S. Wewers, S. Wilke

Kryptographie, SS 06

Lösung 7

Aufgabe 1.

(a) Mit $N := 5989$ ist $m := \lfloor \sqrt{N} \rfloor = 77$. Wir betrachten also die Funktion $f(x) := (x+m)^2 - N$ und werten sie auf dem Intervall $\{-5, \ldots, +5\}$ aus. Anschließend sieben wir solange mit wachsendem B, bis die resultierende Matrix der Exponenten der B-glatten Zahlen über $\mathbb{F}_2$ einen nichttrivialen Kern besitzt.

$x+m$	72	73	74	75	76	77	78	79	80	81	82
$f(x)$	-805	-660	-513	-364	-213	-60	95	252	411	572	735
$B=2$		-165		-91		-15		63		143	
$B=3$		-55	-19		-71	-5		7	137		245
$B=5$	-161	-11				-1	19				49
$B=7$	-23			-13				1			1
$B=11$		-1								13	
$B=13$				-1						1	

Die Matrix der Exponenten bzgl. der Faktorbasis $\{-1, 2, 3, 5, 7, 11, 13\}$ sieht damit wie folgt aus:

$x+m$	73	75	77	79	81	82
$B=-1$	1	1	1	0	0	0
$B=2$	2	2	2	2	2	0
$B=3$	1	0	1	2	0	1
$B=5$	1	0	1	0	0	1
$B=7$	0	1	0	1	0	2
$B=11$	1	0	0	0	1	0
$B=13$	0	1	0	0	1	0

Wir reduzieren die Matrix $\bmod 2$ und bestimmen die Zeilen-Stufen-Form:

$$\begin{pmatrix} 1&1&1&0&0&0\\ 0&0&0&0&0&0\\ 1&0&1&0&0&1\\ 1&0&1&0&0&1\\ 0&1&0&1&0&0\\ 1&0&0&0&1&0\\ 0&1&0&0&1&0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1&1&1&0&0&0\\ 1&0&1&0&0&1\\ 1&0&0&0&1&0\\ 0&1&0&1&0&0\\ 0&1&0&0&1&0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1&1&1&0&0&0\\ 0&1&0&0&0&1\\ 0&1&1&0&1&0\\ 0&1&0&1&0&0\\ 0&0&0&1&1&0 \end{pmatrix}$$

$$\rightsquigarrow \begin{pmatrix} 1&1&1&0&0&0\\ 0&1&0&0&0&1\\ 0&0&1&0&1&1\\ 0&0&0&1&0&1\\ 0&0&0&1&1&0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1&1&1&0&0&0\\ 0&1&0&0&0&1\\ 0&0&1&0&1&1\\ 0&0&0&1&0&1\\ 0&0&0&0&1&1 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1&0&0&0&0&1\\ 0&1&0&0&0&1\\ 0&0&1&0&0&0\\ 0&0&0&1&0&1\\ 0&0&0&0&1&1 \end{pmatrix}$$

Wir erhalten also als Kern $\langle (1,1,0,1,1,1)^T \rangle$. Damit erhalten wir

$$73^2 \cdot 75^2 \cdot 79^2 \cdot 81^2 \cdot 82^2 \equiv (-1)^2 \cdot 2^8 \cdot 3^4 \cdot 5^2 \cdot 7^4 \cdot 11^2 \cdot 13^2 \pmod{N}$$

Wir setzen also

$$x := 73 \cdot 75 \cdot 79 \cdot 81 \cdot 82 = 2872831050 \equiv 3574 \pmod{N}$$
$$y := 2^4 \cdot 3^2 \cdot 5 \cdot 7^2 \cdot 11 \cdot 13 = 5045040 \equiv 2302 \pmod{N}$$

Damit ist $\mathrm{ggT}(x-y, N) = \mathrm{ggT}(1272, 5989) = 53$ ein nicht-trivialer Teiler von N. Der zweite Teiler ergibt sich als $\mathrm{ggT}(x+y, N) = \mathrm{ggT}(5876, 5989) = 113$.

(b) Es ist $f(6) = 83^2 - N = 900 = 2^2 \cdot 3^2 \cdot 5^2$. Daraus folgt $83^2 \equiv (2 \cdot 3 \cdot 5)^2 \pmod{N}$. Mit $x := 83$ und $y := 2 \cdot 3 \cdot 5 = 30$ erhalten wir somit $\mathrm{ggT}(x - y, N) = \mathrm{ggT}(53, 5989) = 53$ und $\mathrm{ggT}(x + y, N) = \mathrm{ggT}(113, 5989) = 113$.

Aufgabe 2.

(a) $x^2 + 3x - 22 \equiv 0 \pmod{97}$
Es gilt: $x^2 + 3x - 22 \equiv x^2 + 100x - 22 \equiv x^2 + 100x + 50^2 - (50^2 + 22) \equiv (x + 50)^2 - 2522 \equiv (x + 50)^2 \pmod{97}$, da $2522 = 97 \cdot 26$. Damit ist die Lösung der Gleichung gegeben durch $x \equiv 50 \pmod{97}$.

(b) $x^2 + 6x + 7 \equiv 0 \pmod{23}$
Es gilt: $x^2 + 6x + 7 \equiv x^2 + 6x + 3^2 + (7 - 3^2) \equiv (x + 3)^2 - 2 \pmod{23}$. Nun ist $2^{\frac{23-1}{2}} = 2^{11} = 2048 \equiv -252 \equiv -22 \equiv 1 \pmod{23}$. Damit ist 2 ein quadratischer Rest mod 23, und eine Wurzel von 2 mod 23 ergibt sich als $2^{\frac{23+1}{4}} = 2^6 = 64 \equiv -5 \pmod{23}$. Damit sind die Lösungen der Gleichung gegeben durch $x \equiv -3 \pm 5 \pmod{23}$, also $x \equiv 2 \pmod{23}$ und $x \equiv -8 \pmod{23}$.

(c) $x^2 - 13x - 1 \equiv 0 \pmod{59}$. Es gilt: $x^2 - 13x - 1 \equiv x^2 + 46x - 1 \equiv x^2 + 46x + 23^2 - (23^2 + 1) \equiv (x + 23)^2 - 530 \equiv (x + 23)^2 - 60 \equiv (x + 23)^2 + 1 \pmod{59}$. Nun ist $59 \equiv 3 \pmod{4}$, also ist $(-1)^{\frac{59-1}{2}} = (-1)^{29} = -1$, also ist -1 kein quadratischer Rest mod 59. Somit besitzt die Gleichung keine Lösungen.