Goethe-Universität, Frankfurt am Main
Sommersemester 2008
Prof. Dr. C.P. Schnorr, Antoine Scemama

Diskrete Mathematik, Übung 10

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.

Abgabetermin dieses Blattes: Donnerstag, der 26.Juni um 12.10 Uhr

Übungsblätter im Internet:
www.mi.informatik.uni-frankfurt.de:
Teaching, Diskrete Mathematik.