

## Fermat Faktorisierung

$n=10379$  , Faktorbasis  $B=\{2,3,5,7\}$

1. Zufällige Liste von Paaren mit  $a,b$  mit  $a^2 \equiv b \pmod{n}$  , wobei  $b$  in der Faktorbasis aufgeht:

	$a$	4422	9461	8506	3117	700
	$b$	48	2025	27	945	2187
Faktorisierung von $b$	2	4	0	0	0	0
innerhalb der	3	1	4	3	3	7
Faktorbasis	5	0	2	0	1	0
	7	0	0	0	1	0
Faktorisierungsmatrix		0	0	0	0	0
mod 2		1	0	1	1	1
		0	0	0	1	0
		0	0	0	1	0
Relationsmatrix		0	1	0	0	0
(Transposition des		1	0	1	0	0
Kerns obiger Matrix)		1	0	0	0	1

Es gibt also drei Kombinationen obiger Einträge, die zu Paaren  $a, b$ :  $a^2 \equiv b^2 \pmod{n}$  führen :

$$9461, \sqrt{(2025)}=45 \quad , \quad \text{ggT}(9461+45, n)=97$$

$$4422*8506, \sqrt{(48*27)}=36 \quad , \quad \text{ggT}(4422*8506+36, n)=1$$

$$4422*700, \sqrt{(48*2187)}=324 \quad \text{ggT}(4422*700+324, n)=107$$

Jedenfalls wurden die Primfaktoren 97 und 107 von  $n=10379$  gefunden.

## 2. Kettenbruchmethode

Wir berechnen jetzt „naiv“ einige Koeffizienten der Kettenbruchentwicklung von  $\sqrt{(n)}$  :

```
(17:43) gp > sqrt(n)
%57 = 101.8773772728764351949228685
(17:43) gp > sqrt(n)-101
%48 = 0.8773772728764351949228684753
(17:44) gp > 1/%
%49 = 1.139760546476833905589454318
(17:45) gp > %-1
%50 = 0.1397605464768339055894543182
(17:45) gp > 1/%
%51 = 7.155095090915057407796914689
(17:45) gp > %-7
%52 = 0.1550950909150574077969146894
(17:46) gp > 1/%
%53 = 6.447657331383110812739449432
(17:46) gp > %-6
%54 = 0.4476573313831108127394494323
(17:47) gp > 1/%
%56 = 2.233851497327958061116729339
```

Dies führt offenbar zu den Kettenbruchkoeffizienten

$$a_0=101, a_1=1, a_2=7, a_3=6, a_4=2$$

und somit zu den  $\sqrt{(n)}$  approximierenden Brüchen:

$$101 + \frac{1}{1} = \frac{102}{1}, \quad 101 + \frac{1}{1 + \frac{1}{7}} = \frac{815}{8}, \quad 101 + \frac{1}{1 + \frac{1}{7 + \frac{1}{6}}} = \frac{4992}{49}, \quad 101 + \frac{1}{1 + \frac{1}{7 + \frac{1}{6 + \frac{1}{2}}}} = \frac{10799}{106}$$

Damit erhalten wir folgende Kette von Gleichungen:

$$\begin{aligned} 102^2 - n &= 25 \\ 815^2 - 8^2 n &= -31 \\ 4992^2 - 49^2 n &= 85 \\ 10799^2 - 106^2 n &= -43 \end{aligned}$$

Es fällt auf, daß wir damit Paare  $a, b$ :  $a^2 \equiv b \pmod{n}$  gewonnen haben mit recht kleinem  $b$ , welches eine gute Chance hat, in einer kleinen Faktorbasis aufzugehen, der jetzt noch das Element -1 beigefügt werden sollte. Wenn die rechte Seite einer dieser Gleichungen durch einen Primfaktor  $p$  geteilt wird und man anschließend diese Gleichung modulo  $p$  betrachtet, sieht man sofort, daß  $n$  ein Quadrat modulo  $p$  ist, also  $\left(\frac{n}{p}\right) = 1$ . Man kann also a priori alle Primzahlen  $p$  mit  $\left(\frac{n}{p}\right) = -1$ , also etwa die Hälfte, aus der Faktorbasis weglassen!

Jetzt ist noch folgendes Problem zu lösen:

Man braucht eine Möglichkeit, die approximierenden Brüche  $\frac{u}{v} \approx \sqrt{(n)}$  und die Differenzen  $u^2 - v^2 n$  zu errechnen ohne verlustbehaftete Floating-Point-Arithmetik. Letztere führt ja recht bald zu Fehlern bei der Errechnung der Kettenbruchkoeffizienten von  $\sqrt{(n)}$ .

Natürlich sollte man auch beweisen, daß obige Differenzen klein werden:  $|u^2 - v^2 n| \leq \sqrt{(n)}$ . Bei einem zufällig gewählten Paar  $a, b$  mit  $a^2 \equiv b \pmod{n}$  liegt  $b$  ja in der Größenordnung von  $n$ , nach obiger Methode ist jedes  $b$  nur halb so lang!

Dazu ist der Kettenbruchmechanismus genauer zu studieren, siehe z.B. das Buch von D. Bressoud, Factorization and Primality Testing. Die Lösung wird genau durch den dort beschriebenen Bhaskara Brouncker Algorithmus geliefert. Sie können natürlich versuchen, diese Lösung selbst zu finden!