Matematiska Institutionen
KTH

Lösningar till tentamensskrivning på kursen Algebra och Kombinatorik för F3, 5B1302, måndagen den 12 januari 2004.

1. $I_0 = \{0\}$, $I_1 = Z_{56}$, $I_2 = \{2, 4, 6, \ldots, 54, 0\}$, $I_4 = \{4, 8, 12, \ldots, 52, 0\}$ och t ex $I_{28} = \{28, 0\}$.

2. Koden är linjär med dimension $5 - rang(H) = 2$ och innehåller då $2^2 = 4$ olika ord.

Då $H(1, 1, 1, 1, 0)^T = (0, 0, 1)^T$, H:s tredjekolonn, således skiljer sig det givna ordet från ett kodord i tredje positionen. Det rättade ordet blir alltså 11010.

Trial and error, t ex, ger att ordet 01001 inte går att rätta eftersom $H(0, 1, 0, 0, 1)^T = (1, 0, 0)^T$ vilket inte är någon av H:s kolonner.

Antalet ord på avstånd ett från ett kodord är fem. Antal kodord är fyra och antal ord som går att rätta $4 + 4 \cdot 5 = 24$. Antalet ord som inte går att rätta blir då totala antalet ord minus 24 dvs 8.

3. Låt e och v beteckna antalet kanter respektive antalet noder. Vi har följande samband för givna grafen:

$3v = 2e$ (på grund av regulariteten),

$v + 6 - 2 = e$ (Eulers formel).

Ett linjärt ekvationssystem för v och e med precis en lösning.

4. a) Om kula nr 1 och kula nr 2 skulle ligga i samma hög skulle man ha att fördela åtta olika objekt i tre icketomma högar vilket går på $S(8, 3)$ olika sätt. Totalt finns $S(9, 3)$ olika sätt. Så svar blir $S(9, 3) - S(8, 3)$. Använder nu rekursionen $S(n, k) = S(n - 1, k - 1) + kS(n - 1, k)$ för att beräkna Stirlingtalen.

$S(9, 3) = S(8, 2) + 3S(8, 3)$.

Så svaret ges av $S(8, 2) + 2S(8, 3)$. Kommer nu ihåg att $S(n, 2) = 2^{n-1} - 1$.

$S(8, 3) = S(7, 2) + 3S(7, 3) = 63 + 3S(7, 3)$.

$S(7, 3) = 31 + 3S(6, 3)$.

$S(6, 3) = 15 + 3S(5, 3)$.

$S(5, 3) = 7 + 3S(4, 3) = 7 + 3 \cdot 6 = 25$.

Således har vi svaret 2059 på denna fråga.

b) Om högarna vore etiketterade skulle svaret ges av $\binom{9}{3}\binom{6}{3}\binom{3}{3} = 1680$. Antalet sätt att sätta etiketter på tre högar är $3! = 6$. Så svar $1680/6 = 280$

c) Placera ut kula nummer ett och kula nummer två i varsin hög. Övriga sex kulor skall placeras i tre olika högar. Antalet sätt att välja kulor till högen innehållande kula nummer ett är $\binom{7}{2}$. Att välja två kulor till högen innehållande kula nummer två går på $\binom{5}{2}$ olika sätt. Så svar på denna deluppgift är $\binom{7}{2}\binom{5}{2} = 210$.

5. Vi vet att Z_{143} är isomorf med ringen $Z_{11} \times Z_{13}$ och om φ betecknar isomorfin så

$$\varphi(x) = (x_1, x_2) \quad \text{där} \quad x \equiv x_1 \pmod{11} \quad \text{och} \quad x \equiv x_2 \pmod{13}.$$

Parallellt löser vi alltså problemen

$$x_1^{12} + x_1 + 1 \equiv 0 \pmod{11} \quad \text{och} \quad x_2^{12} + x_2 + 1 \equiv 0 \pmod{13}.$$

Fermats lilla sats ger att ovanstående problem kan formuleras

$$x_1^2 + x_1 + 1 \equiv 0 \pmod{11} \quad \text{och} \quad 1 + x_2 + 1 \equiv 0 \pmod{13}.$$

Enda möjligheten för x_2 är att $x_2 = 11$ men andragradsekvationen för x_1 saknar lösningar. Då $\varphi(0) = 0$ så gäller om $x^{12} + x + 1 = 0$ i ringen Z_{143} så måste $\varphi(x^{12}) + \varphi(x) + \varphi(1) = 0$ i $Z_{11} \times Z_{13}$. Alltså kan ingen lösning finnas.

6. Snittet mellan två grupper är alltid en grupp, se läroboken. Då H därmed är en delgrupp till både G_1 och G_2 så måste, enligt Lagranges sats, antalet element i H dela antalet element i både G_1 och G_2. Enda möjligheten är att $|H|$ är en delare till 35.

Alla grupper med primtalsordning är cykliska, efterom då har varje element skilt från identiteten en ordning som delar gruppens ordning. Enda möjligheten för att H inte skulle vara cyklisk vore om H bestod av 35 element. Nu finns flera möjligheter till fortsättning av lösningen.

Antag alla element har ordning ett eller fem. Då skulle varje element i H tillhöra en cyklisk delgrupp med fem element. Snittet mellan två sådana grupper vore identiteten. Dessa delgruppers union skulle då ha $n \cdot 4 + 1$ stycken element där n betecknar antalet delgrupper. Då vore $n = (35 - 1)/4$ vilket ju är omöjligt. På precis samma sätt inses att inte alla element i H kan ha ordning sju. Enda möjligheten som kvarstår är att det finns element med ordning 35 i gruppen. Den är då cyklisk.

7. Den största gemensamma delaren till talen 63 och 105 är 21. Euklides algoritm ger på sedvanligt sätt att

$$21 = 2 \cdot 63 - 1 \cdot 105.$$

Då $105 \cdot 63 - 63 \cdot 105 = 0$, får vi en andra lösning

$$21 + 0 = 107 \cdot 63 - 64 \cdot 105.$$

Den största gemensamma delaren till talen 21 och 401 är ett och vi får, med Euklides algoritm,

$$2 = 1 \cdot 401 - 19 \cdot 21.$$

Sätt ihop ekvationerna ovan och vi har t ex (obs flera lösningar finns):

$$1 \cdot 401 - 38 \cdot 63 + 19 \cdot 105 = 2 \quad \text{och} \quad 1 \cdot 401 - 2033 \cdot 63 + 1216 \cdot 105 = 2.$$

8. Eftersom den sökta kroppen F skall innehålla Z_2 som delkropp så måste antalet element i F vara en potens av två. Vi povar med lite trial and error. Rötterna måste finnas i den multiplikativa gruppen. Vi vet att den är cyklisk. Rötternas ordning måste vara fem (eller en delare till fem). Den multiplikativa gruppens ordning måste delas av talet fem. De multiplikativa grupperna till kropparna med fyra resp åtta element har tre resp sju element och kan inte komma ifråga. Kroppen F_{16} har en multiplikativ grupp med 15 element. Om elementet γ genererar denaa grupp så satisfierar de fem olika elementen $\alpha_i = \gamma^{3i}$, för $i = 1, 2, 3, 4, 5$, ekvationen $z^5 = 1$. Faktorsatsen gäller i polynomringen $F_{15}[z]$ och således har vi i denna polynomring faktoriseingen

$$p(z) = (z - \alpha_1)(z - \alpha_2)(z - \alpha_3)(z - \alpha_4)(z - \alpha_5).$$