Matematiska Institutionen
KTH

Tentamensskrivning på kursen Diskret Matematik för F3 och F1spec, 5B1203, onsdagen den 23 augusti, klockan 14.00-19.00.

Examinator: Olof Heden.

Tillåtna hjälpmedel: Inga hjälpmedel är tillåtna.

Betygsgränser: 10 poäng ger betyget 3, 14 poäng ger betyget 4 och 18 poäng ger betyget 5.

Problem: (Obs alla lösningar och svar skall motiveras noga.)

1. (2p) Ett RSA-krypto definieras av att $n = 77$ och $e = 13$. Dechiffrera meddelandet $a = 2$.
2. (3p) Bestäm kontrollmatrisen (parity-check matrix) till en 1-felsrättande linjär kod C med 32 stycken ord och med så kort ordlängd som möjligt. Visa också med ett exempel hur ett ord som inte ligger i koden kan rättas med användning av kodens kontrollmatris.
3. (3p) Undersök om det finns någon graf som består av fem komponenter med sammanlagt 35 noder, 33 kanter och som innehåller precis fyra olika cykler.
4. (3p) De åtta sidoytorna på en ändligt lång stav, vars tvärsnittsyta är en regelbunden sexhörning, skall målas med p stycken olika färger. På hur många olika sätt kan detta ske.

   Anm. Två målningar betraktas som identiska om de kan erhållas ur varandra med hjälp av vridningar av staven.
5. Betrakta kroppen F med de 25 elementen $ax + b$ där $a, b \in Z_5$ och där multiplikationen definieras med hjälp av villkoret $x^2 + x + 1 = 0$.

   (a) (2p) Bestäm ett element $z \in F$ sådant att $z(3x - 2) = x + 2$.

   (b) (2p) Den multiplikativa gruppen till F har en delgrupp med fyra element. Beskriv dessa element på något lämpligt sätt.
6. (3p) Bestäm antalet olika lösningar till ekvationen $x^6 = 1$ i ringen Z_{72}. Ange också minst tre olika lösningar.
7. Elementen 1, 2, 3, 4, 5, 6, 7 och 8 placeras i fem (oetiketterade) lådor på ett sådant sätt att elementen 1, 2 och 3 hamnar i olika lådor. På hur många olika sätt kan detta ske om

   (a) (2p) ingen låda får vara tom.

   (b) (2p) precis en låda är tom.
8. (3p) Ge ett exempel på en ickeabelsk grupp G med 72 element. Beskriv på lämpligt sätt elementen i G och gruppoperationen samt bevisa att den grupp G du valt inte är abelsk.