



Lösungsblatt 12

(Version 2)

Aufgabe 1 (Quadratisches Sieb)

- (a) Bei der CCA auf die Rabin-Verschlüsselung haben wir ein Entschlüsselungsurakel, welches uns eine zweite Quadratwurzel einer Zahl verrät. Bei dem Quadratischen Sieb versuchen wir, ein ebensolches Paar systematisch zu erzeugen.
- (b) Wir erhalten die Nullstellen durch quadratische Ergänzung

$$\begin{aligned}
 x^2 + 232x - 165 &\equiv x^2 - 1 & \pmod{2} &\Rightarrow x \equiv 1 & \pmod{2}, \\
 &\equiv x^2 + x & \pmod{3} &\Rightarrow x \equiv -1, 0 & \pmod{3}, \\
 &\equiv x^2 + 2x & \pmod{5} &\Rightarrow x \equiv -2, 0 & \pmod{5}, \\
 &\equiv (x+4)^2 + 1 & \pmod{7} &\Rightarrow \text{keine Nullstelle} & \pmod{7}, \\
 &\equiv x^2 + x & \pmod{11} &\Rightarrow x \equiv -1, 0 & \pmod{11}.
 \end{aligned}$$

- (c) In der vorangegangenen Aufgabe haben wir ermittelt, daß der Funktionswert $f(x)$ genau dann durch 5 und 11 teilbar ist, wenn

$$x \equiv -2, 0 \pmod{5} \quad \text{und} \quad x \equiv -1, 0 \pmod{11}.$$

Nach dem Chinesischen Restsatz gibt es damit 4 Restklassen x zum Modul 55, für die $55 \mid f(x)$. Dies sind 0, 10, 33 und 43. Im Intervall $[-50, 50]$ gibt es daher insgesamt 7 Argumente $x \in [-50, 50]$, für die $55 \mid f(x)$.

- (d) Wir haben $n = 13621$ und $m = 116$. Es gilt $f(X) = (X + 116)^2 - 13621$. Wir stellen das folgende Sieb auf:

x	-5	-4	-3	-2	-1	0	1	2	3	4	5
$f(x)$											
2	x		x		x		x		x		x
3		x	x		x	x		x	x		x
5	x			x		x			x		x
7											
11					x	x					
Rest	-13	-359	-71	-1	-1	-1	17	101	1	779	17

Offensichtlich nützt uns die Spalte für $x = -2$ alleine nichts, da wir keine Wurzel von -1 kennen. Dafür gilt:

$$\begin{aligned}
 f(-1) &\equiv 115^2 &\equiv -2^2 \cdot 3^2 \cdot 11 & \pmod{n} \\
 f(0) &\equiv 116^2 &\equiv -3 \cdot 5 \cdot 11 & \pmod{n} \\
 f(3) &\equiv 119^2 &\equiv 2^2 \cdot 3^3 \cdot 5 & \pmod{n}
 \end{aligned}$$

Wir erhalten einen Faktor von n als

$$\gcd(115 \cdot 116 \cdot 119 - 2^2 \cdot 3^3 \cdot 5 \cdot 11, n) = 53.$$

Aufgabe 2 (Modulo Rechnen mit Polynomen)

- (a) $g \equiv X^2 \pmod{(X^3 + X + 1)}$.

- (b) $f \equiv X^4 + X^3 + X \pmod{(X^5 + X^3 + 1)}$.
(c) $h \equiv (X^3 + 1)^2 + X^4 + X^3 + X \equiv X^3 + 1 \pmod{(X^5 + X^3 + 1)}$.

Aufgabe 3 (Irreduzible Polynome)

Mindestens ein irreduzibler Teiler eines Polynoms vom Grad ≤ 5 muß ein irreduzibles Polynom vom Grad ≤ 2 sein, d.h. X , $X + 1$ oder $X^2 + X + 1$, da wir $\mathbb{Z}_2[X]$ betrachten.

- (a) Man kann schnell prüfen, daß X und $X + 1$ keine Teiler von g_1 sind, da weder 0 noch 1 Nullstellen von g_1 sind. Ansonsten gilt $1 \equiv g_1 \pmod{(X^2 + X + 1)}$ und damit ist g_1 irreduzibel.
(b) Man kann schnell prüfen, daß X und $X + 1$ keine Teiler von g_2 sind, da weder 0 noch 1 Nullstellen von g_2 sind. Ansonsten gilt $0 \equiv g_2 \pmod{(X^2 + X + 1)}$ und damit ist g_2 nicht irreduzibel.
(c) Man kann schnell prüfen, daß X und $X + 1$ keine Teiler von g_3 sind, da weder 0 noch 1 Nullstellen von g_3 sind. Ansonsten gilt $1 \equiv g_3 \pmod{(X^2 + X + 1)}$ und damit ist g_3 irreduzibel.

Aufgabe 4 (Erweiterter euklidischer Algorithmus mit Polynomringen)

- (a) Wir berechnen mit dem erweiterten euklidischen Algorithmus

$$\begin{array}{rcccc} & X^3 + 1 & X^2 + X + 1 & X^2 + X + 1 & 0 \\ q & & X & 1 & \\ x_i & 1 & 0 & 1 & 1 \\ y_i & 0 & 1 & X & X + 1 \end{array}$$

Es gilt daher $(X^3 + 1) + (X^2 + X + 1)(X) = X^2 + X + 1 \pmod{2}$

- (b) Wir berechnen mit dem erweiterten euklidischen Algorithmus

$$\begin{array}{rcccc} & X^5 + X^3 + 1 & X^2 + 1 & 1 & \\ q & & X^3 & & \\ x_i & 1 & 0 & 1 & \\ y_i & 0 & 1 & X^3 & \end{array}$$

Es gilt daher $X^3(X^2 + 1) = 1 \in \mathbb{F}_{2^5}$.

Aufgabe 5 (Endliche Körper)

- (a) Wir stellen fest, daß $X^5 \equiv 1 \pmod{(X^4 + X^3 + X^2 + X + 1)}$, also ist X kein Generator. Allerdings ist $X + 1$ ein Generator, da $(X + 1)^5 \equiv (X^4 + 1)(X + 1) \equiv X^4 + X^3 + X^2 \pmod{(X^4 + X^3 + X^2 + X + 1)}$ und $(X + 1)^3 \not\equiv 1 \pmod{(X^4 + X^3 + X^2 + X + 1)}$.

Man kann beweisen, daß die multiplikative Gruppe eines endlichen Körpers immer zyklisch ist. Um die Behauptung zu beweisen, stellen wir die multiplikative Gruppe als das Produkt ihrer Untergruppen von maximaler Primzahlpotenzordnung dar. Wenn jede dieser Untergruppen zyklisch ist, kann man analog zu Übung 7 zeigen, daß dann auch \mathbb{F}_q^\times zyklisch ist. Um zu sehen daß jede der Untergruppen von Primzahlpotenzordnung zyklisch ist, sei nun \mathcal{U} eine solche der Ordnung p^{e_p} . Wenn \mathcal{U} nicht zyklisch ist, dann gibt es ein Element γ von maximaler Ordnung $p^r < p^{e_p}$. Offensichtlich gilt dann, daß das Polynom $X^{p^r} - 1$ mehr als p^r Nullstellen hat, was aber nicht sein kann. Dieses beweist unsere Behauptung. Für einen detaillierteren Beweis verweisen wir auf S. Lang: „Algebra“.

- (b) Als Polynom über \mathbb{Z}_2 hat das Polynom genau zwei Nullstellen. Die Gleichung ist eine andere Charakterisierung eines endlichen Körpers. Man kann ihn als Nullstellenmenge des Polynoms $X^{q^m} - X$ sehen. Andersherum ist leicht zu sehen, daß für alle $x \in \mathbb{F}_{q^m}$ gelten muß, daß $x^{q^m} - x = 0$. Das heißt, daß man sich \mathbb{F}_{q^m} als um die Nullstellen von $X^{q^m} - X$ ergänztem \mathbb{F}_q vorstellen kann.

Dies lässt die folgende Behauptung als nicht ganz abwegig erscheinen: Alle endlichen Körper der gleichen Ordnung sind isomorph. Für einen detaillierteren Beweis verweisen wir auf S. Lang: „Algebra“.

- (c) Um die Isomorphie der gegebenen Körper zu sehen, konstruieren wir den gesuchten Isomorphismus. Die Abbildung muß linear sein und das Null- und Einselement festhalten. Wir schließen, daß die Abbildung einen Generator von $\mathbb{F}_2[X]/g_i(X)$ auf einen Generator α von $\mathbb{F}_2[X]/(X^4 + X^3 + X^2 + X + 1)$ abbilden muß.

Sei X der Generator von $\mathbb{F}_2[X]/g_1(X)$, dann muß dieser auf einen Generator α von $\mathbb{F}_2[X]/(X^4 + X^3 + X^2 + X + 1)$ abgebildet werden, so daß $\alpha^4 = \alpha + 1$ (wg. der Linearität des Isomorphismus). Dieser ist $\alpha = X^3 + X + 1$. Man kann diesen Generator wie folgt konstruieren: Der Generator muß offensichtlich eine Nullstelle des Polynoms

$$Y^4 - Y - 1 \in (\mathbb{F}_2[X]/(X^4 + X^3 + X^2 + X + 1))[Y]$$

sein, da $\alpha^4 = \alpha + 1$ gelten muß. Da uns keine Methode bekannt ist, die Nullstellen des Polynoms zu berechnen, müssen wir diese durch Einsetzen in Y finden. Wenn wir $Y = X^3 + X + 1$ setzen, sehen wir, daß

$$\begin{aligned} & (X^3 + X + 1)^4 + (X^3 + X + 1) + 1 \\ \equiv & (X^6 + X^2 + 1)^2 + X^3 + X \\ \equiv & X^{12} + X^4 + 1 + X^3 + X \\ \equiv & X^{12} + X^2 \\ \equiv & 0 \pmod{(X^4 + X^3 + X^2 + X + 1)} \end{aligned}$$

Sei X der Generator von $\mathbb{F}_2[X]/g_3(X)$, dann muß dieser auf einen Generator γ von $\mathbb{F}_2[X]/(X^4 + X^3 + X^2 + X + 1)$ abgebildet werden, so daß $\gamma^4 = \gamma^3 + 1$ (wg. der Linearität des Isomorphismus). Dieser ist $\gamma = X + 1$. Man kann diesen Generator wie folgt konstruieren: Der Generator muß offensichtlich eine Nullstelle des Polynoms

$$Y^4 - Y^3 - 1 \in (\mathbb{F}_2[X]/(X^4 + X^3 + X^2 + X + 1))[Y]$$

sein, da $\gamma^4 = \gamma^3 + 1$ gelten muß. Wieder ist uns keine Methode bekannt, die Nullstellen des Polynoms zu berechnen. Daher müssen wir die Nullstelle wieder durch Einsetzen in Y finden. Wenn wir $Y = X + 1$ setzen, sehen wir, daß

$$\begin{aligned} & (X + 1)^4 + (X + 1)^3 + 1 \\ \equiv & (X^2 + 1)^2 + X^3 + X^2 + X \\ \equiv & X^4 + 1 + X^3 + X^2 + X \\ \equiv & 0 \pmod{(X^4 + X^3 + X^2 + X + 1)} \end{aligned}$$

Da α keine Nullstelle des Polynoms $Y^4 - Y^3 - 1 \in \mathbb{K}[Y]$ ist, ist die Abbildung f nur für \mathbb{K}_1 ein Isomorphismus.

- (d) Ja, man kann mit den Elementen des Körpers rechnen, ohne daß man das Polynom, nach dem man $\mathbb{F}_2[X]$ faktorisiert, genau angibt. Da der Körper $\mathbb{F}_{2^{102}}$ ist bis auf Isomorphie eindeutig bestimmt ist, sind einige Aussagen, z.B. über die Anzahl der Unterkörper, der multiplikativen Untergruppen usw. allgemein gültig.