MATEMATISKA INSTITUTIONEN
KTH
Examinator: Svante Linusson
telefon 790 9444

**Svar på tentamen B i Diskret Matematik 5B1204, 2006-05-16**

Varje rätt löst uppgift är värd 3 poäng. Max är 24 poäng och 10 räcker säkert för godkänt. Möjlighet att kompletera får den som har 9 poäng.
Godkänt på lappskrivning 4 ger två bonuspoäng.
**Hjälpmedel:** Inga hjälpmedel tillåtna.
Motivera dina lösningar!!!

1. Formulera och bevisa Faktorsatsen för polynomringen över en kropp.

   **Svar:** Formulering och bevis, se boken eller det bevis som jag gav på föreläsningen (eller annat bra bevis).

2. Låt $p(x) = x^4+3x^2+3x+2, q(x) = 4x^3+2x^2+4x+1 \in \mathbb{Z}_5[x]$. Bestäm monadiska största gemensamma delaren till $p(x)$ och $q(x)$ i $\mathbb{Z}_5[x]$.

   **Svar:** Vi använder Euklides algoritm och får
   $x^4 + 3x^2 + 3x + 2 = (4x^3 + 2x^2 + 4x + 1)(4x + 3) + x^2 + 2x + 4$ och
   $4x^3 + 2x^2 + 4x + 1 = (x^2 + 2x + 4)(4x + 4)$. Alltså är monadiska $\text{sgd}(p(x), q(x)) = x^2 + 2x + 4$.

3. Du deltar i ett RSA-krypto system och skall skicka ett meddelande till Alice. Hon har bestämt sig för de offentliga nycklarna $n_A = 143$ och $e_A = 11$.

   (a) Kryptera 24 så att du kan skicka det till Alice.

   (b) Du tjuvlyssnar och hör att Bengt skickat 17 till Alice. Dekryptera meddelandet.

   **Svar:**

   (a) Kryptera 24 gör man genom att räkna ut $24^{11} \pmod{143}$. Då $24^2 = 576 \equiv_{143} 4$, $24^4 \equiv_{143} 16$ och $24^8 \equiv_{143} 16^2 = 256 \equiv_{143} -30$. Får vi att $24^{11} \equiv_{143} 24^8 \cdot 24^2 \cdot 24^1 \equiv_{143} -30 \cdot 4 \cdot 24 \equiv_{143} 123$. Du skall skicka iväg 123.

   (b) $143 = 13 \cdot 11$. Först måste vi räkna ut Alice dekrypteringsnyckel $d$. Den skall uppfylla $11d \equiv_m 1$ där $m = (13-1)(11-1) = 120$. Antingen ser man direkt att $d = 11$ eller så får man fram det med Euklides algoritm. Att dekryptera 17 innebär att vi skall räkna ut $17^d \pmod{143}$. Vi beräknar $17^2 = 289 \equiv_{143} 3$, $17^4 \equiv_{143} 3^2 = 9$ $17^8 \equiv_{143} 9^2 = 81$. Det ger att $17^{11} \equiv_{143} 17^8 \cdot 17^2 \cdot 17^1 \equiv_{143} 81 \cdot 3 \cdot 17 \equiv_{143} 100 \cdot 17 \equiv_{143} 127$. Bengt ville säga 127 till Alice.

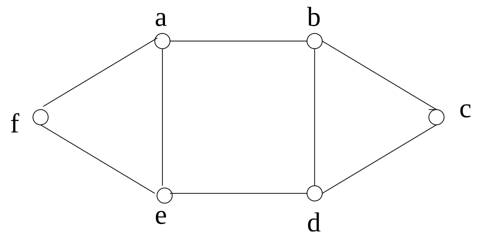
4. Låt $C$ vara en linjär binär felrättande kod som rättar ett fel och har kontrollmatris $H = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}$.

   Tre kodord från $C$ sänds till dig och du tar emot de tre orden $\{100100, 100011, 110111\}$. Om vi antar att högst ett fel har uppstått under sändningen av varje ord, vilka ord sändes?

   **Svar:** Vi multiplicerar $H$ med de mottagna orden och får resultaten $\begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$, $\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ och $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$.

   Det första är kolumn 2 i $H$ och det är alltså ett fel i andra positionen i det första ordet. Det sända ordet var 110100. Det andra är nollkolumnen och alltså har inget fel begåtts i det andra ordet. Det tredje är första kolumnen i $H$ och alltså har ett fel begåtts i första positionen. Det tredje sända ordet var 010111.

5. Låt $G$ vara följande graf.




På hur många sätt kan vi färga noderna i $G$ med 2 färger om vi räknar två färgningar som lika ifall det finns automorfi på grafen som överför den ena till den andra. D.v.s vi tar bort namnen på noderna så att vi inte kan skilja dem åt på så sätt. (Inga andra restriktioner på färgning av noderna finns, t.ex. kan två noder med gemensam kant ha samma färg.)

**Svar:** Vi använder Burnsides Lemma för att räkna ut antalet icke-isomorfa färgningar av $\Gamma$. Först måste vi bestämma automorfigruppen $G$ för $\Gamma$. De enda noderna med valensen 2 är $c$ och $f$ de är antingen fixpunkter eller avbildas på varandra. Om de är fixpunkter så är enda möjliga automorfin, förutom identiteten, en spegling i en horisontell axel, dvs $(ae)(bd)$. Om $c$ och $f$ avbildas på varandra kan det ske på två möjliga sätt. Om vi specifierar bilden av $a$ så följer allting annat. Antingen avbildas $a$ på $b$ (spegling i en vertikal symmetriaxel) eller så avbildas $a$ på $d$ (rotation ett halvt varv). Man kontrollerar lätt att dessa bildar en grupp med fyra element som är automorfigruppen för $\Gamma$.

Vi gör nu en tabell över storleken på fixpunktsmängden av färgningar för varje automorfi. För t.ex. $\pi = (ae)(bd) = (ae)(bd)(c)(f)$ får vi att $a$ och $e$ måste ha samma färg för att färgningen skall vara en fixpunkt under verkan av $\pi$, och även att $b$ och $d$ skall ha samma färg. (Vi får välja en färg godtyckligt för varje cykel i $\pi$.) På samma sätt för övriga permutationer ger:

| $\pi \in G$ | $\lvert X_\pi \rvert$ |
|---|---|
| $id$ | $2^6$ |
| $(ae)(bd)$ | $2^4$ |
| $(cf)(ab)(ed)$ | $2^3$ |
| $(cf)(ad)(be)$ | $2^3$ |

Enligt Burnsides Lemma får vi att antalet icke-isomorfa färgningar av $\Gamma$ med två färger är $\frac{1}{|G|}\sum_{\pi \in G} |X_\pi| = (64 + 16 + 8 + 8)/4 = 24$.

6. Låt $G = \{e, a, b, c, d\}$ vara en grupp med 5 element där $eb = b, aa = d$ och $ad = c$. Bestäm fullständiga grupptabellen för $G$.

**Svar:** Vi ser först att $eb = b$ betyder att $e$ är identitetselementet i $G$ ty identiteten är unik i varje grupp (multiplicera med $b^{-1}$ från höger i båda leden). Nu vet vi följande om de två första raderna i grupptabellen:

| | $e$ | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ | $d$ |
| $a$ | $a$ | $d$ | - | - | $c$ |

Varje element i gruppen förekommer exakt en gång i varje rad och $ab \neq b$ ty identiteten är unik. Alltså måste $ac = b$ och $ab = e$. Gruppen $G$ har fem element, vilket är ett primtal. Alltså har varje element i gruppen ordning 5 förutom identiteten som har ordning 1. Vi kan använda $a$ som en generator för $G$ och räkna ut att $a^2 = d$, $a^3 = aa^2 = ad = c$, $a^4 = aa^3 = ac = b$ och slutligen att $a^5 = aa^4 = ab = e$. Nu kan vi utan problem räkna ut övriga produkter t.ex. $bc = a^4a^3 = a^7 = a^2 = d$. Hela grupptabellen blir:

| | $e$ | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ | $d$ |
| $a$ | $a$ | $d$ | $e$ | $b$ | $c$ |
| $b$ | $b$ | $e$ | $c$ | $d$ | $a$ |
| $c$ | $c$ | $b$ | $d$ | $a$ | $e$ |
| $d$ | $d$ | $c$ | $a$ | $e$ | $b$ |

7. Både $x^2+1$ och $x^2+x+2$ är irreducibla polynom i $\mathbb{Z}_3[x]$. Vi har i kursen lärt oss att både $\mathbb{Z}_3[x]/(x^2+1)$ och $\mathbb{Z}_3[x]/(x^2+x+2)$ är ändliga kroppar med 9 element. Enligt teorin för ändliga kroppar är de isomorfa. Ange en isomorfi av de multiplikativa grupperna i respektive kropp.

   **Svar:** Vi vet att den multiplikativa gruppen i en kropp är cyklisk. Vi vill alltså hitta ett primitivt element (generator) i varje kropp.

   Den multiplikativa gruppen har ordning 8 och möjliga ordningar för elementen är därför 1,2, 4 och 8. Först räknar vi i $\mathbb{Z}_3[x]/(x^2+x+2)$ där är $x^2 = 2x+1$, $x^4 = (2x+1)^2 = x^2+x+1 = 2$. Så $x$ har ordning 8 och är således ett primitivt element i $\mathbb{Z}_3[x]/(x^2+x+2)$.

   Nu räknar vi i $\mathbb{Z}_3[x]/(x^2+1)$ där $x^2 = 2$ och $x^4 = 1$, så $x$ är inte ett primitivt element här. Istället kan man t.ex. ta $2x+1$, ty $(2x+1)^2 = x^2+x+1 = x$, $(2x+1)^4 = x^2 = 2$ och $(2x+1)^8 = 1$. Så $2x+1$ är ett primitivt element.

   Avbildningen som tar $x^j \in \mathbb{Z}_3[x]/(x^2+x+2)$ på $(2x+1)^j \in \mathbb{Z}_3[x]/(x^2+x+2)$ för $1 \leq j \leq 8$ är en isomorfi av de multiplikativa grupperna (men inte nödvändigtvis av hela kroppen).

8. Hur många irreducibla polynom av grad 3 finns det i $\mathbb{Z}_5[x]$?

   **Svar:** Vi noterar att $\mathbb{Z}_5[x]$ är en kropp så satsen om unik (så när som på konstanter) faktorisering i irreducibler gäller. Det är lättare att räkna monadiska polynom ty då är faktoriseringen i monadiska irreducibler helt unik. Vi räknar först ut $I(n) =$antalet monadiska irreducibla polynom av grad $n$ i $\mathbb{Z}_5[x]$. Vi vet att det totala antalet monadiska polynom av grad $n$ är $5^n$ ty vi kan välja de $n$ koefficienterna fritt i $x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$. Först noterar vi att $I(1) = 5$ ty alla linjära polynom är irreducibla. Alla reducibla monadiska polynom av grad 2 kan fås genom att ta två irreducibla av grad 1 och multiplicera ihop dem. Vi skall alltså välja 2 av 5 med repetition tillåten så det finns $\binom{5+2-1}{2} = 15$ sätt. Då blir $I(2) = 5^2 - 15 = 10$. Monadiska reducibla polynom av grad 3 kan fås på två sätt. Dels genom att multiplicera 3 linjära monadiska polynom vilket kan göras på $\binom{5+3-1}{3} = 35$ sätt. Dels genom att multiplicera ett monadiskt linjärt polynom med ett irreducibelt monadiskt andragradspolynom, vilket kan göras på $I(1)I(2) = 50$ sätt. Satsen om unik faktorisering gör att alla reducibla monadiska polynom har räknats exakt en gång i dessa två fall. Då blir $I(3) = 5^3 - (35+50) = 40$.

   Slutligen vet vi att alla irreducibla polynom fås genom att multiplicera ett irreducibelt monadiskt polynom med en nollskild konstant ur kroppen. Totala antalet irreducibla polynom av grad 3 i $\mathbb{Z}_5[x]$ är $4 \cdot 40 = 160$.