Eberhard Karls Universität Tübingen Wintersemester 2018/19
Fachbereich Mathematik
PD Dr. Jörg Zintl

Elliptische Funktionen und elliptische Kurven

Übungsaufgaben zum 6. Tutorium am 27.11.2018

Aufgabe 21
Zeigen Sie: $\overline{29} \in \mathbb{Z}_{288}$ ist eine Einheit, und bestimmen Sie die Inverse $\overline{29}^{-1}$.

Aufgabe 22
Sei $n = \pi_1 \cdot \pi_2$ das Produkt zweier verschiedener Primzahlen π_1 und π_2. Sei φ die Eulersche φ-Funktion. Seien $e, d \in \mathbb{N}_{>0}$ mit $ed \equiv 1 \mod \varphi(n)$. Zeigen Sie für alle $m \in \mathbb{Z}$ die Gleichheit

$$m^{ed} \equiv m \mod n.$$

Aufgabe 23
Decrypt the secret message below. It had been encrypted using the RSA algorithm. The public key is $(17, 253)$, and letters $a, b, c, \ldots$ correspond to numbers $1, 2, 3, \ldots \mod 253$.

245 78 78 26 234 191 26 108 173 215 26 245 20 71 90 173 148 215 245 22 245 215

Aufgabe 24
Sei $C = V(F) \subseteq \mathbb{P}^2$ eine irreduzible projektive ebene Kurve vom Grad 2, mit Minimalpolynom $F \in \mathbb{Q}[X, Y, Z]$. Zeigen Sie: Die Menge der $\mathbb{Q}$-rationalen Punkte $C_{\mathbb{Q}}$ ist entweder leer oder abzählbar unendlich.

Keine Abgabe, nur zur Vorbereitung auf das Tutorium!