Mathematische Grundlagen der Kryptografie (1321) SS 04

Nachklausur am 2.10.2004:

Aufgabenstellungen

Alle Lösungen sollen begründet werden. Wir wünschen Ihnen

Viel Erfolg!

Aufgabe 1

Folgender Text ist mit dem Verschiebe-Kryptosystem und dem Schlüssel 13 verschlüsselt:

XELCGBFLFGRZ

Wie lautet der Klartext?

[*10 Punkte*]

Aufgabe 2

Zeigen Sie , dass $\sqrt{i+\sqrt{3}}$ algebraisch über $\mathbb{Q}$ ist.

[*8 Punkte*]

Aufgabe 3

Beschreiben Sie das Diffie-Hellman-Schlüsselaustauschverfahren über endlichen Körpern.

(a) Was ist der öffentliche Schlüssel?

(b) Woraus besteht Alice' geheimer Schlüssel, und welchen Wert schickt sie an Bob?

(c) Woraus besteht Bobs geheimer Schlüssel, und welchen Wert schickt er an Alice?

(d) Welches ist der gemeinsame Schlüssel, der mit dem Verfahren festgelegt wird?

(e) Warum ist das Verfahren sicher?

(f) Warum ist das Verfahren effizient?

[*2 + 2 + 2 + 2 + 2 + 2 Punkte*]

Aufgabe 4

Berechnen Sie alle Punkte von $E(1, 1, \mathbb{F}_7)$.

[*10 Punkte*]

Aufgabe 5

Sei

$$L = \{ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in \mathbb{Z}^3 \mid 2x_1 + x_3 \equiv 0(\mathrm{mod}3)\}.$$

Zeigen Sie, dass L ein Gitter ist, und bestimmen Sie $\det(L)$.

[*10 Punkte*]

Aufgabe 6

Sei $(G, *)$ eine Gruppe und sei U eine Untergruppe von G mit $[G : U] = 2$. Zeigen Sie: U ist ein Normalteiler von G.

[*10 Punkte*]

Aufgabe 7

Sei $(R, +, \cdot)$ ein Integritätsbereich mit neutralem Element der Multiplikation e (das heißt, $er = re = r$ für alle $r \in R$). Sei R' eine Teilmenge mit mindestens zwei Elementen von R, so dass $(R', +, \cdot)$ ein Ring ist. Sei e' das neutrale Element der Multiplikation von R'. Zeigen Sie: $e = e'$.

[*10 Punkte*]

Aufgabe 8

Sei $n = p_1 \cdot p_2 \cdots p_r$ für ein $r \geq 1$ und verschiedene Primzahlen $p_1, \ldots, p_r \geq 3$. Zeigen Sie: Es gibt genau 2^r verschiedene Elemente $a \in (\mathbb{Z}/n\mathbb{Z})$ mit $a^2 \bmod n = 1$.

(Hinweis: Chinesischer Restsatz)

[*10 Punkte*]