# Elementär grafteori

## 15.1 Introduktion

*Grafteori* är ett av de yngre matematiska ämnena men, har genomgått en enastående utveckling under de senaste 60 åren, mycket tack vare teorins tillämpningar i stort sett alla områden inom vetenskap, teknik och samhällsliv. Och för att det blir så slående snygga figurer, förstås. Det är mycket lätt att peka på otaliga exempel där vi utsätts för grafer: titta bara på en tunnelbanekarta, på en modell av en kemisk molekyl, olika optimeringsproblem som att finna den kortaste vägen mellan två adresser i en stad eller schemaplanering för alla lärare i en skola, en bild av relationer mellan individer i en grupp av människor, flödesscheman i programmering, osv.

Det allra första arbetet som behandlade grafer skrevs av schweizaren Leonard Euler 1736[1]. Den första riktiga läroboken i ämnet kom precis 200 år senare. Den systematiska teorin är alltså relativt ung. Termer i grafteori är inte heller så entydigt bestämda som termer i andra matematiska ämnen, utan relativt flytande. Mycket beror på i vilket sammanhang man studerar graferna. Det vi kommer att kalla för hörn kallar till exempel datafolk för noder, medan andra säger punkter eller till och med vertex. Våra kanter kallas på andra ställen för bågar, eller linjer osv. Visserligen tror jag inte att vi här kommer att ha några problem med sådana otydligheter, men läsaren har nu varnats för världen utanför denna bok.

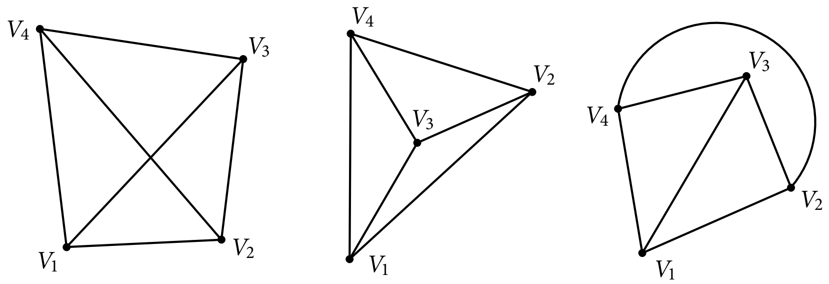
Så här dyker grafer upp. Tänk dig en icke-tom mängd av objekt, till exempel datorer, och uppkopplingar mellan vissa par av dessa. Vi kan representera dessa datorer som punkter i planet och kopplingarna som linjer mellan motsvarande par av punkter. Då har vi en *graf*. Punkterna som representerar objekten ska vi kalla för grafens *hörn*, och linjerna ska vi kalla för *kanter*.

1 Arbetet handlade om det berömda problemet som är känt under namnet *Köningsbergs broar*, och ansågs nog länge som nöjesmatematik. Det är värt att kolla upp detta på Wikipedia.

Kanterna betecknas ofta med hjälp av sina ändpunkter, till exempel $e = (u, v)$, där $u$ och $v$ är hörn i grafen.

Intuitivt är det en bra beskrivning; matematiskt är den inte tillfredsställande. Men nyttan av en strikt definition är här för liten (i jämförelse med hur krånglig den formella definitionen är) för att vi ska försöka oss på den. I vår uppfattning av en graf är det tillåtet att ha multipla kanter mellan två hörn och också ha öglor[2]: kanter från ett hörn till sig självt.

En graf kan alltså representera vilken situation som helst så fort vi bara har en mängd av objekt och någon sorts relation mellan objekt som bildar par. Kanterna har bara en symbolisk betydelse, som beteckning på en relation mellan två objekt (hörn, punkter). De kan ritas som raka linjer eller som böjda kurvor. Ett annat exempel är en mängd människor och relationen ”tycka illa om”, förutsatt att vi antar att denna relation är ömsesidig (senare i avsnittet om riktade grafer, ska vi prata om en mer realistisk modell, men låt oss nu vara naiva...). I figuren nedan finns ett exempel på en graf med fyra hörn och sex kanter ritad på tre olika sätt men, som graf betraktat, representerar alla figurerna precis samma situation.[3].

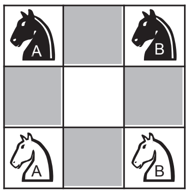



För att nu illustrera grafers förträfflighet vid problemlösning, och ge ett än mer abstrakt exempel på vad kanter i en graf kan representera, betrakta följande uppgift som förekommer i ett 1200 år gammalt arabiskt manuskript om schack.

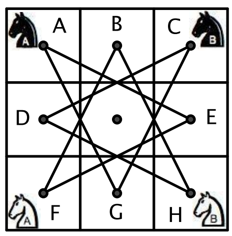
2 I litteraturen kallas de också för *loopar*.

3 Mera formellt säger man att det finns en-entydig motsvarighet mellan hörnen i de två graferna, en motsvarighet som bevarar kanterna: en kant mellan två hörn i den ena grafen svarar mot en kant mellan motsvarande hörn i den andra grafen. En sådan motsvarighet kallas för *grafisomorfi*.

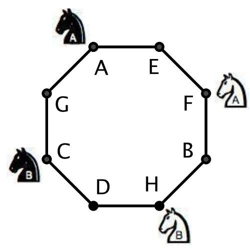
**Exempel 15.1.** *Vilket är det minsta antal drag som man behöver göra på ett stympat* $3 \times 3$ *schackbrädet nedan, för att de två vita springarna ska byta plats med de två svarta? Vad blir svaret, om man dessutom kräver att springarna markerade med A byter plats med varandra, liksom springarna markerade med B? (Två springare får inte befinna sig på samma ruta samtidigt.)*




*Lösning:* Grafteorin erbjuder följade smarta lösning (vi vet inte hur problemets skapare[4] hade tänkt sig lösningen). Markera rutorna på brädet med bokstäverna A, B, C, D, E, F, G och H som i den vänstra figuren nedan (den centrala rutan är ointressant eftersom ingen springare någonsin kan hamna där). Rita därefter ett streck för varje par av rutor som svarar mot ett drag av en springare. Om vi därefter följer linjerna från ruta till ruta, märker vi att det blir en enda sluten "väg". Låt oss då vika ut denna linje som i den högra figuren nedan. Där har vi alltså en graf $T$ med åtta hörn och lika många kanter.




T:




Våra springare kan alltså endast förflytta sig längs kanterna i $T$. Var och en av dessa åtta kanter svarar mot ett giltigt drag av en springare. Från grafen $T$:s utseende följer då att det enda sättet att få de svarta och de vita springarna att byta plats är att låta dem gå runt grafen med fyra steg moturs eller fyra

4 al-Adli ar-Rumi, en berömd schackspelare från Bagdad som levde på 800-talet, i manuskriptet *Kitab ash-shatranj* (Boken om schackspelet).

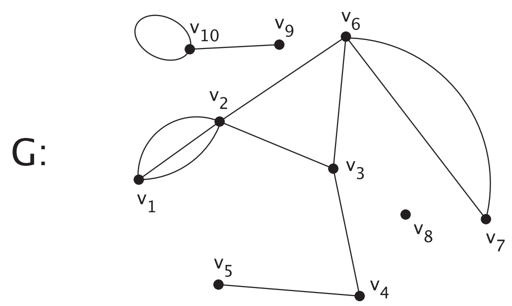
 

steg medurs. Med varje springare måste man alltså utföra fyra drag, ett drag i taget för var och en av pjäserna, så totalt blir det 16 drag.

På detta sätt byter den svarta A-springaren plats med den vita B-springaren, medan den svarta B-springaren byter plats med den vita A-springaren. Från figuren följer också att detta är det enda möjliga bytet, vilket medför att springarna markerade med A aldrig kan byta plats med varandra samtidigt som springarna markerade med B gör det. Springarnas relativa position, svart A – vit A – vit B – svart B, i grafen ändras aldrig. ☻

## 15.2 Handskakningslemma

Grafen $G$ i figuren nedan har tio hörn och tolv kanter. Hörnmängden brukar man beteckna med $V$ och kantmängden med $E$. Vi har alltså $V = \{v_1, v_2, \ldots, v_{10}\}$ och $E = \{$tre gånger $(v_1,v_2), (v_2,v_3), (v_2,v_6), (v_3,v_4), (v_3,v_6), (v_4,v_5),$ två gånger $(v_6,v_7), (v_9,v_{10}), (v_{10},v_{10})\}$.




Grafen $G$ består av tre *komponenter*, den ena med hörnmängden $\{v_1, \ldots, v_7\}$, den andra med ett enda hörn, $\{v_8\}$, och den tredje med två hörn, $\{v_9, v_{10}\}$. Inom varje komponent kan man förflytta sig mellan godtyckliga hörn genom att bara följa kanterna (en sådan vandring brukar man kalla för en *stig*). En graf som består av en enda komponent kallas för *sammanhängande*. Grafen i vårt exempel är alltså icke-sammanhängande. Notera också att i $G$ finns en ögla och multipla kanter. En graf *utan* öglor och multipla kanter kallas helt enkelt för en *enkel graf*.

En *krets* är en stig som börjar och slutar i samma hörn. Det bör också vara uppenbart att om vi från en sammanhängande graf avlägsnar en kant som tillhör en krets, är den resterande grafen fortfarande sammanhängande (men kretsen har eventuellt upphört att existera: betrakta till exempel kretsen

$v_2 - v_3 - v_6 - v_2$ och tag bort en kant). Om en stig mellan hörnen $u$ och $v$ använder en kant $e$ som tillhör en krets, i stället för att passera $e$, gå runt denna krets utan att behöva utnytja kanten $e$.

För varje hörn $v$ i en graf $G$ anger talet $\deg(v)$, graden av hörnet $v$ (från engelskan *degree*), antalet kanter som utgår från hörnet $v$ (notera att när graden bestäms för ett hörn räknas en ögla två gånger, dvs. såväl den ena änden av kanten – öglan – som den andra änden). För grafen $G$ i figuren ovan gäller då: $\deg(v_1) = 3$, $\deg(v_2) = 5$, $\deg(v_3) = 3$, $\deg(v_4) = 2$, $\deg(v_5) = 1$, $\deg(v_6) = 4$, $\deg(v_7) = 2$, $\deg(v_8) = 0$, $\deg(v_9) = 1$ och $\deg(v_{10}) = 3$.

Summan av dessa grader är lika med 24, vilket råkar vara det dubbla antalet kanter i $G$ (notera att vid summeringen räknas öglan som en kant). Det är faktiskt ingen tillfällighet, och detta är innebörden av den första satsen man serverar i grafteori, det viktiga *handskakningslemmat*[5].

**Sats 15.1** (Handskakningslemmat)**.** *Antag att grafen $G$ har $n$ hörn, $\{v_1, v_2, \ldots, v_n\}$, och $k$ kanter. Då är*

$$\deg(v_1) + \deg(v_2) + \cdots + \deg(v_n) = 2k$$

*Bevis.* Tänk dig att vi går runt till vart och ett av hörnen $v_i$ och markerar var och en av de $\deg(v_i)$ kanter som utgår från detta hörn. Totalt har vi då lämnat $\deg(v_1) + \deg(v_2) + \cdots + \deg(v_n)$ markeringar.

Samtidigt har varje kant i grafen fått två markeringar: en vid varje ändpunkt. Detta innebär att antalet markeringar är $2k$ – och beviset är klart. ☻

Låt oss kalla ett hörn $v$ för ett *udda hörn* om $\deg(v)$ är ett udda tal. Annars kallas hörnet för ett *jämnt hörn*. Sats 15.1 har följande korollarium, som nästan är viktigare än satsen själv. Den säger att det inte existerar någon graf med ett udda antal udda hörn.

**Korollarium 15.1.** *Låt $G$ vara en graf med $n$ hörn, $\{v_1, v_2, \ldots, v_n\}$, varav $m$ av dessa är udda. Då är $m$ ett jämnt tal.*

5 Själva namnet *handskakningslemmat* följer från följande tolkning: Om ett antal personer skakar hand med varandra, är summan av antalet handskakningar som var och en gör ett jämnt tal.

*Bevis.* Utan att inskränka på allmängiltigheten kan vi anta att de $m$ första hörnen, $\{v_1, v_2, \ldots, v_m\}$, är udda. Annars döper vi förstås om dem. Låt vidare $k$ vara antalet kanter i $G$. Enligt handskakningslemmat har vi då att

$$2k = \deg(v_1) + \deg(v_2) + \cdots + \deg(v_n) =$$

$$(\deg(v_1) + \cdots + \deg(v_m)) + (\deg(v_{m+1}) + \cdots + \deg(v_n)).$$

Vänstra ledet är ett jämnt tal. Den andra parentesen i högra ledet är också ett jämnt tal (en summa av $n - m$ jämna tal). Därmed är även den första parentesen ett jämnt tal. Men eftersom vi i den första parentesen har en summa av $m$ udda tal måste själva $m$ vara jämnt! ☻

Med en snabb puck visar vi att vår analys av hälsningsceremonier (handskakningar) har vittgående konsekvenser för den mer grafteoretiskt upplysta delen av resebyråbranschen. Glöm nu inte att efterlysa graden av varje flygplats, betraktad som ett hörn i en graf vid nästa resa! ☺

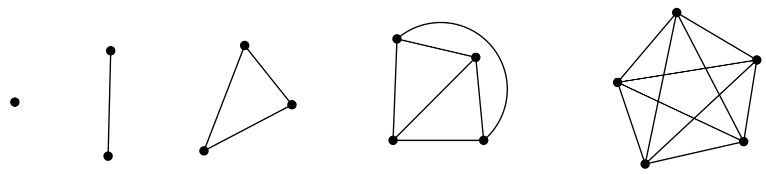
**Exempel 15.2.** *Från Huvudön i ett örike finns direkt flygförbindelse med sju andra öar i riket, medan den lilla Avkroksön bara är i förbindelse med tre andra öar. Var och en av de övriga öarna är i förbindelse med sex eller åtta öar. Visa att man med flyg kan ta sig från Huvudön till Avkroksön, om ej nödvändigtvis direkt.*

*Lösning:* Betrakta grafen $G$ vars hörn utgörs av öar och kanterna är flygförbindelser. Låt $G_1$ vara den komponent i $G$ som innehåller Huvudön. Vi vill visa att Avkroksön också ligger i $G_1$.

Antag att så inte är fallet och betrakta då hörnen i $G_1$. Deras grader är en 7:a och ett antal 6:or och 8:or. Detta är dock omöjligt då en graf (i vårt fall $G_1$) med ett enda udda hörn, enligt Korollarium 15.1, inte kan existera. Därmed måste Avkroksön ligga i $G_1$. ☻

En enkel graf med $n$ hörn och en kant mellan varje par av hörn kallas för en *komplett graf* och betecknas med $K_n$. Graferna $K_1$ till $K_5$ finns i figuren nedan.



$K_1$ $K_2$ $K_3$ $K_4$ $K_5$

Antalet kanter i grafen $K_n$ är $\binom{n}{2} = \frac{n(n-1)}{2}$, eftersom det finns $\binom{n}{2}$ val av par av hörn i en sådan graf.

Observera att medan graferna $K_1$ till $K_4$ kan ritas på sådant sätt att kanterna inte korsar varandra, blir det helt omöjligt med $K_5$. Denna skillnad får oss att dela in grafer i två klasser: *planära grafer* och *icke-planära grafer*. Innan vi tar oss an planära grafer ska vi försöka titta på ett något svårare exempel.

**Exempel 15.3.** *Tjugo personer deltar i ett möte. I början av mötet skakar varje person hand med de deltagare som hen känner sedan tidigare. Vi vet att av tre godtyckligt valda personer är det åtminstone två som inte känner varandra sedan tidigare.*

*Vilket är det maximala antalet handskakningar som kan ha förekommit?*

*Bevis.* Om man tolkar personer som hörn i en graf och handskakningar som kanter, gäller frågan att finna det maximala antalet kanter i en *triangelfri graf*[6] med 20 hörn.

Låt $\{v_1, v_2, \dots, v_{20}\}$ vara grafens hörn och antag att $v_{20}$ är hörnet med den största graden och att denna grad är $k$. Vi kan då anta att $v_{20}$ har kanter till hörnen $v_1, v_2, \dots, v_k$. Eftersom grafen är triangelfri saknas det kanter mellan dessa $k$ hörn. Därmed har alla grafens kanter minst ett av hörnen bland de $20 - k$ hörnen $\{v_{k+1}, v_{k+2}, \dots, v_{20}\}$.

Antalet kanter är därmed som mest lika med $\deg(v_{k+1}) + \deg(v_{k+2}) + \cdots + \deg(v_{20})$. Var och en av dessa grader är $\leq k$ och följaktligen är antalet kanter i grafen $\leq (20-k)k$.

Nu gäller det att finna hur stort talet $(20-k)k$ kan vara som mest, då

6 En graf säges vara *triangelfri* om det för varje val av tre hörn i denna graf saknas åtminstone en av tre kanter mellan dessa hörn.

$0 \le k \le n$. En smart omskrivning och kvadratkomplettering ger $(20 - k)k = -(k^2 - 20k) = -(k - 10)^2 + 100$. Det största antal kanter får man när parentesen är lika med 0, vilket innebär att $k = 10$. Då är antalet kanter $\le 10 \cdot 10 = 100$.

Det återstår att konstruera ett exempel på en situation där det maximala antalet av 100 handskakningar verkligen kan nås. En sådan situation inträffar om vart och ett av hörnen $v_{11}, v_{12}, \ldots, v_{20}$ förbinds med vart och ett av hörnen $v_1, v_2, \ldots, v_{10}$ och inga fler kanter dras. ☻

## 15.3 Planära grafer

Planära grafer, som introducerades i förra avsnittet, upptar en särskild plats i grafteorin på grund av sina vida tillämpningsområden. Livet är ju så ofta platt. Tänk till exempel på gatunät i en stad (eventuella broar och tunnlar exkluderas), eller produktion av ett ett-lagers kretskort.

Det är klart att givet ett antal hörn $n \ge 5$, får grafen, för att vara planär, inte ha alltför många kanter. Ju fler kanter man drar,desto större är ju risken att man blir tvungen att ”korsa” en redan ritad kant, och lämna det plana livet, till exempel med ett hopp. Hur antalet kanter i en planär graf begränsas av antalet hörn kan beskrivas med hjälp av den så kallade *Eulers formel*[7] som vi ska presentera nu.

En planär graf kan man förstås rita på många olika sätt i ett plan. Grafen $K_4$ representerade vi till exempel (den första figuren i detta kapitel) på tre olika sätt, varav det andra och tredje sättet var planära. En sådan planär representation av en (planär) graf delar planet i ett antal områden, varav ett område är oändligt. Det visar sig att *antalet* områden i en planär representation är en *invariant* – det är alltid samma, hur vi än ritar grafen. Detta är just vad Eulers formel säger.

**Sats 15.2** (Eulers formel). *Antag att en planär, sammanhängande graf $G$ har $n$ hörn och $k$ kanter. Då är antalet områden $r$ som grafen delar planet i lika med $r = k - n + 2$.*

*Antalet områden $r$ är alltså en invariant för en planär graf $G$. Sambandet skrivs ofta som $n - k + r = 2$.*

7 Det finns fler snygga formler som bär Eulers namn. Den kanske mest kända är $e^{i\pi} + 1 = 0$.

*Bevis.* Det finns otaliga bevis för denna sats. Vi väljer ett som är baserat på stark induktion[8] med avseende på antalet kanter $k \geq 0$ i $G$.

Induktionsbasen är $k = 0$. I detta fall består grafen av ett enda hörn och en (oändlig) region. Vi får då att $n - k + r = 1 - 0 + 1 = 2$, och vi är klara.

Antag nu att formeln $n-k+r = 2$ är sann för alla planära sammanhängande grafer med upp till $k_0 \geq 0$ kanter och låt $G$ vara en planär sammanhängande graf med $k_0 + 1$ kanter och $n$ hörn. Vi vill visa att $n - (k_0 + 1) + r = 2$.

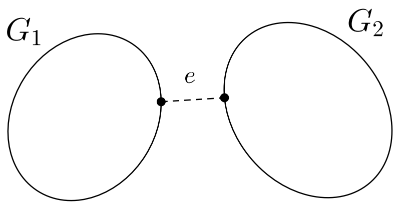
Välj en godtycklig kant $e$ i $G$.

Låt oss avlägsna $e$ från $G$ och betrakta den nya grafen $G'$ som har $k_0$ kanter och (fortfarande) $n$ hörn. Det finns två fall att betrakta nu: (1): $G'$ är sammanhängande, och (2): $G'$ är inte längre är sammanhängande.

I det första fallet förlorar vi utöver en kant också en region: de två regionerna som gränsade till $e$ blir bara en region. $G'$ har alltså $n$ hörn, $k_0$ kanter och $(r-1)$ regioner. Enligt induktionsantagandet är då $n - k_0 + (r-1) = 2$.

Lägger vi tillbaka kanten $e$ så ökar antalet kanter tillbaka till $k_0+1$ samtidigt som antalet regioner ökar till $r$. Vi får då $n-(k_0+1)+r = n-k_0+(r-1) = 2$, vilket skulle bevisas.

I det andra fallet delas $G$ i två sammanhängande komponenter $G_1$ och $G_2$, med $n_i$ hörn, $k_i$ kanter och $r_i$ regioner, respektive, för $i = 1, 2$ (se figuren nedan). Vi har då förstås att $n_1 + n_2 = n$, $k_1 + k_2 = k_0$.




Eftersom $k_1, k_2 \leq k_0$ ger det starka induktionsantagandet $n_i - k_i + r_i = 2$, för $i = 1, 2$.

Lägger vi tillbaka kanten $e$, är det enda som ändras, utöver antalet kanter som ökar med 1, att av två oändliga regioner som räknades i $r_1$ och $r_2$ blir bara en. Därmed är $n-(k_0+1)+r = (n_1+n_2)-(k_1+k_2+1)+(r_1+r_2-1) = (n_1-k_1+r_1) + (n_2-k_2+r_2) - 2 = 2+2-2 = 2$, vilket vi ville visa. Induktionsprincipen medför då att identiteten är sann för alla planära grafer. ☻

8 Mer om stark induktion finns i kapitel 4.6.

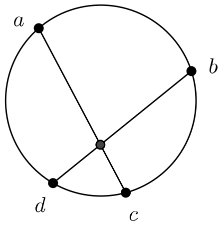
Som en elegant tillämpning, låt oss ge en grafteoretisk lösning till Exempel 4.1 och hemuppgift 52 i kapitel 4. Likheten ska visas med induktion.

**Exempel 15.4.** *På periferin av en cirkel placerar man $m \geq 1$ punkter. Därefter drar man alla möjliga kordor mellan dessa punkter (för $m = 1$ blir det 0 kordor). Det enda villkoret för utplaceringen av punkterna är att tre olika kordor aldrig möts i samma punkt inuti cirkeln.*

*Kordorna delar cirkelskivan i ett antal, $r_m$, områden. Bestäm $r_m$ som en funktion av $m$.*

*Lösning:* Om vi betraktar kordornas ändpunkter samt kordornas skärningspunkter som hörn i en graf, är det sökta antalet områden lika med $r_m = k_m - n_m + 1$ (enligt satsen ovan, där vi ersätter 2:an med en 1:a då vi bortser från det oändliga området utanför cirkelskivan).

För att slutföra uppgiften måste vi bestämma antalet hörn $n_m$ och antalet kanter $k_m$ i denna graf. Hörnen utgörs dels av $m$ punkter på cirkelns periferi, dels av de inre skärningspunkterna. Deras antal är faktiskt enkelt att bestämma, då varje val av fyra punkter på periferin leder till precis ett av hörnen: väljer vi punkterna $a, b, c$ och $d$ i medurs eller moturs ordning så bestämmer kordorna $ac$ och $bd$ entydigt en punkt inuti cirkeln, som i figuren nedan.




Eftersom varje hörn inuti cirkeln kan beskrivas på detta sätt så är antalet inre hörn i grafen lika med $\binom{m}{4}$. Därmed är $n_m = m + \binom{m}{4}$.

Varje hörn inuti cirkeln har grad 4, medan varje hörn på periferin har grad $(m - 1) + 2 = m + 1$: från hörnet $a$ utgår $m - 1$ kordor, men också ytterligare två kanter till $a$:s grannar längs cirkelns bågar.

Enligt sats 15.1 är summan av grader lika med det dubbla antalet kanter, och alltså är $2k_m = 4\binom{m}{4} + m(m+1)$. Därmed är

$$\begin{aligned} r_m &= 2\binom{m}{4} + \frac{m(m+1)}{2} - m - \binom{m}{4} + 1 = \binom{m}{4} + \frac{m(m-1)}{2} + 1 \\ &= \binom{m}{4} + \binom{m}{2} + 1. \end{aligned}$$

☻

En planär graf kan alltså inte ha ”alltför många” kanter. Det är faktiskt inte svårt att visa följande sats:

**Sats 15.3.** *Om $G$ är en enkel, sammanhängande och planär graf med $n \geq 3$ hörn och $k$ kanter, är $k \leq 3n - 6$.*

*Bevis.* Antag att vi ritar $G$ i planet och att $G$ då delar planet i $r$ regioner $s_1, s_2, \ldots, s_r$. Eftersom grafen är enkel begränsas varje region av minst tre kanter. Om vi då definierar $\deg(s)$, *graden av regionen s*, som antalet kanter som begränsar $s$, har vi att $\deg(s_i) \geq 3$, för $i = 1, 2, \ldots, r$. Om vi tänker oss en meditativ promenad runt varje region samtidigt som vi räknar antalet passerade kanter, kommer varje kant att räknas in två gånger (en gång för var och en av de två regioner som kanten gränsar till). Detta innebär att

$$\sum_{i=1}^{r} \deg(s_i) = 2k.$$

Å andra sidan, eftersom $\deg(s_i) \geq 3$, $i = 1, 2, \ldots, r$, samtidigt som vi, enligt Sats 15.2 har $r = 2 - n + k$, är

$$2k = \sum_{i=1}^{r} \deg(s_i) \geq 3r = 3(2 - n + k) = 6 - 3n + 3k,$$

vilket ger den önskade olikheten. ☻

**Exempel 15.5.** *Visa att graferna $K_n$, $n \geq 5$, inte är planära.*

*Lösning:* Det räcker att visa att grafen $K_5$ inte är planär. Antalet hörn är $n = 5$ och antalet kanter är $k = \binom{5}{2} = 10$. Skulle $K_5$ vara planär så skulle olikheten i Sats 15.3 ha formen $10 \leq 3 \cdot 5 - 6 = 9$, vilket uppenbart är helfalskt. ☻

**Exempel 15.6.** *Visa att i en enkel planär graf G måste det finnas ett hörn u med* $\deg(u) \leq 5$.

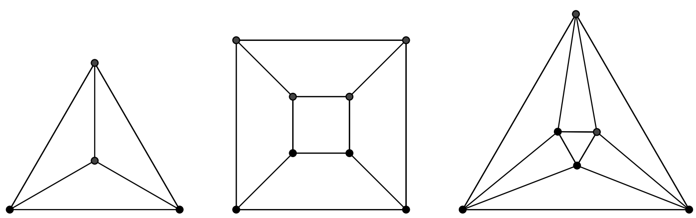
*Lösning:* Antag motsatsen, dvs. antag att $\deg(u) \geq 6$ för alla hörn $u$ och att grafen har $n$ hörn $\{u_1, \ldots, u_n\}$ och $k$ kanter. Då är $2k = \sum_{i=1}^{n} \deg(u_i) \geq 6n$, vilket medför att $k \geq 3n$.

Å andra sidan är $G$ planär, vilket innebär att $k \leq 3n - 6$. Vi får därmed olikheten $3n \leq 3n - 6$, vilken, om vi inte vill försöka leva med de förödande konsekvenserna av att 6 är ett negativt tal, är absurd. Detta innebär att det måste finnas minst ett hörn av grad $\leq 5$. ☻

## 15.4 Platonska kroppar

Teorin för planära grafer kan elegant tillämpas för att bestämma antalet och karaktären av de så kallade *Platonska kropparna*, alltså tredimensionella objekt vars sidor utgörs av kongruenta regelbundna figurer. De tre mest kända sådana objekten är en tetraeder, en kub och en oktaeder (åtta triangulära sidor: tänk två egyptiska pyramider vars baser har limmats ihop). Vi ska visa att det utöver dessa tre finns endast ytterligare två sådana regelbundna kroppar: dodekaedern (12 sidor) och ikosaedern (20 sidor).

Låt oss tänka att vi gör hål i en av sidorna på en sådan kropp och sedan tänjer ut figuren, så att den ligger i planet. Då får vi från kanterna och hörnen en planär graf där den oändliga delen av planet utgörs av den sida som punkterades.



De tre exemplen i figuren ovan svarar just mot en sådan planär representation av en tetraeder, en kub och en oktaeder.

Vår startpunkt är alltså en graf $G$ som representerar en sådan Platonsk kropp. Vi antar att $G$ har $n$ hörn, $k$ kanter och att planet delas in i $r$ regioner. Då är förstås $n - k + r = 2$.

Antag sedan att varje region begränsas av $e$ kanter och att i varje hörn mötts $v$ kanter. Självklart måste både $e$ och $v$ vara minst lika med 3. Då följer dels att $e \cdot r = 2k$, dels att $n \cdot v = 2k$. Dessa likheter kan skrivas som $r = \dfrac{2k}{e} = \dfrac{nv}{e}$ och $k = \dfrac{1}{2}nv$.

Insättning i Eulers formel ger $n - \dfrac{1}{2}nv + \dfrac{nv}{e} = 2$, alltså $n(2e - ve + 2v) = 4e$. Eftersom högra ledet är positivt måste vi ha $2e - ve + 2v > 0$, vilket medför att $ev - 2e - 2v < 0$. Då $ev - 2e - 2v = (e-2)(v-2) - 4$, kan olikheten skrivas som $(e-2)(v-2) < 4$. Detta begränsar de möjliga värdena på $e$ och $v$ väsentligt: både $e$ och $v$ måste vara mindre än 5.

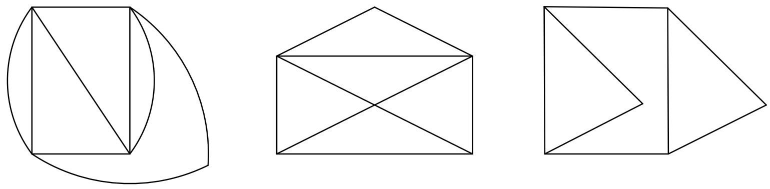
För $e = 3$ (när sidorna utgörs av liksidiga kongruenta trianglar) kan vi ha $v = 3$ (en tetraeder), $v = 4$ (en oktaeder) eller $v = 5$ (en ikosaeder med 20 triangulära sidor). För $e = 4$ kan vi endast ha $v = 3$ (en kub). Slutligen, för $e = 5$ är det också bara för $v = 3$ som olikheten är uppfylld, och vi får en dodekaeder vars sidor utgörs av 12 regelbundna liksidiga femhörningar.

Det finns alltså bara fem sådana regelbundna skapelser. Googla gärna efter bilder på dessa vackra kroppar (men sök nu inte på ”vackra kroppar” ☺).

## 15.5 Eulerska grafer

Vi börjar med en övning som liknar en dagisuppgift:

**Exempel 15.7.** *Innan du läser vidare, försök att rita var och en av nedanstående figurer med ett enda penndrag utan att lyfta pennan från papperet och utan att passera någon sträcka mer än en gång.*

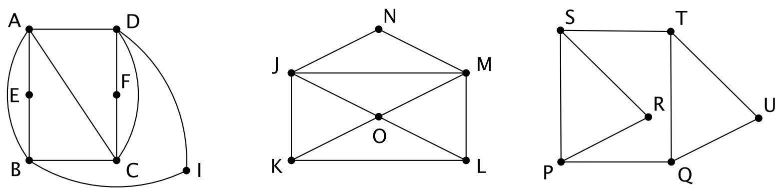


Detta är förstås bara en lek, men lösningen, alltså svaret på frågan huruvida figuren kan ritas med ett enda penndrag, har i alla fall en elegant och enkel grafteoretisk lösning.

Innan vi presenterar den måste vi införa begreppen *stig* och *krets* i en graf $G$. Enkelt talat är en stig en följd av hörn $v_1, v_2, \ldots, v_k$ i $G$, sådana att $v_i, v_{i+1}$ är förbundna med en kant, för $i = 1, \ldots, k-1$ och ingen kant förekommer mer än en gång. *Längden av en stig* definieras då som antalet kanter i stigen. En stig är en krets om $v_k = v_1$. En *Eulerstig* är en stig som passerar *alla* grafens kanter. På motsvarande sätt definieras *Eulerkrets*. En Eulerkrets är alltså en Eulerstig som slutar i samma hörn där den började. En graf som har en Eulerkrets kallas ofta för *Eulersk graf*.

Att rita en figur med ett enda penndrag svarar alltså mot att finna en eventuell Eulerstig (eller Eulerkrets) i den graf som uppstår då alla skärningspunkter i figuren betraktas som grafens hörn.

I exemplet ovan kan vi studera följande tre grafer:




(notera att hörnen E och F (och I) egentligen inte behövs, utan bara anger vilken kant, till exempel mellan A och B, som används) .Uppgiften går alltså ut på att finna en eventuell Eulerstig (eller till och med Eulerkrets) i var och en av figurerna.

*Lösning:* Den första grafen är Eulersk. Ett exempel på en Eulerkrets i denna graf är $AEBCFDCADIBA$.

Den andra grafen har en Eulerstig men ingen Eulerkrets. Dessutom måste stigen börja i ett av hörnen $K$ eller $L$ och sluta i det andra. Ett exempel är stigen $KJNMLOJMOKL$.

I den tredje grafen finns ingen Eulerstig över huvud taget. ☻

Nedanstående sats formulerades av Euler i samband med den promenad längs staden Königsbergs broar som nämndes i inledningen, och som blev startpunkten för utvecklingen av grafteorin. För Königsberg gick det sämre: det utplånades helt i andra världskriget och återuppstod som flottbasen Kaliningrad. Så olika falla ödets lotter.

I satsen karaktäriseras Eulerska grafer fullständigt och det ges en elegant metod för att upptäcka om grafen har en Eulerkrets, Eulerstig eller ingendera.

**Sats 15.4** (Eulers sats)**.** *a) En sammanhängande graf $G$ har en Eulerkrets om och endast om* $\deg(v)$ *är jämn för varje hörn $v$ i $G$.*

*b) En sammanhängande graf $G$ har en Eulerstig (men ingen Eulerkrets), om och endast om* $\deg(v)$ *är jämnt för alla hörn $v$ i $G$ utom precis två hörn. I sådana fall måste stigen börja i ett av dessa udda hörn och sluta i det andra.*

*Bevis.* a) ($\Rightarrow$) Tänk att vi vandrar runt grafen längs en Eulerkrets. Varje gång vi kommer in i ett hörn finns det en kant längs vilken vi kan fortsätta vandringen ut ur detta hörn. Kanterna vid varje hörn kan därför delas in i par. Därmed är $\deg(v)$ jämnt för varje hörn $v$ i $G$.

($\Leftarrow$) Låt oss välja ett hörn $v_1$ och börja en stig längs kanterna så långt det går, utan att upprepa promenaden längs samma kant två gånger. Eftersom antalet kanter är ändligt så kommer vi att åka fast och inte kunna gå vidare förr eller senare. Frågan är i så fall i vilket hörn man åker fast. Det kan inte vara ett hörn $v \neq v_1$ eftersom hörnet $v$ har jämn grad. Om man passerade det tidigare, använde man ju bara två kanter. De ”resterande” kanterna vid $v$ är fortfarande jämnt många, och därför finns det en kant att fortsätta färden med. Följaktligen avslutas vandringen i $v_1$ och vi erhåller en krets $\Gamma_1$.

Om inte $\Gamma_1$ är en Eulerkrets, finns det en kant $f$ i $G$ som inte är med i $\Gamma_1$. Då tar vi ett av hörnen, $v_2$, i $f$, och eftersom $G$ är sammanhängande finns det en stig från $v_2$ till $v_1$. Låt $v_3$ vara det första hörnet i denna stig som tillhör $\Gamma_1$ (det kan hända att det är just $v_2$). Vi vandrar då längs denna stig från $v_3$ mot $v_2$, sedan genom kanten $f$ och fortsätter igen så långt som möjligt, utan att använda kanterna från $\Gamma_1$.

Återigen kommer stigen att ta slut, och av samma anledning som ovan kommer den att sluta i just $v_3$. Kalla den nya kretsen för $\Gamma_2$.

Nu kan vi ”slå ihop” $\Gamma_1$ och $\Gamma_2$ till en enda krets $\Gamma$ genom att vandra från $v_1$ längs $\Gamma_1$ ända till $v_3$, därefter fortsätta runt kretsen $\Gamma_2$ och till slut vandra vidare längs $\Gamma_1$ fram till $v_1$. Motion får vi också!

Om vi nu har använt alla kanter, är vi klara, chipspåsen kan åka fram, annars upprepas proceduren ovan tills alla kanter i $G$ är med i den slutliga Eulerkretsen.

b) ($\Rightarrow$) Låt hörnen $u \neq v$ vara början och slutet i Eulerstigen. Om vi skulle lägga till en ny kant mellan dessa två hörn, skulle vi få en Eulerkrets och därmed skulle alla hörn ha jämn grad (enligt första delen av satsen). Utan denna kant kunde vi ju inte fortsätta från $u$ till $v$ och alltså är graderna för $u$ och $v$ udda.

($\Leftarrow$) Låt oss lägga till en ny kant mellan dessa två udda hörn. Då blir alla hörn jämna och vi får en Eulerkrets i grafen. Utan denna kant krymper kretsen till en Eulerstig med början och slut i dessa udda hörn.

☻

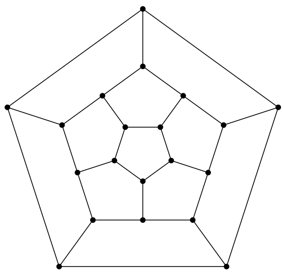
## 15.6 Hamiltonska grafer

Medan en Eulerstig definierades som en stig där varje kant i grafen förekommer precis en gång, definieras en *Hamiltonstig*[9] som en stig där varje hörn i grafen förekommer precis en enda gång. Om det dessutom finns en kant mellan det första och det sista hörnet i grafen, har vi en *Hamiltonkrets* och grafen kallas då *Hamiltonsk*.

Som en övning föreslås att finna en Hamiltonkrets i grafen nedan.

9 Namnet hedrar den irländske 1800-talsmatematikern William Rowan Hamilton, som bodde i Dublin, en stad som är mer känd för sina pubar än för sina broar.



Existensen av en Hamiltonkrets i en sammanhängande graf har betydligt viktigare tillämpningar än Eulerkretsar (till exempel *Hendelsresandeproblemet*[10] eller, för dem som har sociala ambitioner, *Bordsplaceringsproblemet*[11]). Tyvärr så finns det ingen bra och elegant karaktärisering av Hamiltonska grafer, i stil med den för Eulerska grafer (alltså villkoret från Sats 15.4).

Det kanske är klart att ju fler kanter grafen har, desto större är chansen att det finns en Hamiltonkrets. Alla kompletta grafer $K_n$ för $n \geq 3$, är Hamiltonska. Ett av de vackraste tillräckliga villkoren ges i en sats av norrmannen Øystein Ore. Beviset för satsen finns i appendixet till detta kapitel.

**Sats 15.5** (Ores sats). *Låt G vara en enkel graf med $n \geq 3$. Om det för varje par av hörn u och v, som* inte *är förbundna med en kant, gäller att* $\deg(u)+\deg(v) \geq n$, *så är G Hamiltonsk.* ☻

Med andra ord: om grafen har rätt så många kanter, är den Hamiltonsk. Ores villkor är alltså ett tillräckligt villkor för existensen av en sådan krets. Viktigt är att inse att det inte alls är nödvändigt. Tänk bara på en graf som endast består av en enda krets, låt säga med 100 hörn. Då är $\deg(u)+\deg(v) = 4 < 100$ för varje par av hörn, men grafen är ändå Hamiltonsk.

**Exempel 15.8.** *I en fest deltar $n \geq 5$ personer. Alla ska placeras kring ett runt bord, men man vet att person* 1 *och* 2 *inte vill sitta bredvid varandra, person* 2 *inte heller vill sitta bredvid person* 3*, som inte heller vill sitta vid person* 4*, osv.*

10 En handelsresande ska besöka ett antal städer förbundna med vägar. Hur ska hen planera resan, om hen bara vill besöka varje stad en gång och återvända hem?

11 Ett antal personer ska sättas runt en bord. Hur kan bordplaceringen ordnas, om vi vill att varje person ska känna sina närmaste bordsgrannar?

*fram till person $n$ som varken vill sitta vid person $n-1$ eller person 1. I övrigt har ingen några andra önskemål. Kan bordsplaceringen organiseras så att var och en inte sitter bredvid någon som hen inte tycker om?*

*Lösning:* Grafteoretiskt (där hörnen står för personer och kanten mellan två hörn anger att motsvarande två personer får sitta bedvid varandra) har vi att göra med $K_n$ från vilken man har avlägsnat en krets med $n$ hörn (alltså den Hamiltonska kretsen $1-2-3-\cdots-n-1$) och vi är ute efter en annan sådan krets. Eftersom varje hörn i $K_n$ har grad $n-1$ har varje hörn i den nya grafen graden $n-3$. För varje par $u$ och $v$ av hörn gäller då att $\deg(u)+\deg(v) = 2n-6 \geq n$ för alla $n \geq 6$. Enligt Ores sats är grafen Hamiltonsk för $n \geq 6$. För $n = 5$ är det lätt att kontrollera att $K_5$ består av två Hamiltonska kretsar utan gemensamma kanter: om man avlägsnar en krets är den andra kvar. ☻

En svagare variant av Ores sats är följande villkor:

**Korollarium 15.2.** *Låt $G$ vara en enkel graf med $n \geq 3$ hörn. Om det för varje hörn $v$ gäller att $\deg(v) \geq \frac{n}{2}$, är $G$ Hamiltonsk.*

*Bevis.* Slutsatsen följer direkt ur Ores sats. ☻

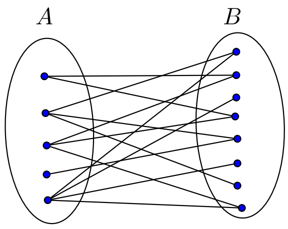
**Exempel 15.9.** *Till en middag skulle ett antal av $\geq 2n+2$ personer sättas runt ett bord. Var och en av deltagarna kände precis $n$ av de övriga gästerna, men värden ville att var och en ska sitta mellan två personer som hen inte kände. Är en sådan bordsplacering möjlig?*

*Bevis.* Låt $G$ vara ”icke-bekant”-grafen. En kant mellan två hörn svarar alltså mot att motsvarande personer inte känner varandra. $G$ har $k \geq 2n+2$ hörn, var och en med grad $k-1-n$. Eftersom $k-1-n \geq \frac{k}{2}$ (kontrollera detta) medför Korollarium 15.2 att $G$ är Hamiltonsk. Alltså är den önskade bordsplaceringen möjlig. ☻

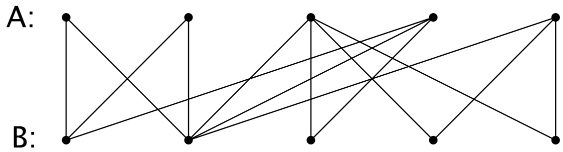
## 15.7 Bipartita grafer

Bipartita grafer bildar en klass för sig och tack vare sin enorma tillämpbarhet har de studerats väldigt ingående. En enkel graf kallas *bipartit* om hörnmängden kan delas in i två disjunkta (alltså utan gemensamma element) delmängder $A$ och $B$, ofta kallade hörnklasser, så att de enda kanter som förekommer har ett hörn i $A$ och ett hörn i $B$. Inga kanter går mellan hörnen i mängden $A$ och inga mellan hörnen i $B$. Detta kan åskådliggöras med följande figur:



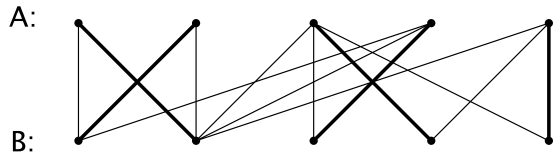

Låt oss nu bli helt seriösa i våra tillämpningar. Här kan det till exempel handla om arbetstilldelning på en arbetsplats: Hörnen i $A$ utgörs av personer och $B$ av arbetsuppgifter. Kanterna kan betyda vilka arbetsuppgifter som personerna i $A$ kan utföra. Tänk till exempel lärarna i en skola och de olika ämnen de kan undervisa i.

**Exempel 15.10.** *Förmannen på ett företag har fem hantverkare och fem arbetsuppgifter att genomföra. Raden A i figuren nedan betecknar hantverkare och raden B betecknar arbetsuppgifterna Kanterna visar vilka uppgifter de respektive hantverkarna är kvalificerade för. Kan förmannen göra en arbetstilldelning så att var och en av hantverkarna gör ett jobb hen är kvalificerad för?*




*Lösning:* Det finns många mer eller mindre snillrika algoritmer för att snabbt finna en så kallad *matchning* i en bipartit graf (om en sådan över huvud taget existerar). I ett litet exempel som det aktuella kan man lätt göra det manuellt. Men om grafen är större, med till exempel tusentals hörn, så kräver situationen en datakörning.

Svaret på uppgiften finns i figuren nedan, där en möjlig matchning är markerad med fetare kanter.




☻

Handskakningslemmat har en speciellt behaglig och nyttig form för bipartita grafer.

**Sats 15.6.** *Låt G vara en bipartit graf med e kanter och hörnklasser* $A = \{a_1, \ldots, a_k\}$ *och* $B = \{b_1, \ldots, b_m\}$. *Då gäller att*

$$\sum_{i=1}^{k} \deg(a_i) = e = \sum_{i=1}^{m} \deg(b_i).$$

*Bevis.* Eftersom varje kant har den ena ändpunkten i $A$ och den andra i $B$ så är slutsatsen omedelbar. ☻

En bipartit graf, där varje par $(a,b)$ av hörn (med $a$ i $A$ och $b$ i $B$) utgör en kant, kallas för en *komplett bipartit graf* och betecknas med $K_{m,n}$, där $m$ är antalet hörn i $A$ och $n$ är antalet hörn i $B$.

En användbar karaktärisering av bipartita grafer är följande sats:

**Sats 15.7.** *En graf G är bipartit om och endast om G saknar kretsar med udda antal kanter (alltså udda kretsar).*

*Bevis.* (⇒) Om $G$ är bipartit med hörnklasser $A$ och $B$, är vartannat hörn i en krets i $A$ och vartannat är i $B$. Därmed måste en krets ha ett jämnt antal hörn.

($\Leftarrow$) Antag att alla kretsar är jämna. Välj ett hörn $v$ och för varje hörn $u$ i samma komponent som $v$ låt $d(u)$ vara längden av den kortaste stigen från $v$ till $u$. Färglägg med rött varje hörn $u$ med udda $d(u)$ och med grönt varje hörn $u$ med jämn $d(u)$. Om det skulle finnas en kant mellan två röda eller två gröna hörn, skulle vi få en udda krets, vilka ju inte fanns i denna graf: till exempel om det finns en kant mellan två röda hörn $u_1$ och $u_2$ så bildar denna kant tillsammans med stigarna från $v$ till $u_1$ och från $v$ till $u_2$ en udda krets.

Upprepas samma procedur för alla komponenter av $G$ så får vi en indelning av hörnen i $G$ i två färgklasser, utan kanter inom varje klass. $G$ är alltså bipartit. ☻

**Exempel 15.11.** *Låt $m$ och $n$ vara två heltal $\geq 2$. Hur många stigar av längd $3$ finns det i $K_{m,n}$? Notera att stigar inte är orienterade, vilket betyder att stigen $a - b - c - d$ är densamma som stigen $d - c - b - a$.*

*Lösning:* Antag att hörnen i $K_{m,n}$ definieras av mängderna $A$ med $m$ hörn och $B$ med $n$ hörn. Varje val av två hörn $x, y$ ur $A$ och två hörn $u, v$ ur $B$ genererar fyra stigar av längd 3: $x - u - y - v$, $x - v - y - u$, $y - u - x - v$ och $y - v - x - u$. Svaret är därför $4\binom{m}{2}\binom{n}{2}$. ☻

## 15.8 Färgläggning

Tänk dig en mottagning med flera gäster. Tyvärr tycker vissa par av gästerna så illa om varandra att värden inte vågar sätta dem vid samma bord. Hur kan värden lösa detta problem? Klart att en lösning vore att se till att det finns lika många bord som gäster, men det vore en ganska tråkig fest. Det gäller att få så få bord som möjligt.

Grafteoretiskt kan vi tänka på följande sätt: Låt hörnen i en graf $G$ representera gäster och kanterna representera ”tycka-inte-om”-relationen. Det gäller att färglägga hörnen i $G$ med så få färger som möjligt, på sådant sätt att två hörn förbundna med en kant får olika färg. Varje färgklass kan då representera ett bord på festen.

En sådan färgläggning av hörnen i en graf $G$ är ett mycket viktigt och väl studerat problem med ett spektrum av tillämpningar, bortom det rent socialpsykologiska. Idén var också en av drivkrafterna i den snabba utvecklingen av grafteorin i mitten av förra århundradet och kulminerade i lösningen av en berömd förmodan, fyrfärgsförmodan.

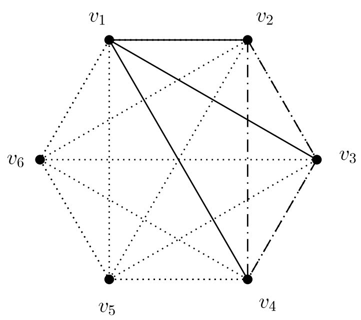
Fyrfärgsformodan, som i dag alltså uppgraderats till fyrfärgssatsen, gällde färgläggningen av planära grafer och har sitt ursprung i färgläggning av kartor (länderna representeras av hörn i en graf och två hörn förbinds med en kant om motsvarande länder har en gemensam gränssträcka). Det är klart att man vill att angränsande länder får olika färg. I praktiken fann man att det alltid räckte med fyra färger, men det visade sig vara mycket svårt att bevisa detta faktum. Det dröjde mer än 120 år innan det till slut bevisades år 1976 med hjälp av bland annat en massiv insats av datorkraft[12].

En annan problemtyp kan grafteoretiskt tolkas som färgläggning av kanterna i en graf, på sådant sätt att kanterna som möts i ett hörn får olika färg. Ett bra exempel på en sådan frågeställning illustreras i följande två exempel.

**Exempel 15.12.** *Visa att det i ett sällskap om sex personer finns tre som är sinsemellan bekanta eller tre som inte känner varandra.*

*Lösning:* Grafteoretiskt kan situationen tolkas som att kanterna i $K_6$ färgläggs i två färger: blå (för bekanta) och röd (för obekanta). Man ska visa att grafen innehåller en enfärgad triangel.

Var och en av de sex hörnen har grad 5, varför minst tre av kanterna måste ha samma färg. Välj hörnet $v_1$ och antag att kanterna $(v_1,v_2)$, $(v_1,v_3)$ samt $(v_1,v_4)$ är blåa (se figuren nedan). Om nu en av de tre kanterna mellan $v_2, v_3, v_4$ är blå så är vi klara: vi har en blå triangel. Annars är alla de tre kanterna röda, och vi har en röd triangel.




☻

**Exempel 15.13.**

12 Kenneth Appel and Wolfgang Haken från University of Illinois.

*Visa att det i ett sällskap om nio personer alltid finns fyra som alla är bekanta med varandra, eller tre som inte känner varandra.*

*Lösning:* Utnyttjande den kompletta grafen $K_9$ på nio element, kan vi formulera informationen som att vi återigen ska färglägga kanterna i $K_9$ i två färger: blå (för bekanta) och röd (för obekanta). Notera att $K_9$ har $\binom{9}{2} = 36$ kanter. Vi ska betrakta två fall: (1) det finns ett hörn $v$ ur vilket utgår minst 6 blå kanter, och (2) det finns ett hörn med som mest fyra blå kanter. Observera att det inte är möjligt att det från alla hörn utgår precis 5 blå kanter. I så fall skulle den ”blåa” delgrafen ha udda grad i alla nio hörn, vilket skulle ge en udda gradsumma för den blå delgrafen.

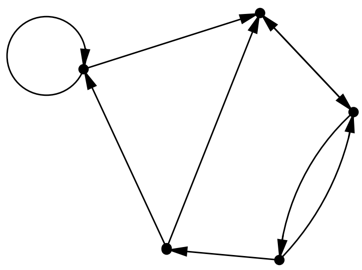
(1): I det första fallet anta att kanterna $(v,v_i)$ är blå för $i = 1, 2, \dots, 6$ och betrakta hörnen $\{v_1, \dots, v_6\}$. Enligt det förra exemplet kommer de sex hörnen att innehålla en blå eller en röd triangel, vilket tillsammans med $v$ skulle ge den konfiguration som uppgiften handlar om: den blå triangeln ger tillsammans med $v$ fyra bekanta, medan den röda triangeln ensamt (utan $v$) ger tre obekanta.

(2): I det andra fallet, finns det som mest fyra blå kanter, utgående ur ett hörn $u$. Då finns det minst fyra röda kanter ur $u$, låt oss säga kanterna $(u,u_j)$ för $j = 1, 2, 3, 4$. Om minst en av kanterna mellan de fyra hörnen $\{u_1, \dots, u_4\}$ är röd, är vi klara. I annat fall är alla dessa kanter blå, och vi är också klara. ☻

Fler exempel, resultat och öppna problem i samma anda får man om man letar i litteraturen eller på internet under rubriken Ramseyteori (efter den brittiske filosofen och logikern Frank P. Ramsey som levde under första hälften av 1900-talet).

## 15.9 Riktade (orienterade) grafer

En *riktad graf*, eller *orienterad graf*, $\overrightarrow{G}$ är en graf vars alla kanter utrustas med pilar som anger riktningen (jämför med enkelriktade gator). Eventuella stigar måste då gå endast i pilarnas riktning. Ett exempel är grafen i figuren nedan. För varje hörn $v$ i $G$ är det då meningsfullt att definiera *in-graden*, $\deg_+(v)$, och *ut-graden* $\deg_-(v)$, som antalet kanter som är riktade till, respektive från $v$.



Så gott som alla begrepp från ”vanliga” grafer överförs automatiskt, dock med små modifikationer, till den riktade varianten. Det är till exempel inte svårt att visa en ”riktad” variant av Eulers sats 15.4 (i beviset använder man sig av antagandet om att antalet in-kanter är samma som antalet ut-kanter vid varje hörn).

**Sats 15.8.** *Givet är en orienterad graf* $\overrightarrow{G}$ *sådan att den underliggande (icke-orienterade) grafen är sammanhängande. Då har* $\overrightarrow{G}$ *en (riktad) Eulerkrets om och endast om* $\deg_+(v) = \deg_-(v)$ *för alla hörn* $v$ *i* $\overrightarrow{G}$.

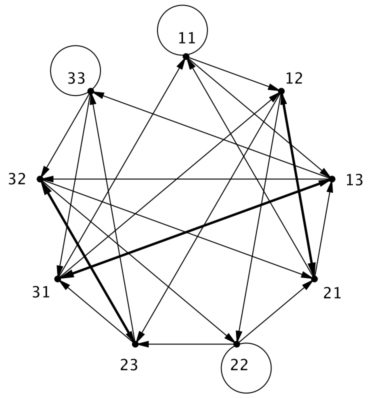
☻

Ett par tillämpningar av riktade grafer visas i de två exempel som följer.

**Exempel 15.14.** *Ett lås har tre knappar markerade med siffrorna* 1, 2 *och* 3. *Låset öppnas om man trycker rätt tresiffrig sifferföljd. Vilket är det minsta antal knappar man måste trycka för att alla möjliga kombinationer av de tre siffrorna* 1, 2 *och* 3 *ska förekomma i denna följd (praktiskt ifall man har glömt koden eller bara vill bryta sig in)?*

*Lösning:* Betrakta grafen $\overrightarrow{G}$ vars hörnmängd består av alla nio par $(a,b)$, där $a$ och $b$ är siffrorna 1, 2 och 3, och där man drar kanten från $(a,b)$ till $(c,d)$ om och endast om $b = c$ (figuren nedan). Varje kant representerar då en tresiffrig kod: kanten $(a,b) \to (b,d)$ representerar koden $abd$. Notera de tre tjockare pilarna, till exempel mellan (1,2) och (2,1), De är riktade åt bägge hållen och representerar dels kanten 121, dels 212. Därmed ska de betraktas som två kanter. Öglorna är förstås också riktade, men i figuren inte markerade med pilar.




Observera att det för varje hörn $v$ i $\overrightarrow{G}$ gäller att $\deg_{in}(v) = \deg_{ut}(v) = 3$ och att grafen är sammanhängande. Därmed existerar en (riktad) Eulerkrets i denna graf. Trycker man på knapparna längs denna krets så får man alla koder. Ett exempel på en sådan Eulerkrets är 11122213223332321211331312311. De första sex siffrorna, 111222 representerar följande kanter: öglan vid (1,1), kanten från (1,1) till (1,2), kanten från (1,2) till (2,2) och öglan vid (2,2), alltså koderna 111, 112, 122 och 222. Det räcker alltså med 29 knapptryckningar. Jämför detta med de 81 knapptryckningar som skulle behövas, om man tryckte in alla 27 olika koder. ☻

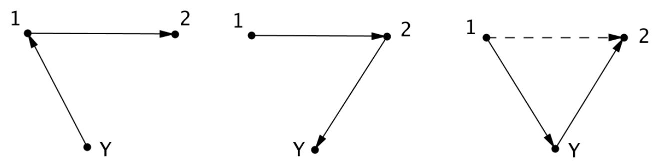
Sist ska vi visa att det i en komplett riktad graf $\overrightarrow{K}_n$ alltid finns en (riktad) Eulerstig. Grafen $\overrightarrow{K}_n$ kallas ofta för en *turnering* för den kan beskriva utgången av en turnering med $n$ deltagare. Pilen mellan två hörn visar vem av de två spelarna som vann i deras match (alla spelar mot alla).

**Exempel 15.15.** *I ett land finns $n \geq 2$ städer och det finns en väg mellan varje par av städer (observera att inga vägar korsar varandra, då eventuella korsningar löses med broar och tunnlar). Statsministern beslutade att alla vägar ska vara enkelriktade. Mellan varje par av städer finns det dessutom bara en väg. Visa att oberoende av hur transportministern bestämmer riktningarna på rikets vägar,* *så kommer det att finnas två städer A och B sådana att det blir möjligt att resa från A till B och på vägen besöka varje annan stad i riket en gång.*

*Lösning:* Vi vill visa att det i en komplett, riktad graf $\overrightarrow{K}_n$ finns två hörn $A$ och $B$, sådana att det finns en (riktad) Hamiltonstig från $A$ till $B$.

För två hörn $X$ och $Y$, låt beteckningen $X \to Y$ betyda att det finns en kant riktad från $X$ till $Y$. Tag ett godtyckligt hörn 1. Om vi nu väljer en annan stad $X$, gäller det antingen att $1 \to X$ eller att $X \to 1$. Låt i det första fallet hörnet $X$ få nummer 2. I det andra fallet får $X$ nummer 1, medan det första hörnet i stället får nummer 2.

Välj nu ett tredje hörn $Y$. Betrakta de tre fallen som kan inträffa (se figur nedan): $Y \to 1$ eller $2 \to Y$ eller $1 \to Y \to 2$. De två första fallen utesluter inte varandra. Det kan nämligen samtidigt hända att $Y \to 1$ och $2 \to Y$. I det första fallet (eller då både fall ett och två inträffar) låt hörnet $Y$ få nummer 1 och öka de övriga två hörnens nummer med 1. Låt i det andra fallet hörnet $Y$ få nummer 3. I det tredje fallet, låt hörnet $Y$ få nummer 2 och öka samtidigt numret på det hörn som tidigare hade nummer 2 med 1. Nu har vi fått tre hörn numrerade på ett sådant sätt att $1 \to 2 \to 3$.




Låt oss anta att vi redan har numrerat $k$ hörn från 1 till $k$ på ett sådant sätt att $1 \to 2 \to 3 \to \cdots \to k$ . Välj nästa hörn och kalla det för $Z$. Det finns nu tre fall att betrakta: (a) $Z \to 1$, (b) $k \to Z$ och (c) ingetdera av de två första alternativen gäller. (Liksom tidigare observerar vi att de två första alternativen inte utesluter varandra.) I vart och ett av dessa tre alternativen kan vi göra följande:

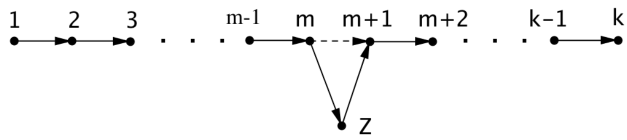
(a) Låt hörnet $Z$ få nummer 1 och låt numren på de övriga $k$ hörnen öka med 1.

(b) Låt hörnet $Z$ få nummer $k + 1$.

(c) Eftersom varken $Z \to 1$ eller $k \to Z$ gäller så har vi både $1 \to Z$ och $Z \to k$. Bland alla numren $1, 2, \ldots, k - 1$, välj det sista numret $m$ som är sådant att $m \to Z$. Ett sådant nummer måste finnas eftersom vi vet att $1 \to Z$ och att för staden $k$ gäller det omvända, nämligen $Z \to k$. Vi har alltså $m \to Z \to m{+}1$

(se figuren nedan). Låt oss då beteckna hörnet $Z$ med nummer $m+1$, medan vi samtidigt ökar (med 1) numren på alla hörn som tidigare hade nummer $m+1, m+2, \ldots, k$.




Alla tre alternativen leder till en följd av $k+1$ hörn som uppfyller $1 \to 2 \to \cdots \to k \to k+1$. Vi fortsätter denna numreringsprocess tills alla hörn i grafen har fått ett nummer. Hörnen har alltså ordnats i en följd sådan att $1 \to 2 \to 3 \to \cdots \to n-1 \to n$. Låt då $A$ och $B$ vara de hörn som fick nummer 1 respektive $n$. ☻

## 15.10 Appendix

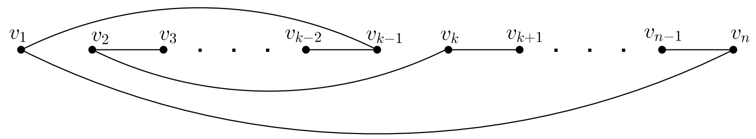
Här kommer beviset för Ores sats, Sats 15.5.

*Bevis.* Antag att $G$ inte är Hamiltonsk. Om vi lägger till tillräckligt många nya kanter till $G$, kommer den att innehålla en Hamiltonkrets (lägger man till alla möjliga kanter får man ju $K_n$ som är Hamiltonsk). Låt $H$ vara den sista icke-Hamiltonska grafen i denna procedur och kanten $e = (v_1, v_2)$ vara den kant som, efter att man lägger den till $H$, kommer att göra grafen Hamiltonsk. Vi har alltså kretsen (om $e$ finns med)

$$v_1 \to v_2 \to v_2 \to v_3 \to \cdots \to v_{n-1} \to v_n \to v_1$$

Antag att i grafen $H$ finns en kant mellan $v_2$ och något $v_k$ för $3 \le k \le n$. Vi ska visa att i så fall kan det inte finnas någon kant mellan $v_1$ och $v_{k-1}$ (notera att kanten $e$ inte finns med i $H$).

Antag motsatsen, dvs. antag att samtidigt som $H$ innehåller kanten $(v_2, v_k)$ innehåller den också kanten $(v_1, v_{k-1})$. Då skulle följande utgöra en Hamiltonkrets i grafen $H$:




$$v_2 \to v_k \to v_{k+1} \to \cdots \to v_n \to v_1 \to v_{k-1} \to v_{k-2} \to \cdots \to v_3 \to v_2,$$

alltså en Hamiltonkrets som helt undviker kanten $e$. Detta motsäger det faktum att $H$ var icke-Hamiltonsk. Därmed, för varje $3 \le k \le n$, får det som mest en av kanterna $(v_2,v_k)$ och $(v_1,v_{k-1})$ finnas i grafen $H$. Följaktligen är $\deg_H(v_1) + \deg_H(v_2) < n$, där $\deg_H(u)$ står för hörnets grad i grafen $H$.

Samtidigt har vi att $\deg_H(u) \ge \deg_G(u)$, då $H$ kom till genom att komplettera $G$ med nya kanter. Därmed är $\deg_G(v_1) + \deg_G(v_2) < n$, vilket strider mot antagandet i Ores sats. Därmed är satsen bevisad. ☻

## 15.11 Hemuppgifter

Flertalet av uppgifterna här kan lösas med andra metoder än grafteoretiska. Det kommer dock att förväntas att man ger uppgifterna grafteoretiska tolkningar och sedan löser dem med hjälp av grafteori.

**Uppgift 15.1** ** I ett gammalt slott spökar det varje natt, men enbart i rum med udda antal dörrar (med ett ”rum” menas här varje utrymme, såväl vanliga rum som hallar, kök, toaletter och dylikt). Slottet har enbart en ingång. Är det möjligt att, vid övernattningsbehov, på slottet hitta ett spökfritt rum?

(L)

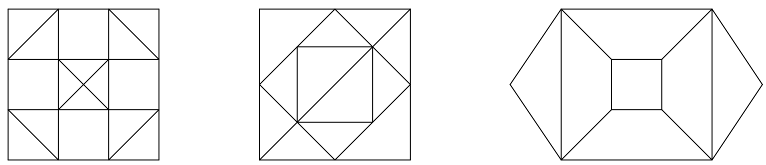
**Uppgift 15.2** *** a) Sats 15.3 säger att om $G$ är en enkel, sammanhängande och planär graf med $n \ge 3$ hörn och $k$ kanter, är $k \le 3n - 6$. I beviset användes det faktum att varje region $r$ begränsas av minst tre kanter, dvs. $\deg(r) \ge 3$.

Låt $t$ vara ett heltal $\ge 3$. Generalisera Sats 15.3 till en planär, sammanhängande och enkel graf, sådan att $\deg(r) \geq t$ för varje region $r$ som grafen delar planet i.

b) Visa att grafen $K_{3,3}$ inte är planär.

(L)

**Uppgift 15.3** * För varje graf i figuren nedan, avgör existensen av en Eulerkrets eller en Eulerstig:



**Uppgift 15.4** * Låt talen $\{1, 2, \ldots, 15\}$ utgöra hörn i en graf $G$ och låt talparet $(a, b)$ vara en kant omm $SGD(a, b) > 1$. Hur många komponenter har $G$? Bestäm den längsta stigen utan upprepade hörn i $G$.

**Uppgift 15.5** * Bestäm alla positiva heltal $m, n$ för vilka grafen $K_{m,n}$ är Eulersk.

**Uppgift 15.6** ** Låt $n$ vara ett positivt heltal och betrakta mängden $V$ av alla följder av 0:or och 1:or av längd $n$. Låt $V$ utgöra hörn i en graf $G$, där två följder förbinds med en kant om och endast om följderna skiljer sig på exakt ett enda ställe. Visa att $G$ är bipartit.

**Uppgift 15.7** ** a) Måste varje Eulersk bipartit graf ha ett jämnt antal kanter?

b) Måste varje enkel, Eulersk graf med jämnt antal hörn ha ett jämnt antal kanter?

**Uppgift 15.8** *** a) Låt $n \geq 2$ vara ett heltal. Konstruera en sammanhängande, enkel graf med $2n$ hörn, sådan att alla hörn har grad 3.

b) Låt $n \geq 1$ vara ett heltal. Konstruera en sammanhängande enkel graf med $2n$ hörn, sådan att det för varje $k$, $1 \leq k \leq n$, finns två hörn av grad $k$.

(L)

**Uppgift 15.9** ** Låt $n \geq 1$ vara ett heltal och antag att $G$ är en enkel sammanhängande graf med $\deg(v) \geq k$ för alla hörn $v$ i $G$. Visa att $G$ har en stig av längd $k$ och utan upprepade hörn.

**Uppgift 15.10** ** Var och en av de 61 regioner som en planär graf $G$ delar planet i begränsas av minst 5 kanter. Visa att grafen $G$ har minst 94 hörn.

(L)

**Uppgift 15.11** ** a) Formulera en generalisering till Sats 15.2 till en planär graf som består av $m$ komponenter.

b) Låt $G$ vara en enkel planär graf som består av tre komponenter och där varje hörn har grad 3. Om $G$ har 27 kanter, hur många regioner delar $G$ planet i?

**Uppgift 15.12** *** a) Hur många olika Hamiltonkretsar finns det i $K_n$, $n \geq 3$?

b) Hur många olika Hamiltonkretsar i $K_9$ är sådana att ingen kant förekommer mer än en gång? Vad blir svaret, om 9 ersätts med $n$, där $n \geq 3$?

c) På hur många sätt kan 10 personer placeras runt ett bord så att två personer inte sitter bredvid varandra mer än en gång?

**Uppgift 15.13** ** a) Hur många Hamiltonkretsar finns det i $K_{n,n}$, $n \geq 2$?

b) Hur många Hamiltonstigar finns det i $K_{n,n}$, $n \geq 1$?

**Uppgift 15.14** * Till en middag anländer 14 gäster. Var och en känner minst 7 andra av de närvarande (bekantskap anses vara en ömsesidig relation). Visa att personerna kan placeras runt ett bord så att varje gäst känner båda sina bordsgrannar.

**Uppgift 15.15** *** Tjugo tävlande deltar i en schackturnering där varje par av deltagare spelar ett parti. Vilket är det minsta antalet partier som måste spelas, för att det bland tre godtyckliga deltagare ska finnas två som redan har spelat mot varandra?

(L)

**Uppgift 15.16** ** Låt hörnen i grafen $G$ utgöras av alla tal från 0 till 999 (inklusive ledande nollor som till exempel 000, 001, 002, ..., 010, 011, 012, ...). Två sådana hörn förbinds med en kant, om de har minst en likadan siffra i samma position (till exempel 318 och 018). Är grafen $G$ Eulersk?

**Uppgift 15.17** *** I ett land har varje par av städer en direkt förbindelse mellan sig med endast ett kommunikationsmedel: buss, tåg eller flyg. Alla tre kommunikationsmedlen används, men ingen stad har alla tre tillgängliga. Dessutom går aldrig parvisa förbindelser mellan godtyckliga tre städer via ett och samma kommunikationsmedel: om $A$, $B$ och $C$ är tre godtyckliga städer, är förbindelser mellan $A$ och $B$, $A$ och $C$ samt $B$ och $C$ ej av samma sort. Bestäm det största möjliga antalet städer i detta land.

(L)

**Uppgift 15.18** *** En ljustekniker på en teater har en lampa och tre olikfärgade filter: ett grönt, ett blått och ett rött. Genom att sätta ett eller flera eller inget filter alls på lampan, kan han åstadkomma åtta olika ljuseffekter. Filtren kan ändras ett i taget: antingen avlägsnar man ett som man just använt eller så lägger man på ett av de andra. Om vi antar att teknikern börjar och slutar utan filter, kan hen då testa alla ljuskombinationerna en efter en utan att behöva upprepa en och samma effekt, förutom den vid starten och avslutningen?

(L)

**Uppgift 15.19** *** I en schackturnering deltar 66 spelare. Varje par av de spelande möts bara en gång. Turneringen pågår i fyra städer. Visa att det säkert finns tre deltagare som spelar alla partier sinsemellan i en och samma stad. (Alternativt: Kanterna i $K_{66}$ målas i fyra färger. Visa att det måste finnas en triangel med likafärgade sidor.)

(L)

**Uppgift 15.20** ** En fabrik producerar tvåfärgade tyger och använder till detta ett urval av sex färger. Varje färg måste förekomma på minst tre olika tyger. Visa att man kan välja tre tyger så att varje färg förekommer i något av tygerna och att detta kan göras på minst två olika sätt.

(L)

**Uppgift 15.21** *** Ett visst samhälle har 1000 invånare. Dagligen berättar varje invånare för sina vänner allt skvaller som hen fick höra dagen innan. Det är känt att varje nyhet förr eller senare kommer att vara känd av alla invånare. Visa att det är möjligt att välja 90 invånare på så sätt att om man meddelar dem en nyhet samtidigt så kommer nyheten att vara allmänt känd inom 10 dagar.

(L)

**Uppgift 15.22** ** Till kung Arthurs slott anlände $2n$ riddare. Var och en av dessa hade som mest $n-1$ fiender bland de övriga riddarna (fientligheten antas vara ömsesidig). Visa att trollkarlen Merlin kan placera ut dessa $2n$ riddare runt det runda bordet på sådant sätt att ingen riddare sitter granne med någon av sina fiender.

**Uppgift 15.23** *** Värdparet på ett party känner alla $n$ inbjudna gäster. Det visar sig att för varje godtycklig uppsättning av tre inbjudna peroner gäller att minst två är bekanta med varandra. Visa att det är möjligt att placera alla de $n + 2$ närvarande personerna runt ett bort så att varje person känner sina båda bordsgrannar.

(L)

**Uppgift 15.24** ** Varje kant i $K_{18}$ målas i en av två färger. Visa att det finns fyra hörn sådana att alla kanter mellan dessa fyra hörn är målade med samma färg.

(L)

**Uppgift 15.25** *** Mellan två godtyckliga öar i ett stort örike finns det direktförbindelse med antingen båt eller flyg. Alla sträckor trafikeras i båda riktningar (och då med samma färdmedel förstås). Visa att

a) man för varje ö kan finna ett transportmedel med vilket det är möjligt att från denna ö nå vilken annan ö som helst med som mest ett båt- respektive planbyte (om man till exempel åker båt till en ö och sedan byter till en annan båt och direkt kommer fram);
b) man kan lägga ner ett av transportmedlen i hela riket och det fortfarande blir möjligt att från vilken ö som helst nå en godtyckligt vald annan ö och dessutom med som mest två byten.

(L)

**Uppgift 15.26** ** Stigarna i denna uppgift har inga upprepade hörn. Dessutom är stigarna inte orienterade: vänder man på ordningen på hörnen så är det samma stig.

a) Hur många stigar av längd 5 finns det i $K_{3,7}$?
b) Hur många stigar av längd 4 finns det i samma graf?

**Uppgift 15.27** *** Låt $k$, $m$ och $n$ vara positiva heltal sådana att $1 \leq k \leq 2m < n$.

Hur många stigar av längd $k$ finns det i $K_{m,n}$? Notera att stigarna inte är orienterade, dvs. vänder man på ordningen på hörnen så är det samma stig.

(L)

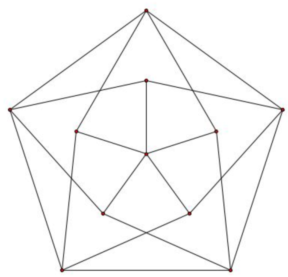
**Uppgift 15.28** ** En dominobricka består av två kvadratiska fält. På varje fält finns det mellan 0 och 6 prickar. I en hel uppsättning finns det alltså 28 olika brickor. Två brickor får läggas intill varandra om antalet prickar är detsamma på de fält som vidrör varandra. Är det möjligt att lägga brickorna i en enda sluten ring?

(L)

**Uppgift 15.29** ** Antag att en sammanhängande graf har $2k$ udda hörn. Visa att kanterna i $G$ kan delas in i $k$ stigar utan gemensamma kanter (dvs. *kant-disjunkta* stigar). Jämför med Sats 15.4b.

**Uppgift 15.30** ** En springare placeras på ett $3 \times 4$-schackbräde. Är det möjligt för springaren att besöka alla brädets rutor, och varje ruta en enda gång? Är det möjligt att efter det sista steget återigen hamna i samma hörnruta där man började?

**Uppgift 15.31** * Är grafen i figuren nedan Hamiltonsk?



**Uppgift 15.32** ** a) Existerar en bipartit graf med tolv hörn med graderna $5, 5, 5, 4, 4, 3, 3, 3, 1, 1, 1, 1$?

b) Visa att det inte finns någon bipartit graf som har hörn med graderna $6, 6, \ldots, 6, 5, 3, 3, \ldots, 3$.

(L)

**Uppgift 15.33** * Antag att en bipartit graf har hörnklasser $A$ och $B$ och är $k$-*reguljär*, vilket innebär att alla hörn har samma grad $k$. Visa att hörnklasserna $A$ och $B$ är lika stora.

**Uppgift 15.34** * Låt $2 \leq m \leq n$ vara heltal.

a) Hur många kretsar av längd 4 innehåller $K_{m,n}$?

b) Hur lång är den längsta kretsen i $K_{m,n}$?

**Uppgift 15.35** *** Låt $3 \leq m \leq n$ vara heltal. Låt $G$ vara den bipartita grafen $K_{m,n}$ utökad med en kant.

a) Vilket är det största antal olika trianglar som då kan uppstå i $G$?

b) Vilket är det största antal olika kretsar av längd 5 som då kan uppstå i $G$?

(L)

**Uppgift 15.36** ** Antag att en graf $G$ har 12 hörn och 17 kanter, och att minsta graden hos ett hörn är 2 och högsta är 4. Antag vidare att grafen har en Eulerstig och är Hamiltonsk.

a) Hur många hörn av grad 3 har $G$?

b) Hur många hörn av grad 2 har $G$?

c) Konstruera en sådan graf.

**Uppgift 15.37** * Hörnen i grafen $G$ har grader, i tur och ordning $7, 7, 6, 6, 5, 5, 4, 4$. Är grafen Hamiltonsk?

**Uppgift 15.38** * Kan kanterna i $\overrightarrow{K}_n$ vara riktade på sådant sätt att det inte finns några kretsar?

**Uppgift 15.39** *** a) Kanterna i $\overrightarrow{K}_{37}$ är riktade på sådant sätt att $\deg_+(v) = \deg_-(v)$ för alla hörn $v$ i grafen. Visa att det för godtyckliga hörn $u$ och $v$ i grafen finns en stig från $u$ till $v$ av längd som mest 2.

b) En del av kanterna i grafen ovan suddades bort, så att $\deg_+(v) = \deg_-(v) = 14$ för varje hörn $v$ i grafen. Visa att det för godtyckliga hörn $u$ och $v$ i grafen fortfarande finns en stig från $u$ till $v$, fast denna gång av längd som mest 3.

(L)

**Uppgift 15.40** ** I ett land finns det bara enkelriktade vägar, men det är möjligt att åka mellan godtyckliga två städer och som mest passera en annan stad. En av vägarna stängdes för reparation, men det är fortfarande möjligt att åka mellan två godtyckligt valda städer. Visa att det kan göras genom att passera som mest två andra städer.

(L)

# Fördjupning i talteori

## 16.1 Introduktion

I detta kapitel kommer vi bland annat att behandla basen för all modern datorbaserad civilisation, i och för sig väl dold som några udda och nördigt intrikata egenskaper hos positiva heltal. Vi förutsätter att man har åtminstone några kunskaper från tidigare talteoretiska avsnitt, alltså kapitel 4, 6 och 7 (om induktion, delbarhet och kongruenser). Vi ska presentera Fermats Lilla Sats och Eulers generalisering av den. För den som tycker att vi tar i, rekommenderar vi att leta på nätet på sökorden Fermat, RSA, chiffer och koder till exempel.

Men vi kommer också att titta på sådana udda talmonster som perfekta tal, samt Fermats och Mersennes tal, som en del (inte vi, som mer är ute efter matematiska skräckupplevelser) kallar matematiska skönheter. Så låt alltså oss då först direkt hoppa in i den perfekta världen.

## 16.2 Perfekta tal

*Perfekta tal* fascinerade grekiska matematiker redan 500 år f.v.t. och har studerats av sådana storheter som Pythagoras och Euklides. De har alltså funnits i stort så länge som man hållit på med matematik. Innan vi definierar dessa tal behöver vi introducera funktionen $\sigma(n)$:

**Definition 16.1.** För varje positivt heltal $n$, låt $\sigma(n)$ (läs: sigma av $n$) stå för summan av alla positiva delare till $n$ (inklusive $n$ självt). Till exempel är $\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28$ och $\sigma(p) = 1 + p$, om $p$ är ett primtal.

Funktionen $\sigma(n)$ har en användbar egenskap: den är *multiplikativ*, vilket innebär att den bevarar en produkt, ifall talen saknar gemensamma delare större än 1. Mer precist:

**Lemma 16.1.** *Om* $\text{SGD}(a,b) = 1$ *så är* $\sigma(ab) = \sigma(a) \cdot \sigma(b)$.

*Bevis.* Låt $a_1, a_2, \ldots, a_s$ vara alla delare till $a$ och låt $b_1, b_2, \ldots, b_r$ vara alla delare till $b$. Då utgör produkterna $a_i b_j$, $1 \le i \le s$, $1 \le j \le r$ alla delare till $ab$. Deras summa är

$$\sigma(ab) = \sum_{\substack{1 \le i \le s, \\ 1 \le j \le r}} a_i b_j = (a_1 + a_2 + \ldots + a_s)(b_1 + b_2 + \ldots + b_r) = \sigma(a) \cdot \sigma(b).$$

☻

**Definition 16.2.** Ett positivt heltal $n$ är *perfekt* om $\sigma(n) = 2n$ (detta kan alternativt definieras som att summan av alla delare till $n$ som är mindre än $n$ är lika med $n$). Till exempel är $\sigma(6) = 1 + 2 + 3 + 6 = 2 \cdot 6$ och $\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 2 \cdot 28$. Talen 6 och 28 är de två minsta perfekta talen.

Tidiga kristna teologer förklarade att Guds skapelse av världen under sex dagar, berodde på just det faktum att 6 är ett perfekt tal. Perfektheten av talet 28 förklarade man med dess koppling till måncykeln, alltså ungefär en månad. Tyvärr så saknar de följande perfekta talen 496 och 8128 liknande associationer, men det finns säkert något avsnitt av Simpsons som förklarar vad det har med modern civilisation att göra.

Fram till i dag har man funnit nästan 50 perfekta tal, och de är alla är jämna. Då verkar det naturligt att gissa att ett perfekt tal *måste* vara jämnt, men hittills har man inte lyckats avgöra om detta är sant. Det bästa kända resultatet i den riktningen är att man har visat att eventuella udda perfekta tal måste vara större än futtigt lilla $10^{1500}$, men vad är det mot oändligheten? Det största kända (år 2015) perfekta talet är $n = 2^{57885160}(2^{57885161} - 1)$ och det har 34850340 siffror. Detta är en konsekvens av följande sats och av att talet $2^{57885161} - 1$ är ett primtal.

**Sats 16.1.** *Låt $n$ vara ett positivt heltal. Om $2^n - 1$ är ett primtal så är talet $d = 2^{n-1}(2^n - 1)$ ett perfekt tal.*

*Bevis.* Alla delare till $2^{n-1}(2^n - 1)$ är av formen $2^k$ för $k = 0,1,\ldots,n-1$ eller $2^k(2^n - 1)$ för $k = 0,1,\ldots,n-1$.

Summan av delarna är därmed

$$\sigma(d) = \sum_{k=0}^{n-1} 2^k + \sum_{k=0}^{n-1} 2^k(2^n - 1)$$

$$= 2^n - 1 + (2^n - 1)(2^n - 1) = 2^n(2^n - 1) = 2 \cdot 2^{n-1}(2^n - 1) = 2d,$$

vilket vi ville visa (vi använde här formeln för summan av en geometrisk talföljd: $\sum_{k=0}^{m} 2^k = 2^{m+1} - 1$) ☻

Omvändningen till denna sats är också sann och bevisades av Euler år 1750:

**Sats 16.2.** *Varje jämnt perfekt tal är på formen $2^{n-1}(2^n - 1)$, där $2^n - 1$ är ett primtal.*

*Bevis.* Antag att $k$ är ett perfekt tal och att $k = 2^n m$, där $n \geq 1$ och $m$ är ett udda tal. Eftersom $k$ är perfekt är $\sigma(k) = 2k$, alltså $\sigma(2^n m) = 2 \cdot 2^n m = 2^{n+1} m$.

Samtidigt, då $\mathrm{SGD}(2^n, m) = 1$, är

$$\sigma(2^n m) = \sigma(2^n) \cdot \sigma(m) = (1 + 2 + \cdots + 2^n)\sigma(m) = (2^{n+1} - 1)\sigma(m),$$

enligt Lemma 16.1. Därmed får vi att $2^{n+1} m = (2^{n+1} - 1)\sigma(m)$.

Låt oss skriva $\sigma(m)$ som $\sigma(m) = m + x$. Talet $x$ är summan av alla delare till $m$ som är mindre än $m$. Insättning i den sista likheten ger då att $2^{n+1} m = (2^{n+1} - 1)(m + x)$ som reduceras till $m = (2^{n+1} - 1)x$. Följaktligen är $x$ en delare till $m$. Vi ska visa att $x = 1$, vilket då förstås medför att $m = 2^{n+1} - 1$ är ett primtal[1].

Antag att $x > 1$. Då har $m$ minst tre olika delare: 1, $m$ och $x$. Således är $\sigma(m) \geq 1 + m + x = 1 + (m + x) = 1 + \sigma(m)$, vilket ger en motsägelse. ☻

**Exempel 16.1.** *Visa att ett udda perfekt tal inte kan ha bara två olika primtalsfaktorer.*

1 Vi visar alltså att ett jämnt perfekt tal är på formen $2^n(2^{n+1} - 1)$, där $2^{n+1} - 1$ är ett primtal, vilket är bara en omskrivning av påståendet som ska visas.

*Lösning:* Antag motsatsen, alltså antag att $n$ är ett udda perfekt tal och $n = p^k q^m$, där $p$ och $q$ är de olika primtalen $\geq 3$ och $k, m \geq 1$. Då är

$$2 = \frac{\sigma(n)}{n} = \frac{\sigma(p^k q^m)}{p^k q^m} = \frac{\sigma(p^k)\sigma(q^m)}{p^k q^m} = \frac{1 + p + \cdots + p^k}{p^k} \cdot \frac{1 + q + \cdots + q^m}{q^m} =$$

$$\left(\frac{1}{p^k} + \frac{1}{p^{k-1}} + \cdots + 1\right) \cdot \left(\frac{1}{q^m} + \frac{1}{q^{m-1}} + \cdots + 1\right) = \frac{1}{1 - \frac{1}{p}} \cdot \frac{1}{1 - \frac{1}{q}} \leq$$

$$\frac{1}{1 - \frac{1}{3}} \cdot \frac{1}{1 - \frac{1}{5}} = \frac{15}{8} < 2,$$

vilket medför motsägelse. Därmed kan inte $n$ ha precis två primtalsfaktorer.

☻

De positiva heltal $n$ för vilka $\sigma(n) < 2n$ kallas för *defekta* och de tal för vilka $\sigma(n) > 2n$ kallas för *ymniga*. Det finns oändligt många tal av varje sort: till exempel är alla primtal $p > 2$ defekta, medan om $n$ är ett perfekt tal, $kn$ år ymnigt för varje $k \geq 2$. Detta följer från att $\sigma(kn) > k \cdot \sigma(n) = k \cdot 2n = 2kn$ (observera att olikheten är en konsekvens av delbarheten: om $x$ är en delare till $n$, är både $x$ och $kx$ delare till $kn$).

Som vi visade ovan, är det avgörande för att ett jämnt tal ska vara perfekt, att det är av formen $2^{n-1}(2^n - 1)$, där $2^n - 1$ är ett primtal. Allmänt kallas talen $2^n - 1$ för *Mersennetal*[2] och primtal på formen $2^n - 1$ kallas för *Mersenneprimtal*. Det är intressant att det endast är för $a = 2$ som talen $a^n - 1$ kan vara primtal. Dessutom måste exponenten $n$ också vara ett primtal. Detta är innebörden av nästa sats, som först bevisades av Pierre de Fermat.

**Sats 16.3.** *Om talet $a^n - 1$ är ett primtal för heltal $a, n > 1$, så är $a = 2$ och $n$ är ett primtal.*

2 Efter den franske 1600-talsfilosofen och matematikern Marin Mersenne.

*Bevis.* Om $a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1)$ är ett primtal, är ju nödvändigtvis $a - 1 = 1$, och alltså $a = 2$.

Om nu $n$ skulle vara ett sammansatt tal $n = k \cdot m$, där $k, m > 1$, är $2^n - 1 = 2^{km} - 1 = (2^k)^m - 1 = (2^k - 1)\left((2^k)^{m-1} + (2^k)^{m-2} + \cdots + 2^k + 1\right)$. Eftersom båda faktorerna i det sista uttrycket är $> 1$ strider det mot antagandet att $2^n - 1$ är ett primtal. Därmed måste $n$ vara ett primtal. ☻

Primtal på formen $2^n - 1$ finns det gott om, till exempel $3 = 2^2 - 1$, $7 = 2^3 - 1$, $31 = 2^5 - 1$, osv.

## 16.3 Fermattalen

Efter att ha funnit villkor för att tal på formen $a^n - 1$ ska vara primtal, ägnade sig Fermat åt att finna villkor för att hitta primtal på formen $a^n + 1$. Han bevisade följande:

**Sats 16.4.** *Om $a^n + 1$ är ett primtal, där $a > 1$ och $n > 0$, så är $a$ jämnt och $n = 2^k$ för något positivt heltal $k$.*

*Bevis.* Antag att $a^n + 1$ är ett primtal. Om $a$ vore ett udda tal, skulle $a^n + 1$ vara ett jämnt tal större än 3, alltså inte ett primtal. Därför måste $a$ vara ett jämnt tal.

Antag att $n = 2^k m$, där $m$ är ett udda tal större än 1. Då är $a^n + 1 =$

$$a^{2^k m} + 1 = \left(a^{2^k}\right)^m + 1 = (a^{2^k} + 1)\left((a^{2^k})^{m-1} - (a^{2^k})^{m-2} + \cdots - a^{2^k} + 1\right).$$

Den sista likheten följer ur Sats 6.7 i kapitel 6. Eftersom båda faktorerna är $> 1$ motsäger detta antagandet att $a^n + 1$ är ett primtal. Därmed är $m = 1$, och vi är klara. ☻

För $a = 2$ visade Fermat att $Fe_n = 2^{2^n} + 1$ är primtal då $n = 0, 1, 2, 3, 4$. Han misstänkte att alla tal av denna typ, i dag kallade *Fermattal*, är primtal, vilket visade sig inte vara fallet. Euler upptäckte att redan $Fe_6$ är sammansatt och fram tills i dag har man inte hittat *något* annat Fermattal som är primtal än dem som Fermat kände till. Det måste vara den i särklass mest misslyckade gissning som någon stor matematiker någonsin gjort.

Fermattalen uppfyller ett flertal vackra identiteter. De flesta kan enkelt visas med induktion. Några av dessa identiteter är samlade i satsen nedan.

**Sats 16.5.** *a) För $n \geq 1$ är $Fe_n = Fe_0 Fe_1 \cdots Fe_{n-1} + 2$.*
*b) För $n \geq 1$ är $Fe_n = (Fe_{n-1} - 1)^2 + 1$.*
*c) För $n \geq 2$ är $Fe_n = (Fe_{n-1})^2 - 2(Fe_{n-2} - 1)^2$.*
*d) För $n \geq 2$ är $Fe_n = Fe_{n-1} + 2^{2^{n-1}} \cdot Fe_0 Fe_1 \cdots Fe_{n-2}$.*

*Bevis.* Alla egenskaper bevisas enkelt med induktiv handviftning.... ☻

Vi avslutar detta avsnitt med en liten övning om Fermattal:

**Exempel 16.2.** *Visa att för alla $n \geq 2$ kan varje Fermattal $Fe_n$ skrivas på oändligt många sätt som $x^2 - 2y^2$, där $x$ och $y$ är positiva heltal.*

*Lösning:* Existensen av *ett* sådant par $(x_0, y_0)$ garanteras av Sats 16.5c ovan, nämligen $x_0 = Fe_{n-1}$ och $y_0 = Fe_{n-2} - 1$.

Läsaren har förstås ofta slagits av att $(3x + 4y)^2 - 2(2x + 3y)^2 = x^2 - 2y^2$. Detta innebär att vi givet ett ynka par $(x_i, y_i)$ som uppfyller villkoren, kan konstruera ett nytt par $(x_{i+1}, y_{i+1})$ genom att sätta $x_{i+1} = 3x_i + 4y_i$ och $y_{i+1} = 2x_i + 3y_i$, som också uppfyller villkoren.

Konstruktionen ger en oändlig mängd av talpar $(x_i, y_i)$ med den önskade egenskapen. ☻

## 16.4 Fermats Lilla Sats, *FLS*

Fermats sats bär namnet *Lilla Sats* som en kontrast till hans *Stora Sats* om frånvaron av heltalslösningar till ekvationen $x^n + y^n = z^n$, fast den Lilla Satsen gör bra mycket mera nytta än sin storebror. Satsen kan formuleras på följande sätt:

**Sats 16.6** (Fermats Lilla Sats, FLS). *Låt $p$ vara ett primtal och låt $a$ vara ett positivt heltal. Då är $a^p - a$ delbart med $p$, dvs.*[3] $a^p \equiv_p a$.

3 Relationen $\equiv_n$, kongruensen modulo $n$, behandlades i detalj i kapitel 7.

*Speciellt, om a ej är delbart med p (dvs.* $\mathrm{SGD}(a, p) = 1$*), är* $a^{p-1} - 1$ *delbart med p, dvs.* $a^{p-1} \equiv_p 1$

Det finns en uppsjö av bevis för denna sats, och vi väljer här ett enkelt induktionsargument.

*Bevis.* För $a = 1$ är $a^p - a = 0$, vilket är delbart med $p$.

Vi kan nu anta att påståendet gäller för något $a = k \geq 1$ dvs. att $k^p - k$ är delbart med $p$ och vill visa att $(k+1)^p - (k+1)$ också är delbart med $p$.

Binomialutveckling av $(k+1)^p$ (se Sats 5.3 i kapitel 5) ger $(k+1)^p - (k+1) = \sum_{i=0}^{p} \binom{p}{i} k^i - k - 1 = \sum_{i=1}^{p-1} \binom{p}{i} k^i + 1 + k^p - k - 1 = \sum_{i=1}^{p-1} \binom{p}{i} k^i + k^p - k$

Men alla tal på formen $\binom{p}{i}$ för $1 \leq i < p$ är delbara med $p$ (detta visades i Exempel **??**) och $k^p - k$ var delbart med $p$ (enligt induktionsantagandet). Därmed är $(k+1)^p - (k+1)$ delbart med $p$, och vi är klara. Induktionsprincipen medför den önskade slutsatsen.

Om $\mathrm{SGD}(a, p) = 1$, måste $p$ dela $a^{p-1} - 1$, då $p$ delar produkten $a(a^{p-1} - 1)$. ☻

Avslutningsvis följer här tre belysande exempel:

**Exempel 16.3.** *Visa att för alla icke-negativa heltal n är talet* $n^5 - n$ *delbart med* 30.

*Lösning: FLS* garanterar att $n^5 - n$ är delbart med 5. Vidare är $n^5 - n = n(n^4 - 1) = n(n^2 - 1)(n^2 + 1) = (n-1)n(n+1)(n^2 + 1)$. De första tre faktorerna är på varandra följande heltal. Minst ett av dessa tal är jämnt (delbart med 2) och precis ett är delbart med 3. Därmed är produkten delbar med 6. Följaktligen är $n^5 - n$ delbart med $5 \cdot 6 = 30$. ☻

Nu en *riktigt* intressant tillämpning av FLS.

**Exempel 16.4.** *Visa att det tal som skrivs med* 2016 *ettor,* $n = 11\ldots11$ *är delbart med* 1009.

*Lösning:* Vi kan skriva om talet $n$ på följande sätt:

$$n = \underbrace{11\dots11}_{2016} = \frac{10^{2016}-1}{9} = \frac{(10^{1008}-1)(10^{1008}+1)}{9}$$

Eftersom 1009 är ett primtal så är det, enligt Fermats sats, en delare till $10^{1009-1}-1$, och därmed också en delare till $n$. ☻

I sista exemplet behöver vi använda kunskaper om kongruenser från kapitel 7.4, speciellt Sats 7.4 om existensen av multiplikativ invers.

**Exempel 16.5.** *Bestäm den multiplikativa inversen modulo* 47 *till talet* $57^{45}$, *dvs. ett tal* $x$ *för vilket* $57^{45} \cdot x \equiv_{47} 1$.

*Lösning:* Eftersom 47 är ett primtal så medför *FLS* att $57^{46} \equiv_{47} 1$. Detta kan skrivas som $57^{45} \cdot 57 \equiv_{47} 1$.

Således är $57^{45} \cdot x \equiv_{47} 57^{45} \cdot 57$. Eftersom $\text{SGD}(47{,}57) = 1$ så kan vi dela bägge leden med $57^{45}$ och vi erhåller $x \equiv_{47} 57$, alltså $x = 10$. ☻

## 16.5 Eulers $\phi$-funktion och Eulers sats

Etthundra år efter Fermat generaliserade Leonard Euler Fermats Lilla Sats till icke-primtalsexponenter. För att vi ska kunna formulera Eulers sats behöver vi introducera ytterligare ett begrepp, nämligen funktionen $\phi(n)$ (läs: fi av $n$), som är definierad för positiva heltal $n$:

$$\phi(n) = \text{antalet heltal } k \text{ sådana att } 1 \le k \le n \text{ och } \text{SGD}(k,n) = 1.$$

Vi har till exempel $\phi(10) = 4$, för det är bara $1, 3, 7$ och 9 som är relativt prima med 10 och inte större än 10. På samma sätt är $\phi(12) = 4$ (talen $1, 5, 7$ och 11). Om $p$ är ett primtal så är $\phi(p) = p - 1$, ty inget tal mindre än $p$ har en gemensam delare med $p$ skild från 1.

Låt oss kalla talen som räknas upp i $\phi(n)$ för ett *reducerat restsystem* modulo $n$. Till exempel kan icke-noll resttermer vid division med 12 vara alla tal från 1 till 11, medan det reducerade restsystemet modulo 12 enbart består av fyra av dessa tal.

Låt nu $m$ vara ett positivt heltal och $a$ vara ett heltal sådant att $\text{SGD}(a,m) = 1$. Låt vidare $r_1, r_2, ..., r_{\phi(m)}$ vara det reducerade restsystemet modulo $m$. Vi ska titta närmare på talen $ar_1, ar_2, ..., ar_{\phi(m)}$. Vi behöver notera två saker:

(1): Talen $ar_1, ar_2, ..., ar_{\phi(m)}$ är relativt prima med $m$. Detta är sant då $\text{SGD}(a,m) = 1$ och $\text{SGD}(r_k,m) = 1$ för $k = 1, ..., \phi(m)$.

(2): Talen $ar_1, ar_2, ..., ar_{\phi(m)}$ är parvis olika modulo $m$, vilket betyder att om $ar_i \equiv_m ar_j$ så är $i = j$. Detta är en konsekvens av förkortningslagen, Sats 7.4 i kapitel 7: eftersom $\text{SGD}(a,m) = 1$ så medför $ar_i \equiv_m ar_j$ att $r_i \equiv_m r_j$, vilket i sin tur medför att $i = j$, ty talen $r_i$ är olika modulo $m$.

Följaktligen är talen $ar_1, ar_2, ..., ar_{\phi(m)}$ räknade modulo $m$, precis desamma som talen $r_1, r_2, ..., r_{\phi(m)}$, fast kanske i en annan ordning. Vi kan därför dra slutsatsen att $ar_1 \cdot ar_2 \cdots ar_{\phi(m)} \equiv_m r_1 \cdot r_2 \cdots r_{\phi(m)}$.

Återigen kan vi åberopa förkortningslagen och dela bägge sidor med produkten $r_1 \cdot r_2 \cdots r_{\phi(m)}$. Vi erhåller $a^{\phi(m)} \equiv_m 1$.

Därmed har vi bevisat Eulers sats:

**Sats 16.7** (Eulers sats). *Låt $m$ vara ett positivt heltal och $a$ vara ett heltal sådant att* $\text{SGD}(a,m) = 1$. *Då är $a^{\phi(m)} \equiv_m 1$, dvs. talet $a^{\phi(m)} - 1$ är delbart med $m$.*

☻

Eulers sats är en uppenbar generalisering av Fermats Lilla Sats, för om $p$ är ett primtal, är $\phi(p) = p - 1$, och om dessutom $p$ inte är en delare till $a$, så att $\text{SGD}(a,p) = 1$, så ger Eulers sats att $a^{p-1} - 1$ är delbart med $p$. Detta är ju just Fermats sats.

Funktionen $\phi(n)$ har en hel del intressanta och nyttiga egenskaper som är värda att nämna.

a) $\phi(n)$ är *multiplikativ*, vilket innebär att om $\text{SGD}(m,n) = 1$ så är $\phi(mn) = \phi(m)\phi(n)$.

b) $\phi(n) = n \cdot \prod_{\substack{p|n, \\ p \text{ primtal}}} \left(1 - \frac{1}{p}\right)$,

där produkten $\prod$ räkans alltså för alla primtalsdelare $p$ till $n$.

Den multiplikativa egenskapen a) följer direkt från formeln b). Att ge ett bevis för b) ligger dock lite över våra ambitioner här[4]. Själva formeln b) ger en elegant metod för att räkna ut värdet på $\phi(n)$. För att till exempel bestämma $\phi(12)$ finner vi tolvans primtalsfaktorer, vilka är 2 och 3, och därmed är $\phi(12) = 12 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 12 \cdot \frac{1}{2} \cdot \frac{2}{3} = 4$.

Vi avslutar detta avsnitt med två exempel på tillämpningar av Eulers sats.

**Exempel 16.6.** *Visa att det finns oändligt många tal $n$ för vilka $\phi(n)$ är ett kvadrattal.*

*Lösning:* Betrakta $n = 2^{2k+1}$ för $k \geq 1$. Då är $\phi(n) = 2^{2k+1} \cdot \frac{1}{2} = 2^{2k} = \left(2^k\right)^2$. ☻

**Exempel 16.7.** *Bestäm ett tal $k$ sådant att talet $S = 1 + 9 + 9^2 + \cdots + 9^k$ är delbart med* 35.

*Lösning:* Observera att $S = \dfrac{9^{k+1} - 1}{9 - 1}$ (summa av en geometrisk talföljd). Därmed är $8S = 9^{k+1} - 1$. Vidare är $\phi(35) = 35 \cdot \frac{4}{5} \cdot \frac{6}{7} = 24$, och eftersom $\mathrm{SGD}(9,35) = 1$ så är, enligt Eulers sats, $9^{24} - 1$ delbart med 35.

Det räcker alltså att ta $k = 23$. ☻

## 16.6 Kinesiska restsatsen

I ett av de tidigare kapitlen behandlade vi linjära ekvationssystem och i ett annat behandlade vi lösningar till linjära kongruenser av typ $ax \equiv_m b$. Nu ska vi i stället titta på linjära system av kongruenser. Vi börjar med ett enkelt exempel som är hämtat från en kinesisk bok skriven för cirka 1600 år sedan, och för övrigt på ett mycket övertygande sätt demonstrerar att galna talentusiaster tidigt dök upp även på andra ställen än i det antika Grekland.

**Exempel 16.8.** *Bestäm alla tal som ger restermen* 1 *vid division med* 3*, resttermen* 2 *vid division med* 5 *samt resttermen* 3 *vid division med* 7.

4 Egenskapen kan till exempel bevisas med hjälp av Kinesiska restsatsen, eller kombinatoriskt med hjälp av Inklusion-Exklusionprincipen, och finns i de flesta läroböcker i talteori.

Vi vill alltså lösa följande system av kongruenser

$$\begin{cases} x & \equiv 1 \pmod{3} \\ x & \equiv 2 \pmod{5} \\ x & \equiv 3 \pmod{7}. \end{cases}$$

Systemet ser enkelt ut, men hur går det till att lösa det? För att få svaret på den sortens frågor, lösning av ett system av linjära kongruenser, går vi tillbaka till ett verk från år 1247 av den kinesiske matematikern Chin Chiu-Shao. Han visade nämligen följande sats:

**Sats 16.8.** *Ett linjärt system av kongruenser $x \equiv_{m_i} a_i$, $1 \leq i \leq k$, där $\mathrm{SGD}(m_i, m_j) = 1$ för $i \neq j$, har en entydig lösning modulo $m_1 m_2 \cdots m_k$.*

*Bevis.* Vi ska bevisa satsen i två steg. I första hand ska vi konstruera en lösning till systemet och sedan ska vi bevisa att denna lösning är entydig.

*Konstruktion av* en *lösning:*

Låt $M = m_1 m_2 \cdots m_k$ och låt $M_i = \dfrac{M}{m_i}$ för $i = 1, 2, .., k$. Uppenbart är $M_i$ delbart med $m_j$ för alla $j \neq i$. Dessutom observerar vi att $\mathrm{SGD}(M_i, m_i) = 1$ för varje $i$.

Den sista observationen, tillsammans med Sats 7.5 ifrån kapitel 7, medför att kongruensen $M_i y_i \equiv_{m_i} 1$ har en entydig lösning $y_i$, som faktiskt är multiplikativ invers til $M_i$ modulo $m_i$.

Vi ska visa att $x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_k M_k y_k$ är en lösning till det givna systemet.

För varje $1 \leq j \leq k$ har vi nämligen att

$x = \sum_{i=1}^{k} a_i M_i y_i = a_j M_j y_j + \sum_{i=1, i \neq j}^{k} a_i M_i y_i \equiv_{m_j} a_j \cdot 1 + \sum_{i=1, i \neq j}^{k} a_i \cdot 0 \cdot y_i = 0 + a_j = a_j$.

*Lösningens entydighet modulo M:*

Nu när vi har visat att $x$ är en lösning så ska vi visa att $x$ är entydigt bestämd modulo $M$.

Antag att $x_0$ och $x_1$ är två lösningar till systemet. Vi måste visa att $x_0 \equiv_M x_1$.

Eftersom både $x_0 \equiv_{m_j} a_j$ och $x_1 \equiv_{m_j} a_j$ så är $m_j$ en delare till $x_0 - x_1$, för alla $1 \leq j \leq k$.

Därmed är $M$ en delare till $x_0 - x_1$, vilket innebär att $x_0 \equiv_M x_1$. ☻

Med hjälp av satsen ovan kan vi nu lösa vår uppgift i Exempel 16.8:

*Lösning:* Eftersom $m_1 = 3, m_2 = 5$ och $m_3 = 7$ är parvis relativt prima har systemet, enligt Kinesiska restsatsen, en entydig lösning. Vi har då $M = 3{\cdot}5{\cdot}7 = 105$ och $M_1 = \dfrac{M}{m_1} = \dfrac{105}{3} = 35$, $M_2 = \dfrac{M}{m_2} = \dfrac{105}{5} = 21$ och $M_3 = \dfrac{M}{m_3} = \dfrac{105}{7} = 15$.
Nu söker vi lösningar $y_1$, $y_2$ och $y_3$ till

$$\begin{cases} 35y_1 & \equiv 1 \pmod 3 \\ 21y_2 & \equiv 2 \pmod 5 \\ 15y_3 & \equiv 3 \pmod 7. \end{cases}$$

och får $y_1 \equiv_3 2$, $y_2 \equiv_5 1$ samt $y_3 \equiv_7 1$. Enligt Kinesiska restsatsen, är därmed $x \equiv_M (1 \cdot 35 \cdot 2 + 2 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1 = 157 \equiv_M 52$.

Följaktligen är 52 den entydiga lösningen av systemet modulo 105. Den allmänna lösningen är därför $52 + 105k$, för alla heltal $k$. ☻

Ytterligare två, lite svårare exempel.

**Exempel 16.9.** *Bestäm $x$ så att* $17x \equiv_{210} 3$.

*Lösning:* Eftersom $210 = 2 \cdot 3 \cdot 5 \cdot 7$, är den givna ekvationen ekvivalent med systemet av kongruenser

$$\begin{cases} 17x & \equiv 3 \pmod 2 \\ 17x & \equiv 3 \pmod 3 \\ 17x & \equiv 3 \pmod 5 \\ 17x & \equiv 3 \pmod 7. \end{cases}$$

Vi reducerar först systemet till:

$$\begin{cases} x & \equiv 1 \pmod 2 \\ x & \equiv 0 \pmod 3 \\ x & \equiv -1 \pmod 5 \\ x & \equiv 1 \pmod 7). \end{cases}$$

(Notera att $17x \equiv_5 3 \iff 2x \equiv_5 3 \iff 6x \equiv_5 9 \iff x \equiv_5 4 \iff x \equiv_5 -1$ och $17x \equiv_7 3 \iff 3x \equiv_7 3 \iff x \equiv_7 1$.)

Vi har $m_1 = 2, m_2 = 3, m_3 = 5$ och $m_4 = 7$, $M_1 = \dfrac{210}{2} = 105$, $M_2 = \dfrac{210}{3} = 70$, $M_3 = \dfrac{210}{5} = 42$ och $M_4 = \dfrac{210}{7} = 30$. Vi behöver alltså lösa kongruenssystemet

$$\begin{cases} 105y_1 & \equiv 1 \pmod 2 \\ 70y_2 & \equiv 1 \pmod 3 \\ 42y_3 & \equiv 1 \pmod 5 \\ 30y_4 & \equiv 1 \pmod 7 \end{cases}$$

som enkelt reduceras till

$$\begin{cases} y_1 & \equiv 1 \pmod 2 \\ y_2 & \equiv 1 \pmod 3 \\ 2y_3 & \equiv 1 \pmod 5 \\ 2y_4 & \equiv 1 \pmod 7 \end{cases}$$

och vi får $y_1 = y_2 = 1, y_3 = 3, y_4 = 4$. Därmed är lösningen $x = 1 \cdot 105 \cdot 1 + 0 \cdot 70 \cdot 1 - 1 \cdot 42 \cdot 3 + 1 \cdot 30 \cdot 4 = 105 - 126 + 120 = 99 \equiv_{210} 99$. ☻

**Exempel 16.10.** *Visa att för varje positivt heltal $n$ existerar ett positivt heltal $N$ sådant att inget av talen $N+1, N+2, \ldots, N+n$ är en primtalspotens.*

*Lösning:* Tricket här är att få alla tal $N+k$, för $k = 1, 2, \ldots, n$, delbara med två *olika* primtal. Låt därför $p_1, p_2, \ldots, p_{2n}$ vara olika primtal. Kinesiska restsatsen garanterar existensen av ett heltal $N$ sådant att $p_1p_2$ delar $N+1$, $p_3p_4$ delar $N+2$, ...., $p_{2n-1}p_{2n}$ delar $N+n$, och därmed kan inget av talen $N+1, N+2, \ldots, N+n$ vara en primtalspotens. ☻

## 16.7 Hemuppgifter

**Uppgift 16.1** *** Visa att varje *äkta delare*[5] till ett perfekt tal är defekt.

(L)

**Uppgift 16.2** *** Visa att[6] $\sum_{k|n} \frac{1}{k} = 2$ om och endast om $n$ är ett perfekt tal.

(L)

**Uppgift 16.3** ** Låt $n = 2^{p-1}(2^p - 1)$ vara ett perfekt tal. Bestäm produkten $\prod_{d|n} d$ av alla delare $d$ till $n$.

**Uppgift 16.4** *** Visa att inget perfekt tal är en primtalspotens, dvs. är inte på formen $p^k$ för något primtal $p$ och heltal $k \geq 1$.

(L)

**Uppgift 16.5** * Visa att inget Fermattal $Fe_n$ är ett kvadrattal.

**Uppgift 16.6** * Visa att inget Fermattal $Fe_n$ är en tredjepotens av ett heltal.

**Uppgift 16.7** ** Visa att sista siffran i Fermattalen $Fe_n$, $n \geq 2$, alltid är 7.

(L)

5 Talet $k$ är en *äkta delare* till talet $n$, om $k$ är en delare till $n$ och $1 < k < n$.

6 Symbolen $k|n$ definierades i kapitel 6 och betyder att $k$ är en delare till $n$.

**Uppgift 16.8** ** Bestäm alla primtal $p$ och $q$ för vilka talet $pq$ är defekt.

**Uppgift 16.9** ** Bestäm alla Fermattal $Fe_n$ som kan framställas som en summa av två primtal.

(L)

**Uppgift 16.10** * Låt $p$ vara ett primtal. Vilken är resttermen då man dividerar $\sum_{k=1}^{p-1} k^{p-1}$ med $p$?

**Uppgift 16.11** * Låt $p$ vara ett primtal > 2. Visa att talet $\sum_{k=1}^{p-1} k^p$ är delbart med $p$.

**Uppgift 16.12** ** Avgör om ett

a) 100-siffrigt tal $A = 11\ldots11$ är delbart med 101,

b) 257-siffrigt tal $B = 22\ldots22$ är delbart med 257.

(L)

**Uppgift 16.13** *** Visa att till varje primtal $p$ finns det ett positivt heltal $n$ sådant att talet $a_n = 3^n - 5^n + 15^n - 1$ är delbart med $p$.

(L)

**Uppgift 16.14** ** Låt $p$ och $q$ vara två olika primtal och låt $a$ vara ett positivt heltal. Visa att $A = a^{pq} - a^p - a^q + a$ är delbart med $pq$.

(L)

**Uppgift 16.15** ** Låt $p$ och $q$ vara två olika primtal. Visa att talet $B = p^q + q^p - p - q$ är delbart med $pq$.

**Uppgift 16.16** ** Visa att 23 är en delare till alla heltal $n^{154} - 1$ sådana att 23 och $n$ är relativt prima.

**Uppgift 16.17** * Vilken restterm får man då $5^{119}$ divideras med 59?

**Uppgift 16.18** * Låt $p$ vara ett primtal och $a, b$ två icke-negativa heltal. Visa att om $a^p \equiv_p b^p$ så är $a \equiv_p b$.

**Uppgift 16.19** ** Låt $p$ och $q$ vara två olika primtal. Visa att $p^{q-1} + q^{p-1} \equiv_{pq} 1$.

**Uppgift 16.20** ** Låt $p$ och $q$ vara två olika primtal. Visa att $p^q + q^p \equiv_{pq} p + q$.

**Uppgift 16.21** ** Låt $p$ vara ett primtal. Visa att $p$ är en delare till $ab^p - a^p b$ för alla heltal $a$ och $b$.

**Uppgift 16.22** *** Låt $p$ vara ett primtal. Visa att det finns oändligt många positiva heltal $n$ sådana att $p$ är en delare till $2^n - n$.

(L)

**Uppgift 16.23** * Visa att $\phi(666) = 6 \cdot 6 \cdot 6$.

**Uppgift 16.24** * Visa att om $\phi(n) = n - 1$ så är $n$ ett primtal.

**Uppgift 16.25** *** Avgör för vilka positiva heltal $n$ som
a) $\phi(n)$ är udda ?
b) $\phi(n) = \dfrac{n}{2}$ ?
c) $\phi(n)$ är en delare till $n$ ?
(L)

**Uppgift 16.26** ** Visa att $1 + 11 + 11^2 + \cdots + 11^{31} \equiv_{51} 0$.

**Uppgift 16.27** * Visa att $\phi(n^2) = n\phi(n)$.

**Uppgift 16.28** * Visa att det finns oändligt många $n$ sådana att $\phi(n)$ är delbart med 10.

**Uppgift 16.29** ** Låt $n$ vara ett positivt heltal. Vilka är möjliga resttermer då $n^{100}$ divideras med 125 ?

**Uppgift 16.30** * Visa att för ett primtal $p$ är $\dfrac{\phi(p)\sigma(p) + 1}{p}$ ett heltal.

**Uppgift 16.31** ** Låt $p$ vara ett primtal. Bestäm $\sum_{k=0}^{n} \phi(p^k)$.

**Uppgift 16.32** ** Vilket är det minsta $n \geq 5000$ sådant att $2|n$, $3|(n+1)$, $5|(n+2)$, $7|(n+3)$ och $11|(n+4)$ ?

**Uppgift 16.33** ** Vilket är det minsta positiva heltalet $n$ som är sådant att $3|n$, $4|(n+1)$, $5|(n+2)$, $7|(n+3)$ och $11|(n+4)$ ?

**Uppgift 16.34** *** Vilket är det minsta positiva heltalet $n$ som är sådant att $2^2|n$, $3^2|(n+2)$, $5^2|(n+3)$, $11^2|(n+5)$ ?

(L)

**Uppgift 16.35** *** Visa att det finns 2016 på varandra följande heltal, sådana att vart och ett är delbart med en tredjepotens av något heltal > 1.

(L)