Wolfgang K. Seiler
Tel. 2515

A5, C201

29. April 2005

3. Übungsblatt Höhere Mathematik I

Fragen: *(je ein Punkt)*
Die Antworten auf die nachfolgenden Fragen sollten nicht länger als etwa zwei Zeilen sein und lediglich eine kurze *Begründung enthalten. Antworten ohne Begründung werden nicht gewertet.*

1) Richtig oder falsch: Für $x, y \in \mathbb{F}_{1024}$ ist $(x+y)^6 = x^6 + y^6$.

2) Richtig oder falsch: Jeder Vektorraum über $\mathbb{F}_2$ ist auch ein Vektorraum über $\mathbb{F}_4$.

3) Richtig oder falsch: $\mathbb{F}_8$ ist ein zweidimensionaler $\mathbb{F}_4$-Vektorraum.

4) Richtig oder falsch: Jeder Vektorraum über $\mathbb{F}_{16}$ ist auch ein Vektorraum über $\mathbb{F}_4$.

5) Richtig oder falsch: Die Abbildung $\varphi\colon \mathbb{F}_{256} \to \mathbb{F}_{256}$ mit $\varphi(x) = x^{16}$ ist $\mathbb{F}_2$-linear.

Aufgabe 1: *(5 Punkte)*

a) Stellen Sie den ggT von 2005 und 1985 als Linearkombination dieser beiden Zahlen dar!

b) Finden Sie alle Paare ganzer Zahlen (x, y) mit $124x + 256y = 20$!

c) Bestimmen Sie im Körper $\mathbb{F}_{2003}$ das multiplikative Inverse von 10!

Problem 2: *(5 points)*

Both *TI unlimited* and `SIT.com` are customers of *THRIFTY PRIMES*; their public keys N, M as well as an encrypted message c sent to *TI unlimited* can be found in the file `ue3.scm` on the home page of the course. Both companies use public exponent $e = 2^{16}+1$. True to their name, *THRIFTY PRIMES* only generated three prime numbers p, q, r, setting $N = pq$ and $M = qr$.

a) Show how `SIT.com` (or anybody else knowing N, M) can decrypt the message c!

b) Fake a signature of `SIT.com` for the original message!

(Hint: c is taken from David Barron, Mike Rees: Text processing and typesetting with UNIX.*)*

Aufgabe 3: *(5 Punkte)*

Addition und Multiplikation im Körper $\mathbb{F}_{256}$ seien über das Polynom $P = x^8+x^4+x^3+x+1$ erklärt, und $\alpha \in \mathbb{F}_{256}$ sei so gewählt, daß $P(\alpha) = 0$ ist. Stellen Sie die folgenden Potenzen und Produkte in der Form

$$a + b\alpha + c\alpha^2 + d\alpha^3 + e\alpha^4 + f\alpha^5 + g\alpha^6 + h\alpha^7$$

dar:

a) α^{15} *b)* $(1+\alpha^4)(1+\alpha^5)$ *c)* $(\alpha^2+\alpha^3+\alpha^4+\alpha^6)^2$ *d)* $(1+\alpha+\alpha^2+\alpha^3)^2$

Abgabe bis zum Freitag, dem 6. Mai 2005, um 12.00 Uhr