Aufgabe H14T3A2 (11 Punkte)

Wieviele Quadrate gibt es im Ring $\mathbb{Z}/2014\mathbb{Z}$?

Lösung:

zu (a) Allgemein gilt: Ist $\phi : R \to S$ ein Ringisomorphismus, dann bildet ϕ die Quadrate in R bijektiv auf die Quadrate in S ab, insbesondere stimmt deren Anzahl in R und S also überein. Ist nämlich $q \in R$ ein Quadrat, also $q = a^2$ für ein $a \in R$, dann ist $\phi(q) = \phi(a^2) = \phi(a)^2$ ein Quadrat in S. Ist andererseits q' ein Quadrat in S, also $q' = b^2$ für ein $b \in S$, dann existiert auf Grund der Surjektivität von ϕ ein $a \in R$ mit $\phi(a) = b$, und es gilt $\phi(a^2) = \phi(a)^2 = b^2 = q'$. Jedes Quadrat in S wird also von mindestens einem Quadrat in R getroffen, auf Grund der Injektivität von ϕ sogar von genau einem.

Die Zahl 2014 hat die Primfaktorzerlegung $2 \cdot 19 \cdot 53$. Auf Grund der Teilerfremdheit der Faktoren gilt nach dem Chinesischen Restsatz also

$$\mathbb{Z}/2014\mathbb{Z} \quad \cong \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/19\mathbb{Z} \times \mathbb{Z}/53\mathbb{Z}.$$

Auf Grund der Vorbemerkung genügt es also, die Quadrate in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/19\mathbb{Z} \times \mathbb{Z}/53\mathbb{Z}$ zu zählen. Die Quadrate in diesem direkten Produkt sind genau die Elemente der Form $(a, b, c)^2 = (a^2, b^2, c^2)$, mit $a \in \mathbb{Z}/2\mathbb{Z}$, $b \in \mathbb{Z}/19\mathbb{Z}$, $c \in \mathbb{Z}/53\mathbb{Z}$. Sind m_2, m_{19}, m_{53} die Anzahlen der Quadrate in $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/19\mathbb{Z}$ und $\mathbb{Z}/53\mathbb{Z}$, dann ist $m_2 m_{19} m_{53}$ also die Anzahl der Quadrate im direkten Produkt.

Wir zeigen nun, dass für jede Primzahl $p > 2$ die Anzahl der Quadrate im Ring $\mathbb{Z}/p\mathbb{Z}$ gleich $\frac{p+1}{2}$ ist. Weil p eine Primzahl ist, handelt es sich bei $\mathbb{Z}/p\mathbb{Z}$ um einen endlichen Körper, und die Einheitengruppe $(\mathbb{Z}/p\mathbb{Z})^\times$ damit laut Vorlesung zyklisch. Sei α ein Erzeuger von $(\mathbb{Z}/p\mathbb{Z})^\times$ und Q die Menge der Quadrate in $(\mathbb{Z}/p\mathbb{Z})^\times$. Dann gilt $\mathrm{ord}(\alpha) = p - 1$, und wegen $2 \mid (p-1)$ folgt $\mathrm{ord}(\alpha^2) = \frac{p-1}{2}$. Also enthält $\langle \alpha^2 \rangle$ genau $\frac{p-1}{2}$ Elemente. Sei nun Q die Menge der Quadrate in $(\mathbb{Z}/p\mathbb{Z})^\times$. Wir zeigen, dass $Q = \langle \alpha^2 \rangle$ gilt. Ist $\beta \in \langle \alpha^2 \rangle$, dann gibt es ein $k \in \mathbb{Z}$ mit $\beta = (\alpha^2)^k = (\alpha^k)^2$, und damit ist β offenbar ein Quadrat. Sei nun umgekehrt $\beta \in Q$ vorgegeben. Dann gibt es ein Element $\beta_1 \in \langle \alpha \rangle$ mit $\beta_1^2 = \beta$. Wegen $\beta_1 \in \langle \alpha \rangle$ gibt es ein $k \in \mathbb{Z}$ mit $\beta_1 = \alpha^k$, und es folgt $\beta = \beta_1^2 = (\alpha^k)^2 = (\alpha^2)^k \in \langle \alpha^2 \rangle$. Damit ist die Gleichung bewiesen, und es folgt $|Q| = |\langle \alpha^2 \rangle| = \frac{p-1}{2}$. Weil auch $\bar{0}$ ein Quadrat in $\mathbb{Z}/p\mathbb{Z}$ ist, beträgt die Gesamtzahl der Quadrate in $\mathbb{Z}/p\mathbb{Z}$ also $\frac{p-1}{2} + 1 = \frac{p+1}{2}$.

Wenden wir nun diese Aussage auf $p = 19$ und $p = 53$ an, so erhalten wir $m_{19} = 10$ und $m_{53} = 27$. In $\mathbb{Z}/2\mathbb{Z}$ sind die Elemente $\bar{0}, \bar{1}$ beides Quadrate, es gilt also $m_2 = 2$. Insgesamt beträgt die Anzahl der Quadrate im direkten Produkt, und damit auch in $\mathbb{Z}/2014\mathbb{Z}$, also $m_2 m_{19} m_{53} = 2 \cdot 10 \cdot 27 = 540$.