac{\sqrt{69}+6}{3} = 4 + \frac{\sqrt{69}-6}{3}$$
$$x_5 = \frac{3}{\sqrt{69}-6} = \frac{3(\sqrt{69}+6)}{33} = \frac{\sqrt{69}+6}{11} = 1 + \frac{\sqrt{69}-5}{11}$$
$$x_6 = \frac{11}{\sqrt{69}-5} = \frac{11(\sqrt{69}+5)}{44} = \frac{\sqrt{69}+5}{4} = 3 + \frac{\sqrt{69}-7}{4}$$
$$x_7 = \frac{4}{\sqrt{69}-7} = \frac{4(\sqrt{69}+7)}{20} = \frac{\sqrt{69}+7}{5} = 3 + \frac{\sqrt{69}-8}{5}$$
$$x_8 = \frac{5}{\sqrt{69}-8} = \frac{5(\sqrt{69}+8)}{5} = \sqrt{69}+8 = 16 + (\sqrt{69}-8)$$
$$x_9 = \frac{1}{\sqrt{69}-8} = 3 + \frac{\sqrt{69}-7}{5}.$$

- Das Ergebnis ist ein periodischer Kettenbruch:

$$\sqrt{69} = 8 + \overline{\frac{1|}{|3} + \frac{1|}{|3} + \frac{1|}{|1} + \frac{1|}{|4} + \frac{1|}{|1} + \frac{1|}{|3} + \frac{1|}{|3} + \frac{1|}{|16}} + \frac{1|}{|3} + \frac{1|}{|3} + \cdots,$$

Bemerkung:

- Jede Kettenbrucherweiterung einer irrationalen Zahl, die Quadratwurzel ist, ist periodisch.

Kettenbrüche und Quadratische Reste

- Folgende Formel ist Basis der Methode zur Bestimmung quadratischer Reste (mod N):

$$(+) \qquad (A_{n-1})^2 - N(B_{n-1})^2 = (-1)^n Q_n$$

- Aus (+) erhält man den Ausdruck

$$A_{n-1}^2 \equiv (-1)^n Q_n \pmod N$$

- D.h. $(-1)^n Q_n$ ist ein quadratischer Rest (mod N)

- Wir haben bereits rausgefunden: $Q_n < 2\sqrt{N}$. Kettenbrucherweiterung von $\sqrt{N}$ liefert daher <u>schnell</u> kleine quadratische Reste.

- Nachteil:
  Die Kettenbrucherweiterung ist periodisch
  => die Q_i werden sich periodisch wiederholen
  Ist die Periode klein, so auch die Anzahl der quadratischen Reste.

- Verbesserung:
  Die Periode kann durch die KB-Erweiterung von $\sqrt{kN},$ verbessert werden, dadurch wird die Periode verlängert. (siehe Continued Fraction Method)

Continued Fraction Method

Dieser Algorithmus benutzt die Idee: $x^2 = y^2 \mod N$

1) Man wählt endlich viele kleine Primzahlen $p_1 \dots p_{n-1}$ und $p_0 = -1$

2) Wir suchen ganze Zahlen P_i und C_i mit $P_i^2 \equiv C_i \ mod \ N$
s.d. die Primfaktorzerlegung von C_i nur mit $p_0, \dots, p_{n-1}$ auskommt d.h. $C_i = (-1)^{\alpha_0} * p_1^{\alpha_1} * \cdots * p_{n-1}^{\alpha_{n-1}}$

3) Nun definiere $v_i = (\alpha_0 \ mod \ 2, \alpha_1 \ mod \ 2, \dots, \alpha_{n-1} \ mod \ 2) \in \mathbb{F}_2^n$
also als $v_i = \left(v_{i,0}, v_{i,1}, \dots, v_{i,n-1}\right)$, sodass gilt:

$$C_i = (-1)^{v_{i,0}} * p_1^{v_{i,1}} * \cdots * p_{n-1}^{v_{i,n-1}}$$

4) Findet man jetzt Indizes $i_1, \ldots, i_l,\ s.d.\ in\ \mathbb{F}_2^n$
$v_{i_1} + v_{i_2} + \cdots + v_{i_l} = 0$ gilt, so ist $C_{i_1} C_{i_2} \ldots C_{i_l}$ eine quadratische Zahl und man erhält:

$$(P_{i_1} \ldots P_{i_l})^2 \equiv (\sqrt{C_{i_1} \ldots C_{i_l}})^2\ mod\ N,$$

5) Nun nur noch probieren ob
$ggT(P_{i_1} \ldots P_{i_l} + \sqrt{C_{i_1} \ldots C_{i_l}}, N)\ oder\ ggT(P_{i_1} \ldots P_{i_l} - \sqrt{C_{i_1} \ldots C_{i_l}}, N)$
ein Teiler von N ist.

Bemerkung: Die in 2) gesuchten P_i und C_i bekommen wir durch die quadratischen Reste aus der vorherigen Teil.

Beispiel 5:

- Sei n= 13290059

  Wir finden folgende quadratische Reste R_i (ohne Rechnung):

i	$a_i \bmod n$	R_i factored
5	171341	$-1 \cdot 2 \cdot 5^2 \cdot 41$
10	6700527	$31 \cdot 43$
22	5235158	$41 \cdot 113$
23	1914221	$-1 \cdot 2 \cdot 113$
26	11455708	$2 \cdot 31 \cdot 53$
31	1895246	$-1 \cdot 2 \cdot 5^2 \cdot 113$
40	3213960	$2 \cdot 43 \cdot 53$

mit $(a_i)^2 = R_i \bmod n$

(die R_i sind die C_i aus der alten Folie)

Und damit die folgende Matrix

$$\begin{array}{cc} & \begin{matrix} \boldsymbol{v}(5) & \boldsymbol{v}(10) & \boldsymbol{v}(22) & \boldsymbol{v}(23) & \boldsymbol{v}(26) & \boldsymbol{v}(31) & \boldsymbol{v}(40) \end{matrix} \\ \begin{matrix} -1 \\ 2 \\ 5 \\ 31 \\ 41 \\ 43 \\ 53 \\ 113 \end{matrix} & \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{pmatrix} \end{array} =: A$$

Gauss -> $(0,1,0,0,1,0,1)^{tr}$, $(1,0,1,0,0,1,0)^{tr}$ und $(1,0,1,1,0,0,0)^{tr}$ liegen im Kern(A)

Nun probieren:

- $$(6700527 \cdot 11455708 \cdot 3213960)^2 \equiv (2 \cdot 31 \cdot 43 \cdot 53)^2 \bmod n$$

  ergibt: $141298^2 \equiv 141298^2 \bmod n$,also keinen Teiler.

- $$(171341 \cdot 5235158 \cdot 1895246)^2 \equiv (2 \cdot 5^2 \cdot 41 \cdot 113)^2 \bmod n$$

  ergibt: $13058409^2 \equiv 231650^2 \bmod n$

  jedoch: ggT(13058409-231650,n)=1, ergibt ebenfalls keinen Teiler.

- $$(171341 \cdot 5235158 \cdot 1914221)^2 \equiv (2 \cdot 5 \cdot 41 \cdot 113)^2 \bmod n$$

  ergibt: $1469504^2 \equiv 46330^2 \bmod n$

  und damit ist ggT(1469504-46330,n)=4261 ein Teiler von n.

Gliederung:

Das Quadratische Sieb:

- 1981 von Carl Pomerance entwickelt.
- Der Algorithmus beruht auf Fermats Faktorisierunsmethode, Gauß` und Kraitchiks Ideen, u.v.A.
- Mit Ausnahme des Siebschrittes gleicht er Dixons Algorithmus.
- Schneller als CFM, da für die Glattheitstests Trail Division durch Sieben ersetzt werden kann.
- Effizient bis zu Zahlen von ca. 100 Dezimalstellen, für größere ist das Zahlkörpersieb schneller.
- Geschwindigkeit: ca. $\sqrt{\ln(N)\ln(\ln(N))}$ Rechenschritte.

Für die Zahl RSA-129 benötigte man 1994 acht Monate

RSA-129 = 114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541 = 3490529510847650949147849619903898133417764638493387843990820577 * 32769132993266709549961988190834461413177642967992942539798288533

Definitionen:

- Legendre-Symbol: $N \in \mathbb{N}$, p Primzahl

$$\left(\frac{N}{p}\right) := \begin{cases} 1 & \text{ggT}(N, p) = 1 \text{ und N ist ein Quadrat mod. p} \\ 0 & \text{p teilt N} \\ -1 & \text{ggT}(N, p) = 1 \text{ und N ist kein Quadrat mod. p} \end{cases}$$

$$z = q * d,\ \text{q B-glatt und } B < d \leq B^2$$

- $z \in \mathbb{N}$ heißt *B-glatt,* falls sie komplett in Primzahlen kleiner-gleich B zerfällt.

  z heißt *B-semiglatt,* falls sie noch einen zusätzlichen Primfaktor kleiner-gleich B² besitzt,

  d.h. $z = q * d,\ \text{q B-glatt und } B < d \leq B^2$

Algorithmus:

1 Liste erstellen: $L := [f_1, \dots, f_S]$ mit $f_i := f(x_i) := x_i^2 - N,\ x_i := \lfloor \sqrt{(N)} \rfloor + i$

2 Wahl der Faktorbasis

3 Ermitteln der B-glatten Werte durch Sieben

4 Faktorisieren der B-glatten Zahlen und Bestimmung eines Quadrats

5 Auswertung

Verbesserungen:

- Sieben über dem Intervall $[S - \lfloor\sqrt{(N)}\rfloor, S + \lfloor\sqrt{(N)}\rfloor]$,

  man fügt eine weitere „Primzahl“ -1 zur Faktorbasis F(B) hinzu.

- Sieben auch nach B-semiglatten Zahlen der Form $f_i = q_i d_i$ mit q_i B-glatt, $B < d_i \leq B^2$

- Multypolynomial Quadratic Sieve (MPQS):

$$U(x) := a^2 x + b\ ,\ W(x) := a^2 x^2 + 2\mathrm{bx} + c \ \Rightarrow\ (U(x))^2 \equiv a^2 W(x) \bmod N\ \forall x \in \mathbb{Z},$$

$$a^2 \approx \sqrt{(2\mathrm{N})}/S,\ \ b^2 - N = a^2 c,\ \ |(b)| < a^2/2,\ a, b, c \in \mathbb{Z}$$

Sieben mit $W(x)$, wobei $U(x_i)$ vorgegeben. Gesucht ist $\prod W(x_i) = y^2$, dann wähle $x := \prod U(x_i)$

„Self Initialisation“: a fest gewählt, b und c werden variiert.

Gliederung: