Beispiel 4.26: Perfekte Quadrate

Stellen wir uns einen langen Korridor mit N Türen vor. Anfangs sind alle Türen geschlossen. Entlang des Korridors laufen nacheinander N Personen und öffnen oder schließen die Türen nach der folgenden Regel: Die k-te Person öffnet bzw. schließt die k-te Tür und jede k-te Tür ab dieser Tür, d. h. sie öffnet bzw. schließt die Türen mit den Nummern $k, 2k, 3k, \ldots$. Welche Türen bleiben offen, wenn alle N Personen durchgelaufen sind?

Antwort: Die Tür n bleibt genau dann offen, wenn n ein *perfektes Quadrat* ist, d. h. wenn $n = m^2$ für eine natürliche Zahl m gilt.

Betrachten wir die Tür n. Diese Tür wurde genau dann von der k-ten Person angefasst (geöffnet oder geschlossen), wenn n durch k teilbar ist. Da am Anfang alle Türen geschlossen waren, bleibt am Ende die Tür n genau dann offen, wenn sie von einer *ungeraden* Anzahl von Personen geöffnet wurde. Somit bleibt die Tür n genau dann offen, wenn die Anzahl $\tau(n)$ der Teiler von n ungerade ist (1 und n sind auch Teiler von n).

Sei $n > 1$ (die erste Tür bleibt sowieso offen). Wir betrachten die Primzahlzerlegung $n = \prod_{i=1}^{m} p_i^{s_i}$ von n. Dann ist

$$\tau(n) = \prod_{i=1}^{m} (s_i + 1)$$

(Aufgabe 4.11). Also ist $\tau(n)$ genau dann ungerade, wenn alle $s_i + 1$ ungerade sind, was genau dann der Fall ist, wenn alle s_i's gerade sind, d. h. $s_i = 2r_i$ für geeignete r_i's gilt. Somit bleibt die n-te Tür genau dann offen, wenn

$$n = \prod_{i=1}^{m} p_i^{s_i} = \prod_{i=1}^{m} p_i^{2r_i} = \Big(\prod_{i=1}^{m} p_i^{r_i} \Big)^2$$

ein perfektes Quadrat ist.

Da die Primzahlzerlegungen teilerfremder Zahlen keine gemeinsamen Primzahlen enthalten dürfen, erhalten wir den folgenden nützlichen Fakt.

Lemma 4.27:

Ist eine ganze Zahl x duch a und durch b teilbar und sind a und b teilerfremd, dann ist x auch durch das Produkt ab teilbar.

Nun beweisen wir den bekannten »kleinen Satz« von Fermat (Pierre de Fermat, 1601-1655), der sich – insbesondere in der Kryptographie – als sehr nützlich erwiesen hat.

Satz 4.28: Kleiner Satz von Fermat

Ist p eine Primzahl und a eine natürliche Zahl, dann gilt

$$a^p \equiv a \bmod p\,.$$