Matematiska Institutionen
KTH

Tentamensskrivning på kursen Algebra och kombinatorik för F3, 5B1302, 14 augusti 2002, klockan 14.00-19.00.

LÖSNINGAR:

1. Då $77 = 11 \cdot 7$ så $m = 10 \cdot 6 = 60$ och det d vi söker satisfierar $13d \equiv_{60} 1$. Med hjälp av Euklides algorithm finner vi att $d = 37$. Vidare har vi $D(2) \equiv_{77} 2^{37} \equiv_{77} 2^{32+4+1}$. Då $2^4 = 16$, $2^8 \equiv_{77} 16^2 \equiv_{77} 256 \equiv_{77} 25$, $2^{16} \equiv_{77} 625 \equiv_{77} 9$ och $2^{32} \equiv_{77} 81 \equiv_{77} 4$ får vi att $D(2) \equiv_{77} 4 \cdot 16 \cdot 2 = 51$.
Svar. $d = 37$ och $D(2) = 51$.

2. a) Matrisen har rangen tre så kodens dimension är $6 - 3 = 3$ och antalet kodord blir då $2^3 = 8$. Eftersom matrisens kolonner är skilda från nollkolonnen och olika är minimiavståndet minst tre. Koden innehåller nollordet och ordet 011100. Alltså är minimiavståndet tre.
Svar. Åtta ord med minimiavståndet tre.

b) Det finns $2^6 = 64$ ord av längd 6. Varje sfär med radien ett runt ett kodord innehåller 1+6=7 kodord. Alltså befiiner sig precis $8 \cdot 7 = 56$ kodord på ett avstånd noll eller ett från något kodord. Precis åtta ord har ett större avstånd.

3. Vi använder inklusion exklusion. Låt A, B och C beteckna mängderna ord som saknar en etta, en två respektive en trea. Låt N beteckna mängden av samtliga ord. Vi söker

$$|N \setminus (A \cup B \cup C)| = |N| - (|A| + |B| + |C|) + (|A \cap B| + |A \cap C| + |B \cap C|) - |A \cap B \cap C|.$$

Multiplikationsprincipen ger $|A| = |B| = |C| = 2^9$, $|A \cap B| = |A \cap C| = |B \cap C| = 2^8$ och $|A \cap B \cap C| = 2^7$. Så
Svar. $2^{10} - 3 \cdot 2^9 + 3 \cdot 2^8 - 2^7 = 128$.

4. a) Skall visa att (i) $a \in I$ och $b \in I$ medför att $a + b \in I$ och (ii) $a \in I$ och $r \in Z_6[x]$ medför att $ra \in I$ och $ar \in I$.

(i) $a = p(x)(x^2 - 1)$ och $b = q(x)(x^2 - 1)$ ger

$$a + b = p(x)(x^2 - 1) + q(x)(x^2 - 1) = (p(x) + q(x))(x^2 - 1)$$

som ju är ett element i I.

(ii) $a = p(x)(x^2 - 1)$ och $r = q(x)$ ger

$$ra = q(x)p(x)(x^2 - 1) = (q(x)p(x))(x^2 - 1) \quad \text{och} \quad ar = p(x)q(x)(x^2 - 1) = (p(x)q(x))(x^2 - 1)$$

som ju också är element i I.

b) Kvotringen har 36 element och vi betraktar, kanske lite trist, samtliga dessa element. Noterar emellertid att produkten av två enheter alltid är en enhet och att en nolldelare aldrig är en enhet samt att en produkt av en nolldelare med ett annat ringelement alltid är en nolldelare.

Noterar också att $x + 1$, $x - 1$, 2, 3 och 4 är nolldelare.

0) Av elementen i Z_6 är bara 1 och 5 enheter.

1) Betraktar polynom av typen $x + a$. $x + 1$ och $x - 1$ är nolldelare. Prövar med $x + 2$. Lite exprimenterande ger att $(x + 2)(x + 4) = x^2 + 2 = 3$ så $(x + 2)2(x + 4) = 0$. Vi har nolldelarna $x+2$ och $x+4$. $(x+3)(x+3) = x^2+3 = 4$ så $(x+3)3(x+3) = 0$. Vi kan sluta att inga polynom av typen $x + a$ är enheter, förutom x, $x \cdot x = 1$.

2) Betraktar polynom av typen $2x + a$. Räcker att undersöka elementen $2x + 1$, $2x + 3$ och $2x + 5$. Vi har $(2x + 1)(ax + b) = (2b + a)x + 2a + b$, så $2x + 1$ enhet om det finns lösning till $2b + a = 0$ och $2a + b = 1$ i Z_6. Adderas ekvationerna får vi $3(a + b) = 1$ vilket är omöjligt i Z_6. Motsvarande ansats för $2x+3$ ger inversen $2x+3$ så $2x+3$ är en enhet. För $2x+5$ finner vi med samma ansats att $2b + 5a = 0$ och $2a + 5b = 1$ vilket ger $3(b - a) = 1$ vilket ju är omöjligt i Z_6.

3) Skall nu bli spännande att se vad fallet $3x + a$ ger för enheter. Vet att polynomen $3x$ och $3x + 3$ är nolldelare. Som i fall 2) får vi enheterna $3x + 2$ och $3x + 4$, och att $3x + 3$ aldrig är en enhet.

Fallen 4) och 5). Noterar att $4x + a = -1(2x - a)$ och $5x + a = -1(x - a)$. Så antalet eneher i dessa fall överenstämmer med antalet enher i fallen 1) och 2).

Vi får

Svar. 2+1+1+2+1+1=8.

c) Betrakta ringen $Z[x]$. Elementet x är varken nolldelare eller enhet.

5. Antag att varje nod har en valens som är minst 5. Låt E beteckna antalet kanter, V antalet noder och $\delta(v)$ valensen hos noden v. Då gäller

$$2E = \sum \delta(v) \geq 5V$$

(med summation över mängden av noder). För sammanhängande planära grafer gäller att

$$E \leq 3V - 6.$$

Kombineras dessa två olikheter får vi

$$\frac{5}{2}V \leq E \leq 3V - 6$$

vilket ger att $V \geq 12$. Då antalet noder är färre än 12 måste vårt antagande vara felaktigt.

6. a) Antag att S_5 verkar på mängden $\{1, 2, 3, 4, 5\}$. Mängden av permutationer som fixerar elementet 5 bildar en delgrupp, precis gruppen S_4. Den har 24 element.

b) Mängden av jämna permutationer bilder en delgrupp till S_5, den s k *alternerande gruppen* A_5. Den har hälften så många element som S_5, d v s 60 element. Den sökta gruppen med 24 element skulle vara en delgrupp till A_5. Enligt Lagranges sats är detta omöjligt.

Svar. Nej.

7. Vi bildar först en kropp med fyra element, nämligen

$$F_4 = Z_2[x]/ < x^2 + x + 1 >,$$

som ju är en kropp eftersom polynomet $x^2 + x + 1$ är irreducibelt i ringen $Z_2[x]$. Vi betraktar nu $F_4[z]$. Med hjälp av polynom $p(z)$ och $q(z)$ av grad två och tre som är irreducibla i ringen $F_4[z]$ kan vi bilda kroppar med 16 respektive 64 element som båda innehåller kroppen F_4:

$$F_{16} = F_4[z]/ < p(z) > \qquad F_{64} = F_4[z]/ < q(z) > .$$

Trial and error ger polynomet $p(z) = z^2 + xz + 1$ som är irreducibelt i $F_4[z]$ eftersom det saknar nollställen i F_4. Polynomet $q(z) = z^3 + x$ är irreducibelt i $F_4[z]$ ty det saknar nollställen i F_4. Kropparna är nu konstruerade.

8. a) Lätt som en plätt. Totalt finns $2+3+2=7$ olika sorters mynt. Multiplikationsprincipen ger **Svar.** 7^n.

b) Låt a_n, b_n och c_n vara antalet tillåtna följder av längd n som börjar med en 10-krona, femkrona respektive enkrona. Vi får då sambanden

$$\left\{\begin{array}{lcl} a_n & = & 2b_{n-1} + 2c_{n-1} \\ b_n & = & 3a_{n-1} + 3c_{n-1} \\ c_n & = & 2a_{n-1} + 2b_{n-1} \end{array}\right.$$

Vi söker ett uttryck för $a_n + b_n + c_n$.

Vi betraktar de genererande funktionerna $A(x)$, $B(x)$ och $C(x)$ för dessa följder. Efter multiplikation med x^n i respektive likhet, och summation över n, med start när $n = 1$, ger systemet ovan sambanden

$$\left\{\begin{array}{lcl} A(x) - a_0 & = & 2xB(x) + 2xC(x) \\ B(x) - b_0 & = & 3xA(x) + 3xC(x) \\ C(x) - c_0 & = & 2xA(x) + 2xB(x) \end{array}\right.$$

Med begynnelsevärdena $a_0 = b_0 = c_0 = 1/2$ blir rekursionen ovan korrekt för $n = 1$. Vi får då systemet

$$\left\{\begin{array}{ccccccc} A(x) & - & 2xB(x) & - & 2xC(x) & = & 1/2 \\ -3xA(x) & + & B(x) & - & 3xC(x) & = & 1/2 \\ -2xA(x) & - & 2xB(x) & + & C(x) & = & 1/2 \end{array}\right.$$

Summerar vi ekvationerna får vi att

$$(1-5x)A(x) + (1-4x)B(x) + (1-5x)C(x) = 3/2.$$

Så svaret ges av

$$A(x) + B(x) + C(x) = \tfrac{3/2 - xB(x)}{1-5x}.$$

Man finner att

$$B(x) = \frac{1-14x}{2(1-2x)(1-6x)}$$

så efter något räknande får vi

$$A(x) + B(x) + C(x) = \tfrac{3-10x}{2(1-2x)(1-6x)}.$$

Partialbråksuppdelning ger

$$A(x) + B(x) + C(x) = \frac{1/2}{1-2x} + \frac{1}{1-6x}.$$

Detta ger

$$a_n + b_n + c_n = \frac{1}{2}2^n + 6^n.$$