Übungen zur **Blatt 9**
Elementaren Zahlentheorie 12.12.2014

Falko Lorenz, Karin Halupczok WiSe 2014/15

Abgabetermin: Freitag, 19. Dezember 2014, bis 10:10 Uhr in die Briefkästen

Aufgabe 33:

(a) Sei r eine Primitivwurzel mod n. Man zeige: r^k genau ist dann eine Primitivwurzel mod n, wenn $\mathrm{ggT}(k, \varphi(n)) = 1$ ist.

(b) Man zeige: Für eine ungerade Primzahl p besitzt $(\mathbb{Z}/2p^n\mathbb{Z})^\times$ genausoviele Primitivwurzeln wie $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

(c) Man bestimme die vier Primitivwurzeln von $(\mathbb{Z}/26\mathbb{Z})^\times$ und die acht Primitivwurzeln von $(\mathbb{Z}/25\mathbb{Z})^\times$.

Aufgabe 34:

Sei $f(X) = a_nX^n + \cdots + a_1X + a_0$ ein Polynom vom Grade $n \geq 1$ mit Koeffizienten in $\mathbb{Z}$. Es bezeichne P_f die Menge aller Primzahlen p, für welche die Kongruenz

$$f(X) \equiv 0 \bmod p$$

lösbar in $\mathbb{Z}$ ist. Zeige: Die Menge P_f ist unendlich.
(Hinweis: Es gibt ein $c \in \mathbb{N}$ mit $|f(x)| \geq 2$ für alle $x \geq c$. Übergang zu $g(X) = f(cX)$ zeigt, daß man o. E. $c = 1$ annehmen darf. Ferner kann man von $a_0 \neq 0$ ausgehen. Ist nun $a_0 = 1$, so verfahre man ganz ähnlich wie in Euklids Beweis. Auf den Fall $a_0 = 1$ kann man sich aber per Übergang zu $g(X) = f(a_0X)$ leicht zurückziehen.)

Aufgabe 35:

Sei u_k eine Fibonaccizahl mit ungeradem Index k. Zeige: Jeder ungerade Teiler von u_k ist kongruent zu 1 mod 4; außerdem ist u_k nicht durch 4 teilbar. (Dazu gehe man z. B. aus von der Relation $u_{2m-1} = u_m^2 + u_{m-1}^2$.) Man folgere daraus: Es gibt unendlich viele Primzahlen p mit $p \equiv 1 \bmod 4$. Wie folgt das auch aus Aufgabe 34?
Zeige (für 2P extra), daß es auch unendlich viele Primzahlen $p \equiv 3 \bmod 4$ gibt.

Aufgabe 36:

Da F_5 nach Aufgabe 27 nur Primteiler $\equiv 1 \bmod 4$ besitzt und nicht prim ist, hat F_5 neben der offensichtlichen eine davon wesentlich verschiedene Darstellung als Summe zweier Quadrate. *Euler* gab diese *1742* an (ohne weiteren Kommentar). Man finde sie.
(Hinweis: Wir wissen $F_5 = 641(a^2 + b^2) = (25 + 4i)(25 - 4i)(a + bi)(a - bi)$. Wären a und b schon bekannt, so ist die Lösung klar. Wegen $F_5 = (2^{16} + i)(2^{16} - i)$ ist das Primelement $25 - 4i$ entweder ein Teiler von $2^{16} + i$ oder $2^{16} - i$. Ist ersteres der Fall, wäre also

$$\frac{2^{16} + i}{25 - 4i} = a + bi$$

zu berechnen.)