Matematik, KTH
B.Ek

Lösningar tentan TENA SF1630(/1631) DISKRET MATEMATIK, D(, F)
11 december 2012
Tryckfel kan förekomma.

1) (3p) Givet ett RSA-system med de offentliga parametrarna $n = 143$ och $e = 103$, skall vi dekryptera meddelandena 2, 3 och 4.

Lösning:
$n = 11 \cdot 13$ (båda primtal) ger $m = 10 \cdot 12 = 120$. För att bestämma dekrypteringsparametern d använder vi Euklides algoritm, $120 = 1 \cdot 103 + 17$, $103 = 6 \cdot 17 + 1$, (så $\text{sgd}(120, 103) = 1$, $e = 103$ fungerar verkligen och) $1 = 103 - 6 \cdot 17 = 103 - 6(120 - 103) = 7 \cdot 103 - 6 \cdot 120$ och vi tar $d = 7$. Det ger $2^7 = 128$, $3^7 = 3^5 \cdot 3^2 = 243 \cdot 3 \cdot 3 \equiv_{143} 100 \cdot 3 \cdot 3 = 300 \cdot 3 \equiv_{143} 14 \cdot 3 = 42$ och $4^7 = 128^2 \equiv_{143} (-15)^2 = 225 \equiv_{143} 82$, så $D(2) = 128$, $D(3) = 42$, $D(4) = 82$.

Svar: De krypterade meddelande 2, 3 och 4 dekrypteras som 128, 42 och 82.

---

2) (3p) Vi skall avgöra om 32 genererar $(G, \cdot) = (U(\mathbb{Z}_{697}, \cdot)$, gruppen av inverterbara element i $\mathbb{Z}_{697}$. $[697 = 17 \cdot 41]$

Lösning:
$|G| = \phi(697) = 16 \cdot 40$, så alla $x \in G$ uppfyller $x^{16 \cdot 40} = 1$. Eftersom $\text{sgd}(2, 697) = 1$ gäller $2 \in G$, så $1 = 2^{16 \cdot 40} = (2^5)^{16 \cdot 8} = 32^{16 \cdot 8}$ och $o(32) < |G|$. 32 genererar alltså **inte** G.

Svar: 32 genererar inte $(U(\mathbb{Z}_{697}), \cdot)$.

---

3) (3p) $(G, \cdot)$ är en grupp och vi skall visa att om $a \in G$ är det enda elementet i G som har ordning k, så ligger a i G:s centrum, dvs $ga = ag$ för alla $g \in G$.

Lösning:
Låt $g \in G$. $(gag^{-1})^m = ga^m g^{-1}$, så $(gag^{-1})^m = 1 \Leftrightarrow a^m = 1$. Det betyder att gag^{-1} och a har samma ordning, så enligt förutsättningarna är $gag^{-1} = a$, dvs $ga = ag$. g var godtyckligt i G, så **saken är klar.**
(I själva verket måste k vara 1 eller 2. a och a^{-1} har alltid samma ordning, så $a = a^{-1}$ och alltså $a^2 = 1$.)

---

4) (3p) $(R, +, \cdot)$ är en ring vars additiva grupp $(R, +)$ är cyklisk. Vi skall visa att R är kommutativ under multiplikationen, $a \cdot b = b \cdot a$ för alla $a, b \in R$.

Lösning:
Låt $(R, +)$ genereras av c och låt $a, b \in R$. Då är $a = \underbrace{c + c + \ldots + c}_{m \text{ st}}$ och $b = \underbrace{c + c + \ldots + c}_{n \text{ st}}$ för några $m, n \in \mathbb{Z}$ (om t.ex. $m < 0$ skall $\underbrace{c + c + \ldots + c}_{m \text{ st}}$ tolkas som $\underbrace{(-c) + (-c) + \ldots + (-c)}_{-m \text{ st}}$). Då fås med distributiva lagen att $a \cdot b = \underbrace{c \cdot b + c \cdot b + \ldots + c \cdot b}_{m \text{ st}} = \underbrace{c^2 + c^2 + \ldots + c^2}_{m \cdot n \text{ st}} = \underbrace{c^2 + c^2 + \ldots + c^2}_{n \cdot m \text{ st}} = b \cdot a$. **Saken är klar.**

---

5) Koden $\mathcal{C}$ definieras av kontrollmatrisen $H = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix}$. Vi söker (a, 1p) antalet ord i $\mathcal{C}$ och (b, 2p) de sända orden då 10110, 11011, 01101 togs emot med högst ett fel i varje.

Lösning:
H:s rader är linjärt oberoende (se tredje och fjärde positionerna), så rangen är 3 och kodens dimension $5 - 3 = 2$, så antalet ord $|\mathcal{C}| = 2^2 = 4$.
Eftersom $H(10110)^T = (011)^T =$ kolonn 2, $H(11011)^T = (011)^T =$ kolonn 2, $H(01101)^T = (000)^T$, har det blivit fel i positionerna 2, 2 och ingenstans.
Svar a: $|\mathcal{C}| = 4$, b: De sända orden var 11110, 10011, 01101.

---

6) Vi har $f(x) = x^4 + 3x^3 + x^2 + x + 3$ och $g(x) = x^4 + 4x^3 + 3x^2 + 2x + 4$ i $\mathbb{Z}_5[x]$ och söker (a, 2p) den monadiska största gemensamma delaren $k(x)$ till $f(x)$ och $g(x)$ och (b, 2p) $\lambda(x), \mu(x) \in \mathbb{Z}_5[x]$ så att $k(x) = \lambda(x)f(x) + \mu(x)g(x)$.

Lösning:
Vi använder Euklides algoritm för att finna en största gemensam delare.
Polynomdivisioner ger $f(x) = 1 \cdot g(x) + h(x)$ med $h(x) = 4x^3 + 3x^2 + 4x + 4$,
$g(x) = (4x + 3)h(x) + i(x)$ med $i(x) = 3x^2 + 4x + 2$ och sedan $h(x) = (3x + 2)i(x)$.
$i(x)$ är alltså en största gemensam delare till $f(x)$ och $g(x)$ och $i(x) = g(x) - (4x+3)h(x) = g(x)+(x+2)h(x) = g(x)+(x+2)(f(x)+4g(x)) = (x+2)f(x)+(4x+4)g(x)$. Den monadiska sgd:n $k(x)$ får vi genom att multiplicera med $3^{-1} = 2$. Den blir $k(x) = x^2 + 3x + 4 = (2x + 4)f(x) + (3x + 3)g(x)$.

Svar a: $k(x) = x^2 + 3x + 4$, b: $\lambda(x) = 2x + 4$, $\mu(x) = 3x + 3$.

---

7) (4p) En kub skall få en enfärgad kula i varje hörn. Vi söker antalet väsentligt olika sätt det kan ske om man får använda högst en röd kula och godtyckliga antal kulor med k andra färger.

Lösning:
Vi använder Burnsides lemma (Thm 21.4 i Biggs). Symmetrigruppen G har 24 element ($|Gx||G_x| = 8 \cdot 3 = 24$ om x är ett av kubens hörn):
identitets"rotationen" id,
8 rotationer $\frac{2\pi}{3}$ kring axlar genom motsatta hörn rot_{hh},
6 rotationer π kring axlar genom mittpunkter av motsatta kanter rot_{kk},
3 rotationer π kring axlar genom mittpunkter av motsatta sidor $\text{rot}_{ss\pi}$ och
6 rotationer $\frac{\pi}{2}$ kring axlar genom mittpunkter av motsatta sidor $\text{rot}_{ss\frac{\pi}{2}}$.
$|F(g)|$, antalet konfigurationer som inte ändras av g för de olika $g \in G$ blir:

g	antal element	$\lvert F(g)\rvert$
id	1	$k^8 + 8k^7$ (alla kulor godtyckligt färgade; med 0, 1 röd)
rot_{hh}	8	$k^4 + 2k^3$ (kulorna samma färg 1,3,3,1; ev. en av två röd)
rot_{kk}	6	$k^4 + 0$ (kulorna samma färg parvis)
$\text{rot}_{ss\pi}$	3	$k^4 + 0$ (kulorna samma färg parvis)
$\text{rot}_{ss\frac{\pi}{2}}$	6	$k^2 + 0$ (kulorna samma färg 4 och 4)

Så antalet olika utsmyckningar = antalet banor under G:s verkan på färgningarna =
$= \frac{1}{|G|}\sum_{g\in G}|F(g)| = \frac{1}{24}(1 \cdot (k^8 + 8k^7) + 8 \cdot (k^4 + 2k^3) + 6 \cdot k^4 + 3 \cdot k^4 + 6 \cdot k^2) = \frac{1}{24}(k^8 + 8k^7 + 17k^4 + 16k^3 + 6k^2)$.
Svar: Det finns $\frac{1}{24}(k^8 + 8k^7 + 17k^4 + 16k^3 + 6k^2)$ olika sådana utsmyckningar.

---

8) G är en grupp och $a, b \in G$ har ordningar $o(a) = m$, $o(b) = n$, där $\text{sgd}(m, n) = 1$. Vi skall visa (a, 1p) att om $a^r = b^s$ för några $r, s \in \mathbb{Z}$ så är $a^r = b^s = 1$ och (b, 3p) att alla $a^i b^j$, $0 \le i < m$, $0 \le j < n$ är olika.

Lösning:
Om $g = a^r = b^s$ ligger g i båda de delgrupper $\langle a\rangle$ och $\langle b\rangle$ i G som genereras av a och b. De har ordning m respektive n, så g:s ordning delar både m och n, så $o(g) = 1$ och $g = 1$ (G:s identitetselement). **a-Saken är klar.**
Om $a^i b^j = a^k b^l$, $0 \le i, k < m$, $0 \le j, l < n$ ger multiplikation från vänster med a^{-k} och från höger med b^{-j} att $a^{i-k} = b^{l-j}$, där $-m < i - k < m$ och $-n < l - j < n$. Enligt a) gäller $a^{i-k} = 1$, så enligt känd sats $m \mid i - k$, så ($|i - k| < m$) $i - k = 0$, dvs $i = k$. På motsvarande sätt fås att $j = l$. **b-Saken är också klar.**

---

9) Vi skall (a, 1p) visa att polynomet $k(x) = x^2 + x + 1$ är irreducibelt i $\mathbb{Z}_2[x]$, (b, 1p) ställa upp additions- och multiplikationstabellerna för kroppen $(F, +, \cdot)$, där $F = \{0, 1, \alpha, \beta\}$ och består av ekvivalensklasser modulo $k(x)$ och α, β är x:s respektive $x + 1$:s klasser och (c, 3p) faktorisera polynomet $f(x) = x^4 + \beta x^3 + \alpha x^2 + \alpha x + \beta$ i irreducibla faktorer i $F[x]$.

Lösning:

Eftersom $k(x)$ är av grad 2 är det irreducibelt precis om det saknar nollställen.

$k(0) = k(1) = 1 \neq 0$, så **saken är klar i a)**.

Konstruktionen av F innebär precis att $\alpha^2 + \alpha + 1 = 0$ i F, dvs att $\alpha^2 = \alpha + 1$. Det (och tabellerna för $\mathbb{Z}_2$) ger tabellerna för F:

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\times$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

För att se om $f(x)$ har några förstagradsfaktorer söker vi nollställen. $f(0) = \beta$, $f(1) = 1$, $f(\alpha) = \alpha + \beta + 1 + \beta + \beta = 0$, så $x - \alpha = x + \alpha$ är en faktor i $f(x)$. Division ger att $f(x) = (x + \alpha)g(x)$, där $g(x) = x^3 + x^2 + \alpha$.

$g(x)$ kan inte ha nollställen 0 eller 1. $g(\alpha) = 1 + \beta + \alpha = 0$, så också $g(x)$ har en faktor $x + \alpha$. Division ger $g(x) = (x + \alpha)h(x)$, där $h(x) = x^2 + \beta x + 1$. $h(\alpha) = \beta$ och $h(\beta) = 1$, så $h(x)$ är irreducibelt. Den sökta faktoriseringen är alltså $f(x) = (x + \alpha)^2(x^2 + \beta x + 1)$.

Svar a: Visat ovan, b: se tabellerna ovan, c: $\boldsymbol{f(x) = (x + \alpha)^2(x^2 + \beta x + 1)}$.

---

10) (5p) $(G, \cdot)$ är en grupp och vi skall visa att för varje funktion $f : G \to G$ är $\mathcal{Z}_f = \{g \in G \mid f(g \cdot x) = f(x \cdot g)$ för alla $x \in G\}$ en delgrupp till G.

Lösning:

För att visa att $\mathcal{Z}_f$ är en delgrupp räcker det enligt en känd sats att visa att $\mathcal{Z}_f \neq \varnothing$, $a, b \in \mathcal{Z}_f \Rightarrow ab \in \mathcal{Z}_f$ och $a \in \mathcal{Z}_f \Rightarrow a^{-1} \in \mathcal{Z}_f$.

$1 \cdot x = x \cdot 1 (= x)$ för alla $x \in G$, så $1 \in \mathcal{Z}_f$.

$a, b \in \mathcal{Z}_f \Rightarrow f(abx) \overset{a \in \mathcal{Z}_f}{=} f(bxa) \overset{b \in \mathcal{Z}_f}{=} f(xab)$ för alla $x \in G \Rightarrow ab \in \mathcal{Z}_f$.

$a \in \mathcal{Z}_f \Rightarrow f(a^{-1}x) = f(a^{-1}xa^{-1}a) \overset{a \in \mathcal{Z}_f}{=} f(aa^{-1}xa^{-1}) = f(xa^{-1})$ för alla $x \in G \Rightarrow a^{-1} \in \mathcal{Z}_f$.

Saken är klar.