

Agraval-Kayal-Saxena-Primtest

Aufgabe 1. Für $n = 512, 100$ und $n = 13$ finden Sie die kleinste Primzahl r mit

$$\text{ord}_r(n) > \log_2^2 n.$$

Aufgabe 2. Seien $f(x), g(x), h(x) \in \mathbb{Z}[x]$ drei Polynome und sei n eine natürliche Zahl. Beweisen Sie, daß die Kongruenz

$$f(x) \equiv g(x) \pmod{(n)}$$

impliziert die Kongruenz

$$f(x) \equiv g(x) \pmod{(h(x), n)}.$$

Aufgabe 3. Für $n = 13$ und $r = 3, 5$ finden Sie

a) den Rest von $(x + 1)^n \pmod{(x^r - 1, n)}$,

b) den Rest von $x^n + 1 \pmod{(x^r - 1, n)}$;

c) bestimmen Sie die Kongruenz $(x + 1)^n \equiv x^n + 1 \pmod{(x^r - 1, n)}$.

Aufgabe 4. Sei

a) $n = 823543$,

b) $n = 82403082019807$.

Es ist bekannt, daß n eine Potenz einer Primzahl ist. Finden Sie diese Primzahl und diese Potenz.

Aufgabe 5. Bestimmen Sie mit Hilfe des Agraval-Kayal-Saxena Satzes und mit Hilfe des Computers, daß 127 eine Primzahl ist.