Übungen zu Vertiefung Elementare Zahlentheorie

WS 2010/2011, Blatt 11

Aufgabe 41. (Refinement of exercise 37) (a) Show: If p is a prime divisor of $2^{2^n}+1$ ($n \geq 2$), then 2^{n+2} divides $p-1$. (You know already that 2 has order 2^{n+1} modulo p. Now show that there is an x such that $x^2 \equiv 2 \pmod{p}$; determine the order of x.)

(b) Find again the smallest prime divisor of $2^{32}+1$, now with a shorter calculation.

Aufgabe 42. Let p be an odd prime. Show:

(a) The number of solutions of the congruence $x^2 \equiv a \pmod{p}$ is $1 + (\frac{a}{p})$.

(b) The number of solutions of the congruence $ax^2 + bx + c \equiv 0 \pmod{p}$ is $1 + (\frac{b^2-4ac}{p})$.

($(\frac{a}{p})$ and $(\frac{b^2-4ac}{p})$ are Legendre symbols; one puts $(\frac{d}{p}) := 0$ for $p \mid d$.)

Aufgabe 43. Calculate the Legendre symbol $(\frac{p}{q})$ for all nine combinations of $p = 7, 11, 13$ and $q = 227, 229, 1009$.

Aufgabe 44. Find all primes p such that $x^2 \equiv 13 \pmod{p}$ has a solution.

Abgabe bis Freitag, 14.1.2011, 12:00 Uhr