

Blatt 5

Prof. Dr. N-P. Skoruppa und Dr. Jan Fricke
w3.countnumber.de

Abgabe: Fr, 16. Mai 08

- Aufgabe 1.** (i) Sei $p \equiv 1 \pmod{4}$ eine Primzahl. Zeigen Sie, dass für 50% aller zu p teilerfremden Zahlen $0 < a < p$ die Potenz $x := a^{\frac{p-1}{4}}$ eine Lösung der Kongruenz $x^2 \equiv -1 \pmod{p}$ ist. Schreiben Sie, dies ausnutzend, eine SAGE-Funktion `wurzelAusMinusEins(p)`, die eine Lösung der Kongruenz $x^2 \equiv -1 \pmod{p}$ zurückgibt.
- (ii) Schreiben Sie eine Funktion `zerlegeInZweiQuadrate(p)`, die für eine Primzahl p eine Lösung $(a, b) \in \mathbb{Z}^2$ der Gleichung $p = a^2 + b^2$ zurückgibt, falls diese existiert.
- (iii) Tabellieren Sie für die ersten 100 Primzahlen $p \equiv 1 \pmod{4}$ jeweils eine Darstellung von p als Summe zweier Quadrate.
- (iv) Schreiben Sie die in http://w3.countnumber.de/lehre/sose_08/zahlentheorie/uebungen/addon-5.1.p eingelegte¹ Primzahl als Summe zweier Quadrate. (Falls Ihre Funktion aus (ii) diese Zerlegung nicht liefert, so bekommen Sie für Ihre Lösung von (ii) keinen Punkt.)

Aufgabe 2. Faktorisieren Sie die unter http://w3.countnumber.de/lehre/sose_08/zahlentheorie/uebungen/addon-5.2-a.p eingelegte Zahl. Ein Hinweis ist unter http://w3.countnumber.de/lehre/sose_08/zahlentheorie/uebungen/addon-5.2-b.p zu finden.

Aufgabe 3. Man bestimme alle natürlichen Zahlen n mit

1. $\varphi(n) = 6$,
2. $\varphi(n) = 7$.

Aufgabe 4. Man zeige, dass für zusammengesetzte Zahlen n die Ungleichung $\sqrt{n/2} \leq \varphi(n) \leq n - \sqrt{n}$ gilt.

¹Pyth.: pickled