Matematiska Institutionen
KTH

Lösningar till tentamensskrivning på kursen Algebra och Kombinatorik för F3, 5B1302, onsdagen den 20 augusti 2003.

1. Det dechiffrerande talet d satisfierar $de \equiv 1 \pmod{120}$ eftersom $143 = 11 \cdot 13$ och $120 = (11-1)(13-1)$. Euklides algoritm ger $120 = 4 \cdot 31 - 4$ och $31 = 8 \cdot 4 - 1$ varur erhålles att $1 = 8 \cdot 4 - 31 = 8(4 \cdot 3 - 120) - 31 = 31 \cdot 31 - 8 \cdot 120$. Alltså är $d = 31$. Vi finner att $2^8 \equiv_{143} -30$, $2^{16} \equiv_{143} 42$, $2^{32} \equiv_{143} 48$. Därur $2^{31} \equiv_{143} 48/2$.

Svar 24.

2. Man finner att a_n är koefficienten för z^n i produkten av polynomen $(z + z^2 + z^3 + \ldots)$, $((z^2) + (z^2)^2 + (z^2)^3 + \ldots)$ och $((z^4 4) + (z^4)^2 + (z^4)^3 + \ldots)$. Dessa polynom är geometriska serier vars summa är respektive

$$\frac{z}{1+z}, \quad \frac{z^2}{1+z^2}, \quad \frac{z^4}{1+z^4}$$

Således

Svar

$$A(z) = \frac{z^7}{(1+z)(1+z^2)(1+z^4)}.$$

3. Trial and error metoden används. Polynomet $x^2 - x - 4$ testas först främst kanske för att då är $x^2 = x + 4$ i den av polynomet definierade kroppen med 49 element. Inga nollställen i Z_7 ger att polynomet är irreducibelt. Det är då primitivt om ordningen av elementet x är 48. Vi gör följande kalkyler

$$x^4 = (x+4)^2 = x^2 + 8x + 16 = (x+4) + (x+2) = 2x - 1$$

$$x^8 = (2x-1)^2 = 4x^2 - 4x + 1 = 4(x+4) - 4x + 1 = 3$$

$$x^{16} = 3^2 = 2$$

$$x^{24} = x^{16}x^8 = 2 \cdot 3 = -1.$$

Ordingen av elementet x är med nödvändighet en delare till talet 48. Då denna ordning enligt kalkylerna ovan varken delar 24 eller 16, så måste ordningen vara 48.

Svar T ex polynomet $x^2 - x - 4$ är primitivt i $Z_7[x]$.

4.Koden skall definieras av en kontrollmatris av formatet 3×7 vars kolonner samtliga är skilda från nollkolonnen och olika. För att de givna orden skall tillhöra koden måste summan av första, andra och tredje kolonnen vara noll och summan av första, femte och sjätte kolonnen vara noll. En sådan kontrollmatris är lätt att ställa upp. Vi får

Svar

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

5. Låt k och r vara hela tal sådana att $a = kb + r$ där $0 \leq r < b$. Kongruensekavationen ovan kan då uttryckas som att

$$p^{kb+r} - 1 - (p^r - 1) \equiv 0 \pmod{p^b - 1}.$$

för något heltal d. Då $p^b \equiv 1 \pmod{p^b - 1}$ är ovanstende ekvivalent med att

$$p^r 1^k - p^r \equiv 0 \pmod{p^b - 1}$$

vilket ju uppenbarligen är sant.
6. a) Av nio positioner skall tre väljas ut till placeringa av E:na, två till A:na osv. Vi får multinomialkoefficienten

Svar a)

$$\binom{9}{3,2,2,1,1}.$$

b)*Fall 1: Tre olika bokstäver i ordet* Välj bland A, N, B, E och L. Antalet möjliga ord är $5 \cdot 4 \cdot 3 = 60$.

Fall 2: Tre lika bokstäver i ordet Enda möjliga ord är AAA.

Fall 3: Två olika bokstäver i ordet Tre möjliga positioner för dubbelbokstaven, tre möjliga val av dubbelbokstav (A, N eller L) och fyra möjligheter för den enstaka bokstaven ger antalet möjliga sådan ord är $3 \cdot 3 \cdot 4 = 36$.

Antalet möjligheter i respektive fall summeras och vi får

Svar b) 60+1+36=97.

c) Bilda ny bokstav som heter AL, så nu har vi åtta bokstäver, bokstäverna AL, A, A N, N, L, B, E, att kombinera ihop till ord som garanterat innehåller delordet AL. Vissa av dessa kommer dessvärre att innehåll två AL som delord. Det första AL:et i kan var bokstaven AL och det andra kombinationen av bokstäverna A och L, eller vice versa. Det ordet kommer alltså med två gånger i vår första uppräkning av ord. För att beräkna antalet ord med två stycken AL bildar vi en andra bokstav AL, sammanlagt alltså sju bokstäver, AL, AL, N, N, B, E och A. Totala antalet ord med dessa sju bokstäver blir

$$\binom{7}{2,2,1,1,1}.$$

Svar c)

$$\binom{8}{1,2,2,1,1,1} - \binom{7}{2,2,1,1,1}.$$

7.Använder rekursiv formel för beräkning av kromatiska polynom. Låt G_e beteckna den graf man får när kanten mellan nod 3 och 4 tas bort och G'_e beteckna den graf som erålls när i grafen G_e noderna 0 och 3 identifieras.
Antalet sätt att färga grafen med λ stycken färger är lika med summan av antalet sätt att färga graferna G_e och G'_e i λ olika färger. Dessa antal är lätta att beräkna

För G_e. Om noden 0 färkas med färgen c_1 så finns $\lambda-1$ möjligheter för noden 5 och $\lambda-2$ möjliga färger för noden 4. För noderna 1, 2 och 3 finns $\lambda - 1$ möjligheter. Totala antalet möjligheter är

$$\lambda(\lambda - 1)^4(\lambda - 2).$$

För G'_e Motsvarande resonemang ger att antalet möjligheter är

$$\lambda(\lambda - 1)^2(\lambda - 2)^2.$$

Med $\lambda = 7$ insatt i summan av ovanstående uttryck får vi

Svar $7(6^4 5 + 6^2 5^2) = 51660$

8. Identitetselementet i G är elementet $(1, 1, \ldots, 1)$. Ett element α_i i kroppen F_{p_i} är inverterbart precis då $\alpha_i \neq 0$. Elmenten i G är alltså de element $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ där $\alpha_i \neq 0$ för $i = 1, 2, \ldots, k$. Således antalet element i G är

$$|G| = \prod_i^k (p_i - 1).$$

Nu gäller

(i) *Om H är en delgrupp till G så gäller att mängden*

$$H_i = \{h_i \in F_{p_i} \mid (h_1, h_2, \ldots, h_k) \in H\}$$

bildar en delgrupp till den multiplikativa gruppen $F_{p_i}^*$ i F_{p_i}.

Denna grupp $F_{p_i}^*$ är cyklisk med $p_i - 1$ stycken element. Alltså gäller enligt känt eller lättbevist faktum att

(ii) *För varje delare d_i till en cyklisk grupp med $p_i - 1$ stycken element finns precis en delgrupp, och inga andra delgrupper finns.*

Den slutsats vi kan dra av (i) och (ii) är till varje uppättning av tal d_1, d_2, ..., d_k som är delare till respektive p_1, p_2, ..., p_k så finns en delgrupp H med $\prod_{i=1}^k d_i$ element sådan att H_i, (se definition ovan), har d_i element och är en delgrupp till $F_{p_i}^*$ för $i = 1, 2, \ldots, k$.