Wolfgang K. Seiler
Tel. 2515

A5, Zimmer C201

Themenvorschläge für die kleinen Übungen am 19. März 2007

a) 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.

b) 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.

c) Berechnen Sie den diskreten Logarithmus modulo 13 von Fünf zur Basis Sieben!

Lösung: Da wir keine besseren Verfahren kennen, bleibt uns nicht anderes übrig, als so lange Potenzen von Sieben zu berechnen, bis wir daß Ergebnis Fünf erhalten.

$$7^2 = 49 \equiv 10 \bmod 13, \qquad 7^3 \equiv 10 \cdot 7 = 70 \equiv 5 \bmod 13\,.$$

Damit ist der diskrete Logarithmus von Fünf zur Basis Sieben gleich Drei.

d) Zeigen Sie, daß es keinen diskreten Logarithmus modulo 13 von Fünf zur Basis Drei gibt!

Lösung: $3 \cdot 3 = 9$ und $3^3 = 27 \equiv 1 \bmod 13$. Somit ist in $\mathbb{F}_{13}$ bereits $3^3 = 1$, d.h. nur die drei Elemente 1, 3 und 9 lassen sich als Dreierpotenzen darstellen.

e) Zeigen Sie, daß sich jedes $x \neq 0$ aus $\mathbb{F}_{13}$ als Potenz von Sieben darstellen läßt!

Lösung: Aus der vorletzten Aufgabe kennen wir bereits die Potenzen $7^2 = 10$ und $7^3 = 5$. Weiter geht es mit $7^4 \equiv 5 \cdot 7 = 35 \equiv 9 \bmod 13$, $7^5 \equiv 9 \cdot 7 = 63 \equiv 11 \bmod 13$ und $7^6 \equiv 11 \cdot 7 = 77 \equiv 12 \equiv -1 \bmod 13$. Damit ist dann

$$\begin{aligned} 7^7 &= 7^6 \cdot 7 \equiv -7 \equiv 4 \bmod 13, & 7^8 &= 7^6 \cdot 7^2 \equiv -10 \equiv 3 \bmod 13, \\ 7^9 &= 7^6 \cdot 7^3 \equiv -5 \equiv 8 \bmod 13, & 7^{10} &= 7^6 \cdot 7^4 \equiv -9 \equiv 4 \bmod 13, \\ 7^{11} &= 7^6 \cdot 7^5 \equiv -11 \equiv 2 \bmod 13, & 7^{12} &= 7^6 \cdot 7^6 \equiv (-1) \cdot (-1) = 1 \bmod 13\,. \end{aligned}$$

Somit sind die Potenzen $7^i \bmod 13$ für $i = 1, \ldots, 12$ alle verschieden, sind also die sämtlichen Zahlen von 1 bis 12.

f) 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.

g) 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.

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

$$(a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n)^2 = a_0 + a_1 x^2 + a_2 x^4 + \cdots + a_n x^{2n}\,.$$

Lösung: Über jedem Körper ist (nach dem Distributivgesetz)

$$\left(\sum_{i=0}^{n} a_i x^i\right)^2 = \left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{j=0}^{n} a_j x^j\right) = \sum_{i=0}^{n}\sum_{j=0}^{n} a_i a_j x^{i+j}\,.$$

Für $i = j$ ist der Summand gleich $a_i^2 x^{2i}$, für $i \neq j$ haben wir außer $a_i a_j x^{i+j}$ auch noch den Summanden $a_j a_i x^{j+i}$, 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

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

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.

i) 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

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

alle mittleren Terme heben sich weg.

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

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

k) 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 $x+1$.

l) 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.

m) 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.

n) 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 $\mathbb{F}_p$.

o) 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 $z = \frac{1}{\alpha} = \alpha^2 + 1$.

p) 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

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