Prof. Dr. M. Rapoport
Dr. J. Ludwig

WS 2016/17

Algebra II

12. Übungsblatt

Aufgabe 1:
a) Es gibt unendlich viele Primzahlen p mit $p \equiv 3 \mod 4$.
b) Es gibt unendlich viele Primzahlen p mit $p \equiv 5 \mod 6$.
Hinweis: Erinnere Dich an Euklid's Beweis, dass es unendlich viele Primzahlen gibt, und betrachte $2^2 \cdot 3 \cdots p - 1$, bzw. $2 \cdot 3 \cdots p - 1$.

Aufgabe 2:
Es gibt unendlich viele Primzahlen p mit $p \equiv 5 \mod 8$.
Hinweis: Angenommen es gebe nur endlich viele. Sei dann p_0 die größte. Betrachte

$$q = 3^2 5^2 \cdots p_0^2 + 2^2 = a^2 + b^2.$$

Zeige, dass $q \equiv 5 \mod 8$. Benutze Fermat's Satz über die Primzahlzerlegung von Summen zweier Quadrate um zu zeigen, dass q einen Primteiler p mit $p \equiv 5 \mod 8$ hat.

Aufgabe 3:
Zu jeder natürlichen Zahl n gibt es unendlich viele Primzahlen p mit $p \equiv 1 \mod n$.
Hinweis: Angenommen es gebe nur endlich viele und sei P ihr Produkt. Sei ϕ_n das n-te Kreisteilungspolynom, d.h.

$$\phi_n(X) = \prod_{\substack{(j,n)=1 \\ 1 \le j \le n}} (X - e^{2\pi i j/n}) \in \mathbb{Z}[X].$$

Betrachte $\phi_n(xnP)$ für $x \in \mathbb{Z}$. Dann gibt es ein $y \in \mathbb{Z}$ mit $\phi_n(ynP) > 1$. Sei p eine Primzahl mit $p | \phi_n(ynP)$. Zeige, dass $p \nmid nP$. Leite einen Widerspruch her.
Die folgenden Eigenschaft des Kreisteilungspolynoms ist dafür hilfreich:
Sei $x \in \mathbb{Z}$. Falls $p | \phi_n(x)$, dann ist $x^m \not\equiv 1 \mod p$ für alle $m | n$.

Abgabe: Montag, 30. Januar 2017.