Übungen zu Vertiefung Elementare Zahlentheorie

WS 2010/2011, Blatt 11

Aufgabe 41. (Verfeinerung von Aufgabe 37) (a) Zeigen Sie: Ist p ein Primteiler von $2^{2^n}+1$ ($n \geq 2$), dann ist 2^{n+2} ein Teiler von $p-1$. (Sie wissen schon, dass 2 die Ordnung 2^{n+1} modulo p hat. Zeigen Sie nun, dass es ein x gibt mit $x^2 \equiv 2 \pmod{p}$; bestimmen Sie die Ordnung von x.)

(b) Finden Sie nochmals den kleinsten Primteiler von $2^{32}+1$, nun mit kürzerer Rechnung.

Aufgabe 42. Sei p eine ungerade Primzahl. Zeigen Sie:

(a) Die Anzahl der Lösungen der Kongruenz $x^2 \equiv a \pmod{p}$ ist $1+(\frac{a}{p})$.

(b) Die Anzahl der Lösungen der Kongruenz $ax^2+bx+c \equiv 0 \pmod{p}$ ist $1+(\frac{b^2-4ac}{p})$.

($(\frac{a}{p})$ und $(\frac{b^2-4ac}{p})$ sind Legendre-Symbole; es wird $(\frac{d}{p}) := 0$ gesetzt für $p \mid d$.)

Aufgabe 43. Berechnen Sie das Legendre-Symbol $(\frac{p}{q})$ für alle neun Kombinationen von $p = 7, 11, 13$ und $q = 227, 229, 1009$.

Aufgabe 44. Finden Sie alle Primzahlen p so, dass $x^2 \equiv 13 \pmod{p}$ eine Lösung hat.

Abgabe bis Freitag, 14.1.2011, 12:00 Uhr