Mathematisches Institut
Abt. für Reine Mathematik
Dr. K. Halupczok

22.06.2006

Übungen zur Vorlesung

Elementare Zahlentheorie

SoSe 2006

Blatt 7

Abgabe: Donnerstag, den 29.06.2006, zu Beginn der Vorlesung

Aufgabe 1.

(a) Bestimme alle Lösungen der Kongruenz $x^3 - 2x + 4 \equiv 0\ (125)$.

(b) Sei p prim. Bestimme alle Lösungen der Kongruenz
$x^{p-2} + \cdots + x + 1 \equiv 0\ (p)$.

Aufgabe 2.

Bestimme ohne Rechnereinsatz den Rest von $\dfrac{70!}{18}$ nach Division durch 71.

Aufgabe 3.

Zeige den Satz von Wilson für Primzahlzwillinge:
Sei $n \geq 2$, dann sind äquivalent:

(a) n und $n+2$ sind Primzahlen,

(b) $4((n-1)! + 1) + n \equiv 0 \pmod{n(n+2)}$.

Hinweis: $n(n+1) \equiv (-2)(-1) \pmod{n+2}$.

Aufgabe 4.

Zeige das folgende Primzahlkriterium: Sei $N \geq 3$ eine ungerade Zahl und sei $N - 1 = \prod_{i=1}^{r} p_i^{k_i}$ die Primfaktorzerlegung von $N-1$ (p_i paarweise verschiedene Primzahlen). Genau dann ist N eine Primzahl, wenn es eine Zahl a gibt mit

$$a^{N-1} \equiv 1 \pmod{N}$$

und

$$a^{(N-1)/p_i} \not\equiv 1 \pmod{N} \quad \text{für alle } i = 1, \ldots, r.$$

In diesem Fall ist a eine Primitivwurzel mod N.