Matematiska Institutionen
KTH

**Lösningar till tentamensskrivning på kursen Algebra och Kombinatorik för F3, 5B1302, onsdagen den 8 januari 2003.**

1. Ansätt, enligt receptet i kinesiska restsatsmetoden,

$$x = a \cdot 35 \cdot 61 + b \cdot 27 \cdot 61 + c \cdot 27 \cdot 35 + n \cdot 27 \cdot 35 \cdot 61.$$

Räkna modulo 27, 35 och 61. Man får ekvationerna

$$4 \equiv_{27} 2a, \qquad 28 \equiv_{35} 2b, \qquad 1 \equiv_{61} -31c.$$

Detta ger att $a = 2$, $b = 14$ och $c = -2$. Så

**SVAR:** $x = 2 \cdot 35 \cdot 61 + 14 \cdot 27 \cdot 61 - 2 \cdot 27 \cdot 35 + n \cdot 27 \cdot 35 \cdot 61 = 26438 + n \cdot 57645$

b) Vi primfaktoriserar $1010 = 2 \cdot 5 \cdot 101$.
$x \equiv 408^{2004} \pmod{1010}$ är ekvivalent med systemet $\begin{cases} x \equiv 408^{2004} \pmod 2 \\ x \equiv 408^{2004} \pmod 5 \\ x \equiv 408^{2004} \pmod{101} \end{cases}$ Vi finner med hjälp av Fermats lilla sats m.m. att $408^{2004}$ är kongruent med 0 (mod 2), kongruent med 1 (mod 5) och kongruent med 54 (mod 101). Systemet kan alltså ekvivalent skrivas $\begin{cases} x \equiv 0 \pmod 2 \\ x \equiv 1 \pmod 5 \\ x \equiv 54 \pmod{101} \end{cases}$
Vi löser detta med beteckningar enligt kompletteringskompendiet:
$M = 2 \cdot 5 \cdot 101,\ M_1 = 505,\ M_2 = 202,\ M_3 = 10,$
$y_1 = ...$ (behöver ej räknas ut),
$y_2 = b_2 M_2 \equiv 1 \pmod 5$, t.ex. $b_2 = 3,\ y_2 = 606$
$y_3 = b_3 M_3 \equiv 1 \pmod{101}$, t.ex. $b_3 = -10,\ y_3 = -100$. Detta ger $x = 0 \cdot y_1 + 1 \cdot y_2 + 54 \cdot y_3 = 606 - 5400 \equiv 606 - 5400 + 5 \cdot 1010 \pmod{1010}$. Detta uträknas till 256, vilket är svaret på uppgiften.

2. Då $n = 143 = 11 \cdot 13$ så $m = (11-1) \cdot (13-1) = 120$. RSA-parametrarna $d$ och $e$ satisfierar då $e \cdot d \equiv_{120} 1$. Då $e = 11$ ger t ex en enkel prövning att $d = 11$. Om $E(k) = 2$ så $k = D(E(k)) = D(2) = 2^{11} = 46$ i ringen $Z_{143}$

**SVAR:** 46.

3. Valenssumman $1+1+1+1+1+3+2+2+4+4 = 20$ vilket ger att antalet kanter i grafen är 10. I ett träd gäller alltid att antalet kanter är ett mindre än antalet noder. Men antalet noder var 10.

4. a) **SVAR:** Multinomialkoefficienten

$$\binom{8}{2,2,2,2} = 2520$$

.

b) (2p) Hur många av orden ovan innehåller inte någon av kombinationerna aa, bb, cc eller dd. Vi använder metoden med inklusion och exklusion. Låt $A$ beteckna mängden ord som innehåller kombinationen aa och motsvarande för mängderna $B$, $C$ och $D$.

Det sökta svaret ges av

$$2520 - |A \cup B \cup C \cup D|$$

där, enligt inklusion exklusionen,

$$|A\cup B\cup C\cup D| = (|A|+|B|+|C|+|D|)-(|A\cap B|+|A\cap C|+|A\cap D|+|B\cap C|+|B\cap D|+|C\cap D|)+$$

$$(|A \cap B \cap C| + |A \cap B \cap D| + |A \cap C \cap D| + |B \cap C \cap D|) - |A \cap B \cap C \cap D|.$$

När vi gör våra beräkningar kan vi vid behof tänka oss bokstäverna a och a ihopklistrade till bokstaven aa, och likadant för b, c och d. Då får man som ovan

$$|A| = |B| = |C| = |D| = \binom{7}{1,2,2,2} = 630$$

$$|A \cap B| = \ldots = |C \cap D| = \binom{6}{1,1,2,2} = 180$$

$$|A \cap B \cap C| = \ldots = |B \cap C \cap D| = \binom{5}{1,1,1,2} = 60$$

$$|A \cap B \cap C \cap D| = 4! = 24.$$

Så

**SVAR.** $2520 - 4 \cdot 630 + 6 \cdot 180 - 4 \cdot 60 + 24 = 864.$

5. Eftersom den beskrivna mängden är en delmängd till en ring behöver vi inte kontrollera att räknelagarna för en ring gäller. Eftersom summan av två uppåt triangulära matriser är en uppåt triangulär matris så är mängden sluten med avseende på addition. För multiplikationen får vi

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} = \begin{pmatrix} aa' & ab' + bc' \\ 0 & cc' \end{pmatrix}. \qquad (A)$$

Uppenbarligen är ringen sluten med avseende på multiplikationen också. Eftersom $ab' + bc'$ inte alltid är lika med $a'b + b'c$ så är ringen inte kommutativ. Då

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \cdot \begin{pmatrix} -a & -b \\ 0 & -c \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

så har varje element en additiv invers. Vi övergår nu till idealen.

Varje ideal är en additiv delgrupp till ringen. Då $R$ har 27 element så består eventuella ideal av tre eller nio element, med undantag för de triviala idealen.

Vi konstaterar först med hjälp av $(A)$ att mängden av matriser

$$\begin{pmatrix} 0 & b' \\ 0 & 0 \end{pmatrix} \quad \text{där} \quad b' \in Z_3$$

bildar ett vänster ideal bestående av tre element. Likaledes bildar mängderna

$$\begin{pmatrix} a' & b' \\ 0 & 0 \end{pmatrix} \quad \text{där} \quad a', b' \in Z_3$$

och

$$\begin{pmatrix} 0 & b' \\ 0 & c' \end{pmatrix} \quad \text{där} \quad b', c' \in Z_3$$

vänsterideal i ringen $R$. Då systemen

$$ab' + bc' = x$$

$$cc' = y$$

är lösbara för varje val av $b'$ och $c' \neq 0$ så innehåller det andra idealet nio element. Den första likaså.

Antag nu att ett ideal $I$ innehåller matrisen

$$\begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} \quad \text{där} \quad a', b', c' \in Z_3$$

och där $a' \neq 0$ och $c' \neq 0$. Det går då alltid att hitta $a \neq 0$ och $b$ så att $ab' + bc' = 0$. Idealet $I$ måste då även innehålla matrisen

$$\begin{pmatrix} aa' & 0 \\ 0 & c' \end{pmatrix} \quad \text{där} \quad aa' \neq 0 \quad .$$

Multiplicerar vi nu denna matris till vänster med matrisen

$$\begin{pmatrix} (aa')^{-1} & 0 \\ 0 & (c')^{-1} \end{pmatrix}$$

får vi identitetsmatrisen och $I = R$.

Alla ideal är nu bestämda. Vi testar vilka som är högerideal. Använder vi $(A)$ ånyo finner vi att samtliga ideal också är högerideal.

6. Brädets automorfigrupp består av åtta element:

$id$

$\varphi = (1 \quad 3 \quad 9 \quad 7)(2 \quad 6 \quad 8 \quad 4)$

$\varphi^2 = (1 \quad 9)(3 \quad 7)(2 \quad 8)(4 \quad 6)$

$\varphi^3 = (1 \quad 7 \quad 9 \quad 3)(2 \quad 4 \quad 8 \quad 6)$

$\psi = (1 \quad 3)(4 \quad 6)(7 \quad 9)$

$\gamma = (1 \quad 7)(2 \quad 8)(3 \quad 9)$

$\delta = (3 \quad 7)(2 \quad 4)(6 \quad 8)$

$\epsilon = (1 \quad 9)(2 \quad 6)(4 \quad 8).$

Antalet olika färgläggningar som fixeras av identiteten är $2^9 = 512$. Antalet färgläggningar som fixeras av $\varphi$ är 8 eftersom rutor som tillhör samma cykel i $\varphi$ mste ha samma färg. På samma sätt får vi att antalet fixerade färgläggningar blir fÖr respektive automorfi, i den ovan givna ordningsföljden, 32, 8, 64, 64, 64, 64.

Totala antalet färgläggningar blir då

**SVAR:** $\frac{1}{8}(512+8+32+8+64+64+64+64) = 104$.

7. Enligt Lagranges sats måste talen 24 och 30 dela antalet element i den cykliska gruppen $C$, till vilken $G$ och $H$ är delgrupper. Detta ger att antalet element i $C$ är en multipel av 120, $|C| = n \cdot 120$ och $C = \{c, c^2, \ldots, c^{120n} = 1\}$. Då gäller att

$$G = \{c^{5n}, (c^{5n})^2, \ldots, (c^{5n})^{24} = e\},$$

$$H = \{c^{4n}, (c^{4n})^2, \ldots, (c^{4n})^{30} = e\}.$$

Om elementet $d$ tillhör både $H$ och $G$ så

$$d = (c^{5n})^t = (c^{4n})^s$$

för några hela tal $s$ och $t$. Vi får ekvationen $5nt = 4ns$ där $1 \leq t \leq 24$ och $1 \leq s \leq 30$. Vi ser att lösningen till denna ekvation blir precis och alltid

**SVAR:** $t$ =4, 8, 12, 16, 20 och 24 samt att elementen $a^4$, $a^8$, ..., $a^{20}$ och $e$ är de gemensamma elementen.

8. Polynomet ifråga kontrolleras lätt vara primitivt. Kroppen $F$ består då av elementen $0, x, x^2$, $x^3, \ldots, x^{15} = 1$. Om $z^5 = (x^k)^5 = 1$ så gäller att $5k$ är en multipel av 15. Detta ger att enda möjliga värdena för talet $k$ är 3, 6, 9 och 12. Vi får

$$x^5 = x^2 + x, \quad x^6 = x^3 + x^2, \quad x^9 = x^3(x^3 + x^2) = x^6 + x^5 = x^3 + x^2 + x^2 + x = x^3 + x,$$

$$x^{12} = x^3(x^3 + x) = x^3 + x^2 + x + 1.$$

Så

**SVAR:** $x^3$, $x^3 + x^2$, $x^3 + x$ och $x^3 + x^2 + x + 1$.