Prof. Dr. R. Weissauer Sommersemester 2013
Th. Krämer Abgabe: 03. Juni 2013, 11:14 Uhr

Aufgabe 22. Die Fibonacci-Zahlen F_n sind rekursiv definiert durch $F_0 = 0, F_1 = 1$ und $F_n = F_{n-1} + F_{n-2}$ für $n \geq 2$. Beweisen Sie durch vollständige Induktion die explizite Formel

$$F_n \;=\; \frac{1}{\sqrt{5}} \cdot \left(\frac{1+\sqrt{5}}{2}\right)^n \;-\; \frac{1}{\sqrt{5}} \cdot \left(\frac{1-\sqrt{5}}{2}\right)^n$$

und finden Sie $a, b \in \mathbb{R}$, $c > 0$ mit $a + c \cdot n \leq \log(F_n) \leq b + c \cdot n$ für alle $n \in \mathbb{N}$.

Aufgabe 23. Für $r_0, r_1 \in \mathbb{N}$ mit $r_0 > r_1$ betrachte man wie in der Vorlesung den Euklidischen Algorithmus, wobei $m_0, m_1, \cdots \in \mathbb{N}_0$ und $r_2, r_3, \cdots \in \mathbb{N}_0$ definiert seien durch

$$\begin{array}{lllll} r_0 &=& m_0 r_1 + r_2 & \text{mit} & 0 \leq r_2 < r_1, \\ r_1 &=& m_1 r_2 + r_3 & \text{mit} & 0 \leq r_3 < r_2, \\ \vdots & & \vdots & \vdots & \vdots \end{array}$$

Die Zahl der benötigten Schritte sei mit $n = n(r_0, r_1) \in \mathbb{N}$ bezeichnet, d.h. es gelte $r_{n+1} = 0$ und $r_n = ggT(r_0, r_1)$. Beweisen Sie die Abschätzung $r_i \geq F_{n+1-i}$ für $i = 0, 1, \ldots, n+1$, und folgern Sie mittels Aufgabe 22, dass Konstanten $d, e \in \mathbb{R}$ existieren mit

$$n(r_0, r_1) \;\leq\; d + e \cdot \log(r_1) \quad \text{für} \quad r_0 > r_1 > 1.$$

Wieviele Schritte benötigt der Algorithmus, um $ggT(F_{n+1}, F_n) = 1$ zu bestimmen?

Aufgabe 24. Sei $n = 3^{4m}$ mit $m \in \mathbb{N}$. Zeigen Sie $n \equiv 1 \pmod{16}$, und berechnen Sie hiervon ausgehend den eindeutig bestimmten Repräsentanten $a \in \{0, 1, \ldots, 16\}$ mit der Eigenschaft

$$a \;\equiv\; 3^n \pmod{17}.$$

Aufgabe 25. Zeigen Sie für $a \in \mathbb{Z}$ und hierzu teilerfremde $m, n \in \mathbb{N}$, dass für $m \mid n$ auch $\mathrm{ord}_m(a) \mid \mathrm{ord}_n(a)$ gilt. Folgern Sie die Existenz von Primitivwurzeln modulo beliebiger Potenzen von Primzahlen $p \neq 2$, indem Sie durch Binomialentwicklung zeigen:

(a) Ist a eine Primitivwurzel modulo einer Primzahl p, dann ist a oder $a + p$ eine Primitivwurzel modulo p^2.

(b) Ist a eine Primitivwurzel modulo p^2 für eine Primzahl $p \neq 2$, dann ist a auch eine Primitivwurzel modulo beliebiger Potenzen p^k mit $k \in \mathbb{N}$.

Hinweis: Wenn a eine Primitivwurzel modulo p^k ist, gilt $a^{(p-1)p^{k-2}} = 1 + dp^{k-1}$ für ein $d \in \mathbb{Z}$ mit $p \nmid d$. Teil (b) folgt hieraus mit vollständiger Induktion.

Wo geht im Induktionsschritt die Voraussetzung $p \neq 2$ ein, und für welche $k \in \mathbb{N}$ gibt es modulo 2^k eine Primitivwurzel?

Die Übungsblätter und Informationen zur Vorlesung über Elementare Zahlentheorie finden Sie auch auf der zugehörigen Homepage:

`www.mathi.uni-heidelberg.de/~tkraemer/ElementareZahlentheorie/`