

Svar till övning 10, den 9 maj 2012

1. $|G| = |G_x| \cdot |Gx|$ om G verkar på en mängd X , där $x \in X$.

Då x är ett hörn fås $|G_x| = 4$ (fyra rotationer kring en axel genom oktaederns mittpunkt och hörnet) och $|Gx| = 6$ (hörnet kan rotera till alla oktaederns hörn).

Om x är mittpunkten av en sidoyta fås på liknande sätt $|G_x| = 3$, $|Gx| = 8$.

I båda fallen blir $|G| = 24$.

2. Burnsidess lemma. (Den regelbundna) tetraederns grupp av symmetrirotationer har 12 element: Identitets-elementet (bevarar alla konfigurationer, $|X_{id}| = k^6$), åtta rotationer $\pm \frac{2\pi}{3}$ kring axlar genom ett hörn och mittpunkten av motstående sidoyta (bevarar konfigurationer med samma färg på kanterna vid hörnet och samma på kanterna vid sidoytan, $|X_g| = k^2$) och tre rotationer π kring axlar genom mittpunkterna av motstående kanter (bevarar konfigurationer med övriga fyra kanter parvis likfärgade, $|X_g| = k^4$).

Lemmat ger antalet väsentligt olika färgningar, $\frac{1}{12}(k^6 + 3k^4 + 8k^2)$.

3. RSA med $n = 77 = 7 \cdot 11$, så $m = (7-1)(11-1) = 60$.

a. $\text{sgd}(45, m) = 15 \neq 1$, så 45 duger inte som e .

b. Euklides algoritmen ger $1 = -8 \cdot 60 + 37 \cdot 13$, så $d = 37$.

c. 3 krypteras som $E(3) \equiv 3^{13} \pmod{77}$. Man finner $(3^2 = 9, 3^4 = 81 \equiv 4, 3^8 \equiv 16) \quad 3^{13} = 3^8 \cdot 3^4 \cdot 3 \equiv 16 \cdot 4 \cdot 3 \equiv 38 \pmod{77}$, så 3 krypteras som 38.

d. 2 avkrypteras som $D(2) \equiv 2^{37} \pmod{77}$. Man finner $D(2) = 51$.

4. RSA med $n = 265 = 5 \cdot 53$, så $m = (5-1)(53-1) = 208$. $e = 37$ och Euklides algoritmen ger $1 = -8 \cdot 208 + 45 \cdot 37$, så $d = 45$. Meddelandet 2 avkrypteras alltså som $D(2) \equiv 2^{45} \equiv 147 \pmod{265}$, så som 147.

5. $E(x) \equiv 718^e = 718^{143} \pmod{1333}$ och $e = 143 = (10001111)_2$.

$x^2 = 718^2 = 515524 \equiv 986 \pmod{1333}$, $x^4 = 986^2 = 972196 \equiv 439 \pmod{1333}$

etc. ger $E(x) \equiv x^{128} \cdot x^8 \cdot x^4 \cdot x^2 \cdot x \equiv 986 \cdot 769 \cdot 439 \cdot 986 \cdot 718 \equiv 707 \pmod{1333}$, så $E(718) = 707$.

Alternativt kan man räkna så (eftersom $143 = (10001111)_2$):

$E(x) \equiv (((((((1^2 \cdot x)^2 \cdot 1)^2 \cdot 1)^2 \cdot 1)^2 \cdot x)^2 \cdot x)^2 \cdot x)^2 \cdot x \pmod{1333}$.

P.s.s. fås $E(719) \equiv (((((((1^2 \cdot 719)^2 \cdot 1)^2 \cdot 1)^2 \cdot 1)^2 \cdot 719)^2 \cdot 719)^2 \cdot 719)^2 \cdot 719 \equiv \dots \equiv 615 \pmod{1333}$ och $E(719) = 615$.

$n = 1333 = 31 \cdot 43$ ger $m = 30 \cdot 42 = 1260$.

Euklides algoritmen: $1260 = 8 \cdot 143 + 116$, $143 = 1 \cdot 116 + 27$, $116 = 4 \cdot 27 + 8$, $27 = 3 \cdot 8 + 3$, $8 = 2 \cdot 3 + 2$, $3 = 1 \cdot 2 + 1$, så $1 = 3 - 2 = 3 - (8 - 2 \cdot 3) = -8 + 3 \cdot 3 = \dots = -53 \cdot 1260 + 467 \cdot 143$, så vi tar $d = 467$.

Man finner $D(707) \equiv 707^{467} \equiv \dots \equiv 718$ och $D(615) \equiv 615^{467} \equiv \dots \equiv 719$

6. Vi gör Fermatstestet med bas 2: $2^{62} = (2^6)^{10 \cdot 2} = 64^{10} \cdot 4 \equiv 1^{10} \cdot 4 = 4 \not\equiv 1 \pmod{63}$, så Fermatstestet ger att 63 inte är ett primtal.

7. Eftersom 101 är ett primtal och $101 \nmid 43$, gäller (Fermats lilla sats) att $43^{100} \equiv 1 \pmod{101}$ och $43^{139702} = (43^{100})^{1397} \cdot 43^2 \equiv 1^{1397} \cdot 1849 \equiv 31 \pmod{101}$.

8. Med n hörn i grafen är möjliga valenser $0, 1, \dots, n-1$, men 0 och $n-1$ kan inte båda förekomma om $n \neq 1$. Postfacksprincipen.

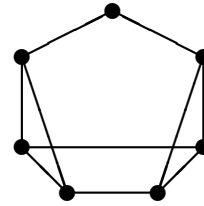
9. Nej. Den vänstra är inte bipartit (a, b, c alla grannar), men det är den högra (inga grannar av samma paritet).

10. Småkubernas grannförhållanden beskrivs av en bipartit graf, där mittkuben är av minoritetstyp.

11. i) 0,2,3,3,4,4,5 : omöjligt, ty summan av valenserna skall vara 2 gånger antalet kanter, ett jämnt tal.

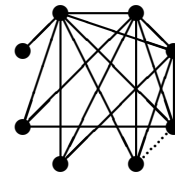
ii) 2,3,3,3,3,3,3 : möjligt, se figuren till höger.

iii) 2,2,3,5,5,5,6 : omöjligt, ty de tre första hörnen kan ha högst 7 kanter till de sista fyra, men dessa måste ha minst 9 kanter till de första tre (minst 2,2,2,3 "utåt").



12. T.ex. kubgrafen (hörn och kanter i en kub) och två stycken K_4 (som en graf).

13. Låt hörnens valenser vara 1, 3, 3, 4, 5, 6, 7, x . Summan av valenserna skall vara 2 gånger antalet kanter, ett jämnt tal, så x är udda och ≤ 7 . $x = 1$ är omöjligt, ty hörnen med valenser 6,7 medför att det går minst 3 kanter till varje par av hörn. $x = 7$ är också omöjligt, ty två hörn med valens 7 skulle innebära att alla hörn hade valens minst 2. $x = 3, 5$ går båda, se fig. (utan och med den prickade kanten). Ett sätt att finna dessa är att notera att en graf med valenser 1, 3, 3, 4, 5, 6, 7, x finns omm en med valenser 0, 2, 2, 3, 4, 5, $x - 1$ finns omm en med 1, 1, 2, 3, $x - 2$ finns omm en med 1, 2, 2, $x - 2$ finns etc.



14. En möjlighet är dessa grafer (boken ger andra i övning 6.31).

a.



b.



c.



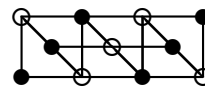
d.



15a. Om rutorna är omväxlande svarta och vita (som på ett vanligt schackbräde) leder varje drag från svart till vit eller från vit till svart. Eftersom den skall återkomma till startrutorna måste det finnas lika många svarta som vita rutor (om den gör minst ett drag), dvs totalt ett jämnt antal.

b. Antag att det funnes en sådan sluten väg (dvs en hamiltoncykel). Färga nu rutorna i rad 1 och 4 röda och de i rad 2 och 3 blå. Då kan springaren aldrig gå från röd till röd och eftersom brädet har lika många av varje färg, måste varannan ruta den besöker vara blå och varannan röd. Men detsamma gäller för de svarta och vita rutorna i den vanliga färgningen (som i a.). Det betyder att alla röda rutor vore vita eller alla svarta. Motsägelse.

16. Enligt figuren är grafen bipartit. Eftersom den har ett udda antal hörn kan den inte ha någon hamiltoncykel (en sådan måste ha varannat svart och vitt hörn, dvs lika många av vardera), så **svaret är nej**.



17. Om grafen $G = (V, E)$ är osammanhängande, finns disjunkta $V_i \neq \emptyset$, $i = 1, 2$ med $V = V_1 \cup V_2$ och inga kanter mellan dem. Om $x \in V_1, y \in V_2$, gäller $\delta(x) \leq |V_1| - 1, \delta(y) \leq |V_2| - 1$, så $\delta(x) + \delta(y) \leq |V_1| + |V_2| - 2 = n - 2$.

18. Om den bipartita grafen $G = (X \cup Y, E)$ har $|X| = k, |Y| = n - k$ gäller att $\delta(x) \leq n - k$ för $x \in X$, så (i alla kanter ingår precis ett $x \in X$) antalet kanter $e \leq k(n - k) = \left(\frac{n}{2}\right)^2 - \left(\frac{n}{2} - k\right)^2 \leq \left(\frac{n}{2}\right)^2$.

19a. $\bar{\delta}_i = v - 1 - \delta_i$, $i = 1 \dots v$. b. Direkt ur a.

c. De är komplementgrafer till 2-reguljära grafer med 8 hörn. Det finns bara 3 sådana: C_8 , $C_5 + C_3$, $C_4 + C_4$. (Där C_n är cykelgraferna, dvs 2-reguljära och sammanhängande grafer med n hörn.)

20. Följer av att $\sum_{v \in V} \delta(v) = 2|E|$.

21. Eftersom $\sum_{v \in V} \delta(v) = 2 \cdot 28 = 56$ och alla $\delta(v) \geq 3$, måste $|V| \leq 18$. En graf med 18 hörn och 28 kanter ges av två kopior av kubgrafen med två disjunkta kanter mittpunkter "hopsnörda" till ett nytt hörn.

22. Om hörnen x, y ligger i olika komponenter i G , är xy en väg i $\overline{G}$. Om de ligger i samma komponent och z ligger i en annan, är xzy en väg i $\overline{G}$.