Zahlentheorie und Kryptologie, Wintersemester 2012/13
M. Hortmann

Blatt 5

bitte heften Sie dieses Blatt vor Ihre Lösungen

Namen					**Gruppe**	**Tutor**
1a	b	2a	b	c	**Summe**	**bearbeitet**
1	2	1	1	1	4 punkte=100%	

Aufgabe 1

Ist $n \in \mathbb{N}$ keine Quadratzahl, so generiert der Bhaskara-Brouncker-Algorithmus 5 Folgen natürlicher Zahlen:

Ausgehend von $s := [\sqrt{n}]$ wird zunächst eine Induktionsbasis geschaffen mit
$a_0 := s$, $b_{-1} := 0$, $b_1 := s$, $c_{-1} := 1$, $c_0 := n - s^2$, $p_{-1} := 1$, $p_0 := s$, $q_{-1} := 0$, $q_0 := 1$.
Es folgen die Rekursionen

$$a_{i+1} = (s + b_i) \backslash c_i$$
$$b_{i+1} = a_{i+1} c_i - b_i$$
$$c_{i+1} = c_{i-1} - a_{i+1}(b_{i+1} - b_i)$$

$$p_{i+1} = a_{i+1} p_i + p_{i-1}$$
$$q_{i+1} = a_{i+1} q_i + q_{i-1}$$

Wesentlich ist, daß hier ausschließlich mit natürlichen Zahlen operiert wird und keine Näherungsdarstellungen für reelle Zahlen ins Spiel kommen.

Es ergibt sich, daß die a_i die Koeffizienten der Kettenbruchentwicklung von $\sqrt{n}$ sind und p_i / q_i die zugehörigen Näherungsbrüche.

Wichtig im Zusammenhang mit der Fermat-Faktorbasis-Faktorisierungsmethode sind insbesondere die Gleichungen $p_i^2 - n q_i^2 = (-1)^{i+1} c_i$, wobei $0 < c_i < 2\sqrt{n}$. Dann gilt ja in $\mathbb{Z}_n$: $(-1)^{i+1} c_i = p_i^2$. D.h. wir haben Quadrate modulo *n*, die mit deutlich größerer Wahrscheinlichkeit in einer Faktorbasis $B = \{-1, p_1, \ldots, p_k\}$ aufgehen, als dies bei Zufallszahlen der Fall wäre.

Für diese Anwendung ist die Berechnung der q_i überflüssig, und die p_i müssen auch nur modulo *n*

berechnet werden, so daß sie im Laufe der Rekursion nicht über *n* hinaus wachsen. Im übrigen bleiben auch die b_i klein: man zeigt: $0 \leqslant b_i < \sqrt{n}$. Der Algorithmus operiert also bei der Berechnung der Kettenbruchentwicklung mit Zahlen der Größenordnung $\sqrt{n}$ und nur bei der Berechnung der p_i mod *n* mit Zahlen der Größenordnung *n*.

Folgendes soll die obigen Rekursionen klarer verständlich machen.

a) Zeigen Sie
$\mathbb{Q}(\sqrt{n}) := \{ r + s\sqrt{n} \mid r, s \in \mathbb{Q} \}$ ist ein Unterkörper von $\mathbb{C}$ und ein zweidimensionaler $\mathbb{Q}$ -Vektorraum.

Ein Element $\frac{u}{v} + \frac{z}{w}\sqrt{n} \in \mathbb{Q}(\sqrt{n})$ mit $z \neq 0$ läßt sich offenbar schreiben in der Form $\frac{\sqrt{n}+b}{c}$ mit $b, c \in \mathbb{Q}, c \neq 0$

b) Geht man aus von den Gleichungen $x_0 := \sqrt{n}$, $a_i := [x_i]$, $x_{i+1} := \frac{1}{x_i - a_i}$, so ist klar, daß

$\forall i \in \mathbb{N}_0 \colon x_i \in \mathbb{Q}(\sqrt{n}), x_i \notin \mathbb{Q}$, also $\forall i \geq -1 \colon x_{i+1} = \frac{\sqrt{n}+b_i}{c_i}$ mit $b_i, c_i \in \mathbb{Q}, c_i \neq 0$.

Zeigen Sie, daß sogar gilt: $\forall i \geq -1 \colon x_{i+1} = \frac{\sqrt{n}+b_i}{c_i}$ mit $b_i, c_i \in \mathbb{Z}, c_i \neq 0$.

Hinweis: Führen Sie diesen Beweis durch Induktion, ausgehend von $x_{i+1} = \frac{1}{x_i - a_i}$.
Dabei stoßen Sie auf die Gleichung $b_i = a_i c_{i-1} - b_{i-1}$ und auf die Gleichungen $c_i c_{i+1} = n - b_{i+1}^2$ und $c_i c_{i-1} = n - b_i^2$. Folgern Sie hieraus $c_{i+1} = c_{i-1} - a_{i+1}(b_{i+1} - b_i)$.
Damit haben Sie einen induktiven Ansatz für die Ganzzahligkeit der b_i und der c_i .

Will man zeigen, daß diese Folgen sogar ausschließlich positive Glieder haben, muß man die Ungleichungen $0 < b_i < \sqrt{n}$ und $0 < c_i < 2\sqrt{n}$ gleichzeitig mitbeweisen.

Aufgabe 2
Sei $\omega = \frac{-1 + i\sqrt{3}}{2}$.
Betrachten Sie den Ring der Eisensteinschen Zahlen $E = \{ a + b\omega \mid a, b \in \mathbb{Z} \}$.
Mit der Norm $N(z) := z\bar{z}$ ist *E* ein Euklidischer Ring.

a) Zeigen Sie: $2 + 3\omega$ ist ein Primelement in *E*.

b) Weil $p = 2 + 3\omega$ ein Primelement in E ist, muß $K := E / < p >$ ein Körper sein. Dessen Elemente sind Restklassen $\overline{a + b\omega}$ modulo $<p>$. Wie üblich ist $\overline{a + b\omega} = \overline{c + d\omega}$ genau dann wenn *p* Teiler von $(a - c) + (b - d)\omega$ ist. Machen Sie eine Liste aller Restklassen in *K*, in der keine doppelt vorkommt und zeigen Sie, daß die Liste vollständig ist. Geben sie einen Erzeuger der multiplikativen Gruppe von *K* an und schreiben Sie alle Elemente von K^* als Potenzen dieses Erzeugers hin.

c) Finden Sie die eindeutige Primfaktorzerlegung von $5 + 11\omega$.