LÖSUNG 53. Berechnen Sie in $\mathbb{Z}_2[x]/_{x^4+1}$:

(1) $(x^2 + x) + (x^3 + x + 1)$
(2) $(x^2 + 1) \cdot (x^3 + x + 1)$

Rechnung in $\mathbb{Z}_2[x]/_{x^4+1}$: Es gilt $2 \equiv 0 \mod 2$ und $x^4 + 1 \equiv 0$ bzw. $x^4 \equiv 1 \mod x^4 + 1$.

(1)

$$\begin{aligned} (x^2 + x) + (x^3 + x + 1) &= x^3 + x^2 + 2x + 1 \\ &\equiv x^3 + x^2 + 1 && \mod 2 \end{aligned}$$

(2)

$$\begin{aligned} (x^2 + 1) \cdot (x^3 + x + 1) &= x^5 + x^3 + x^2 + x^3 + x + 1 \\ &= x^5 + 2x^3 + x^2 + x + 1 \\ &\equiv x^5 + x^2 + x + 1 && \mod 2 \\ &= x \cdot x^4 + x^2 + x + 1 \\ &\equiv x \cdot 1 + x^2 + x + 1 && \mod x^4 + 1 \\ &= x^2 + 2x + 1 \\ &= x^2 + 1 && \mod 2 \end{aligned}$$

LÖSUNG 54. Berechnen Sie in $\mathbb{Z}_2[x]/_{x^5+x+1}$:

(1) $(x + 1) + (x^2 + 1) + (x^3 + x + 1)$
(2) $(x + 1)^3 \cdot (x^3 + x^2 + 1)$

Rechnung in $\mathbb{Z}_2[x]/_{x^5+x+1}$: Es gilt $2 \equiv 0 \mod 2$ und $x^5+x+1 \equiv 0$ bzw. $x^5 \equiv x+1 \mod x^5+x+1$.

(1)

$$\begin{aligned} (x + 1) + (x^2 + 1) + (x^3 + x + 1) &= x^3 + x^2 + 2x + 3 \\ &\equiv x^3 + x^2 + 1 && \mod 2 \end{aligned}$$

(2)

$$\begin{aligned} (x + 1)^3 \cdot (x^3 + x^2 + 1) &= (x^3 + 3x^2 + 3x + 1) \cdot (x^3 + x^2 + 1) \\ &\equiv (x^3 + x^2 + x + 1) \cdot (x^3 + x^2 + 1) && \mod 2 \\ &= x^6 + 2x^5 + 2x^4 + 3x^3 + x + 1 \\ &\equiv x^6 + x^3 + x + 1 && \mod 2 \\ &\equiv x \cdot (x + 1) + x^3 + x + 1 && \mod x^5 + x + 1 \\ &= x^2 + x + x^3 + x + 1 \\ &= x^3 + x^2 + 1 && \mod 2 \end{aligned}$$

LÖSUNG 55. Bestimmen Sie in $\mathbb{Z}_2[x]/_{x^6+1}$ alle Polynome $x^k \cdot (x^3 + x + 1)$, $k \in \mathbb{N}$ und deren binäre Repräsentation.

(1) $x \cdot (x^3 + x + 1) = x^4 + x^2 + x$, $(0, 1, 0, 1, 1, 0)$
(2) $x^2 \cdot (x^3 + x + 1) = x^5 + x^3 + x^2$, $(1, 0, 1, 1, 0, 0)$
(3) $x^3 \cdot (x^3 + x + 1) \equiv 1 + x^4 + x^3$, $(0, 1, 1, 0, 0, 1)$

(4) $x^4 \cdot (x^3 + x + 1) \equiv x + x^5 + x^4$, $(1, 1, 0, 0, 1, 0)$
(5) $x^5 \cdot (x^3 + x + 1) \equiv x^2 + 1 + x^5$, $(1, 0, 0, 1, 0, 1)$
(6) $x^6 \cdot (x^3 + x + 1) \equiv x^3 + x + 1$, $(0, 0, 1, 0, 1, 1)$

LÖSUNG 56. Bestimmen Sie in $\mathbb{Z}_2[x]/_{x^6+1}$ alle Polynome $x^k \cdot (x^4 + x + 1)$, $k \in \mathbb{N}$ und deren binäre Repräsentation.

(1) $x \cdot (x^4 + x + 1) = x^5 + x^2 + x$, $(1, 0, 0, 1, 1, 0)$
(2) $x^2 \cdot (x^4 + x + 1) = 1 + x^3 + x^2$, $(0, 0, 1, 1, 0, 1)$
(3) $x^3 \cdot (x^4 + x + 1) \equiv x + x^4 + x^3$, $(0, 1, 1, 0, 1, 0)$
(4) $x^4 \cdot (x^4 + x + 1) \equiv x^2 + x^5 + x^4$, $(1, 1, 0, 1, 0, 0)$
(5) $x^5 \cdot (x^4 + x + 1) \equiv x^3 + 1 + x^5$, $(1, 0, 1, 0, 0, 1)$
(6) $x^6 \cdot (x^4 + x + 1) \equiv x^4 + x + 1$, $(0, 1, 0, 0, 1, 1)$

LÖSUNG 57. Zeigen Sie, dass $x^3 + x^2 + 1$ in $\mathbb{Z}_2[x]/_{x^7+1}$ ein Generatorpolynom eines zyklischen Codes ist, und bestimmen Sie den binären Code von $(1, 0, 0, 1)$.

Eine Polynomdivision ergibt: $x^7 + 1 = (x^3 + x^2 + 1) \cdot (x^4 + x^3 + x^2 + 1)$, also teilt $x^3 + x^2 + 1$ das Polynom $x^7 + 1$ und ist damit Generatorpolynom eines zyklischen Codes. Die Polynomrepräsentation von $(1, 0, 0, 1)$ ist $x^3 + 1$ und damit berechnet sich der Code zu

$$\begin{aligned}(x^3 + 1) \cdot (x^3 + x^2 + 1) &= x^6 + x^5 + 2x^3 + x^2 + 1 \\ &\equiv x^6 + x^5 + x^2 + 1 && \mod 2\end{aligned}$$

und damit lautet der binäre Code $(1, 1, 0, 0, 1, 0, 1)$.

LÖSUNG 58. Zeigen Sie, dass $x^4 + x^2 + x + 1$ in $\mathbb{Z}_2[x]/_{x^7+1}$ ein Generatorpolynom eines zyklischen Codes ist, und bestimmen Sie den binären Code von $(0, 1, 0, 1)$.

Eine Polynomdivision ergibt $x^7 + 1 = (x^4 + x^2 + x + 1) \cdot (x^3 + x + 1)$, also teilt $x^4 + x^2 + x + 1$ das Polynom $x^7 + 1$ und ist damit Generatorpolynom eines zyklischen Codes. Die Polynomrepräsentation von $(0, 1, 0, 1)$ ist $x^2 + 1$ und damit berechnet sich der Code durch

$$\begin{aligned}(x^2 + 1) \cdot (x^4 + x^2 + x + 1) &= x^6 + 2x^4 + x^3 + 2x^2 + x + 1 \\ &\equiv x^6 + x^3 + x + 1 && \mod 2\end{aligned}$$

und damit lautet der binäre Code $(1, 0, 0, 1, 0, 1, 1)$.

LÖSUNG 59. Alice und Bob möchten mit dem Diffie-Hellman Verfahren einen geheimen Sitzungsschlüssel vereinbaren. Sie entscheiden sich, das Verfahren auf $\mathbb{Z}_{17}$ mit $\alpha = 11$ durchzuführen. Alice wählt die Zufallszahl $a = 7$ und Bob die Zufallszahl $b = 9$. Welche Nachrichten schicken sich Alice und Bob und was wird ihr Sitzungsschlüssel sein?

	Alice	Bob
1.	Sendet öffentlich $p = 17$, $\alpha = 11$	
2.	Geheime Zufallszahl $a = 7$	Geheime Zufallszahl $b = 9$
	Berechne $\alpha^a = 11^7 \equiv 3 \bmod 17$	Berechnet $\alpha^b = 11^9 \equiv 6 \bmod 17$
	Sendet öffentlich 3	Sendet öffentlich 6
3.	Berechnet $(\alpha^b)^a = 6^7 \equiv 14 \bmod 17$	Berechnet $(\alpha^b)^a = 3^9 \equiv 14 \bmod 17$
4.	Beide verwenden 14 als temporären Schlüssel	

LÖSUNG 60. Alice und Bob wollen sich mit dem Diffie-Hellman-Verfahren auf einen gemeinsamen Schlüssel einigen. Im Vorfeld haben sie abgesprochen, dass sie in $\mathbb{Z}_{11}$ rechnen werden, und $\alpha = 2$ verwenden. Alice hat sich das Geheimnis $a = 3$, Bob das Geheimnis $b = 4$ ausgedacht.

	Alice	Bob
1.	Sendet öffentlich $p = 11$, $\alpha = 2$	
2.	Geheime Zufallszahl $a = 3$	Geheime Zufallszahl $b = 4$
	Berechne $\alpha^a = 2^3 \equiv 8 \bmod 11$	Berechnet $\alpha^b = 2^4 \equiv 5 \bmod 11$
	Sendet öffentlich 8	Sendet öffentlich 5
3.	Berechnet $(\alpha^b)^a = 5^3 \equiv 4 \bmod 11$	Berechnet $(\alpha^b)^a = 8^4 \equiv 4 \bmod 11$
4.	Beide verwenden 4 als temporären Schlüssel	

LÖSUNG 61. RSA-Schlüsselberechnung: Sie haben die zwei Primzahlen $p = 61$ und $q = 83$ bestimmt, und versuchen Ihr Glück mit den Kandidaten 27, 29 und 65537 für den öffentlichen Exponenten e. Prüfen Sie mit dem Euklidischen Algorithmus, welcher Exponent in Frage kommt, und berechnen Sie für diese den zugehörigen geheimen Exponenten d.

Gegeben sind die beiden Primzahlen $p = 61$ und $q = 83$. Damit erhalten wir

$$n = 61 \cdot 83 = 5063\,.$$

Als ersten Kandidaten für den öffentlichen Exponenten versuchen wir $e = 27$, und berechnen wegen $(p-1)(q-1) = 60 \cdot 82 = 4920$ den $\mathrm{ggT}(27, 4920)$ mit dem Euklidischen Algorithmus:

k	a_k	r_k	u_k	v_k
0	4920		1	0
1	27	$\lfloor \frac{4920}{27} \rfloor = 182$	0	1
2	$4920 - 182 \cdot 27 = 6$	$\lfloor \frac{27}{6} \rfloor = 4$	$1 - 182 \cdot 0 = 1$	$0 - 182 \cdot 1 = -182$
3	$27 - 4 \cdot 6 = 3$	$\lfloor \frac{6}{3} \rfloor = 2$	$0 - 4 \cdot 1 = -4$	$1 - 4 \cdot (-182) = 729$

Da $\mathrm{ggT}(27, 4920) = 3$ ist $e = 27$ nicht geeignet. Da 27 keine Primzahl ist, hat sie selbst noch Teiler, und es ist etwas leichter, einen gemeinsamen Teiler zu finden. Man kann aber auch mit Nicht-Primzahlen Glück haben, nur hier klappte es nicht.

Als zweiten Kandidaten für den öffentlichen Exponenten versuchen wir $e = 29$, und berechnen den $\mathrm{ggT}(29, 4920)$ mit dem Euklidischen Algorithmus:

k	a_k	r_k	u_k	v_k
0	4920		1	0
1	29	$\lfloor \frac{4920}{29} \rfloor = 169$	0	1
2	$4920 - 169 \cdot 29 = 19$	$\lfloor \frac{29}{19} \rfloor = 1$	$1 - 169 \cdot 0 = 1$	$0 - 169 \cdot 1 = -169$
3	$29 - 1 \cdot 19 = 10$	$\lfloor \frac{19}{10} \rfloor = 1$	$0 - 1 \cdot 1 = -1$	$1 - 1 \cdot (-169) = 170$
4	$19 - 1 \cdot 10 = 9$	$\lfloor \frac{10}{9} \rfloor = 1$	$1 - 1 \cdot (-1) = 2$	$-169 - 1 \cdot 170 = -339$
5	$10 - 1 \cdot 9 = 1$		$-1 - 1 \cdot 2 = -3$	$170 - 1 \cdot (-339) = 509$

Da $\mathrm{ggT}(29, 4920) = 1$ ist $e = 29$ als Exponent geeignet. Wir bestimmen nun den zugehörigen geheimen Exponenten d mit $e \cdot d \equiv 1 \mod (p-1)(q-1) = 4920$ durch $509 \cdot 29 = 1 + 3 \cdot 4920$ bzw. $29 \cdot 509 \equiv 1 \mod 4920$, also ist $d = 509$ der gesuchte geheime Exponent.

Als dritten Kandidaten für den öffentlichen Exponenten versuchen wir $e = 65537$ (das ist der Exponent fast aller öffentlicher Schlüssel), und berechnen den $\mathrm{ggT}(65537, 4920)$ mit dem Euklidischen Algorithmus:

k	a_k	r_k	u_k	v_k
0	65537		1	0
1	4920	$\lfloor \frac{65537}{4920} \rfloor = 13$	0	1
2	$65537 - 13 \cdot 4920 = 1577$	$\lfloor \frac{4920}{1577} \rfloor = 3$	$1 - 13 \cdot 0 = 1$	$0 - 13 \cdot 1 = -13$
3	$4920 - 3 \cdot 1577 = 189$	$\lfloor \frac{1577}{189} \rfloor = 8$	$0 - 3 \cdot 1 = -3$	$1 - 3 \cdot (-13) = 40$
4	$1577 - 8 \cdot 189 = 65$	$\lfloor \frac{189}{65} \rfloor = 2$	$1 - 8 \cdot (-3) = 25$	$-13 - 8 \cdot 40 = -333$
5	$189 - 2 \cdot 65 = 59$	$\lfloor \frac{65}{59} \rfloor = 1$	$-3 - 2 \cdot 25 = -53$	$40 - 2 \cdot (-333) = 706$
6	$65 - 1 \cdot 59 = 6$	$\lfloor \frac{59}{6} \rfloor = 9$	$25 - 1 \cdot (-53) = 78$	$-333 - 1 \cdot 706 = -1039$
7	$59 - 9 \cdot 6 = 5$	$\lfloor \frac{6}{5} \rfloor = 1$	$-53 - 9 \cdot 78 = -755$	$706 - 9 \cdot (-1039) = 10057$
8	$6 - 1 \cdot 5 = 1$		$78 - 1 \cdot (-755) = 833$	$-1039 - 1 \cdot 10057 = -11096$

Also ist $\mathrm{ggT}(65537, 4920) = 1$. Damit ist $e = 65537$ als Exponent geeignet und $833 \cdot 65537 = 1 + 11096 \cdot 4920$ bzw. $65537 \cdot 833 \equiv 1 \mod 4920$, also ist $d = 833$ der gesuchte geheime Exponent.

LÖSUNG 62. Es seien $p = 13$ und $q = 19$ zwei geheime Primzahlen mit Produkt $p \cdot q = 247$. Zeigen Sie, dass $e = 5$ als Exponent für einen geheimen RSA-Schlüssel in $\mathbb{Z}_{247}$ in Frage kommt. Bestimmen Sie den zugehörigen Exponenten des öffentlichen Schlüssels und schreiben Sie das Schlüsselpaar auf.

Es ist $(p-1)\cdot(q-1) = 216$. Ob der Exponent $e = 5$ als (Achtung! Die Rollen sind getauscht!) geheimer Schlüssel geeignet ist, prüfen wir durch $\mathrm{ggT}(216, 5) \stackrel{!}{=} 1$.
Der Grund dafür ist, dass wir ja auch den Exponenten d ausrechnen wollen, und da das RSA-Verfahren über das Potenzieren mit den beiden Exponenten funktioniert, und damit dann $\left(m^d\right)^e \equiv m$ erfüllt werden soll. Wie in der Aufgabe zuvor erklärt, bestimmen wir dies über den erweiterten Euklidischen Algorithmus:

k	a_k	r_k	u_k	v_k
0	216		1	0
1	5	$\lfloor \frac{216}{5} \rfloor = 43$	0	1
2	$216 - 43 \cdot 5 = 1$		$1 - 43 \cdot 0 = 1$	$0 - 43 \cdot 1 = -43$

die ggT-Bedingung $\mathrm{ggT}(216, 5) = 1$ ist also erfüllt, und somit ist

$$1 = 1 \cdot 216 - 43 \cdot 5\,.$$

Mit der Umkehrung der Vorzeichen ergibt sich:

$$1 = 1 \cdot 216 \underline{- 5 \cdot 216} - 43 \cdot 5 \underline{+ 216 \cdot 5} = -4 \cdot 216 + 173 \cdot 5$$

Damit ist $d = 173$ der Exponent des öffentlichen Schlüssels.

$$k_{SEC} = (5, 247)\,,\ k_{PUB} = (173, 247)$$