

## Übungen zur Elementaren Zahlentheorie

### Blatt 12 - Abgabe bis 25.1.2006

57. Es sei  $p = 2r + 1$  eine Primzahl, wobei  $r$  gerade ist. Folgern Sie aus dem Satz von Wilson, dass

$$(r!)^2 \equiv -1 \pmod{p}.$$

58. Finden Sie für jede der folgenden Zahlen entweder eine Darstellung als Summe von zwei Quadraten oder begründen Sie, warum es eine solche Darstellung nicht gibt:

29, 118, 231, 245.

59. Zeigen Sie, dass eine natürliche Zahl  $n$  mit der Eigenschaft

$$n \equiv -1 \pmod{8}$$

nicht als Summe von drei Quadraten darstellbar ist.

Hinweis: Reduktion.

60. Es sei  $p \neq 2$  eine Primzahl. Zeigen Sie, dass die Kongruenz

$$x^4 \equiv -4 \pmod{p}$$

genau dann lösbar ist, wenn  $p \equiv 1 \pmod{4}$  ist.

Hinweis:  $x^4 + 4 = ((x + 1)^2 + 1)((x - 1)^2 + 1)$ .

- 61.\* Es sei  $q$  eine Primzahl, wobei  $q \equiv -1 \pmod{4}$ . Zeigen Sie, dass jede prime Restklasse modulo  $q$  gleich oft als Differenz von zwei Quadraten primer Restklassen auftritt.