

23. Mai 2007

12. Übungsblatt Zahlentheorie

Aufgabe 1: (6 Punkte)

- a) Finden Sie alle Lösungen der Gleichung $x^2 \equiv 13 \pmod{2^{16} + 1}$!
- b) Finden Sie alle Lösungen der Gleichung $x^2 \equiv 1 \pmod{105}$!

Aufgabe 2: (3 Punkte)

Modulo der Zahl $N = 5\,352\,499$ gilt: $12\,345^2 \equiv 74\,195^2 \pmod{N}$. Finden Sie zwei Faktoren von N !

Aufgabe 3: (7 Punkte)

- a) Ist m ein Teiler von n , so ist auch $2^m - 1$ Teiler von $2^n - 1$ und $2^m + 1$ ist genau dann ein Teiler von $2^n + 1$, wenn n/m ungerade ist.
- b) Welche notwendige Bedingung muß ein Exponent n erfüllen, damit $2^n - 1$ bzw. $2^n + 1$ eine Primzahl ist? Für welche $n \in \mathbb{N}$ sind beides Primzahlen?
- c) Für welche $n \in \mathbb{N}$ ist die Gleichung $x^2 \equiv 3 \pmod{2^n - 1}$ lösbar?
- d) Für welche $n \in \mathbb{N}$ ist die Gleichung $x^2 \equiv 3 \pmod{2^n + 1}$ lösbar?
- e) Zeigen Sie: $2^n + 1$ ist genau dann eine Primzahl, wenn $3^{2^n} \equiv 1 \pmod{2^n + 1}$ ist.
- f) Folgern Sie daraus, daß 257 eine Primzahl ist!

Aufgabe 4: (4 Punkte)

Finden Sie mit dem Sieb des ERATOSTHENES alle Primzahlen zwischen 1000 und 1050 !