WOLFGANG K. SEILER
Tel. 2515

A5, ZIMMER C201

Themenvorschläge für die kleinen Übungen am 17. Mai 2006

a) Stellen Sie den ggT von 2010 und 123 als Linearkombination dieser Zahlen dar!

Lösung:

$$\begin{aligned}
2010 : 123 = 16 \text{ Rest } 42 &\Longrightarrow 42 = 1 \cdot 2010 - 16 \cdot 123 \\
123 : 42 = 2 \text{ Rest } 39 &\Longrightarrow 39 = 1{\cdot}123 - 2{\cdot}42 = 1{\cdot}123 - 2(1{\cdot}2010 - 16{\cdot}123) = -2{\cdot}2010 + 33{\cdot}123 \\
42 : 39 = 1 \text{ Rest } 3 &\Longrightarrow 3 = 42 - 39 = (1 \cdot 2010 - 16 \cdot 123) - (-2 \cdot 2010 + 33 \cdot 123) \\
&\qquad = 3 \cdot 2010 - 49 \cdot 123
\end{aligned}$$

Da 39 durch drei teilbar ist, ist drei der größte gemeinsame Teiler von 2010 und 123; wir sind also fertig.

b) Bestimmen Sie im Körper $\mathbb{F}_{1031}$ die multiplikativen Inversen von zwei, zehn und zwanzig!

Lösung: Auch hier geht es darum, den größten gemeinsamen Teiler als Linearkombination darzustellen, allerdings wissen wir, daß der ggT von 1031 und jeder der angegebenen Zahlen eins ist, so daß tatsächlich nur die Koeffizienten der Linearkombination interessieren.

$$1031 : 2 = 515 \text{ Rest } 1 \Longrightarrow 1 = 1031 - 515 \cdot 2 \Longrightarrow -515 \cdot 2 \equiv 1 \bmod 1031\,.$$

Somit ist $-515 \equiv 1031 - 515 = 516 \bmod 1031$ invers zu zwei.

$$1031 : 10 = 103 \text{ Rest } 1 \Longrightarrow 1 = 1031 - 103 \cdot 10\,,$$

hier ist das Inverse also $-103 \equiv 928 \bmod 1031$. Für zwanzig wird die Rechnung etwas umfangreicher:

$$\begin{aligned}
1031 : 20 = 51 \text{ Rest } 11 &\Longrightarrow 11 = 1 \cdot 1031 - 51 \cdot 20 \\
20 : 11 = 1 \text{ Rest } 9 &\Longrightarrow 9 = -1 \cdot 1031 + 52 \cdot 20 \\
11 : 9 = 1 \text{ Rest } 2 &\Longrightarrow 2 = 2 \cdot 1031 - 103 \cdot 20 \\
9 : 2 = 4 \text{ Rest } 1 &\Longrightarrow 1 = -9 \cdot 1031 + 464 \cdot 20
\end{aligned}$$

Damit ist $464 \cdot 20 \equiv 1 \bmod 1031$, das multiplikative Inverse von 20 in $\mathbb{F}_{1031}$ ist 464.

c) Berechnen Sie den Bruch $\frac{3}{4}$ aus $\mathbb{F}_{17}$!

Lösung: Auch ohne EUKLIDischen Algorithmus sieht man, daß $17 - 4{\cdot}4 = 1$ die Darstellung der Eins als Linearkombination von 17 und 4 ist, also ist in $\mathbb{F}_{17}$

$$\frac{1}{4} = -4 = 17 - 4 = 13 \quad \text{und} \quad \frac{3}{4} = 3 \odot 13 = 39 \bmod 17 = 5\,.$$

d) Finden Sie sämtliche ganzzahligen Lösungen der Gleichung $120x + 81y = 24$!

Lösung: Wir bestimmen zunächst den ggT von 120 und 81:

$$\begin{aligned}
120 : 81 &= 1 \text{ Rest } 39 & 39 &= 120 - 81 \\
81 : 39 &= 2 \text{ Rest } 3 & 3 &= 81 - 2 \cdot 39 = 81 - 2(120 - 81) = 3 \cdot 81 - 2 \cdot 120 \\
39 : 3 &= 13 \text{ Rest } 0
\end{aligned}$$

Also ist $3 = 3 \cdot 81 - 2 \cdot 120$ der ggT. Multiplikation dieser Gleichung mit acht ergibt

$$120 \cdot (-16) + 81 \cdot 24 = 24\,,$$

also ist $(-16,\, 24)$ eine Lösung. Für zwei Lösungen (x, y) und (u, v) ist

$$120(x - u) + 81(y - v) = 24 - 24 = 0\,;$$

Kürzen durch den ggT drei macht daraus $40(x - u) + 27(y - v) = 0$.
Da 40 und 27 teilerfremd sind, hat die Gleichung $40z + 27w = 0$ als ganzzahlige Lösungen genau die Paare $(27k,\, -40k)$ mit $k \in \mathbb{Z}$; die allgemeine Lösung der Ausgangsgleichung ist also

$$x = -16 + 27k \quad \text{und} \quad y = 24 - 40k \quad \text{mit} \quad k \in \mathbb{Z}\,.$$

e) Geben Sie eine notwendige und hinreichende Bedingung dafür an, daß die lineare Gleichung $ax + by = c$ mit $a, b, c \in \mathbb{Z}$ ganzzahlige Lösungen (x, y) hat!

Lösung: Da jeder gemeinsame Teiler von a und b im Falle der Lösbarkeit auch $ax+by = c$ teilt, muß notwendigerweise $\mathrm{ggT}(a, b)$ ein Teiler von c sein. Diese Bedingung ist auch hinreichend, denn dann läßt sich $\mathrm{ggT}(a, b)$ linear kombinieren, und Multiplikation dieser Darstellung mit $c/\,\mathrm{ggT}(a, b)$ liefert eine Lösung der Gleichung.

f) Ein Teilnehmer eines RSA-Systems hat den öffentlichen Schlüssel $(55, 9)$. Verschlüsseln Sie die an ihn zu sendende Nachricht $x = 2$ und unterschreiben Sie sie mit seinem privaten Schlüssel!

Lösung: Die Verschlüsselung ist $2^9 \bmod 55$. Da $2^6 = 64 \equiv 9 \bmod 55$ und $2^3 = 8$ ist, läßt sich dies leicht berechnen als $9 \cdot 8 = 72 \equiv 17 \bmod 55$.
Zum Unterschreiben brauchen wir den privaten Schlüssel. Offensichtlich ist $55 = 5 \cdot 11$; da $(5 - 1) \cdot (11 - 1) = 40$ ist, müssen wir den ggT vom 40 und 9 linear kombinieren:

$$\begin{aligned} 40 : 9 &= 4 \text{ Rest } 4 & 4 &= 40 - 4 \cdot 9 \\ 9 : 4 &= 2 \text{ Rest } 1 & 1 &= 9 - 2 \cdot 4 = 9 - 2 \cdot (40 - 4 \cdot 9) = 9 \cdot 9 - 2 \cdot 40\,. \end{aligned}$$

Somit ist der private Exponent d hier gleich dem öffentlichen und die Unterschrift $2^d \bmod 55$ ist die gerade berechnete Zahl 17.

g) Ein Teilnehmer eines RSA-Systems hat den öffentlichen Schlüssel (N, e) mit $N = 25\,957 = 257 \cdot 101$ (beide Faktoren sind prim) und $e = 12\,047$. Berechnen Sie seinen privaten Exponenten!

Lösung: Mit $p = 257$ und $q = 101$ ist $(p - 1)(q - 1) = 25\,600$; wenn das Ganze funktionieren soll, muß diese Zahl teilerfremd zu e sein, und wir brauchen die Darstellung des größten gemeinsamen Teilers eins als Linearkombination der beiden Zahlen.

$$\begin{aligned} 25\,600 : 12\,047 &= 2 \text{ Rest } 1\,506 & 1\,506 &= 25\,600 - 2 \cdot 12\,047 \\ 12\,047 : 1\,506 &= 7 \text{ Rest } 1\,505 & 1\,505 &= 12\,047 - 7 \cdot 1\,506 = 15 \cdot 12\,047 - 7 \cdot 25\,600 \\ 1\,506 : 1\,505 &= 1 \text{ Rest } 1 & 1 &= 1\,506 - 1\,505 = -17 \cdot 12\,047 + 8 \cdot 25\,600 \end{aligned}$$

Also ist -17 ein multiplikatives Inverses von 12 407 modulo 25 600, und damit auch

$$d = -17 + 25\,600 = 25\,583\,,$$

der private Exponent.

h) Ein Text wird mit RSA verschlüsselt, indem man seine Buchstaben durch ihre ASCII-Codes (als Zahlen zwischen 0 und 255) ersetzt, diese als Ziffern von Zahlen $< N$ zur Basis 256 auffaßt, und dann diese Zahlen verschlüsselt. Schicken Sie die Nachricht „ja“ an den Inhaber des Schlüssels $(28\,891, 3)$!
Hinweis: „a“ hat den ASCII-Code 97.

Lösung: Da die ASCII-Codes der Kleinbuchstaben fortlaufend sind, hat „j“ den ASCII-Code 106, die Zahl ist also

$$106 \times 256 + 97 = 27\,233\,.$$

Zu dieser Zahl muß modulo 28 891 die dritte Potenz berechnet werden:

$$\begin{aligned} 27\,233 \times 27\,233 &= 741\,636\,289, & 741\,636\,289 \bmod 28\,891 &= 4\,319 \\ 4\,319 \times 27\,233 &= 117\,619\,327, & 117\,619\,327 \bmod 28\,891 &= 4\,066 \end{aligned}$$

Somit wird die Zahl 4 066 übermittelt.

i) *Richtig oder falsch:* Die Vektoren $\begin{pmatrix}\alpha\\1\end{pmatrix}$ und $\begin{pmatrix}\alpha+1\\\alpha\end{pmatrix}$ aus $\mathbb{F}_4^2$ sind linear unabhängig.

Lösung: Zwei Vektoren sind genau dann linear abhängig, wenn einer der beiden ein Vielfaches des anderen ist. Falls, wie hier, keiner der beiden der Nullvektor ist, muß sogar jeder der beiden Vielfaches des anderen sein, denn dann kann in einer Relation $\lambda\vec{u} + \mu\vec{v} = \vec{0}$ keiner der beiden Koeffizienten verschwinden.
Wenn hier $\binom{\alpha+1}{\alpha}$ Vielfaches von $\binom{\alpha}{1}$ ist, sieht man sofort an der zweiten Komponente, daß der Proportionalitätsfaktor gleich α sein muß. Da auch $\alpha \cdot \alpha = \alpha + 1$ ist, gilt dies in der Tat; die beiden Vektoren sind also linear abhängig.

j) *Richtig oder falsch:* Die Abbildung $\varphi\colon \mathbb{F}_4 \to \mathbb{F}_4$, die α und $\alpha+1$ miteinander vertauscht und $0, 1$ auf sich selbst abbildet, ist $\mathbb{F}_2$-linear.

Lösung: Da es hier um $\mathbb{F}_2$-Linearität geht, ist es zweckmäßig, die Elemente von $\mathbb{F}_4$ als Vektoren über $\mathbb{F}_2$ zu schreiben. Wenn wir α mit dem Basisvektor $\binom{0}{1}$ identifizieren, heißt das

$$0 = \begin{pmatrix}0\\0\end{pmatrix}, \quad 1 = \begin{pmatrix}1\\0\end{pmatrix}, \quad \alpha = \begin{pmatrix}0\\1\end{pmatrix} \quad \text{und} \quad \alpha + 1 = \begin{pmatrix}1\\1\end{pmatrix}.$$

φ ist dann gerade die Abbildung, die $\binom{x}{y}$ auf $\binom{x+y}{y}$ abbildet, und die ist natürlich linear.

k) *Richtig oder falsch:* Für ein Polynom mit Koeffizienten in $\mathbb{F}_2$ ist

$$(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n)^2 = a_0 + a_1x^2 + a_2x^4 + \cdots + a_nx^{2n}\,.$$

Lösung: Über jedem Körper ist (nach dem Distributivgesetz)

$$\left(\sum_{i=0}^{n} a_ix^i\right)^2 = \left(\sum_{i=0}^{n} a_ix^i\right)\left(\sum_{j=0}^{n} a_jx^j\right) = \sum_{i=0}^{n}\sum_{j=0}^{n} a_ia_jx^{i+j}\,.$$

Für $i = j$ ist der Summand gleich $a_i^2x^{2i}$, für $i \neq j$ haben wir außer $a_ia_jx^{i+j}$ auch noch den Summanden $a_ja_ix^{j+i}$, der offensichtlich denselben Wert hat. Da in $\mathbb{F}_2$ wie auch in jedem Vektorraum über $\mathbb{F}_2$ die Addition eines Elements zu sich selbst Null ergibt, heben sich diese beiden Terme gegenseitig weg, also ist

$$(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n)^2 = \sum_{i=0}^{n} a_i^2x^{2i} = a_0^2 + a_1^2x^2 + a_2^2x^4 + \cdot + a_n^2x^{2n}\,.$$

Soweit gilt alles auch noch über Körpern wie $\mathbb{F}_4$ oder $\mathbb{F}_{256}$; nur in $\mathbb{F}_2$ aber ist auch noch $a^2 = a$ für alle $a \in \mathbb{F}_2$ – es gibt schließlich nur die beiden Elemente $a = 0$ und $a = 1$. Somit lassen sich auf der rechten Seite die Koeffizienten a_i^2 durch a_i ersetzen, die Behauptung ist also richtig.

l) Was ist $(x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)(x^2 + 1)$, wenn man mit Koeffizienten aus $\mathbb{F}_2$ rechnet?

Lösung: Multiplikation von $(x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$ mit x^2 ergibt $x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2$, während die Multiplikation mit eins natürlich nichts ändert. Da $x^i + x^i = 0$ für alle i, folgt

$$\begin{aligned}
&(x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)(x^2 + 1) \\
= x^{12} + x^{11} &+ x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 \\
&+ x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\
= x^{12} + x^{11} &+ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad x + 1\,;
\end{aligned}$$

alle mittleren Terme heben sich weg.

m) Zeigen Sie: Das Polynom $x^4 + 1$ ist reduzibel über $\mathbb{F}_2$.

Lösung: $x^4 + 1 = (x^2 + 1)(x^2 + 1) = (x + 1)^4$

n) Berechnen Sie den ggT der beiden Polynome $x^4 + 1$ und $x^3 + 1$ sowohl über $\mathbb{R}$ als auch über $\mathbb{F}_2$!

Lösung: Über den reellen Zahlen ist

$$\begin{aligned}
(x^4 + 1) : (x^3 + 1) &= x \text{ Rest } -x + 1 \\
(x^3 + 1) : (-x + 1) &= -x^2 - x - 1 \text{ Rest } 2\,,
\end{aligned}$$

die Polynome sind also teilerfremd, d.h. der ggT ist Eins (oder jede andere von Null verschiedene Konstante).
Über dem Körper mit zwei Elementen ist

$$\begin{aligned}
(x^4 + 1) : (x^3 + 1) &= x \text{ Rest } x + 1 \\
(x^3 + 1) : (x + 1) &= x^2 + x + 1 \text{ Rest } 0\,,
\end{aligned}$$

der ggT ist also $x + 1$.

o) Berechnen Sie über $\mathbb{F}_2$ den ggT der beiden Polynome $f = x^4 + x^2 + 1$ und $g = x^3 + 1$, und stellen Sie ihn in der Form $\alpha f + \beta g$ dar!

Lösung:

$$\begin{aligned}
(x^4 + x^2 + 1) : (x^3 + 1) = x \text{ Rest } x^2 + x + 1 &\Longrightarrow x^2 + x + 1 = 1 \cdot (x^4 + x^2 + 1) + x \cdot (x^3 + 1) \\
(x^3 + 1) : (x^2 + x + 1) &= x + 1 \text{ Rest } 0\,.
\end{aligned}$$

Damit haben wir bereits in der ersten Division den ggT und seine lineare Darstellung gefunden.

p) Zeigen Sie: In $\mathbb{F}_{2^n}$ hat jedes Element genau eine Quadratwurzel.

Lösung: Haben $x, y \in \mathbb{F}_{2^n}$ dasselbe Quadrat $x^2 = y^2$, so ist $(x/y)^2 = 1$. Da das Polynom $z^2 - 1 = (z - 1)^2$ nur die eine Nullstelle $z = 1$ hat, muß $x = y$ sein, d.h. die Abbildung $x \mapsto x^2$ ist injektiv und damit auch surjektiv.

q) Für welche Primzahlen p gilt dies auch im Körper $\mathbb{F}_p$?

Lösung: Nur für $p = 2$, denn modulo jeder anderen Primzahl p sind 1 und $p - 1$ zwei verschiedene Nullstellen von $z^2 - 1$, d.h. jedes von Null verschiedene Element, das überhaupt eine Quadratwurzel hat, hat gleich zwei. Somit gibt es $\frac{p+1}{2}$ Elemente mit und $\frac{p-1}{2}$ Elemente ohne Quadratwurzel aus $\mathbb{F}_p$.

r) Multiplikation in $\mathbb{F}_8 = \mathbb{F}_2^3$ mit Basis $1, \alpha, \alpha^2$ sei über das Polynom $\alpha^3 + \alpha + 1$ definiert. Berechnen Sie die Elemente

$$x = (\alpha^2 + 1)(\alpha + 1), \quad y = (\alpha^2 + 1)^2 \quad \text{und} \quad z = \frac{1}{\alpha}\,!$$

Lösung: $x = (\alpha^2 + 1)(\alpha + 1) = \alpha^3 + \alpha^2 + \alpha + 1$ hat Grad drei, muß also noch modulo $\alpha^3 + \alpha + 1$ reduziert werden. Bei der Division ist offensichtlich der Quotient gleich eins, und als Rest bleibt $x = \alpha^2$ übrig.

$y = (\alpha^2 + 1)^2 = \alpha^4 + 2\alpha^2 + 1 = \alpha^4 + 1$, und

$$(\alpha^4 + 1) : (\alpha^3 + \alpha + 1) = \alpha \text{ Rest } \alpha^2 + \alpha + 1\,,$$

also ist $y = \alpha^2 + \alpha + 1$.

Zur Berechnung von $z = 1/\alpha$ müssen wir den ggT Eins von $\alpha^3 + \alpha + 1$ und α linear kombinieren:

$$(\alpha^3 + \alpha + 1) : \alpha = \alpha^2 + 1 \text{ Rest } 1 \Longrightarrow \alpha \cdot (\alpha^2 + 1) \equiv 1 \bmod \alpha^3 + \alpha + 1\,.$$

Damit ist $z = \frac{1}{\alpha} = \alpha^2 + 1$.

s) Multiplikation in $\mathbb{F}_{64} = \mathbb{F}_2^6$ mit Basis $1, \alpha, \alpha^2, \ldots, \alpha^6$ sei über das Polynom $\alpha^6 + \alpha + 1$ definiert. Berechnen Sie die Elemente

$$x = (\alpha^2 + 1)^3, \quad y = (\alpha^3 + 1)^3 \quad \text{und} \quad z = \frac{1}{\alpha + 1}\,!$$

Lösung: $(\alpha^2+1)^3 = \alpha^6+\alpha^4+\alpha^2+1$ führt bei Division durch $\alpha^6+\alpha+1$ zum Quotienten Eins und Rest

$$\alpha^4 + \alpha^2 + \alpha\,,$$

der somit gleich x ist.

$(\alpha^3 + 1)^3 = \alpha^9 + \alpha^6 + \alpha^3 + 1$. Nach der angegebenen Relation ist

$$\alpha^6 = \alpha + 1 \Longrightarrow \alpha^9 = \alpha^4 + \alpha^3\,.$$

Damit ist $y = (\alpha^3 + 1)^3 = (\alpha^4 + \alpha^3) + (\alpha + 1) + \alpha^3 + 1 = \alpha^4 + \alpha$.

Zur Berechnung von z müssen wir den ggT von $\alpha+1$ und $\alpha^6+\alpha+1$ aus diesen Elementen linear kombinieren:

$(\alpha^6 + \alpha + 1) : (\alpha + 1) = \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha$ Rest 1, d.h.

$$(\alpha + 1)(\alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha) = (\alpha^6 + \alpha + 1) + 1$$

(in $\mathbb{F}_{64}$ sind $+$ und $-$ dieselbe Operation), und

$$z = \frac{1}{\alpha + 1} = \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha\,.$$