

Diskrete Mathematik

Zusatz-Blatt 10, 28.06.2010, Abgabe 08.07.2010, 12.10 Uhr

Aufgabe 1. Zeige, dass es zu \mathbb{Z}_n^* mit n prim genau $\varphi(\varphi(n))$ primitive α mit $\langle \alpha \rangle = \mathbb{Z}_n^*$ gibt.

Aufgabe 2. $P = (-3, 9)$ und $Q = (-2, 8)$ sind Punkte der elliptischen Kurve

$y^2 = x^3 - 36x$ über \mathbf{Q} . Bestimme $P + Q$ und $2P$.

Aufgabe 3. Bestimme alle Punkte der elliptischen Kurve $E_{1,1}(\mathbb{Z}_{11})$ und prüfe, ob die Kurve zyklisch ist.

6 Punkte pro Aufgabe