

Präsenzübungen zur Vorlesung
Diskrete Mathematik II
SoSe 2010

Blatt 5 / 15. Juni 2010

AUFGABE 34:

Sei QR_n die Menge aller quadratischen Reste in $\mathbb{Z}_n^*$.

- (a) In der Vorlesung haben wir gezeigt, dass $(QR_p, \cdot)$ eine Gruppe bildet. Zeigen Sie, dass auch $(QR_n, \cdot)$ eine Gruppe bildet. Warum ist $(QR_n, +, \cdot)$ kein Körper?
- (b) Geben sie QR_9 , QNR_9 , QR_{15} und QNR_{15} an. Geben Sie zu jedem quadratischen Rest die Quadratwurzeln an. Was fällt auf?
- (c) In der Vorlesung haben wir für $\mathbb{Z}_p^*$ gezeigt, dass das Produkt eines quadratischen Restes und eines quadratischen Nichtrestes stets ein quadratischer Nichtrest ist. Zeigen Sie dies auch für $\mathbb{Z}_n^*$. Können Sie eine ähnliche Aussage über das Produkt zweier quadratischer Nichtreste treffen?

AUFGABE 35:

Berechnen Sie

$$\left(\frac{2}{53}\right), \left(\frac{8}{53}\right), \left(\frac{10}{17}\right), \left(\frac{8}{15}\right) \text{ und } \left(\frac{131}{211}\right).$$

AUFGABE 36:

Betrachten Sie die über $\mathbb{F}_{17}$ durch folgende Gleichung definierte Kurve

$$E : y^2 = x^3 + 2x + 3.$$

- (a) Zeigen Sie, dass E eine elliptische Kurve ist.
- (b) Bestimmen Sie alle Punkte auf E über $\mathbb{F}_{17}$.