

Inleveropgaven deel III
Elementaire getaltheorie 2005

NB: Geef bij al je antwoorden aan hoe je aan het resultaat komt.

1. Voor welke oneven priemgetallen p is -7 een kwadraatrest?
2. (a) Zij p een priemgetal van de vorm $4n + 1$. Zij r een kwadratische niet-rest modulo p . Laat zien dat $x = r^n$ een oplossing van $x^2 \equiv -1 \pmod{p}$ is.
(b) Voor dit onderdeel kun je het beste Mathematica gebruiken. Kies een priemgetal van 10 cijfers dat van de vorm $4n + 1$ is (je kunt hierbij de Mathematica-functie PrimeQ gebruiken). Bepaal nu een oplossing van $x^2 \equiv -1 \pmod{p}$ volgens voorgaand onderdeel. Gebruik de functies JacobiSymbol en PowerMod).
3. Bepaal alle gehele getallen a, b, c met $\text{ggd}(a, b, c) = 1$ zó dat $a^2 + 7b^2 = c^2$. (Hint: volg het idee van het bewijs van Stelling 13.1.2)
4. Bepaal alle gehele oplossingen x, y van $y^2 = x^4 + x^3$. (Hint: ontbindt de rechterzijde).
5. (Deze is niet moeilijk, je moet er alleen op komen) Bepaal alle gehele oplossingen van $y^2 = x^4 + x + 2$