LÖSNINGAR till tentamensskrivning på kursen Algebra och kombinatorik för F3, 5B1302, 25 maj 2000.

1. $91x+41 \equiv 18 \pmod{101}$ ger att $x \equiv 91^{-1}(18-41) \pmod{101}$. Från Euklides algoritm för talen 101 och 91 erhålles $91^{-1} = 10$ och man får att $x \equiv -230 \pmod{101}$. Således

SVAR: $x = -230 + n101$ där n godtyckligt heltal.

2. a) $\alpha\beta =$(1 4 3 2)(5).
b) $\psi = \beta\alpha^{-1}$=(1 3 4)(2 5)(1 5 2 4 3)=(1 2)(3)(4)(5).

3. a) Vi skall välja tre platser av tio till de tre M:n, tre platser till de tre O:na och tre platser till de tre R:na. Svaret ges då av en multinomialkoefficient som är lika med talet

$$\frac{10!}{3!3!3!1!}$$

som enkelt förkortas till SVAR: 16800.

b) Vi kommer att använda inklusion exklusion. Låt M, R och O beteckna mängderna av de ord där man har tre stycken M, R respektive O i rad. Svaret ges då av

$$16800 - (|M| + |R| + |O|) + (|M \cap R| + |R \cap O| + |M \cap O|) - |M \cap R \cap O|.$$

Tänker vi oss bokstäverna som bokstavsklossar och klistrar i hop de tre M:en till en enda kloss får vi med samma motivering som i uppgift a) att $|M| = 8!/3!3! = 1120$. Mängderna R och O är förstås lika stora. Med samma teknik erhålles $|M \cap R| = 6!/3! = 120$ och $|M \cap R \cap O| = 4! = 24$.

SVAR:16800-3360+360-24=13476.

4. En alternerande stig är $a2, 2b, b4, 4d, d1$. Ersätter vi kanterna $2b$ och $4d$ i matchningen M med kanterna $a2, b4$ och $d1$ så erhåller vi alltså en större matchning innehållande fem kanter. Då $|a,b,c,d| - |J(a,b,c,d)| = 1$ så finns enligt sats i boken ingen matchning med fler än 6-1 kanter. Alltså är vår funna matchning maximal.

5. Vi får tre olika fall att reda ut: *fall 1:* Alla klossar i en rad; *fall 2:* en rektangel med sidorna två respektive åtta klossar; *fall 3:* en kvadrat.

I samtliga fall använder vi oss av att antalet olika färgläggningar är

$$\frac{1}{|G|}\sum_{g\in G} F(g)$$

där $F(g)$ är antalet färgläggningar som fixeras av vridningen g.

fall 1: (Alla klossar i en rad) $G = \{id, \phi\}$ där ϕ betecknar vridning ett halvt varv. Om en färgläggning skall fixeras av ϕ måste kloss nummer i ha samma färg som kloss nummer $16-i$. För varje kloss finns tre möjliga färger. Således $F(\phi) = 3^8$. Då $F(id) = 3^{16}$ så finns

$$\frac{1}{2}(3^{16} + 3^8)$$

olika utläggningar i fallet 1.

fall 2: (rektangel med sidan 2) $G = \{id, \phi\}$ där ϕ som i fall 1. Om en färgläggning skall fixeras av ϕ måste kloss i position (i, j) ha samma färg som klossen succesivt speglad i båda av rektangelns axlar. För varje kloss finns tre möjliga färger. Således $F(\phi) = 3^8$ Då $F(id) = 3^{16}$ så finns

$$\frac{1}{2}(3^{16} + 3^8)$$

olika utläggningar i fallet 2.

fall 3: (kvadrat) $G = \{id, \psi, \psi^2, \psi^3\}$ där ψ betecknar vridning ett kvarts varv. Om en färgläggning skall fixeras av ψ^k måste kloss i position (i, j) ha samma färg som motsvarande kloss ett k st kvarts varv bort. För varje kloss finns tre möjliga färger. Således $F(\psi) = 3^4$, $F(\psi^3) = 3^4$ och $F(\psi^2) = 3^8$. Då $F(id) = 3^{16}$ så finns

$$\frac{1}{2}(3^{16} + 3^8 + 3^4 + 3^4)$$

olika utläggningar i fallet 3.

SVAR: $\frac{1}{2}(3^{16} + 3^8 + 3^{16} + 3^8 + 3^{16} + 3^8 + 3^4 + 3^4)$.

6. a) Om det vore primitivt skulle elementet x ha ordning 24 i den kropp med 25 element som ges av polynomet. Vi vet att x måste ha en ordning som delar 24, dvs ordningarna 1, 2, 3, 4, 6, 8, 12 eller 24. Sedvanliga kalkyler ger att

$$x^2 = 4x + 3,\ x^3 = 4x + 2,\ x^4 = 3x + 2,\ x^6 = (4x + 2)^2 = 2,\ x^{12} = 2^2 = -1.$$

Om x^8 vore lika med 1 skulle x^4 vara lika med -1 ty -1 är enda element jämte 1 som löser ekvationen $z^2 = 1$.

Vi kan således sluta oss till att x varken har ordning, 1, 2, 3, 4, 6, 8, eller 12. Enda möjligheten är då att x:s ordning är 24.

b) Vi sätter polynomet lika med noll för att söka hitta nollställen. Kvadratkomplettering ger ekvationen

$$(z + 3x)^2 + 1 - 9x^2 = 0$$

som förenklas till ekvationen

$$(z + 3x)^2 = x + 1.$$

Vi undersöker nu om det finns element i F vars kvadrat är lika med $x + 1$. Kvadraterna äro potenserna x^{2k} där k är ett heltal varav några har vi redan räknat ut. Med hjälp av räkningarna i uppgift a) får vi de återstående 2-potenserna av x:

$$x^8 = x^6x^2 = 2(4x + 3),\ x^{10} = x^6x^4 = 2(3x + 2),\ x^{14} = x^{12}x^2 = -1(4x + 3),$$

$$x^{16} = x^{12}x^4 = -1(3x + 2),\ x^{18} = x^{12}x^6 = -2,$$

$$x^{20} = x^{18}x^2 = -2(4x + 3),\ x^{22} = x^{18}x^4 = -2(3x + 2).$$

.

Ingen 2-potens är lika med $x + 1$ och givna polynomet saknar nollställen i F och är då p gr a att graden är två irreducibelt.

SVAR: Polynomet är irreducibelt.

7. SVAR: Ja

Motivering: Låt $c_1,\ c_2,\ ...,\ c_k$ vara en bas för den linjära koden C dvs om $d \in C$ så är d en linjärkombination av dessa ord.

Låt C' vara mängden av linjärkombinationer av orden $c_1,\ c_2,\ ...,\ c_k$ och ordet c. Det räcker att visa att kodens minimalvikt är minst tre eftersom koden är linjär. Om någon linjärkombination $\lambda_1 c_1 + \lambda_2 c_2 + ... + \lambda_k c_k + \lambda c$ av dessa ord skulle ha en lägre vikt än tre skulle avståndet mellan orden $\lambda_1 c_1 + \lambda_2 c_2 + ... + \lambda_k c_k$ och λc vara mindre än tre där $\lambda = 0$ eller 1. Detta beror på att $d(x, y) = w(x + y)$. Således måste minimalvikten i C' vara tre.

8. Betrakta ringen $Z_{p^n - 1}$. Då sgd$(p, p^n - 1) = 1$ så ligger p i gruppen G av enheter i denna ring. Då $p^n = 1$ och $p^k \neq 1$ för $k < n$ så är $p : s$ ordning i gruppen G lika med n. Antalet element i G är just $\phi(p^n - 1)$ och enligt välkänd sats så har varje gruppelement en ordning som delar antalet element i gruppen.