Diskret matematik för F1, 5B1203
alternativ studiegång, VT 2004

UPPGIFTER Nr. 4

Rekommenderade extrauppgifter
(utöver uppgifterna som ges i anslutning till resp. avsnitt)

Avsnitt i Biggs	Uppgifter
23.10	2, 3, 12, 18
24.7	4, 8, 9, 12, 15

Inlämningsuppgifter 4 (inlämnas 11 maj.)

1. Låt F vara en ändlig kropp av ordning q och låt b vara ett primitivt element. Den *diskreta logaritmfunktionen* $\log_b : F^* \to \{0, 1, \ldots, q-2\}$ definieras av

$$k = \log_b x \quad \Longleftrightarrow \quad b^k = x \ , \quad x \in F^*.$$

Bestäm:

(a) $\log_3(15)$ i $\mathbb{Z}_{17}$,

(b) $\log_{2x+1}(x+2)$ i $\mathbb{Z}_3[x]/(x^2+1)$.

2. Låt $f(x) = x^4 + x^3 + x^2 + x + 1$ och $g(x) = x^5 + x^2 + 1$.

(a) Avgör om $f(x)$ är irreducibelt i $\mathbb{Z}_2[x]$. Om så är fallet, avgör om $f(x)$ är ett primitivt polynom.

(b) Avgör om $g(x)$ är irreducibelt i $\mathbb{Z}_2[x]$. Om så är fallet, avgör om $f(x)$ är ett primitivt polynom.

VÄND!

3. Binära koder kan generaliseras till koder som är vektorrum över andra ändliga kroppar. Speciellt kan Hammingkoden konstrueras över $\mathbb{Z}_3$.

Låt H vara en $m \times n$ matris med element i $\mathbb{Z}_3$ där ingen kolonn är en multipel av en annan (speciellt ingår inte en kolonn med bara nollor), och där antalet kolonner är maximalt med avseende på detta.

(a) Bestäm n som funktion av m.

(b) Hamming-avståndet $\partial(x, y)$ mellan två n-tupler $x, y \in \mathbb{Z}_3^n$ definieras som i det binära fallet som antalet positioner där x och y skiljer sig åt. Hur många element i $\mathbb{Z}_3^n$ innehålls i en sfär av radie e med centrum x:

$$S_e(x) = \{y \in \mathbb{Z}_3^n : \partial(x, y) \leq e\} \ ?$$

(c) Matrisen H definierar en kod $C \subseteq \mathbb{Z}_3^n$ via: $x \in C \Leftrightarrow Hx = 0$.
Bestäm minimala avståndet mellan två kodord.

(d) Visa att koden C är perfekt.
(Detta innebär att det existerar ett tal e sådant att för varje $y \in \mathbb{Z}_3^n$ existerar ett unikt $x \in C$ sådant att $y \in S_e(x)$.)