

## Aufgaben rund um die Zahl 2018

*Aufgabe 1.* a) Wieviele Quadrate gibt es modulo 2018?

b) Hat die Gleichung  $X^2 + Y^2 = 0$  eine nichttriviale Lösung modulo 2018 (d.h.  $X, Y \in \mathbb{Z}_{2018}$  und  $(X, Y) \neq ([0], [0])$ )?

*Aufgabe 2.* Wie viele Lösungen hat die Gleichung

$$X^2 + 978X + 173 = 0$$

in  $\mathbb{Z}_{2018}$ ?

*Aufgabe 3.* Gib (mit Begründung!) eine Galoiserweiterung  $K \subset L$  an, so dass

a)  $\text{Gal}(L|K) \simeq \mathbb{Z}_{2018}$ ,

b)  $\text{Gal}(L|K) \simeq D_{1009}$ .

*Aufgabe 4.* Bestimme alle Gruppen der Ordnung 2018 bis auf Isomorphie.

(*Tipp:* Zeige, dass jede nicht-abelsche Gruppe der Ordnung 2018 isomorph zu  $D_{1009}$  ist.)

*Aufgabe 5.* Erinnere Dich (oder beweise durch Induktion), dass gilt

$$\sum_{i=1}^n i^2 = \frac{n(n+1)(2n+1)}{6}.$$

Finde  $a, b \in \mathbb{N}$ , so dass gilt

$$2018 = \sum_{i=a}^b i^2,$$

und zwar ohne erschöpfendes Testen von  $(a, b)$ -Werten!

(*Tipp:* Betrachte das Problem modulo geeigneter Primzahlen...)

*Aufgabe 6.* Es bezeichne  $U_n^p$  die Menge der primitiven  $n$ -ten Einheitswurzeln.

a) Gib (mit Begründung) eine Bijektion (von Mengen)  $U_{2018}^p \leftrightarrow U_{1009}^p$  an.

b) Bestimme das Kreisteilungspolynom  $\phi_{2018} \in \mathbb{Q}[X]$ .

c) Zeige, dass für ein  $n \in \mathbb{N}$  und eine Primzahl  $p$ , so dass  $p$  nicht  $n$  teilt, gilt:

$$\phi_n \in \mathbb{Z}_p[X] \text{ irreduzibel} \iff \mathbb{Z}_n^\times = \langle [p] \rangle,$$

wobei  $\phi_n \in \mathbb{Z}[X]$  das  $n$ -te Kreisteilungspolynom ist, welches wir durch Reduktion der Koeffizienten als Polynom in  $\mathbb{Z}_p[X]$  auffassen. (*Tipp:* Betrachte  $\text{Gal}_{\mathbb{Z}_p}(\phi_n)$ .)

- d) Finde eine Primzahl  $p$  (mit Begründung), so dass  $\phi_{2018}$  in  $\mathbb{Z}_p[X]$  zerfällt (also reduzibel ist). (*Tipp*: Wie kann das Legendre-Symbol dabei helfen, schnell Elemente  $a \in \mathbb{Z}$  mit  $\text{ord}([a]) < 1008$  in  $\mathbb{Z}_{1009}^\times$  zu finden?)