DISKRETE MATHEMATIK

Prof. Dr. Thomas Ihringer

Aufgabenblatt Nr. 8

106. Finde ein n mit $30\mathbb{Z}+12\mathbb{Z}=n\mathbb{Z}$.

107. Stelle eine Vermutung auf: Welches $n\in\mathbb{Z}$ muß zu gegebenen $n_1,\dots,n_k\in\mathbb{Z}$ gewählt werden, so daß $n_1\mathbb{Z}+\dots+n_k\mathbb{Z}=n\mathbb{Z}$ gilt?

108. Zeige: Ist R ein kommutativer Ring, dann ist für alle $a_1,\dots,a_k\in R$ die Menge $a_1R+\dots+a_kR=\{a_1r_1+\dots+a_kr_k \mid r_1,\dots,r_k\in R\}$ ein Ideal von R.

109. Sei F der zweielementige Körper und $p(x)=x^6-1$. Welche der Mengen $I_1=\{0, x^4+1, x^5+x, x^5+x^4+x+1\}$ und $I_2=\{0, x^4+x^2+1, x^5+x^3+x, x^5+x^4+x^3+x^2+x+1\}$ ist ein Ideal von $F[x]_{p(x)}$?

---

110. Finde für das Ideal in 109 ein erzeugende Polynom $g(x)$.

111. a) Wieviele Codewörter hat der Code mit Kontrollmatrix $H=\begin{pmatrix}0&0&0&1&1&1&1\\0&1&1&0&0&1&1\\1&0&1&0&1&0&1\end{pmatrix}$?
b) Ist dieser Code zyklisch?

112. Beweise: Jeder Hamming-Code ist <u>ähnlich</u> zu einem zyklischen Hamming-code, d.h. kann durch Vertauschung der Koordinaten zu einem solchen gemacht werden.

113. Beschreibe alle linearen zyklischen Codes der Länge 7 über $F=\{0,1\}$, z.B. durch Angabe der Generatorpolynome.

---

114. Finde für den Code $\mathcal{C}\subseteq F[x]_6$ mit Generatorpolynom $g(x)=1+x^2+x^4$ eine Generatormatrix, das Kontrollpolynom und eine Kontrollmatrix.

115. Decodiere $v(x)=1+x^2+x^4$ und $w(x)=1+x+x^2+x^5$ für den Hammingcode $\mathcal{H}_3$ aus Beispiel 4.7 im Buch, d.h. mit Kontrollmatrix $H=\begin{pmatrix}0&0&1&0&1&1&1\\0&1&0&1&1&1&0\\1&0&0&1&0&1&1\end{pmatrix}$.

116. Welcher Code ergibt sich in Satz 4.10 im Buch für $r=3$?

117. Zeige, daß $(\mathbb{Z}; \oplus, \odot)$ ein Ring ist mit $a\oplus b:=a+b+1$ und $a\odot b:=ab+a+$

H118. Beweise: Sei I ein Ideal von $K[x]_{p(x)}$ und $g(x)$ ein Element minimalen Grads von $I\setminus\{0\}$ (und damit ein erzeugendes Element von I). Dann ist $g(x)$ ein Teiler von $p(x)$ (in $K[x]$).

H119. Finde alle Codewörter des Codes in 114. Was „tut" dieser Code?

*H120. Sei $\mathcal{C}$ ein zyklischer Code über F_q der Länge $n=q^r-1$. Das Generatorpolynom $g(x)$ habe in F_{q^r} genau die Nullstellen $b_1,\dots,b_s$. Zeige, daß für alle $v(x)\in F_q[x]_n$ folgendes gilt:

$$v(x)\in\mathcal{C} \iff v(b_1)=\dots=v(b_s)=0 \quad (\text{in } F_{q^r}).$$