CARL VON OSSIETZKY universität OLDENBURG

Shanks' Verfahren zur Faktorisierung: „Square Forms Factorization“

Bachelorarbeit

Björn Wolff

Universität Oldenburg

3. Juni 2011

Übersicht

CARL VON OSSIETZKY universität OLDENBURG

Einleitung

- „Square Forms Factorization“ (SQUFOF)
- 1975 von Daniel Shanks entwickelt
- Jedoch nie offiziell veröffentlicht
- Basiert auf Faktorisierung mit Hilfe der Legendre-Kongruenz
- Nutzt die Kettenbruchentwicklung von $\sqrt{N}$
- Theorie der binären quadratischen Formen

CARL VON OSSIETZKY universität OLDENBURG

Zahlentheoretische Grundlagen

CARL VON OSSIETZKY universität OLDENBURG

Zahlentheoretische Grundlagen
Inhalt

- Legendre-Kongruenz
- Kettenbrüche

Legendre-Kongruenz

- $x^2 \equiv y^2 \pmod{N}$, für $N \in \mathbb{N}$
- Triviale Lösung: $x \equiv \pm y \pmod{N}$
- Ist N zusammengesetzt,
  - dann existieren weitere nicht-triviale Lösungen
  - diese können zur Faktorisierung benutzt werden

CARL VON OSSIETZKY universität OLDENBURG

Legendre-Kongruenz

- Basiert auf: $x^2 \equiv y^2 \pmod{N} \Rightarrow N \mid (x^2 - y^2)$
- Mit binomischer Formel: $N \mid (x+y)(x-y)$
- Da $N = pq$:
  - $pq \mid (x+y)(x-y)$
  - Daher muss $p \mid (x+y)$ und $q \mid (x-y)$ oder $p \mid (x-y)$ und $q \mid (x+y)$
  - Dann gilt $p = ggT((x+y), N)$ und $q = ggT((x-y), N)$
- Viele Faktorisierungsverfahren nutzen diese Tatsache
- Suche nach Lösungen für die Kongruenz unterscheidet sich

CARL VON OSSIETZKY universität OLDENBURG

Kettenbrüche

Definition: Kettenbruch

Ein Bruch heißt Kettenbruch, wenn er folgende Form besitzt:

$$x = b_0 + \cfrac{1}{b_1 + \cfrac{1}{b_2 + \cfrac{1}{b_3 + \dots}}} = [b_0; b_1, b_2, b_3, \dots]$$

mit $x \in \mathbb{R}$, $b_i \in \mathbb{Z}$, für alle $i \in \mathbb{N}_0$.

- Rekursiv:

$$x_0 = x; b_0 = \lfloor x_0 \rfloor$$

$$\forall i \geq 1 : x_i = \frac{1}{x_{i-1} - b_{i-1}}; b_i = \lfloor x_i \rfloor$$

Kettenbrüche

Definition: Kettenbruchentwicklung der Quadratwurzel

Für eine nicht quadratische Zahl $N \in \mathbb{Z}$ ist die reguläre Kettenbruchentwicklung von $\sqrt{N}$ rekursiv definiert als

$$x_0 = \sqrt{N},\ b_i = \lfloor x_i \rfloor,\ x_{i+1} = \frac{1}{(x_i - b_i)},$$

wobei $b_i \in \mathbb{Z}$ und $x_i \in \mathbb{R}$, für alle $i \in \mathbb{N}_0$, gilt. In Perron-Darstellung ist also $\sqrt{N} = [b_0; b_1, b_2, \ldots]$, wobei $b_i > 0$ für $i \in \mathbb{N}_0$.

- Durch $\sqrt{N}$ erzeugte Kettenbrüche sind unendlich
- Beispiele: $\sqrt{2} = [1; \overline{2}]$, $\sqrt{52} = [7; \overline{4, 1, 2, 1, 4, 14}]$

Kettenbruch: Beispiel

Für $N = 52$ ergibt sich $x_0 = \sqrt{52}$ und $b_0 = \lfloor \sqrt{52} \rfloor = 7$. Weitere Berechnungen liefern:

$$x_1 = \frac{1}{\sqrt{52} - 7} = \frac{1(\sqrt{52} + 7)}{3} = \frac{\sqrt{52} + 7}{3} = 4 + \frac{\sqrt{52} - 5}{3}$$

$$x_2 = \frac{3}{\sqrt{52} - 5} = \frac{3(\sqrt{52} + 5)}{27} = \frac{\sqrt{52} + 5}{9} = 1 + \frac{\sqrt{52} - 4}{9}$$

$$x_3 = \frac{9}{\sqrt{52} - 4} = \frac{9(\sqrt{52} + 4)}{36} = \frac{\sqrt{52} + 4}{4} = 2 + \frac{\sqrt{52} - 4}{4}$$

$$x_4 = \frac{4}{\sqrt{52} - 4} = \frac{4(\sqrt{52} + 4)}{36} = \frac{\sqrt{52} + 4}{9} = 1 + \frac{\sqrt{52} - 5}{9}$$

$$x_5 = \frac{9}{\sqrt{52}-5} = \frac{9(\sqrt{52}+5)}{27} = \frac{\sqrt{52}+5}{3} = 4 + \frac{\sqrt{52}-7}{3}$$

$$x_6 = \frac{3}{\sqrt{52}-7} = \frac{3(\sqrt{52}+7)}{3} = \sqrt{52}+7 = 14 + \sqrt{52} - 7$$

$$x_7 = \frac{1}{\sqrt{52}-7} = \frac{1(\sqrt{52}+7)}{3} = \frac{\sqrt{52}+7}{3} = 4 + \frac{\sqrt{52}-5}{3} = x_1$$

CARL VON OSSIETZKY universität OLDENBURG

$$x_5 = \frac{9}{\sqrt{52}-5} = \frac{9(\sqrt{52}+5)}{27} = \frac{\sqrt{52}+5}{3} = 4 + \frac{\sqrt{52}-7}{3}$$

$$x_6 = \frac{3}{\sqrt{52}-7} = \frac{3(\sqrt{52}+7)}{3} = \sqrt{52}+7 = 14 + \sqrt{52} - 7$$

$$x_7 = \frac{1}{\sqrt{52}-7} = \frac{1(\sqrt{52}+7)}{3} = \frac{\sqrt{52}+7}{3} = 4 + \frac{\sqrt{52}-5}{3} = x_1$$

- $\sqrt{52} = [7; \overline{4, 1, 2, 1, 4, 14}]$

CARL VON OSSIETZKY universität OLDENBURG

$$x_5 = \frac{9}{\sqrt{52}-5} = \frac{9(\sqrt{52}+5)}{27} = \frac{\sqrt{52}+5}{3} = 4 + \frac{\sqrt{52}-7}{3}$$

$$x_6 = \frac{3}{\sqrt{52}-7} = \frac{3(\sqrt{52}+7)}{3} = \sqrt{52}+7 = 14 + \sqrt{52} - 7$$

$$x_7 = \frac{1}{\sqrt{52}-7} = \frac{1(\sqrt{52}+7)}{3} = \frac{\sqrt{52}+7}{3} = 4 + \frac{\sqrt{52}-5}{3} = x_1$$

- $\sqrt{52} = [7; \overline{4, 1, 2, 1, 4, 14}]$
- Symmetrie

Kettenbrüche

Satz: Rekursive Formeln zur Berechnung

Sei $N \in \mathbb{Z}$. Mit den Startwerten $b_0 = P_1 = \lfloor \sqrt{N} \rfloor$ und $Q_0 = 1$ lassen sich die Teilbrüche x_i der Kettenbruchentwicklung von $\sqrt{N}$, für jedes $i \in \mathbb{N}$, mit den ineinander verschachtelten rekursiven Formeln

$$Q_i = \frac{N - P_i^2}{Q_{i-1}},$$

$$x_i = \frac{\sqrt{N} + P_i}{Q_i},$$

$$P_{i+1} = b_i Q_i - P_i,$$

bestimmen. Es ist damit möglich, die b_i in jedem Iterationsschritt mit $b_i = \lfloor x_i \rfloor = \left\lfloor \frac{\sqrt{N}+P_i}{Q_i} \right\rfloor$ zu berechnen.

Kettenbrüche

Satz: Periodische Kettenbrüche

Für jede nicht quadratische ganze Zahl N ist die reguläre Kettenbruchentwicklung von $\sqrt{N}$ periodisch.

- Beweis durch Abschätzung der möglichen Werte für Q_i und P_i:
  - $P_i < \sqrt{N}$, da $b_i = \lfloor \sqrt{N} \rfloor$
  - $Q_i = \frac{P_i + P_{i+1}}{b_i} < 2\sqrt{N}$
  - Anzahl möglicher Brüche ist somit beschränkt auf: $\lfloor \sqrt{N} \rfloor \cdot 2\lfloor \sqrt{N} \rfloor < 2N$
  - Periode kann maximal eine Länge von $2N - 1$ haben

Näherungsbrüche

Definition: Näherungsbruch

Sei $\sqrt{N} = [b_0; b_1, b_2, \dots]$ eine Kettenbruchentwicklung in Perron-Darstellung. Wird der Kettenbruch an einer bestimmten Stelle $n \in \mathbb{N}_0$, je nach benötigter Genauigkeit der Approximation, abgeschnitten, so heißt der dadurch berechnete Bruch

$$\frac{A_n}{B_n} = b_0 + \cfrac{1}{b_1 + \cfrac{1}{\dots + \cfrac{1}{b_n}}} = [b_0; b_1, \dots, b_n]$$

n-ter Näherungsbruch von $\sqrt{N}$. Hierbei gilt A_n, $B_n \in \mathbb{N}$ und N ist eine nicht quadratische ganze Zahl.

CARL VON OSSIETZKY universität OLDENBURG

Näherungsbruch: Beispiel

Gegeben sei die Entwicklung $\sqrt{52} = [7; \overline{4, 1, 2, 1, 4, 14}]$ aus vorigem Beispiel. Soll der 6-te Näherungsbruch bestimmt werden, so kann dies wie folgt gemacht werden:

i	-1	0	1	2	3	4	5	6
b_i		7	4	1	2	1	4	14
A_i	1	7	29	36	101	137	649	9223
B_i	0	1	4	5	14	19	90	1279

$$A_{-1} = 1;\ A_0 = b_0;\ A_n = b_n A_{n-1} + A_{n-2}$$
$$B_{-1} = 0;\ B_0 = 1;\ B_n = b_n B_{n-1} + B_{n-2}$$

CARL VON OSSIETZKY universität OLDENBURG

Näherungsbruch: Beispiel

Gegeben sei die Entwicklung $\sqrt{52} = [7; \overline{4, 1, 2, 1, 4, 14}]$ aus vorigem Beispiel. Soll der 6-te Näherungsbruch bestimmt werden, so kann dies wie folgt gemacht werden:

i	-1	0	1	2	3	4	5	6
b_i		7	4	1	2	1	4	14
A_i	1	7	29	36	101	137	649	9223
B_i	0	1	4	5	14	19	90	1279

$$A_{-1} = 1;\ A_0 = b_0;\ A_n = b_n A_{n-1} + A_{n-2}$$
$$B_{-1} = 0;\ B_0 = 1;\ B_n = b_n B_{n-1} + B_{n-2}$$

- Somit ist $\sqrt{52} \approx \frac{9223}{1279} = \frac{A_6}{B_6}$

CARL VON OSSIETZKY universität OLDENBURG

Das Verfahren

CARL VON OSSIETZKY universität OLDENBURG

Das Verfahren
Inhalt

- Algorithmus
- Beispiel

CARL VON OSSIETZKY universität OLDENBURG

Algorithmus

- Ausgelegt auf Faktorisierung von zusammengesetzten Zahlen mit zwei „großen“ Primfaktoren
- Hauptbereich: 36- bis 64-Bit-Zahlen
- Kettenbruchvariante des Verfahrens von Hans Riesel

CARL VON OSSIETZKY universität OLDENBURG

Algorithmus
Ablauf

- Berechnung der Kettenbruchentwicklung mit

$$b_i = \left\lfloor \frac{\sqrt{N} + P_i}{Q_i} \right\rfloor,$$
$$P_{i+1} = b_i Q_i - P_i,$$
$$Q_1 = N - P_1^2,$$
$$Q_{i+1} = Q_{i-1} + (P_i - P_{i+1}) b_i$$

- Suche nach einer Quadratzahl R^2 in der Kettenbruchentwicklung von $\sqrt{N}$
- $A_{n-1}^2 \equiv Q_n = R^2 \pmod{N}$
- Suche nach einem Symmetriepunkt in der Kettenbruchentwicklung von $\sqrt{N}$

CARL VON OSSIETZKY universität OLDENBURG

Beispiel
Suche nach Quadratzahl

Für $N = 78731$ ergibt sich $x_0 = \sqrt{78731}$, $b_0 = \lfloor \sqrt{78731} \rfloor = 280$ und weiter:

$$x_1 = \frac{1}{\sqrt{78731} - 280} = \frac{\sqrt{78731} + 280}{331} = 1 + \frac{\sqrt{78731} - 51}{331}$$

$$x_2 = \frac{331}{\sqrt{78731} - 51} = \frac{\sqrt{78731} + 51}{230} = 1 + \frac{\sqrt{78731} - 179}{230}$$

$$\ldots$$

$$x_8 = \frac{338}{\sqrt{78731} - 147} = \frac{\sqrt{78731} + 147}{169}$$

CARL VON OSSIETZKY universität OLDENBURG

Beispiel
Suche nach Quadratzahl

Für $N = 78731$ ergibt sich $x_0 = \sqrt{78731}$, $b_0 = \lfloor \sqrt{78731} \rfloor = 280$ und weiter:

$$x_1 = \frac{1}{\sqrt{78731} - 280} = \frac{\sqrt{78731} + 280}{331} = 1 + \frac{\sqrt{78731} - 51}{331}$$

$$x_2 = \frac{331}{\sqrt{78731} - 51} = \frac{\sqrt{78731} + 51}{230} = 1 + \frac{\sqrt{78731} - 179}{230}$$

$$\ldots$$

$$x_8 = \frac{338}{\sqrt{78731} - 147} = \frac{\sqrt{78731} + 147}{169}$$

- Quadratzahl: $Q_8 = 169 = 13^2$

CARL VON OSSIETZKY universität OLDENBURG

Beispiel

Suche nach Quadratzahl

Für $N = 78731$ ergibt sich $x_0 = \sqrt{78731}$, $b_0 = \lfloor \sqrt{78731} \rfloor = 280$ und weiter:

$$x_1 = \frac{1}{\sqrt{78731} - 280} = \frac{\sqrt{78731} + 280}{331} = 1 + \frac{\sqrt{78731} - 51}{331}$$

$$x_2 = \frac{331}{\sqrt{78731} - 51} = \frac{\sqrt{78731} + 51}{230} = 1 + \frac{\sqrt{78731} - 179}{230}$$

$$\ldots$$

$$x_8 = \frac{338}{\sqrt{78731} - 147} = \frac{\sqrt{78731} + 147}{169}$$

- Quadratzahl: $Q_8 = 169 = 13^2$
- Wichtig: Index i muss gerade sein

CARL VON OSSIETZKY universität OLDENBURG

Beispiel
Berechnung der Faktoren

- Kettenbruchentwicklung bis zur Quadratzahl: $\sqrt{78731} = [280; 1, 1, 2, 3, 1, 3, 1]$

i	-1	0	1	2	3	4	5	6	7
b_i		280	1	1	2	3	1	3	1
A_i	1	280	281	561	1403	4770	6173	23289	29462

CARL VON OSSIETZKY universität OLDENBURG

Beispiel
Berechnung der Faktoren

- Kettenbruchentwicklung bis zur Quadratzahl: $\sqrt{78731} = [280; 1, 1, 2, 3, 1, 3, 1]$

i	-1	0	1	2	3	4	5	6	7
b_i		280	1	1	2	3	1	3	1
A_i	1	280	281	561	1403	4770	6173	23289	29462

- $A_7^2 = 29462^2 \equiv 169 = 13^2 = Q_8 \pmod{78731}$

CARL VON OSSIETZKY universität OLDENBURG

Beispiel
Berechnung der Faktoren

- Kettenbruchentwicklung bis zur Quadratzahl: $\sqrt{78731} = [280; 1, 1, 2, 3, 1, 3, 1]$

i	-1	0	1	2	3	4	5	6	7
b_i		280	1	1	2	3	1	3	1
A_i	1	280	281	561	1403	4770	6173	23289	29462

- $A_7^2 = 29462^2 \equiv 169 = 13^2 = Q_8 \pmod{78731}$
- $ggT((29462 + 13), 78731) = 131$ und $ggT((29462 - 13), 78731) = 601$

CARL VON OSSIETZKY universität OLDENBURG

Beispiel
Suche nach Symmetriepunkt

- Shanks' Überlegungen zur Bestimmung der Faktoren
- Modifikation des letzten Terms der Kettenbruchentwicklung
- $\frac{\sqrt{78731}+147}{169}$ wird zu $\frac{\sqrt{78731}-147}{13}$
- $\frac{\sqrt{78731}-147}{13} = 10 + \frac{\sqrt{78731}-277}{13}$

CARL VON OSSIETZKY universität OLDENBURG

Beispiel

Suche nach Symmetriepunkt

$$y_1 = \frac{13}{\sqrt{78731} - 277} = \frac{\sqrt{78731} + 277}{154} = 3 + \frac{\sqrt{78731} - 185}{154}$$

$$y_2 = \frac{154}{\sqrt{78731} - 185} = \frac{\sqrt{78731} + 185}{289} = 1 + \frac{\sqrt{78731} - 104}{289}$$

$$y_3 = \frac{289}{\sqrt{78731} - 104} = \frac{\sqrt{78731} + 104}{235} = 1 + \frac{\sqrt{78731} - 131}{235}$$

$$y_4 = \frac{235}{\sqrt{78731} - 131} = \frac{\sqrt{78731} + 131}{262} = 1 + \frac{\sqrt{78731} - 131}{262}$$

CARL VON OSSIETZKY universität OLDENBURG

Beispiel
Suche nach Symmetriepunkt

- $P_3 = 131 = P_4$

CARL VON OSSIETZKY universität OLDENBURG

Beispiel
Suche nach Symmetriepunkt

- $P_3 = 131 = P_4$
- Da Q_4 gerade: $\frac{Q_4}{2} = \frac{262}{2} = 131$

CARL VON OSSIETZKY universität OLDENBURG

Beispiel
Suche nach Symmetriepunkt

- $P_3 = 131 = P_4$
- Da Q_4 gerade: $\frac{Q_4}{2} = \frac{262}{2} = 131$
- $78731 = 131 \cdot 601$

CARL VON OSSIETZKY universität OLDENBURG

Implementierung

CARL VON OSSIETZKY universität OLDENBURG

Implementierung
Inhalt

- Methode zur Faktorisierung
- Tests zur Laufzeit

CARL VON OSSIETZKY universität OLDENBURG

Methode zur Faktorisierung

- 1. Schleife: Suche nach Quadratzahl

```
public static BigInteger factorize(BigInteger n) {
...
    for (int i = 1; i <= maxCycles; i++) {
        b = sqrtN.add(p0).divide(q1);
        p1 = b.multiply(q1).subtract(p0);
        q2 = q0.add(p0.subtract(p1).multiply(b));
        listCandidate = q1;

        q0 = q1;
        q1 = q2;
        p0 = p1;

        if ((listCandidate.compareTo(sqrt2sqrtN) == -1)
                && (listCandidate.compareTo(ONE) == 1)) {
            list.add(listCandidate);}

        if ((i % 2) == 1) {
                sqrtQ1 = sqrt(q1);

                if ((sqrtQ1.pow(2).equals(q1))) {

                    if ((!list.contains(sqrtQ1))
                            && (sqrtQ1.compareTo(ONE) ==1)) {
                        break; }}}
        ...
    }
```

CARL VON OSSIETZKY universität OLDENBURG

Methode zur Faktorisierung

- 2. Schleife: Suche nach Symmetriepunkt

```
        q0 = sqrtQ1;
        b = sqrtN.subtract(p0).divide(q0);
        p0 = b.multiply(q0).add(p0);
        q1 = n.subtract(p0.pow(2)).divide(q0);

        for (int i = 1; i <= secCycles; i++) {
            b = sqrtN.add(p0).divide(q1);
            p1 = b.multiply(q1).subtract(p0);
            q2 = q0.add(p0.subtract(p1).multiply(b));

            q0 = q1;
            tmp = p0;
            p0 = p1;
            q1 = q2;

            if (tmp.equals(p1)) {
                if (!q0.testBit(0)) {
                    q0 = q0.divide(TWO);
                }

                return q0;
            }
    ...
    }
```

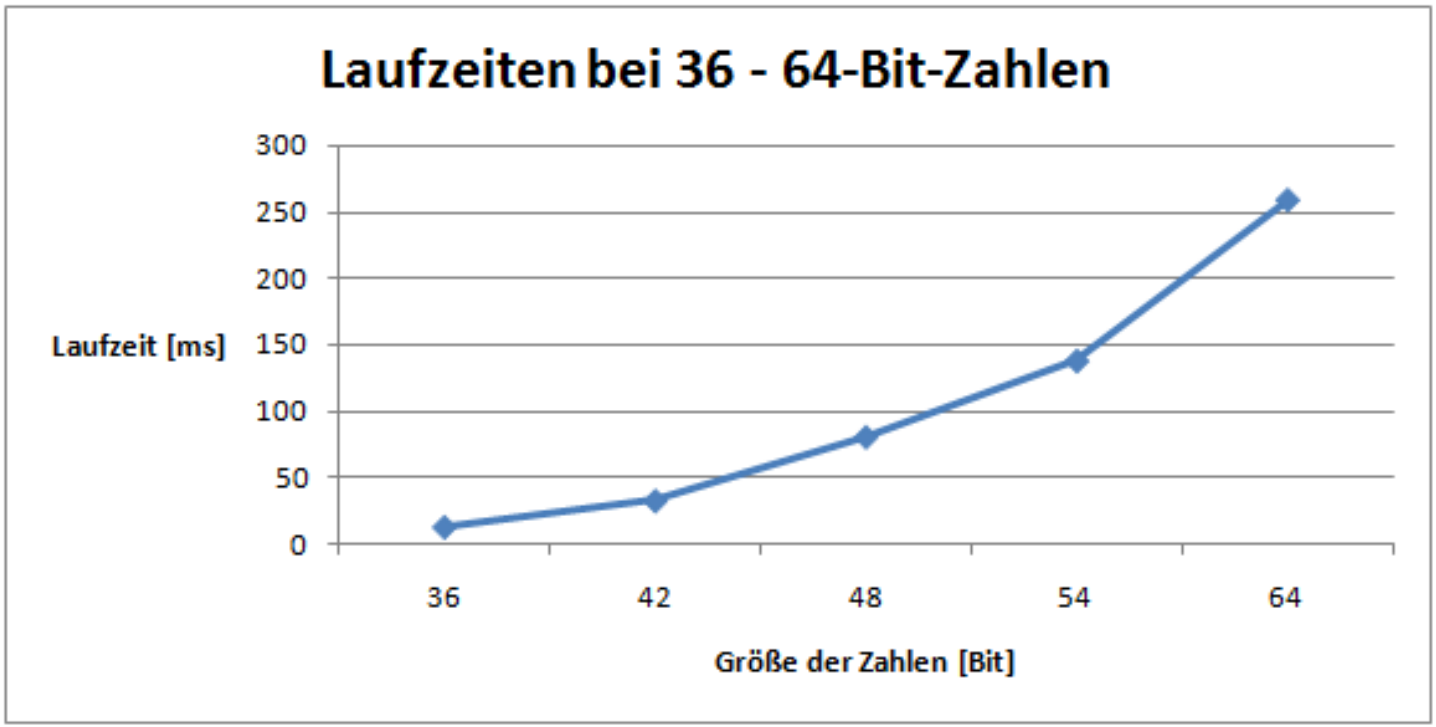
CARL VON OSSIETZKY universität OLDENBURG

Tests zur Laufzeit

- 36- bis 64-Bit-Zahlen
- 64- bis 100-Bit-Zahlen
- Besondere Zahlen

CARL VON OSSIETZKY universität OLDENBURG

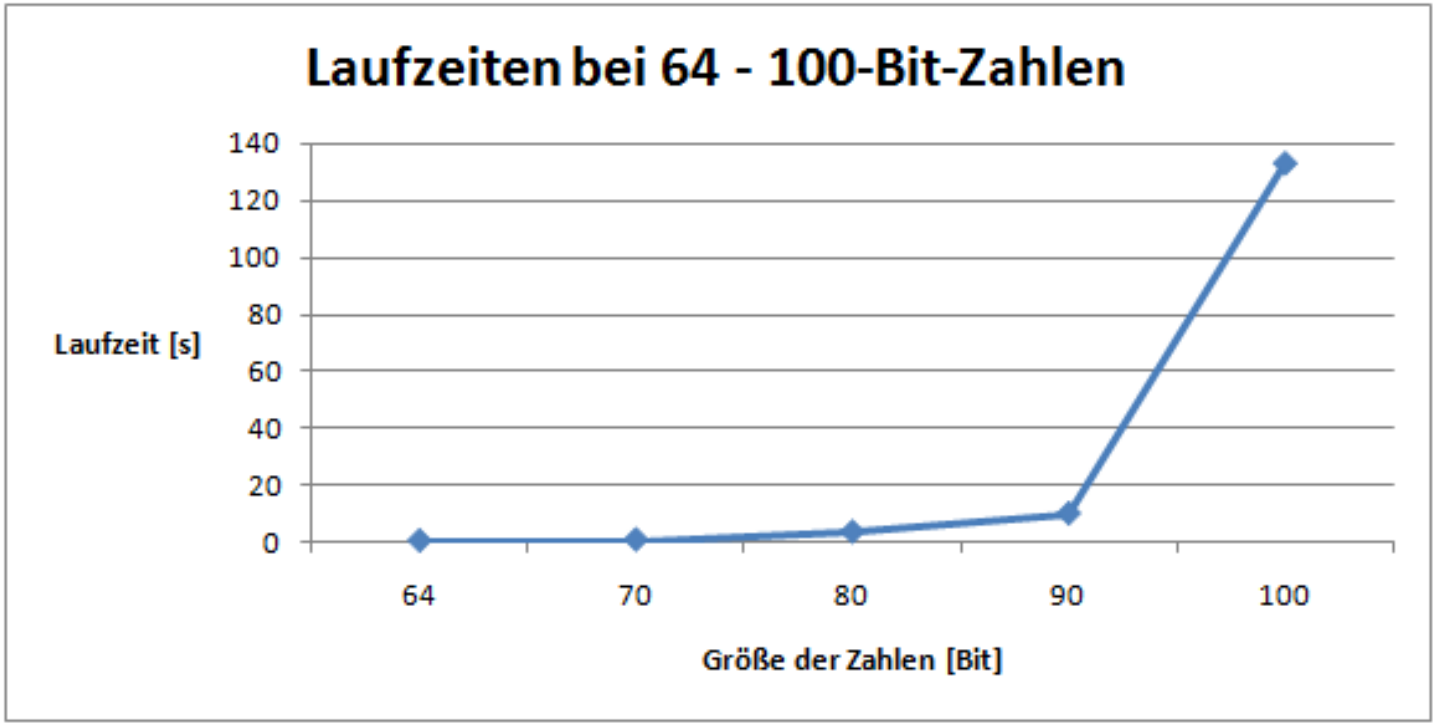
36- bis 64-Bit-Zahlen



Größe der Zahlen [Bit]	36	42	48	54	64
Berechnungszeit(∅) [ms]	13	32	80	137	258

CARL VON OSSIETZKY universität OLDENBURG

64- bis 100-Bit-Zahlen



Größe der Zahlen [Bit]	64	70	80	90	100
Berechnungszeit(∅) [ms]	258	615	3353	9818	132528

Besondere Zahlen

- Zusammengesetzte Zahlen mit bestimmter Struktur werden schneller faktorisiert als andere
- Durch empirische Versuche bestimmt: $N = (a^2 m + c)(b^2 m + d)$
- Mit a, b, c, d werden zwei etwa gleichgroße Primzahlen beschrieben, die nah an m liegen
- Der Spezialfall $N = p(p + 2a)$, mit $p, a \in \mathbb{N}$ und $0 < a < \sqrt{p}$ wird im Folgenden getestet

CARL VON OSSIETZKY universität OLDENBURG

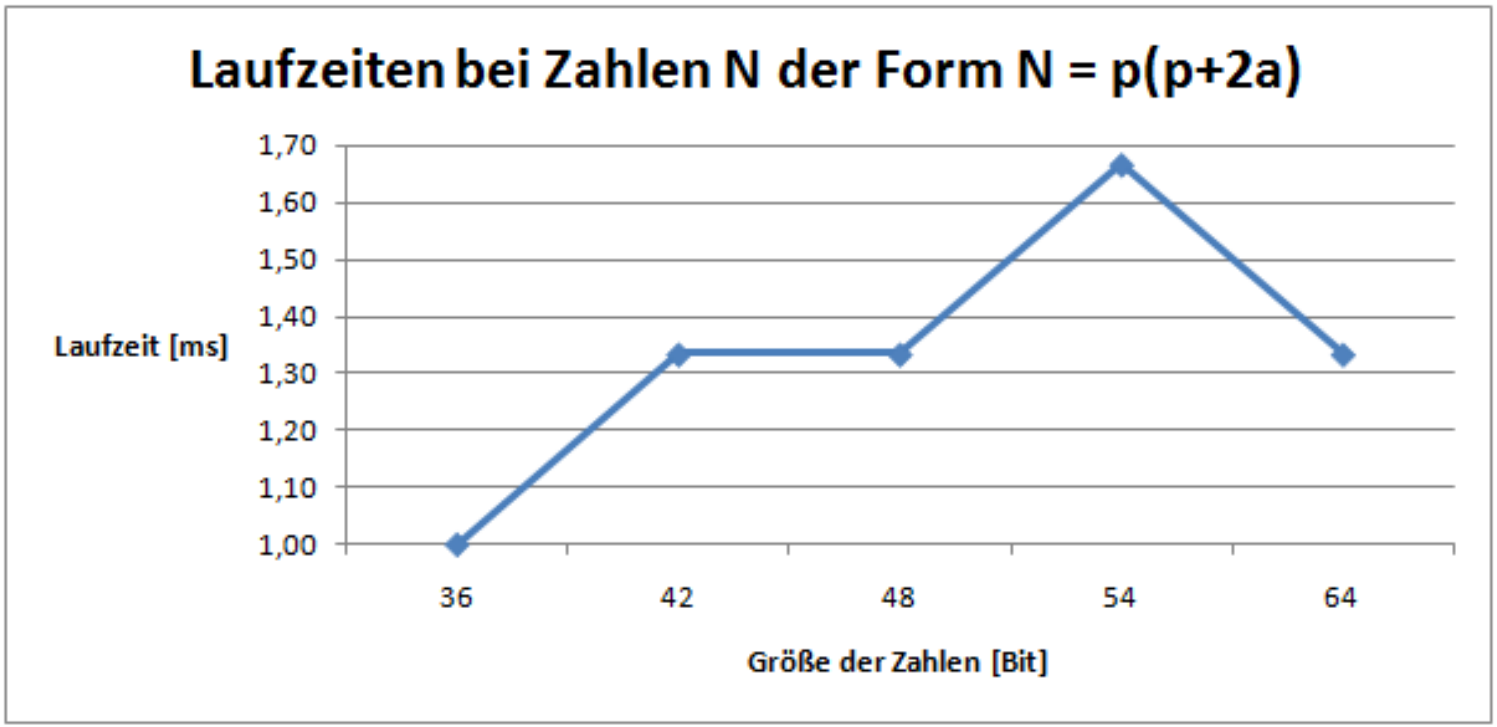
Besondere Zahlen

Bit	Zusammengesetzte Zahl N	p	$p+2a$	$\varnothing$ [ms]
36	17490462623	131893	132611	1,00
42	3209359435561	1790149	1792789	1,33
48	98189063930959	9905911	9912169	1,33
54	35506157532969293	188417071	188444483	1,67
64	7889941993004993536	2808851063	2808957049	1,33

- $N = p(p+2a)$, wobei $p, a \in \mathbb{N}$ und $0 < a < \sqrt{p}$

CARL VON OSSIETZKY universität OLDENBURG

Besondere Zahlen



- $N = p(p + 2a)$, wobei $p, a \in \mathbb{N}$ und $0 < a < \sqrt{p}$

CARL VON OSSIETZKY universität OLDENBURG

Vorführung

- $N_1 = 923485606685672008805989842584990592120422$
  $139212156118563407814170747436693 23$

- $N_2 = 58264906265460312646928 5879$

CARL VON OSSIETZKY universität OLDENBURG

Parallelisierung

CARL VON OSSIETZKY universität OLDENBURG

Parallelisierung
Inhalt

- Multiplikatoren
- Segmente
- Vergleich

Multiplikatoren

- Bereits 1982 machten Shanks und Cohen erste Versuche mit Multiplikatoren
- Auf mehreren Recheneinheiten läuft der selbe Algorithmus
- Jede Recheneinheit bekommt einen anderen Multiplikator zugewiesen
- Als Multiplikatoren dienen kleine Zahlen (z.B. $2N, 3N, 5N$)
- Ziel: Perioden mit kürzerer Länge als die der Hauptperiode zu finden

CARL VON OSSIETZKY universität OLDENBURG

Segmente

- 2005 von Stephen McMath entwickelt und getestet
- Basiert auf Komposition von binären quadratischen Formen f
- Nach wenigen Schritten der Kettenbruchentwicklung wird mehrfach die Wurzel gezogen, wodurch mehrere Segmente entstehen
- Die verschiedenen Recheneinheiten bekommen von einer Recheneinheit Segmente zugeteilt (z.B. f-f^2, f^2-f^3)
- Ziel: Innerhalb der Segmente Perioden mit kürzerer Länge zu finden

CARL VON OSSIETZKY universität OLDENBURG

Vergleich
Laufzeit Segmente

Bit	Anzahl an Prozessoren			
	20	30	40	50
80	5,04	3,03	2,53	2,13
100	157,27	116,76	74,50	77,67
120	5416,97	4287,37	2690,76	2538,80

- Halbierung der Laufzeit zwischen 20 und 40 Prozessoren

CARL VON OSSIETZKY universität OLDENBURG

Vergleich
Laufzeit Multiplikatoren

Bit	Anzahl an Prozessoren			
	20	30	40	50
80	2,95	1,95	1,68	1,23
100	82,62	59,75	52,90	53,60
120	3255,65	2028,72	1683,57	1287,80

- Nur geringere Verbesserung im Vergleich zu Segmenten

CARL VON OSSIETZKY universität OLDENBURG

Vergleich

- Weitere Beobachtungen:
  - Effizienz der Segmente wird bei steigender Prozessoranzahl nicht beeinträchtigt
  - Bei Multiplikatoren sinkt die Effizienz mit steigender Prozessoranzahl
- Ab 180 Prozessoren sollten die Segmente den Multiplikatoren überlegen sein, weil die Effizienz nicht sinkt
- Diese Grenze liegt wahrscheinlich niedriger, da die Multiplikatoren zunehmend größer werden

CARL VON OSSIETZKY universität OLDENBURG

Fazit

CARL VON OSSIETZKY universität OLDENBURG

Fazit

- Obwohl Parallelisierungen möglich sind, ist SQUFOF den heutigen Verfahren unterlegen (Berechnungszeit RSA-768: $6,667 \cdot 10^{24}$ Jahre)
- Dennoch ist SQUFOF leicht zu implementieren und benötigt wenig Speicher (3 Register möglich)
- Im Bereich von 36- bis 64-Bit immer noch konkurrenzfähig und wird in diesem Bereich auch weiterhin genutzt

CARL VON OSSIETZKY universität OLDENBURG

Vielen Dank für die Aufmerksamkeit!

CARL VON OSSIETZKY universität OLDENBURG

Literatur

- **Shanks, Daniel:** *SQUFOF notes*, 1975 (von McMath digitalisierte Aufzeichnungen)
- **Shanks, Daniel:** *The infrastructure of a real quadratic field and its applications*. Proceedings of the Number Theory Conference, Seiten 217-224, 1972.
- **Gower, Jason und Samuel Wagstaff:** *Square Forms Factorization*. Mathematics of Computation, 77: 551-588, 2008.
- **McMath, Stephen:** *Parallel integer factorization using quadratic forms*, 2005.
- **Riesel, Hans:** *Prime Numbers and Computer Methods for Factorization*. Birkhäuser, 1985.

Näherungsbrüche

Satz: Rekursive Formeln

Der Zähler A_n und der Nenner B_n des n-ten Näherungsbruch von $\sqrt{N}$, für alle $n \in \mathbb{N}$, können mit den b_i aus der Kettenbruchentwicklung von $\sqrt{N} = [b_0; b_1, \ldots, b_n, \ldots]$ wie folgt bestimmt werden:
Wenn die Werte

$$A_{-1} = 1, \; A_0 = b_0,$$
$$B_{-1} = 0, \; B_0 = 1$$

gesetzt werden, so lässt sich der Näherungsbruch $\frac{A_n}{B_n}$ bestimmen mit

$$A_n = b_n A_{n-1} + A_{n-2},$$
$$B_n = b_n B_{n-1} \; + B_{n-2}.$$

CARL VON OSSIETZKY universität OLDENBURG

Vergleich

Bit	Anzahl an Prozessoren			
	20	30	40	50
80	0,39	0,38	0,39	0,30
100	0,37	0,34	0,43	0,40
120	0,35	0,31	0,29	0,39

- Prozent der schnelleren Faktorisierungen mit der Segmentmethode
- Multiplikatoren sind überlegen

Binäre quadratische Formen

Definition: Binäre quadratische Form

Eine quadratische Form in zwei Variablen, X und Y, wird als binäre quadratische Form bezeichnet. Es handelt sich dabei um ein Polynom der Form

$$f(X, Y) = aX^2 + bXY + cY^2, \tag{1}$$

wobei $a, b, c \in \mathbb{Z}$ gilt. Abkürzend wird das Polynom dargestellt als

$$f = (a, b, c). \tag{2}$$

CARL VON OSSIETZKY universität OLDENBURG

Beispiel: Verfahren mit quadratischen Formen

Sei $N = 78731$. Somit ist $P_1 = b_0 = \lfloor \sqrt{N} \rfloor = 280$, $Q_0 = 1$ und $Q_1 = N - b_0^2 = 78731 - 280^2 = 331$.

$$
\begin{aligned}
f_1 &= (Q_1, P_2, -Q_2) = (1, 280, -331) \\
f_2 &= (-Q_2, P_3, Q_3) = (-331, 51, 230) \\
f_3 &= (Q_3, P_4, -Q_4) = (230, 179, -203) \\
f_4 &= (-Q_4, P_5, Q_5) = (-203, 227, 134) \\
f_5 &= (Q_5, P_6, -Q_6) = (134, 175, -359) \\
f_6 &= (-Q_6, P_7, Q_7) = (-359, 184, 125) \\
f_7 &= (Q_7, P_8, -Q_8) = (125, 191, -338) \\
f_8 &= (-Q_8, P_9, Q_9) = (-338, 147, 13^2)
\end{aligned}
$$

An dieser Stelle wird die Quadratzahl $169 = 13^2$ gefunden.

CARL VON OSSIETZKY universität OLDENBURG

Beispiel: Verfahren mit quadratischen Formen

Nun lässt sich

$$f^{-\frac{1}{2}} = (-13, 147, 4394)$$

bestimmen und zu

$$g_0 = (-S_{-1}, R_0, S_0) = (-13, 277, 154)$$

reduzieren. Die weitere Berechnung liefert:

$$\begin{aligned} g_1 &= (S_0, R_1, -S_1) = (154, 185, -289) \\ g_2 &= (-S_1, R_2, S_2) = (-289, 104, 235) \\ g_3 &= (S_2, R_3, -S_3) = (235, 131, -262) \\ g_4 &= (-S_3, R_4, S_4) = (-262, 131, 235) \end{aligned}$$

Hier kann der Algorithmus abgebrochen werden, da $R_3 = R_4$ ist. Somit wird der nicht-triviale Faktor $\frac{S_3}{2} = \frac{262}{2} = 131$ bestimmt und durch Division erhält man den zweiten Faktor, also insgesamt: $78731 = 131 \cdot 601$.