

Tentamen i 5B1118 Diskret Matematik 5p.  
24 Maj, 2004

**DEL A**, 3p per uppgift.

- (1) (3p) Hitta alla positiva heltal  $m, n$  som uppfyller

$$15m + 30n = 45$$

Kan dela ekvationen med 5 och lösa

$$3m + 6n = 9$$

Det finns en positiv lösning  $(m, n) = (1, 1)$ .

- (2) (3p) Hur många arrangemang av bokstäverna i ordet MATEMATIK finns det? Hur många av dessa innehåller inte sekvensen "AA"?

Ordet matematik har två M, två A och två T. Antalet arrangemang är alltså

$$\binom{9}{2, 2, 2} = \frac{9!}{2 \cdot 2 \cdot 2} = \frac{362880}{8} = 45360$$

Antalet arrangemang som innehåller AA kan man bestämma genom att räkna antalet arrangemang av bokstäverna i MTEMTIK□, där □ = AA. Det är:

$$\binom{8}{2, 2} = \frac{8!}{2 \cdot 2} = \frac{40320}{4} = 10080$$

Arrangemang som innehåller inte AA är alltså  $45360 - 10080 = 35280$

- (3) (3p) Låt  $G = (V, E)$  vara en enkel graf. Bestäm  $|V|$  om  $G$  har 12 kanter och varje nod har grad 4. Rita en geometrisk representation av  $G$ .

Enligt formulan

$$2|E| = \sum_{v \in V} \deg(v)$$

är  $24 = |V| \cdot 4$  och därför  $|V| = 6$ .

(4) (3p) Betrakta funktionen:

$$f : \mathbb{Z}_+ \times \mathbb{Z}_+ \rightarrow \mathbb{Q}_+; \quad f(m, n) = \frac{m}{n}$$

(a) Är  $f$  surjektiv?

Varje positivt rationellt tal kan skrivas som  $\frac{m}{n}$ , där  $m, n \in \mathbb{Z}_+$ . Det visar att  $f$  är surjektiv.

(b) Är  $f$  bijektiv? Funktionen  $f$  är inte injektiv. Man har, till exempel att:

$$f(2, 4) = f(1, 2) = 1/2$$

Det visar att funktionen är INTE bijektiv.

(5) (3p) Givet ett RSA-system med krypteringsnyckel  $n = 77$  och  $e = 7$ . Dekryptera meddelandet 3.

$n = 11 \cdot 7$ ,  $m = 10 \cdot 6 = 60$ . Vi ska hitta  $d$  så att  $7d \equiv_{60} 1$ . Eftersom  $(60, 7)$  är relativt prima, Euklides algoritm ger

$$1 = 2 \cdot 60 - 17 \cdot 7 \equiv_{60} -17 \cdot 7$$

Det följer att  $d = -17 \equiv_{60} 43$ .

Meddelandet 3 dekrypteras som  $3^{43}$ , mod 77.

$$3^4 = 81 \equiv_{77} 4 \quad 3^8 \equiv_{77} 16 \quad 3^{16} \equiv_{77} 256 \equiv_{77} 25 \quad 3^{32} \equiv_{77} 625 \equiv_{77} 9$$

svaret blir  $3^{32} \cdot 3^8 \cdot 3^3 \equiv_{77} 38$

**DEL B**, 5p per uppgift.

(6) (5p) Betrakta den fullständiga bipartita grafen  $K_{m,n}$ .<sup>1</sup>

(a) För vilka värden på  $m$  och  $n$  är  $K_{m,n}$  en Eulergraf? Om  $m = 0$  eller  $n = 0$  då har  $K_{m,n}$  isolerade noder och då är den inte sammanhängande. Om  $m, n > 0$  är den fullständiga bipartita grafen  $K_{m,n}$  en graf utan isolerade noder, så  $K_{m,n}$  är en Eulergraf om och endast om den är sammanhängande och varje nod har jämn grad.

---

<sup>1</sup>Grafen har  $m + n$  noder, uppdelad i två mängder  $V_1, V_2$  med  $m$  respektive  $n$  element, där kanter förbinder varje nod i  $V_1$  med varje nod i  $V_2$ , men inga kanter går mellan två noder i  $V_1$  och inga mellan två noder i  $V_2$

Låt  $w, v$  vara två noder i  $K_{m,n}$ . Om  $v \in V_1, w \in V_2$  (eller viceversa) då finns det en kant mellan dem. Om  $v, w \in V_1$  (eller  $v, w \in V_2$ ) då kan man välja en nod  $x \in V_2$  och kanter  $vxw$  för att gå från  $v$  till  $w$ . Det visar att  $K_{m,n}$  är sammanhängande för varje  $m, n$ .

Varje nod i  $V_1$  har grad  $|V_2| = n$  och varje nod i  $V_2$  har grad  $|V_1| = m$ .

Alltså är  $K_{m,n}$  en Eulergraf om och endast om  $m$  och  $n$  är jämna.

- (b) Välj ett par  $m, n$  sådan att  $K_{m,n}$  är en Eulergraf och rita en Eulerkrets.

Man kan välja till exempel  $K_{2,2}$ .

- (c) Finns det något par  $m, n$  sådan att  $K_{m,n}$  inte är en Eulergraf, men har en Eulerväg?

$K_{m,n}$  har en Eulerväg om och endast om högst två noder har udda grader. Det följer att för varje udda positivt heltal  $n$  är  $K_{2,n}$  inte en Eulergraf men har en Eulerväg

- (7) (5p) Visa att om  $a, b \in \mathbb{Z}_n$  är inverterbara<sup>2</sup> då är  $ab$  och  $b^{-1}$  inverterbara. ( $b^{-1}$  betecknar multiplikativa inversen av  $b$ ).

Låt  $G = \{0 \neq a \in \mathbb{Z}_{32} \text{ sådan att } a \text{ är inverterbart}\}$ . Är  $(G, \cdot)$  en grupp? (multiplicationen  $\cdot$  är multiplicationen modulo 32).

Ett element  $a \in \mathbb{Z}_n$  är inverterbart om och endast om  $\text{sgd}(a, n) = 1$ , dvs  $a$  och  $n$  är relativt prima.

Antag att  $a, b \in \mathbb{Z}_n$  är inverterbara, dvs  $\text{sgd}(a, n) = 1$  och  $\text{sgd}(b, n) = 1$ . Låt  $\text{sgd}(ab, n) = c = p_1 \cdot \dots \cdot p_k$ , där  $p_i$  är primtal. Då gäller att  $p_i$  delar  $n$  och  $p_i$  delar  $ab$  för  $i = 1 \dots k$ . Det följer att  $p_i$  delar  $n$  och  $p_i$  delar minst en mellan  $a$  och  $b$ . Men det betyder att  $p_i$  delar  $\text{sgd}(a, n) = 1$  eller  $p_i$  delar  $\text{sgd}(b, n) = 1$  och då är  $p_i = 1$ . Det visar att  $ab$  är inverterbar.

Alternativt ska man visa att det finns en multiplikativa invers för  $ab$ , dvs ett element  $c$  sådan att  $ac = ca = 1$ . Låt  $a^{-1}, b^{-1}$  vara de multiplikativa inverserna av respektive  $a, b$  då är  $b^{-1}a^{-1}$  den multiplikativa inversen till  $ab$ .

Det är klart att  $b$  är den multiplikativa inversen av  $b^{-1}$ .

$\text{sgd}(a, 32) = 1$  för varje udda heltal  $a$ . Det följer att

$$G = \{[1], [3], [5], [7], [9], [11], [13], [15], [17], [19], [21], [23], [25], [27], [29], [31]\}$$

Aftersom  $ab$  är inverterbart för varje  $a, b \in \mathbb{Z}_{32}$  är multiplicationen slut på  $G$ . Den är associativ för att operationen är associativ på  $\mathbb{Z}_{32}$ . Identitetelementet är  $[1]$ . För varje element  $a \in G$ , i.e. för varje inverterbart element  $a \in \mathbb{Z}_{32}$  är invertsens  $a^{-1}$  inverterbar och då  $a^{-1} \in G$ .

Det visar att  $(G, \cdot)$  är en grupp.

---

<sup>2</sup>Med avseende på multiplicationen.

(8) (5p) Visa att grupperna  $(\mathbb{Z}_4, +)$  och  $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$  är inte isomorfa.

$(\mathbb{Z}_4, +)$  är en cyklisk grupp av kardinalitet 4. Elementen  $[1]$  har ordningen  $ord([1]) = 4$ . Om det finns en isomorfi  $\phi$  mellan  $(\mathbb{Z}_4, +)$  och  $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$  då måste  $ord(\phi([1])) = 4$ . Men det finns inget element i  $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$  med ordningen 4.

$$ord(1, 1) = ord(1, 0) = ord(0, 1) = 2$$

(9) (5p) Bestäm antalet permutationer  $\sigma \in \mathbb{S}_5$  som uppfyller:

$$\sigma \neq id \text{ och } \sigma^2 = id.$$

En permutation  $\sigma \neq id$  av 5 element kan ha en av följande typer:

$$[1, 1, 1, 2], [1, 1, 3], [1, 2, 2], [1, 4], [2, 3], [5]$$

Ordningen av en  $k$ -cykel är  $k$  så bara permutationer av typer

$$[1, 1, 1, 2], [1, 2, 2]$$

är så att  $\sigma^2 = id$ .

Antalet permutationer av typ  $[1, 1, 1, 2]$  är lika med antalet 2-cyklar i  $\mathbb{S}_5$ , som är  $\binom{5}{2} = 10$ .

Antalet permutationer av typ  $[1, 2, 2]$  är  $\frac{1}{2} \binom{5}{2} \cdot 3 = 15$  (för varje val av en 2-cykel det finns tre olika sätt att välja ett element och en annan 2-cykel. Så där dubbelräknar man varje två-cykel så ska man dela med två).

Totalt finns det 25 stycken permutationer  $\sigma \in \mathbb{S}_5$  som uppfyller:

$$\sigma \neq id \text{ och } \sigma^2 = id.$$