

## Bhaskara Brouncker (Pari-Pseudocode)

BB\_init(n) =

```
{      s=floor(sqrt(n));
      A1=s;
      B0=0; B1=s;
      C0=1; C1=n-s2;
      P0=1; P1=s;
      Q0=0; Q1=1;
      i=0
}
```

BB(n) =

```
{      i++;
      while(true,
          Ai+1=(s+Bi) \ Ci;
          Bi+1=Ai+1Ci - Bi;
          Ci+1=Ci-1 - Ai+1(Bi+1-Bi);

          Pi+1=Ai+1Pi+Pi-1;
          Qi+1=Ai+1Qi+Qi-1
      )
}
```

Dann gilt für  $i \geq 0$  :  $P_i^2 - nQ_i^2 = (-1)^i C_i$  ,  $0 < C_i < 2\sqrt{n}$  .

Für die Fermat-Faktorbasis-Faktorisierungsmethode rechnet man jetzt modulo  $n$  und kann sofort testen, ob  $(-1)^i C_i$  in der Faktorbasis aufgeht.

Es wird nur skizziert, daß die  $A_i$  die Koeffizienten der Kettenbruchentwicklung von  $\sqrt{n}$  sind:

A) Für  $i \geq 1$  zeigt man (Aufgabenblatt 9) durch Induktion:  $B_i^2 + C_i C_{i-1} = n$

B) Man setze dann für  $i > 0$   $E_i := \frac{\sqrt{n} + B_{i-1}}{C_{i-1}}$  , damit ist  $A_i = [E_i]$  , und somit  $0 < E_i - A_i < 1$  , und

zeige unter Benutzung von A) durch Induktion  $E_i - \frac{1}{E_{i+1}} = A_i$  , d.h.  $E_i = A_i + \frac{1}{E_{i+1}}$  .

Also  $\sqrt{n} = E_1 = A_1 + \frac{1}{E_2} = A_1 + \frac{1}{A_2 + \frac{1}{E_3}} = A_1 + \frac{1}{A_2 + \frac{1}{A_3 + \frac{1}{E_4}}} = \dots$  ,

d.h. die  $A_i$  sind die Koeffizienten der Kettenbruchentwicklung von  $\sqrt{n}$  .