Aufgaben: Quadrate in Restklassen

1. Bestimme ob 173 und 177 kongruent zu einem Quadrat modulo $8 \cdot 37$ sind.

   Lösung:

   Wir finden $173 \equiv 5 \mod (8)$ und $173 \equiv 25 \mod (37)$. Nun ist $25 = 5^2$ ein Quadrat modulo 37 aber 5 ist kein Quadrat modulo 8, d.h. 173 ist kein Quadrat modulo $8 \cdot 37$.

   Analog finden wir, dass $177 \equiv 1 \mod (8)$ und $177 \equiv -8 \mod (37)$. Nun ist 1 ein Quadrat modulo 8 und wir berechnen
   $$\left(\frac{-8}{37}\right) = \left(\frac{-1}{37}\right)\left(\frac{2}{37}\right)^3 = (-1)^{\frac{37-1}{2}}(-1)^{3\frac{37^2-1}{8}} = -1,$$
   d.h. -8 ist kein Quadrat modulo 37 und somit ist 177 kein Quadrat modulo $8 \cdot 37$.

2. Sei $p > 5$ eine Primzahl. Zeige, dass -5 genau dann ein Quadrat modulo p ist, wenn $p \equiv 1, 3, 7, 9 \mod (20)$.

   Lösung:

   Wir bemerken zuerst, dass 5 und p teilerfremd sind, ebenso 2 und p. Wir berechnen dann
   $$\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{5-1}{2}}\left(\frac{p}{5}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{5}\right).$$
   Der erste Faktor hängt nur von p modulo 4 ab und der zweite von p modulo 5. Um 1 zu erhalten müssen also beide Faktoren 1 sein oder beide Faktoren -1 sein. Das erste ist der Fall genau dann wenn $p \equiv 1 \mod (4)$ und $p \equiv \pm 1 \mod (5)$. Nach dem Chinesisischen Restsatz ist dies genau dann der Fall falls $p \equiv 1, 9 \mod (20)$.

   Im zweiten Fall müssen wir $p \equiv 3 \mod (4)$ und $p \equiv \pm 2 \mod (5)$ haben und dies ist genau der Fall falls $p \equiv 3, 7 \mod (20)$.