MATEMATISKA INSTITUTIONEN
KTH
Examinator: Svante Linusson
telefon 790 9444

Svar på tentamen B i Diskret Matematik 5B1204, 2006-08-23

Varje rätt löst uppgift är värd 3 poäng. Max är 24 poäng och 10 räcker för godkänt. Möjlighet att komplettera får den som har 9 poäng.
Hjälpmedel: Inga hjälpmedel tillåtna.

1. Låt u, v vara godtyckliga element i en grupp G. Visa att det finns ett unikt element $x \in G$ så att $ux = v$.

   Svar: Detta är sats 20.3.2 i boken. Formulering och bevis, se boken eller det bevis som jag gav på föreläsningen (eller annat bra bevis).

2. Låt $p(x) = x^5 + 3x^3 + 3x^2 + 4, q(x) = x^4 + 2x^3 + 4x^2 + x + 3 \in \mathbb{Z}_5[x]$. Vad är det monadiska största gemensamma delaren till $p(x)$ och $q(x)$ i $\mathbb{Z}_5[x]$?

   Svar: Vi använder Euklides algoritm och får
   $x^4 + 2x^3 + 4x^2 + x + 3 = (3x^3 + 4x)(2x + 4) + x^2 + 3$
   $3x^3 + 4x = (x^2 + 3)(3x)$. Detta ger att $x^2 + 3$ är monadiska största gemensamma delare till $p(x)$ och $q(x)$.

3. Bush och Condoleezza skickar hemliga meddelanden till varandra med hjälp av RSA-krypto. Bush har bestämt sig för de offentliga nycklarna $n_B = 451 (= 41 \cdot 11)$ och $e_B = 89$. Condoleezza har bestämt sig för de offentliga nycklarna $n_C = 77$ och $e_C = 11$.

   (a) Hur skall Bush kryptera meddelandet 9 innan han skickar det till Condoleezza.

   (b) Bush får svaret 21 från Condoleezza. Vilket var det hemliga meddelandet från Condoleezza?

   Svar:

   (a) Kryptera 9 gör man genom att räkna ut $9^{11} \pmod{77}$. Först räknar vi $9^2 = 81 \equiv_{77} 4$, $9^4 \equiv_{77} 16$ och $9^8 \equiv_{77} 16^2 = 256 \equiv_{25}$. Sedan får vi att $9^{11} \equiv_{77} 9^8 \cdot 9^2 \cdot 9^1 \equiv_{77} 25 \cdot 4 \cdot 9 \equiv_{77} 900 \equiv_{77} 53$. Bush skall skicka iväg 53.

   (b) Först måste vi räkna ut Bushs dekrypteringsnyckel d. Den skall uppfylla $89d \equiv_m 1$ där $m = (41-1)(11-1) = 400$. Antingen ser man genom prövning att $d = 9$ eller så får man fram det med Euklides algoritm. Att dekryptera 21 innebär att vi skall räkna ut $21^d \pmod{451}$. Vi beräknar $21^2 = 441 \equiv_{451} -10$, $21^4 \equiv_{451} (-10)^2 = 100$ $21^8 \equiv_{451} 100^2 = 10000 \equiv_{451} 980 \equiv_{451} 78$. Det ger att $21^9 \equiv_{451} 21^8 \cdot 21^1 \equiv_{451} 78 \cdot 21 = 1638 \equiv_{451} 285$. Condoleezza ville säga 285 till Bush.

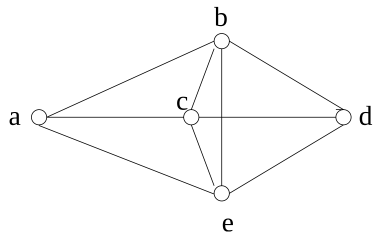
4. En lärare vill tilldela alla elever på kursen var sitt identitetsnummer i form av en binär sträng av längd n. Det finns 27 elever på kursen och läraren vill använda en linjär felrättande kod för att konstruera identitetsnumret. Han vill att det skall gå att korrigera ett fel i strängen. Vilket är det minsta möjliga värdet på n?

   Svar: Om C är en linjär, binär felrättande kod som har $k \times n$-matrisen H som kontrollmatris så har kodorden längd n och dimension $n - k$, dvs C har 2^{n-k} kodord. Vi har m.a.o. villkoret $2^{n-k} \geq 27$, eller $n - k \geq 5$. Då C skall rätta ett fel så måste alla kolumner vara olika och nollskilda. Det innebär att vi får ett andra villkor $n \leq 2^k - 1$.

   Nu prövar vi hur litet n som kan uppfylla dessa villkor. Då $k \geq 1$ får vi direkt från första villkoret att $n \geq 6$, som i sin tur i andra villkoret säger $2^k - 1 \geq 6$ som ger att $k \geq 3$. Då använder vi första villkoret igen som ger $n \geq 8$, vilket i andra villkoret ger $k \geq 4$. Sista steget i denna iteration blir att från första villkoret få att $n \geq 9$ vilket stämmer med båda villkoren.

   Vi kontrollerar också lätt att det går att skapa en 4×9 matris med alla kolumner olika och nollskilda. Den får 32 kodord vilket räcker gott och väl. Svar: $n = 9$.

5. Låt Γ vara följande graf.



På hur många sätt kan vi färga noderna i Γ med 2 färger om vi räknar två färgningar som lika ifall det finns en 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 Γ. Först måste vi bestämma automorfigruppen G för Γ. De enda noderna med valensen 3 är a och d de är antingen fixpunkter eller avbildas på varandra. Vi ser att övriga tre noder är sammanbunda med varandra och alla tre har dessutom både a och d som grannar. Vi kan alltså ha vilken permutation som helst av c, d, e oavsett om a, d byter plats eller inte.

Automorfigruppen G för Γ blir alltså alla permutationer av c, d, e kombinerat med båda möjliga permutationerna för a, d d.v.s $G \cong S_3 \times S_2$.

Vi gör nu en tabell över storleken på fixpunktsmängden av färgningar för varje automorfi. För t.ex. $\pi = (ad)(be) = (ad)(be)(c)$ får vi att a och d måste ha samma färg för att färgningen skall vara en fixpunkt under verkan av π, och även att b och e skall ha samma färg. (Vi får välja en färg godtyckligt för varje cykel i π.) Antalet möjliga färgningar som är fixa under verkan av π är alltså 2^3. På samma sätt för övriga permutationer ger:

$\pi \in G$	$\lvert X_\pi \rvert$
id	2^5
(ad)	2^4
$(ad)(bc)$	2^3
$(ad)(be)$	2^3
$(ad)(ce)$	2^3
$(ad)(bce)$	2^2
$(ad)(bec)$	2^2
(bc)	2^4
(be)	2^4
(ce)	2^4
(bce)	2^3
(bec)	2^3

Enligt Burnsides Lemma får vi att antalet icke-isomorfa färgningar av Γ med två färger är $\frac{1}{|G|}\sum_{\pi\in G}|X_\pi| = (32 + 4 \cdot 2^4 + 5 \cdot 2^3 + 2 \cdot 2^2)/12 = 12$.

6. Låt $G = \{u, v, x, y, z\}$ vara en mängd med 5 element. Avgör vilka av följande multiplikationstabeller som ger en korrekt grupptabell (svar utan motivering ger som vanligt inga poäng).

(a)

$\cdot$	u	v	x	y	z
u	u	v	x	y	z
v	v	x	y	z	u
x	x	y	z	u	v
y	y	z	u	v	x
z	z	u	v	x	y

(b)

	u	v	x	y	z
u	x	z	u	v	y
v	y	x	v	z	u
x	u	v	x	y	z
y	z	u	y	x	v
z	v	y	z	u	x

(c)

	u	v	x	y	z
u	u	v	x	y	z
v	v	x	z	u	y
x	x	z	u	y	v
y	y	u	v	z	x
z	z	y	y	x	u

Svar: (a) Ja. Tabellen är en latinsk kvadrat och man ser att $v^2 = x, v^3 = y, v^4 = z$ och $v^5 = u$. Även resten av tabellen stämmer med grupptabbelen för $C_5 =< v >$, den cykliska gruppen med fem element.

(b) Nej. Detta är en latinsk kvadrat men är trots det inte en grupptabell. Om det vore en grupptabell så skulle x vara identitetselementet. Alla andra element i gruppen skulle då ha ordning två (ty $u^2 = x$ etc). Men enligt Lagranges sats så måste ett elements ordning dela gruppens ordning, som här skulle vara fem. En motsägelse.

(c) Nej. Detta är inte ens en latinsk kvadrat, ty t.ex. har understa raden y två gånger, så det kan inte vara en grupptabell.

7. Är permutationsgruppen S_3 isomorf med $C_2 \times C_3$? (C_n betecknar här som i hela kursen den cykliska gruppen med n element.)

   Svar: Båda grupperna har 6 element, men är inte isomorfa. Notera att enligt en sats i boken är $C_2 \times C_3 \cong C_6$, ty 2 och 3 är relativt prima. Men S_3 är inte den cykliska gruppen med 6 element. Det kan motiveras på olika sätt. Ett sätt att visa det är att inget element har ordning 6. Ett annat sätt är att visa att S_3 inte är kommutativ.

8. Visa att om ett element x i en grupp G har ordning st, där $s > 1$ och $t > 1$ är relativt prima, så kan x skrivas som en produkt av två andra element i G med ordning s respektive t.

   Svar: Då s och t är relativt prima finns heltal u, v så att $us + vt = 1$. Låt $a = x^{us}, b = x^{vt}$. Då är $a \cdot b = x^{us+vt} = x^1 = x$.

   Återstår att visa att a och b har ordning t respektive s. Först ser vi att $a^t = x^{ust} = 1$.

   Låt nu r vara ett postivit heltal sådant att $a^r = 1$, dvs $x^{usr} = 1$. Det medför att ordningen st delar usr, vilket i sin tur medför att $t|ur$. Då $us + vt = 1$ så är t och u relativt prima vilket medför att $t|r$. Det följer att a har ordning t. På samma sätt visas att b har ordning s.