Grundkurs Codierung

Lösungsvorschläge zu den Fragen in den Unterkapiteln „Was blieb?“
Stand 03.12.2006

Zu Unterkapitel 2.3, Seite 48

Zu Frage 1: Es ist die Frage zu beantworten, für welche Zahl u die Gleichung

$$(u \cdot 35) \text{ MOD } 74 = 1$$

erfüllt wird? Dazu durchläuft man zunächst den Euklidischen Algorithmus, s. S. 43:

$$74 = 2 \cdot 35 + 4$$
$$35 = 8 \cdot 4 + 3$$
$$4 = 1 \cdot 3 + 1$$
$$3 = 3 \cdot 1 + 0$$

An der “1” in Zeile 3 sieht man zunächst, dass die beiden Zahlen 35 und 74 teilerfremd sind. Sie haben demnach den größten gemeinsamen Teiler ggT(35, 74) =1. Das ist die Voraussetzung dafür, dass überhaupt eine modulare inverse Zahl zu 35 existiert.

Die erste Zahl in Zeile 1 (die “74”) hat den Index “0”, die erste Zahl in Zeile 2 (die “35”) hat den Index 1 usw. Daher hat die zweite “3” in Zeile 4 den Index 4, also ist n = 4. Mit diesen Informationen geht man in die Rekursionsgleichung für z_i auf S. 45. Man erhält $z_2 = 9$ und $z_3 = -19$.

Die modulare inverse Zahl ist demnach u = -19 MOD 74 oder u = 74 - 19 MOD 74 = 55. Probe: (-19 · 35) MOD 74 = - 665 MOD 74 = 75 MOD 74 = 1.

Zu Frage 2: Nein, da 57 = 3 · 19 keine Primzahl ist, s. S. 37 ff.

Zu Frage 3: Über das irreduzible Polynom $f(x) = x^4 + x^3 + x^2 + x + 1$ ist die Nullstelle β als f(β) = 0 mit $f(\beta) = \beta^4 + \beta^3 + \beta^2 + \beta + 1 = 0 \rightarrow \beta^4 = \beta^3 + \beta^2 + \beta + 1$ definiert. Daraus ergeben sich folgende Elemente:

Nr.	Element		alternativ		als Polynom in b		Kurzform
1	0	=	0	=	0	=	0000
2	β^0	=	1	=	$0\cdot\beta^3+0\cdot\beta^2+0\cdot\beta^1+1\cdot\beta^0$	=	0001
3	β^1	=	$\beta^0\cdot\beta$	=	$0\cdot\beta^3+0\cdot\beta^2+1\cdot\beta^1+0\cdot\beta^0$	=	0010
4	β^2	=	$\beta^1\cdot\beta$	=	$0\cdot\beta^3+1\cdot\beta^2+0\cdot\beta^1+0\cdot\beta^0$	=	0100
5	β^3	=	$\beta^2\cdot\beta$	=	$1\cdot\beta^3+0\cdot\beta^2+0\cdot\beta^1+0\cdot\beta^0$	=	1000
6	β^4	=	β^4	=	$1\cdot\beta^3+1\cdot\beta^2+1\cdot\beta^1+1\cdot\beta^0$ **(Definition !)**	=	1111
7	β^5	=	$\beta^4\cdot\beta$	=	$0\cdot\beta^3+0\cdot\beta^2+0\cdot\beta^1+1\cdot\beta^0$	=	0001

siehe dazu auch S. 41 oder die ähnliche Tabelle 3-20 auf S. 124. Die Ordnung dieses Elements ist also ord = 5, da sich nach 5-maliger Potenzierung wieder $\beta^0 = 1$ ergibt. Es ist also **kein** primitives Element und bildet damit auch **keinen Erweiterungskörper**!

Zu Frage 4: **Vorsicht, Falle!** Der Effektivwert (= Wurzel aus dem quadratischer Mittelwert, siehe auch Unterkapitel 1.3, S. 14, "Rauschquelle", sowie Unterkapitel 4.2, S. 249) wird nur dann der Streuung σ (= Standardabweichung) gleich, wenn der Mittelwert $x_{mittel} = 0$ ist. Es gilt: Quadratischer Effektivwert= $x_{mittel}^2 + \sigma^2$. Da alle drei beteiligten Größen positiv sind, wird die Gleichung für die angegebenen Werte nicht erfüllt. Wenn der Mittelwert statt -1.2 [Volt] jedoch -0.2 [Volt] betragen würde, wäre die gesuchte Verteilungsdichtefunktion

$$p(x)=\frac{1}{\sqrt{2\cdot\pi\cdot\sigma^2}}\cdot e^{-\frac{(x-x_{mittel})^2}{2\cdot\sigma^2}}$$

mit x_{mittel} = -0.2 [Volt] und sigma = 0.5^2. Das Rauschsignal hätte dann eine Streuung

$$\sigma=\sqrt{0.5^2-(-0.2)^2}=0.4583\,[\text{Volt}]$$

Zu Frage 5: Das Restpolynom der Division ist $r(x)=(x^7+1)\ \text{MOD}\ (x^3+x^21)=0$ und damit ohne Rest teilbar, siehe auch den Hinweis auf S. 44, Mitte, und das Fermat'sche Theorem, S. 46.

Zu Frage 6: In erster Näherung kann man für die Geburten wegen des menschlichen Zeugungsverhaltens eine Gleichverteilung annehmen. Bei vielen Tierarten ist das durchaus anders! Bei genauerer Untersuchung werden sich aber wohl Schwerpunkte ergeben (man denke an den "Wonnemonat" Mai und seine Folgen im Februar 9 Monate später ...)