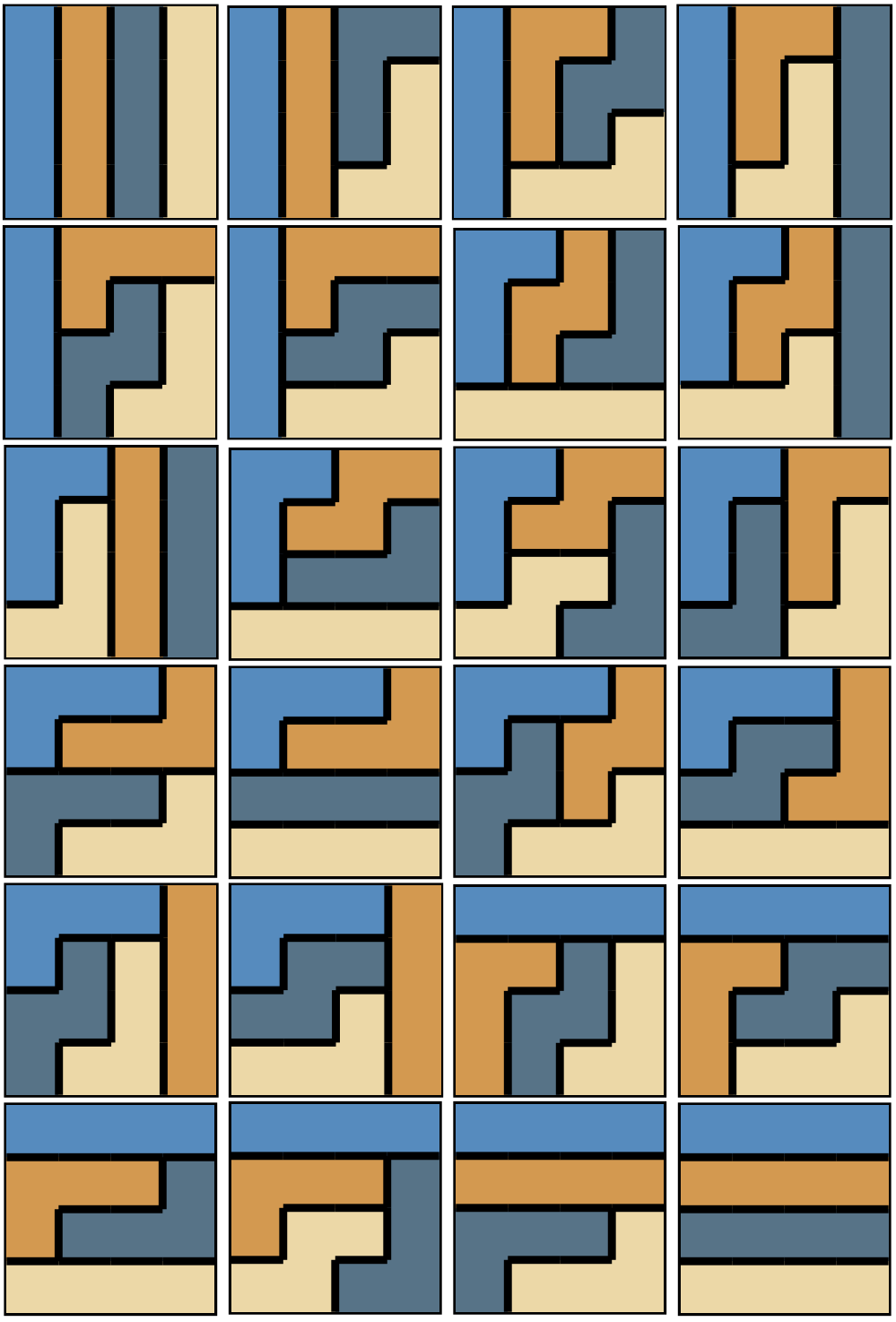
MM2001: Diskret matematik
Föreläsningsanteckningar

Per Alexandersson



Innehåll

Föreläsning 1
Introduktion och talteori

1.1. Kort information

- Kursmaterial: *Algebra I*. Se till att läsa kompendiet.
- Läs kurssidorna och informationsforumen. `https://kurser.math.su.se/`
- Använd handledningsforumet!
- Det som skrivs på tavlan är sällan hela resonemanget!
- Senare kommer vi gå igenom Mathematica. Installera gärna tidigt.

1.1.1. Vad är diskret matematik?

Diskret matematik innefattar många olika delar av matematiken:

- Talteori — heltal, delbarhet, primtal
- Algebra — Moduloräkning, komplexa tal, polynom. Räkneoperationer.
- Kombinatorik — räkna antalet sätt att göra något.
- Logik — matematiken bakom sanningar (och vad som inte kan bevisas)
- Grafteori — noder och kanter, stigar, träd.
- Krypteringsmatematik — skicka meddelanden säkert.

Områden som inte är diskret matematik är oftast fokuserade på studier av funktioner, och involverar främst reella eller komplexa tal.

- Analys — Derivator, integraler
- Linjär algebra — Vektorer och matriser
- Differentialekvationer
- Komplex analys — derivator och integraler med komplexa tal
- Fourieranalys
- Dynamiska system och kaosteori (men det finns diskreta dynamiska system också!)
- Många tillämpningar inom fysiken är kontinuerliga modeller.

1.2. Rationella tal och kursens första sats

De mängder av tal vi kommer arbeta med är $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Detta är de **naturliga talen**, **heltalen**, **rationella talen**, **reella talen** samt **de komplexa talen**. I denna kurs gäller det att $0 \in \mathbb{N}$.

1.3. Delbarhet

Ett heltal a är **jämnt** om det kan skrivas på formen $2k$ för något heltal k. Om ett heltal ej är jämnt kallas det **udda**.
En **sats** är ett (viktigt) påstående som är sant.

Sats 1. *Om a är jämnt, så är även a^2 jämnt.*

Bevis. Vi vet att $a = 2k$ för något heltal k, så $a^2 = (2k)^2 = 4k^2 = 2(2k^2)$. Notera att $2k^2$ är heltal, så alltså är a^2 på formen som krävs för att vara ett jämnt tal. □

Definition 2 (Delbarhet, delare)**.** Vi säger att d är en **delare** till n om det finns heltal k så att $n = dk$. Vi skriver detta som $d \mid n$, eller d *delar* n eller n **delas av** d.

Vi skriver $d \nmid n$ om d *inte* är delare till n.

- Finns det något heltal som delar alla heltal? (Ja, 1 och -1).
- Vilka är delarna till talet 6? (± 1, ± 2, ± 3 samt ± 6)
- Visa att n alltid är en delare till n.
- Visa att alla heltal delar 0.

1.4. Talet $\sqrt{2}$ är ej rationellt

Kom ihåg att **ett rationellt tal** är tal som kan skrivas som kvoten av två heltal. Tal som inte är rationella kallas **irrationella**.

Sats 3. *Talet $\sqrt{2}$ är irrationellt.*

Bevis. Vi använder *motsägelsebevis*. Utgå ifrån motsatsen, och visa att detta leder till motsägelse. Vi *antar* $\sqrt{2} = \frac{a}{b}$ som *förkortat*[1] bråk. Då är $2 = \frac{a^2}{b^2}$ så $2b^2 = a^2$. Detta leder till att $2 \mid a$. Det finns då ett heltal, $\hat{a}$ som uppfyller att $a = 2\hat{a}$ som leder till att $b^2 = 2\hat{a}^2$, så $2 \mid b$. Men nu har vi en motsägelse: både a och b är jämna tal men vi utgick ifrån att a/b var förkortat. □

Man kan visa att π och e är irrationella tal, men bevisen är avsevärt mer invecklade.

[1] Så minst ett av talen a och b är udda.

1.5. Sammansatta tal och primtal

Definition 4 (Primtal, sammansatta tal)**.** Ett positivt tal $p \geq 2$ kallas för **primtal** om dess enda heltalsdelare är ± 1 samt $\pm p$. Ett positivt tal $n \geq 2$ som inte är ett primtal kallas för **sammansatt**. Notera att n är sammansatt precis om det finns heltal $a > 1$ och $b > 1$, så att $n = ab$.

De första primtalen är

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots .$$

Att avgöra om ett tal är primtal eller inte, kan en dator göra "snabbt"[2]. Att däremot faktorisera sammansatta tal går inte att göra effektivt—vi vet ej om en snabb sådan algoritm finns eller inte. Dock finns det snabba kvantdatoralgoritmer som gör detta, men de är i praktiken begränsade i hur mycket minne ("qubits") som de kan använda.

Vi ska senare visa att varje positivt heltal kan på ett *entydigt* sätt uttryckas som en produkt av primtal.

1.6. Kvot och rest

Sats 5. *För varje heltal n och positivt heltal b, finns det tal k och r, så att $n = kb + r$, där $0 \leq r < b$.*

Bevis. I fallet då n är icke-negativt, kan vi upprepade gånger subtrahera b från n, tills vi har något tal r, som ligger mellan 0 och $b - 1$. Antalet subtraktioner är då k.

Om n är negativt, så kan vi istället addera b upprepade gånger tills vi får ett tal r mellan 0 och $b - 1$. □

Definition 6 (Kvot och rest)**.** För ett heltal n och positivt heltal b finns k och r så att $n = kb + r$, enligt satsen ovan. Talen k och r kallas för **kvot** och **rest**.

Exempel 7. Skriv talet 59 på formen $7k + r$, där $0 \leq r < 7$.

Lösning. Vi har att $59 = 7 \cdot 8 + 3$.

Exempel 8. Visa att om $a \mid n$ och $b \mid a$, så gäller det att $b \mid n$. Utgå ifrån definitionen av delbarhet.

Lösning. Delbarhet säger att det finns ett heltal, k så att $n = ak$. Vi vet också att det finns heltal m så att $a = bm$. Sätter vi samman dessa får vi att

$$n = (bm)k, \text{ så } n = b(mk).$$

Detta visar nu att b delar n, då n är en heltalsmultipel av b.

Sats 9 (Linjärkombinationssatsen)**.** *Om a och b är heltal, och $d \mid a$, $d \mid b$, gäller det att $d \mid ax + by$ för godtyckliga $x, y \in \mathbb{Z}$.*

Bevis. Vi vet[3] att $a = d\hat{a}$ samt $b = d\hat{b}$. Tittar vi nu på

$$ax + by = d\hat{a}x + d\hat{b}y = d(\hat{a}x + \hat{b}y)$$

så är det en multipel av d, så $d \mid ax + by$ och vi är klara. □

[2] Se AKS primality test, *PRIMES is in P* från 2002.

[3] Här använder jag a med en "hatt" istället för en ny bokstav, för att indikera att $\hat{a}$ är nära relaterad till a. Andra vanliga variabel-dekorationer är $\tilde{a}$ och a'.

Observera speciellt att om $d \mid a$, $d \mid b$ så gäller $d \mid a + b$, $d \mid a - b$ etc.

Exempel 10. I Mathematica, så kan man beräkna kvoten och resten då 100 delas med 23, med kommandot

```
QuotientRemainder[100, 23]
```

Man kan också lista delare, eller testa delbarhet direkt:

```
Divisors[60]
Divisible[100, 4]
```

Föreläsning 2
Euklides algoritm och Diofantiska ekvationer

2.1. Största gemensamma delaren

Varje heltal har ju delare. Talen 12 och 20 har de positiva delarna

$$1, 2, 3, 4, 6, 12 \qquad \text{samt } 1, 2, 4, 5, 10, 20.$$

Givet två heltal, så kan vi fråga vad den **största gemensamma delaren** är. Denna betecknas $\mathrm{SGD}(a, b)$.

Två heltal vars största gemensamma delare är 1, kallas **relativt prima**.

Lemma 11. *Vi har att* $\mathrm{SGD}(a, b)$ *är samma som* $\mathrm{SGD}(b, a - b)$.

Bevis. Låt d vara en gemensam delare till a och b. Eftersom $d \mid a$ och $d \mid b$, gäller enl. linjärkombinationssatsen att $d \mid a - b$ också. Speciellt så är d en gemensam delare till b och $a - b$.

Nu, om d' är en delare till både b och $a - b$, så är enl. linjärkombinationssatsen d' en delare till $b + (a - b) = a$, så d' är en gemensam delare till a och b.

Vi har alltså visat att de gemensamma delarna till a och b, är *samma* som de gemensamma delarna till b och $a - b$. Alltså måste de ha samma *största* gemensamma delare också. □

Vi kan nu använda lemmat ovan upprepade gånger:

$$\mathrm{SGD}(a, b) = \mathrm{SGD}(b, a-b) = \mathrm{SGD}(b, a-2b) = \mathrm{SGD}(b, a-3b) = \cdots = \mathrm{SGD}(b, a-kb) = \mathrm{SGD}(b, r)$$

där r är resten man får då a delas med b.

2.1.1. Euklides algoritm

Genom att utnyttja $\mathrm{SGD}(a, b) = \mathrm{SGD}(b, r)$ där $a = kb + r$, så får vi en metod för att beräkna $\mathrm{SGD}(a, b)$. Denna metod kallas **Euklides algoritm**.

Exempel 12. Till exempel, $\mathrm{SGD}(72, 19)$ beräknas genom

$$\begin{aligned} 72 &= 3 \cdot 19 + 15 \\ 19 &= 1 \cdot 15 + 4 \\ 15 &= 3 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1 \end{aligned}$$

Alltså ser vi att

$$\text{SGD}(72, 19) = \text{SGD}(19, 15) = \text{SGD}(15, 4) = \text{SGD}(4, 3) = \text{SGD}(3, 1) = 1.$$

Så deras största gemensamma delare är 1.

2.2. Diofantiska ekvationer

En **Diofantisk ekvation** är en ekvation där vi bara är intresserade av heltalslösningar. Vi ska fokusera på Diofantiska ekvationer av formen $ax + by = c$. Notera att om $\text{SGD}(a, b)$ inte delar c, så saknas lösning. Annars kan vi dela båda led med $\text{SGD}(a, b)$, och få en ny (ekvivalent) ekvation men med $\text{SGD}(a, b) = 1$.
Antag nu att vi hittat *en* sådan lösning (partikulärlösning) (x_0, y_0). Då är alla par på formen

$$\begin{cases} x = x_0 + bk \\ y = y_0 - ak \end{cases} \qquad k \in \mathbb{Z}$$

också lösningar. Man kan visa att alla lösningar är på denna form (Sats 5.17 i boken).

Sats 13. *En Diofantisk ekvation $ax + by = c$ har lösningar om och endast om $\text{SGD}(a, b)$ är en delare till c.*

Så hur hittar man en partikulärlösning? Om vi kan hitta lösning till $ax + by = 1$, så har vi också en lösning till $ax + by = c$ genom multiplikation med c.
Man kan hitta en partikulärlösning via Euklides algoritm (och Bezouts identitet).

Exempel 14. Lös $34x + 37y = 3$.

Lösning. Vi ser först att $\text{SGD}(37, 34) = 1$. Euklides algoritm ger

$$\begin{aligned} 37 &= 1 \cdot 34 + 3 \\ 34 &= 11 \cdot 3 + 1. \end{aligned}$$

Alltså gäller

$$\overline{1} = \overline{34} - 11 \cdot \overline{3} = \overline{34} - 11 \cdot (\overline{37} - \overline{34}) = 12 \cdot \overline{34} - 11\overline{37}.$$

Alltså är $x = 12$, $y = -11$ en lösning till $34x + 37y = 1$. Detta ger att $x_0 = 3 \cdot 12$, $y_0 = 3 \cdot (-11)$ en lösning till $34x + 37y = 3$. Den allmänna lösningen är då

$$\begin{cases} x = 36 + k \cdot 37 \\ y = -33 - k \cdot 34, \end{cases} \qquad k \in \mathbb{Z}.$$

Exempel 15. Finns det heltalslösningar till $171x - 66y = 7$?

Lösning. Nej, vi ser att vänsterledet är alltid en multipel av 3, men det är inte högerledet. Med andra ord, $\text{SGD}(171, 66) \nmid 7$.

Exempel 16. En butik säljer lådor med 15 och 27 ägg. Du vill köpa 300 ägg. Finn alla sätt att göra detta på.

Lösning. Vi modellerar detta som: $15x + 27y = 300$, $x, y \geq 0$. Båda led delas med största gemensamma delaren till 15 och 27. Detta leder till den ekvivalenta ekvationen $5x + 9y = 100$. Vi söker nu en partikulärlösning, så vill först lösa $5x + 9y = 1$. Euklides ger att $x = 2$, $y = -1$ löser denna. Alltså är $x_p = 200$, $y_p = -100$ en lösning till $5x + 9y = 100$. Den allmänna lösningen är då

$$x = 200 - 9n, \qquad y = -100 + 5n, \qquad n \in \mathbb{Z}.$$

Vi ser att vi måste ha $n \geq 20$, samt $200/9 \geq n$, för att ha icke-näggativa lösningar. Detta leder till att n är antingen 20, 21 eller 22.

Lösningarna är då $(x, y) = (20, 0), (11, 5), (2, 10)$.

Exempel 17. Finn alla heltalslösningar till $171x - 66y = 6$.

Lösning. Efter division med största gemensamma delare av 171 och 66 får vi ekvationen $57x - 22y = 2$. Nu,

$$\begin{aligned} 57 &= 2 \cdot 22 + 13 \\ 22 &= 1 \cdot 13 + 9 \\ 13 &= 1 \cdot 9 + 4 \\ 9 &= 2 \cdot 4 + 1 \end{aligned}$$

Således,

$$1 = 9 - 2 \cdot 4 = 9 - 2(13 - 9) = 3 \cdot 9 - 2 \cdot 13 = 3(22 - 13) - 2 \cdot 13 = 3 \cdot 22 - 5 \cdot 13.$$

Detta ger att $1 = 3 \cdot 22 - 5(57 - 2 \cdot 22) = 13 \cdot 22 - 5 \cdot 57$. Vidare, $57x - 22y = 1$ har lösningen $(x, y) = (-5, -13)$, och $57x - 22y = 2$ löses av $(x, y) = (-10, -26)$. Den allmänna lösningen är då

$$x = -10 + 22n, \qquad y = -26 + 57n, \quad n \in \mathbb{Z}.$$

Exempel 18. Finn alla heltalslösningar till $17x - 23y = 3$.

Lösning. Euklides ger

$$\begin{aligned} 23 &= 1 \cdot 17 + 6 \\ 17 &= 3 \cdot 6 - 1 \end{aligned}$$

Således, $1 = 3 \cdot 6 - 17 = 3(23 - 17) - 17 = 3 \cdot 23 - 4 \cdot 17$. Detta ger då att $17(-4) - (-3)23 = 1$ så $17(-12) - (-9)23 = 3$. Den allmänna lösningen är då

$$x = -12 + 23n, \qquad y = -9 + 17n \qquad n \in \mathbb{Z}.$$

Exempel 19. Finn det minsta positiva heltalet x, så att när $11x$ delas med 31, får man resten 3.

Lösning. Vi vill lösa den diofantiska ekvationen $11x = 31y + 3$ med så litet positivt x som möjligt. Detta ger $11x - 31y = 3$. Euklides algoritm för SGD$(31, 11)$ ger

$$\begin{aligned} 31 &= 3 \cdot 11 - 2 \\ 11 &= 5 \cdot 2 + 1. \end{aligned}$$

Nu,

$$1 = 11 - 5(2) = 11 - 5(3(11) - 31) = 11(-14) - (31)(-5).$$

En lösning är alltså $(x, y) = 3 \cdot (-14, -5)$, så generella lösningen ges av $x = -42 + 31n$. Väljer vi $n = 2$ får vi den minsta positiva lösningen; $x = 20$.

En slutlig kontroll: $11 \cdot 20 = 220$ och $220 = 7 \cdot 31 + 3$.

Problem 20. (Tentan 2024-04-07) För ett heltal a, betrakta den diofantiska ekvationen

$$170x + 289y = a.$$

(a) Bestäm det minsta positiva heltal a som gör att ekvationen har lösningar.

(b) Bestäm två olika lösningar till ekvationen $170x + 289y = 17$.

Lösning. (a) Den diofantiska ekvationen har en lösning om och endast om $\text{SGD}(170, 289) \mid a$, enligt sats. Vi kan med Euklides algoritm beräkna $\text{SGD}(170, 289)$:

$$\begin{aligned} 289 &= 170 + 119 \\ 170 &= 119 + 51 \\ 119 &= 2 \cdot 51 + 17 \\ 51 &= 3 \cdot 17 + 0. \end{aligned}$$

Så största gemensamma delaren är 17. Alltså finns det en lösning omm $17 \mid a$, och det minsta positiva värdet på a som uppfyller detta är $a = 17$.

(b) Genom division med 17 ser vi att ekvationen är ekvivalent med

$$10x + 17y = 1.$$

Vi vet sedan tidigare att $17 \cdot 3 = 51$, så $10(-5) + 17 \cdot 3 = 1$. En lösning är då $(x, y) = (-5, 3)$. Alla andra lösningar skiljer sig från denna, enligt utlärd sats, med heltalsmultiplar av $(17, -10)$; dvs, den allmänna lösningen ges av

$$(x, y) = (-5, 3) + k(17, -10) \quad \text{där } k \in \mathbb{Z}.$$

Alltså fås en till lösning av $(x, y) = (-5, 3) + (17, -10) = (12, -7)$.

Svar: $(x, y) = (-5, 3)$ eller $(12, -7)$ är två lösningar.

Exempel 21. Lös $72x - 47y = 2$.

Lösning. Vi ser först att $\text{SGD}(72, 47) = 1$. Detta innebär att ekvationen har lösningar.
Euklides algoritm ger

$$\begin{aligned} 72 &= 1 \cdot 47 + 25, \\ 47 &= 1 \cdot 25 + 22, \\ 25 &= 1 \cdot 22 + 3, \\ 22 &= 7 \cdot 3 + 1, \\ 3 &= 3 \cdot 1 + 0. \end{aligned}$$

Alltså gäller

$$\overline{1} = \overline{22} - 7 \cdot \overline{3} = \overline{22} - 7 \cdot (\overline{25} - \overline{22}) = 8 \cdot \overline{22} - 7 \cdot \overline{25},$$

och vi substituerar vidare:

$$\overline{1} = 8 \cdot (\overline{47} - \overline{25}) - 7 \cdot \overline{25} = 8 \cdot \overline{47} - 15 \cdot \overline{25},$$

$$\overline{1} = 8 \cdot \overline{47} - 15 \cdot (\overline{72} - \overline{47}) = 23 \cdot \overline{47} - 15 \cdot \overline{72}.$$

Alltså är $x = -15$, $y = -23$ en lösning till $72x - 47y = 1$. Multiplicerar vi med 2 får vi en lösning till $72x - 47y = 2$:

$$x_0 = 2 \cdot (-15) = -30, \quad y_0 = 2 \cdot (-23) = -46.$$

Den allmänna lösningen är då

$$\begin{cases} x = -30 + k \cdot 47, \\ y = -46 + k \cdot 72, \qquad k \in \mathbb{Z}. \end{cases}$$

Exempel 22. Mathematica har kommandon för största gemensamma delare och Bezouts identitet:

```
GCD[72, 19]
ExtendedGCD[72, 47]
```

Kommandot `FindInstance` kan hitta en partikulärlösning till en Diofantisk ekvation:

```
FindInstance[34 x + 37 y == 3, {x, y}, Integers]
```

Exempel 23. Problemet med äggen ovan, kan i Mathematica lösas med följande:

```
 Solve[15 x + 27 y == 300 && x >= 0 && y >= 0, {x, y}, Integers]
```

`Reduce` ger svaret som logiska villkor, och är ofta bättre när man vill se alla lösningar:

```
Reduce[15 x + 27 y == 300 && x >= 0 && y >= 0, {x, y}, Integers]
```

Föreläsning 3
Primtal och aritmetikens fundamentalsats

Sats 24. *Varje positivt heltal $n \geq 2$ kan skrivas som en produkt av primtal.*

Bevis. Om talet n är ett primtal är vi klara. Annars är det sammansatt, $n = ab$.
Var och en av delarna är nu antingen primtal, eller ett *mindre* sammansatt tal, och vi kan fortsätta uppdelningen. Denna process måste till sist stanna, då vi i varje steg får mindre tal som faktorer. □

Det är inte alls klart från detta argument att uppdelningen är unik; detta ska vi visa nedan i **aritmetikens fundamentalsats**.

Sats 25. *Det finns oändligt många primtal.*

Bevis. Vi ska visa att om vi har en ändlig lista med primtal, $p_1, \ldots, p_k$ så finns det ett (annat) primtal som inte är med i listan.
Vi betraktar talet $N = p_1 \cdots p_k + 1$, och noterar att detta ger rest 1 då det delas med något av primtalen p_j. Talet N är då antingen själv ett primtal som inte finns i listan, eller en produkt av primtal (som inte är med i listan). □

Den sekvens av (nya) primtal man får från denna procedur om man startar med listan $p_1 = 2$, är sekvensen `https://oeis.org/A000945` (Euclid–Mullin-sekvensen), som börjar

$$2, 3, 7, 43, 13, 53, 5, 6221671, \ldots .$$

Det är en naturlig fråga om denna sekvens innehåller alla primtal—denna fråga ställdes ursprungligen av Guy och Nowakowski.

3.0.1. *Eratosthenes såll*

Eratosthenes såll är en metod för att generera primtal:

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
91	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Lemma 26. *Om $p \mid ab$, gäller det att $p \mid a$ eller $p \mid b$.*

Bevis. Antag att p inte delar a. Vi har då att det finns x och y så att $xa + yp = 1$, enligt det faktum att $\text{SGD}(p, a) = 1$. (Här använder vi att p är primtal!)
Men då följer det att

$$bxa + byp = b \iff (ab)x + p(by) = b.$$

Eftersom vänsterledet delas av p, måste p dela b. □

Detta lemma kan generaliseras till fler än två faktorer.

Sats 27. *Varje positivt heltal n kan skrivas unikt som en produkt av primtal:*

$$n = p_1 p_2 \dots p_k.$$

(Samma primtal kan förekomma flera gånger).

Bevis. Vi såg att det finns minst en sådan faktorisering tidigare. Antag nu att

$$n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_\ell,$$

där p_i och q_j är primtal. Eftersom p_1 delar vänsterledet, så måste detta dela en av talen i högerledet. Men då har vi att $p_1 = q_j$ för något j. Vi kan då dividera bort dessa faktorer från vardera sida, och fortsätta. För varje primtal p_i som delas bort, måste det finnas samma primtal som faktor i högerledet. Detta gör att vi är klara. □

3.1. Största gemensamma delare för primtalsfaktoriserade tal

Problem 28. Vad är $\text{SGD}(2^5 \cdot 3^7 \cdot 7^8 \cdot 11,\ 2^2 \cdot 3^{12} \cdot 5^2 \cdot 7^3 \cdot 11)$?

Exempel 29. Några användbara Mathematica-kommandon för primtal är:

```
Prime[100]
PrimeQ /@ {97, 221, 9973}
FactorInteger[840]
FactorInteger[2^5 3^7 7^8 11]
```

`Prime[n]` ger det n:te primtalet, `PrimeQ` testar om ett tal är primtal, och `FactorInteger` ger primtalsfaktoriseringen.

3.2. Primtalstvillingar

Läs om primtalstvillingar och Yitang Zhangs bevis från 2013 på Wikipedia.

3.3. Kuriosa: Lite om perfekta tal

Definition 30. Ett positivt heltal n är **perfekt**[1] om alla dess positiva delare (mindre än n) summerar till n.

T.ex är 6 perfekt, då 6 delas av $1, 2, 3$ och $6 = 1 + 2 + 3$. Nästa perfekta tal är 28, då detta delas av talen $\{1, 2, 4, 7, 14\}$ som har summan 28.

Varje jämnt perfekt tal är på formen $\frac{q(q+1)}{2}$, där q är ett primtal på formen $2^p - 1$, där p självt är primtal. Primtal av denna form kallas Mersenne-primtal, och det finns 52 sådana kända i skrivande stund—det senaste hittades 2024, och är primtalet $q = 2^{136,279,841} - 1$. Senaste innan upptäcktes $2^{82,589,933} - 1$, år 2018.

Det är okänt om det finns oändligt många Mersenne-primtal. Det är också okänt om det finns något udda perfekt tal (troligen inte).

3.4. Problemlösning

Problem 31. Antag att p är ett primtal. Visa att om $p^k \mid ab$ och om $\text{SGD}(a, p) = 1$ så gäller det att $p^k \mid b$.

Lösning. Låt $a = p_1^{s_1} \cdots p_m^{s_m}$ och $b = q_1^{t_1} \cdots q_\ell^{t_\ell}$ vara primtalsfaktoriseringarna av a och b. Eftersom $\text{SGD}(a, p) = 1$ kan ingen av p_i:na vara p. Dock vet vi att p^k delar produkten

$$ab = (p_1^{s_1} \cdots p_m^{s_m})(q_1^{t_1} \cdots q_\ell^{t_\ell})$$

så enligt aritmetikens fundamentalsats p^k måste dela något $q_i^{t_i}$. Detta ger att $p^k \mid b$.

Problem 32. Visa att ekvationen $x^3 + 7y^3 = 490$ saknar heltalslösningar.

Lösning. Vi faktoriserar, $490 = 2 \cdot 5 \cdot 7^2$. Omskrivning ger att $x^3 = 2 \cdot 5 \cdot 7^2 - 7y^3$. Alltså är högerledet delbart med 7 och då måste även vänsterledet vara det. Eftersom 7 är ett primtal, måste $7 \mid x$. Vi skriver då om $x = 7k$ och får

$$(7k)^3 = 2 \cdot 5 \cdot 7^2 - 7y^3 \iff 7^3k^3 = 2 \cdot 5 \cdot 7^2 - 7y^3 \iff y^3 = 2 \cdot 5 \cdot 7 - 7^2k^3.$$

Detta ger nu att $7 \mid y$, så $y = 7m$. Omskrivning igen ger

$$7^3m^3 = 2 \cdot 5 \cdot 7 - 7^2k^3 \iff 7^2m^3 + 7k^3 = 2 \cdot 5.$$

Men denna nya ekvation saknar lösningar eftersom vänsterledet alltid är delbart med 7, men det är aldrig högerledet.

Problem 33 (Från tentan 2024-03-07)**.** Visa att om $\text{SGD}(a, b) = 1$ så kan $\text{SGD}(6a, b)$ bara anta värdena $1, 2, 3$ eller 6.

[1] `https://en.wikipedia.org/wiki/Perfect_number`

Lösning. Låt $d = \text{SGD}(6a, b)$. Antag att p^k är en primtalspotens som delar d, för något $k \geq 1$. Då måste $p^k \mid 6a$ och $p^k \mid b$. Om $p \mid a$, skulle p vara gemensam delare till a och b. Alltså måste $p^k \mid 6$. Då måste p^k antingen vara 2 eller 3. Detta innebär att d som mest kan delas av 2 och 3 och vi får värdena ovan.

Alternativt, låt $a = p_1 p_2 \dots p_k$ och $b = q_1 q_2 \dots q_\ell$ vara primtalsfaktoriseringarna av a och b (samma primtal kan finnas med flera gånger i vardera lista). Eftersom $\text{SGD}(a, b) = 1$ så har de två produkterna ingen gemensam primtalsfaktor.

Nu tittar vi på

$$\text{SGD}(6a, b) = \text{SGD}(2 \cdot 3 \cdot p_1 p_2 \dots p_k, q_1 q_2 \dots q_\ell).$$

Den enda skillnaden nu är om något/några av primtalsfaktorerna i b är lika med 2 eller 3. I så fall blir största gemensamma delaren 2, 3 eller 6.

Föreläsning 4
Reella tal, potenser och ekvationer

4.1. Potenser

- Vi *definierar* först a^n, där n är positivt heltal, som upprepad multiplikation.
- Notera att $a^{m+n} = a^m \cdot a^n$ samt $a^{mn} = (a^m)^n$. *(Satser).*
- Första formeln kräver då att $a^{m-n} = a^m \cdot a^{-n}$, som kräver att $a^0 = 1$ och $a^{-n} = \frac{1}{a^n}$ *(Definitioner)*
- Den andra formeln kräver att om vi generaliserar till rationella exponenter, att $a^1 = a^{m/m} = (a^{1/m})^m$, så $a^{1/m} = \sqrt[m]{a}$. *(Definitioner)*

Vi har också att $(ab)^n = a^n \cdot b^n$. *(Sats)*
Hur vet vi att $\sqrt[m]{a}$ finns? Detta är enligt definition, **det positiva reella tal som löser ekvationen** $x^m = a$. Vi kan då i princip hitta x genom att testa oss fram (binärsökning) och hitta ett mindre och mindre intervall där $x = \sqrt[m]{a}$ befinner sig inom. Filosofiskt kan vi då övertyga oss om att det finns ett unikt reellt tal *i gränsen*.

4.1.1. Reella exponenter

Hur beräknar vi då 3^π? Man får ta och kika på

$$3^{3.1}, \quad 3^{3.14}, \quad 3^{3.141}, \ldots$$

och använda egenskaper hos gränsvärden samt gå in på hur reella tal faktiskt definieras. Att definiera reella tal är lite mer invecklat än man kan tro, men i denna kurs använder vi den intuition man fått från gymnasiet.

4.2. Polynomekvationer av grad 1 och 2

Vi har sett förstagradsekvationer, andragradsekvationer (med kvadratkomplettering).

Sats 34. *Vi kan lösa $x^2 + px + q = 0$ med hjälp av kvadratkomplettering (pq-formeln).*

Bevis. Vi har att

$$x^2 + px + q = 0 \iff \left(x + \frac{p}{2}\right)^2 - \frac{p^2}{4} + q = 0.$$

Skriver vi om det får vi

$$\left(x + \frac{p}{2}\right)^2 = \frac{p^2}{4} - q.$$

Alltså måste $x + \frac{p}{2}$ vara ett tal vars kvadrat är $\frac{p^2}{4} - q$. Så

$$x + \frac{p}{2} = \pm\sqrt{\frac{p^2}{4} - q}$$

och slutligen

$$x = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}.$$

□

Detta kallas för **pq-formeln** i folkmun. Notera att man får komplexa tal om $\frac{p^2}{4} - q < 0$.

4.3. Rotekvationer

Exempel 35. (a) Lös rotekvationen (Svar: $x = \sqrt{2}$)

$$\sqrt{2x+3} = 1 + x.$$

(b) Förenkla sedan uttrycket $\sqrt{2\sqrt{2}+3}$.

Lösning. (a) Båda led kvadreras, vilket implicerar att x måste lösa även ekvationen

$$(2x+3) = 1 + 2x + x^2 \iff x^2 = 2.$$

Dock är det bara $x = \sqrt{2}$ som är en lösning.

(b) Eftersom $x = \sqrt{2}$ löser ekvationen tidigare, så måste $\sqrt{2\sqrt{2}+3} = 1 + \sqrt{2}$.

Exempel 36. Lös rotekvationen

$$\sqrt{2x+2} = 1 + \sqrt{3x-12}.$$

Lösning. Svar: $x = 7$.

Exempel 37. Lös rotekvationen

$$\sqrt{x-4} - 2x = 1 - \sqrt{1-x}.$$

Lösning. Lösning saknas, eftersom första rotuttrycket kräver $x \geq 4$, men samtidigt måste vi ha $x \leq 1$ i andra rotuttrycket.

4.4. Substitutionsmetoden

Exempel 38. Lös ekvationen $t^4 - 5t^2 + 6 = 0$.

Lösning. Vi får $t^2 = 2$ eller $t^2 = 3$, så lösningarna är $\pm\sqrt{2}$ samt $\pm\sqrt{3}$.

Exempel 39. Lös ekvationen

$$\left(x^2 + 3x\right)^2 - 14\left(x^2 + 3x\right) + 40 = 0.$$

Lösning. Vi sätter $t = x^2 + 3x$. Då måste vi lösa $t^2 - 14t + 40 = 0$. Denna ekvation har lösningarna $t_1 = 4$ samt $t_2 = 10$.

Fall 1: $t_1 = 4$ ger att x måste lösa $x^2 + 3x = 4$. Detta leder till $x_1 = -4$ samt $x_2 = 1$.

Fall 2: $t_2 = 10$ ger att x måste lösa $x^2 + 3x = 10$. Detta leder till $x_1 = -5$ samt $x_2 = 2$.

Sammanfattningsvis har vi fyra lösningar: $x \in \{-5, -4, 1, 2\}$.

4.5. Fler uppgifter

Problem 40. Lös ekvationen

$$\sqrt{x - 2\sqrt{x-1}} = a \tag{4.1}$$

för alla $a \geq 1$.

Lösning. Vi löser den generella ekvationen. Kvadrerar man båda led fås

$$x - 2\sqrt{x-1} = a^2.$$

Vi löser ut roten och kvadrerar igen:

$$\left(-2\sqrt{x-1}\right)^2 = \left(a^2 - x\right)^2.$$

Detta leder till

$$4(x-1) = (a^4 - 2a^2x + x^2) \iff x^2 - (2a^2+4)x + (a^4+4) = 0.$$

Den sista ekvationen löser vi med pq-formeln, och får

$$x = (a^2+2) \pm \sqrt{(a^2+2)^2 - (a^4+4)}$$

så

$$x = (a^2+2) \pm \sqrt{4a^2} \iff x = (a^2+2) \pm 2a.$$

Vi måste dock sätta in dessa lösningar i ursprungliga ekvationen (4.1). Lösningen $x = a^2 - 2a + 2$ insatt i vänsterledet evalueras till[1]

$$\begin{aligned}&\sqrt{(a^2-2a+2) - 2\sqrt{a^2-2a+2-1}} \\ &\quad = \sqrt{(a^2-2a+2) - 2(a-1)} = \sqrt{a^2-4a+4} = \sqrt{(a-2)^2}.\end{aligned}$$

Detta är lika med a bara om $a = 1$.

Lösningen $x = a^2 + 2a + 2$ ger

$$\sqrt{(a^2+2a+2) - 2\sqrt{a^2+2a+2-1}} = \sqrt{(a^2+2a+2) - 2(a+1)} = a$$

så detta är alltid en lösning.

Sammanfattningsvis: om $a = 1$ finns det två lösningar, $x = 1$ och $x = 5$. Annars, om $a > 1$ finns bara lösningen $x = a^2 + 2a + 2$.

Problem 41. Lös rotekvationen

$$2\sqrt{3 + (2 - x^2)} + \sqrt{2 + (2 - x^2)} = 2.$$

Lösning. Lösningarna är $x = \pm 2$.

Exempel 42. Mathematica kan lösa ekvationer med `Solve`. Ibland vill man ange om man bara söker reella lösningar:

```
Solve[x^2 - 2 == 0, x]
Solve[x^2 + 1 == 0, x, Reals]
Solve[x^2 + 1 == 0, x, Complexes]
Solve[{x^2 + y^2 == 25, x + y == 7}, {x, y}, Reals]
```

[1] Kom ihåg att $a \geq 1$.

Föreläsning 5
Olikheter och absolutbelopp

Uttryck som alltid är positivt, kan förkortas bort.

5.1. Olikheter och teckentabeller

Exempel 43. Lös olikheten

$$\frac{(x+1)(x-4)e^x}{\sqrt{2x-1}(x-2)} > 0.$$

Lösning. Vi ser att $x > \frac{1}{2}$, annars är uttrycket inte definierat. Om $x > \frac{1}{2}$ kan vi förlänga bort rotuttrycket (som alltid är positivt) så olikheten är ekvivalent med

$$\frac{(x+1)(x-4)}{(x-2)} > 0.$$

Teckenstudium av denna olikhet ger att om $-1 < x < 2$ eller $x > 4$ löses olikheten. Lösningarna till ursprungliga olikheten är då intervallen $\frac{1}{2} < x < 2$ samt $x > 4$.

Metoden med teckentabell är att skriva olikheten som $f(x) > 0$ där man faktoriserat $f(x)$. Man studerar därefter tecknet på varje faktor av $f(x)$. Enbart tecknet avgör ju därefter om olikheten gäller eller inte.

Problem 44. Lös olikheten

$$\frac{3x+2}{x-2} \geq 2x - 1.$$

Lösning. Vi skriver om det som

$$\frac{3x+2}{x-2} - (2x-1) \geq 0 \iff \frac{(3x+2) - (2x-1)(x-2)}{x-2} \geq 0.$$

Detta blir

$$\frac{8x - 2x^2}{x-2} \geq 0 \iff \frac{(2x)(4-x)}{x-2} \geq 0.$$

Teckenstudium för punkter mellan $x = 0, 2, 4$ ger att lösningarna är de x som uppfyller $x \leq 0$ eller $2 < x \leq 4$.

Problem 45. Lös olikheten

$$\frac{3}{x+2} + \frac{4}{x+4} > 1.$$

Lösning. Vi skriver om som

$$\frac{3(x+4)}{(x+2)(x+4)} + \frac{4(x+2)}{(x+2)(x+4)} - 1 > 0.$$

Detta blir

$$\frac{(3x+12)+(4x+8)-(x+2)(x+4)}{(x+2)(x+4)} > 0 \iff \frac{12+x-x^2}{(x+2)(x+4)} > 0,$$

och pq-formeln ger faktoriseringen av täljaren:

$$\frac{(4-x)(x+3)}{(x+2)(x+4)} > 0.$$

Teckenstudium ger därefter lösningarna $-4 < x < -3$ samt $-2 < x < 4$.

Problem 46. Lös olikheten

$$\frac{\sqrt{10-x}(x^2+2x+4)(x^2-3x+2)(x+3)^2}{2x-1} \geq 0.$$

Lösning. Rotuttrycket är alltid positivt eller 0, och enbart definierat om $x \leq 10$. Första polynomfaktorn har inga reella rötter. Denna är då alltid positiv. Den andra polynomfaktorn har rötterna 1 och 2, så den är negativ däremellan. Tredje polynomfaktorn är alltid positiv, utom då $x = -3$ då den är noll. I nämnaren får vi teckenbyte vid $x = \frac{1}{2}$ och uttrycket är odefinierat exakt då $x = \frac{1}{2}$.
Lösningen blir då $\frac{1}{2} < x \leq 1$, $2 \leq x \leq 10$ samt $x = -3$.

Sats 47 (Olikheten för aritmetiska- och geometriska medelvärdet)**.** *Om $a, b \geq 0$ gäller*

$$\frac{a+b}{2} \geq \sqrt{ab}.$$

Bevis. Vi har att

$$(\sqrt{a} - \sqrt{b})^2 \geq 0.$$

Utvecklar vi, får vi

$$a - 2\sqrt{ab} + b \geq 0 \iff a + b \geq 2\sqrt{ab}$$

och vi är klara. □

5.2. Ekvationer med absolutbelopp

Vi introducerar **absolutbeloppet** av ett reellt tal som

$$|x| = \begin{cases} x & \text{om } x \geq 0 \\ -x & \text{annars.} \end{cases}$$

Alternativt ser vi att $|x| = \sqrt{x^2}$. Man kan tolka det som **avståndet** till origo.

Ekvationer löses genom att dela upp i olika fall, där man i varje fall vet vad respektive absolutbelopp har för tecken inuti.

Problem 48. Lös ekvationen $|x+5|+|2x+3|=5$ samt olikheten $|x+5|+|2x+3|\geq 5$.

Lösning. (a) Absolutbeloppen byter tecken vid $x=-5$ och $x=-3/2$. Vi har då tre fall att undersöka.

Fall 1: $x<-5$**:** Ekvationen blir

$$-(x+5)-(2x+3)=5 \iff -3x-8=5 \iff -3x=13 \iff x=-\frac{13}{3}.$$

Men $-\frac{13}{3}$ ligger inte i intervallet $x<-5$, så detta fall saknar lösningar.

Fall 2: $-5\leq x<-3/2$**:** Ekvationen blir

$$(x+5)-(2x+3)=5 \iff -x+2=5 \iff x=-3.$$

Talet -3 ligger i intervallet, så detta är en lösning.

Fall 3: $-3/2\leq x$**:** Ekvationen blir

$$(x+5)+(2x+3)=5 \iff 3x+8=5 \iff x=-1.$$

Talet -1 ligger i intervallet, så detta är en lösning.

Sammanfattningsvis: Vi har $x=-3$ samt $x=-1$ som lösningar.

(b) Vi har $x\leq -3$ samt $x\geq -1$ som lösningar.

Problem 49. Lös ekvationen

$$|(x-3)(x-5)|+|(x-3)(x+4)|=9.$$

Lösning. Man får falluppdelning, med de fyra intervallen $x<-4$, $-4\leq x\leq 3$, $3\leq x<5$ samt $x\geq 5$.

Fall 1: $x<-4$**:** Ekvationen blir

$$(x-3)(x-5)+(x-3)(x+4)=9 \iff (x-3)(2x-1)=9.$$

Man kan lösa denna andragradsekvation[1] och se att de två lösningarna ej uppfyller $x<-4$. Alternativt ser vi att om $x<-4$, så är första parentesen strikt mindre än -7 och andra parentesen strikt mindre än -9. Produkten kan då inte vara lika med 9.

Fall 2: $-4\leq x\leq 3$**:** Ekvationen blir

$$(x-3)(x-5)-(x-3)(x+4)=9 \iff (x-3)(-9)=9 \iff x=2.$$

Så här har vi en lösning.

Fall 3: $3\leq x<5$ **:** Ekvationen blir

$$-(x-3)(x-5)+(x-3)(x+4)=9 \iff (x-3)(9)=9 \iff x=4.$$

Så här är en till lösning.

Fall 4: $x\geq 5$ **:** Ekvationen blir återigen

$$(x-3)(x-5)+(x-3)(x+4)=9,$$

som saknar lösningar.

Sammanfattningsvis har ekvationen lösningarna $x=2$ samt $x=4$.

[1]Den blir $2x^2-7x-6=0$, med rötter $\frac{1}{4}(7\pm\sqrt{97})$.

Problem 50. Lös ekvationen

$$|3x| - |2x+1| + |x-2| = 1.$$

Lösning. Absolutbeloppen byter tecken vid $x = -\frac{1}{2}$, $x = 0$ och $x = 2$. Falluppdelning ger följande:
Fall $x < -\frac{1}{2}$: Ekvationen blir

$$-3x + (2x+1) - (x-2) = 1 \implies x = 1.$$

Denna lösning ligger utanför intervallet.
Fall $-\frac{1}{2} \leq x < 0$ ger ekvationen

$$-3x - (2x+1) - (x-2) = 1 \implies x = 0.$$

Återigen ligger lösningen utanför intervallet.
Fall $0 \leq x < 2$ ger ekvationen

$$3x - (2x+1) - (x-2) = 1, \text{ vilket alltid gäller.}$$

Alla x i intervallet är lösningar.
Fall $2 \leq x$ ger ekvationen

$$3x - (2x+1) + (x-2) = 1 \implies x = 2.$$

Vi får en till lösning, $x = 2$.
Sammanfattningsvis, de x som uppfyller $0 \leq x \leq 2$ löser ekvationen.

Problem 51 (Från 2024-08-13)**.** Lös ekvationen $|x^2 - 1| + |x - 1| = x + 1$ för $x \in \mathbb{R}$.

Lösning. Uttrycken inom absolutbeloppen byter tecken vid $x = -1$ och $x = 1$, respektive. Vi delar upp i tre fall.

- Fall $x < -1$: Här blir ekvationen

  $$(x^2 - 1) - (x - 1) = x + 1 \iff x^2 - 2x - 1 = 0 \iff x = 1 \pm \sqrt{2}.$$

  Ingen av lösningarna uppfyller $x < -1$.

- Fall $-1 \leq x < 1$: Här blir ekvationen

  $$-(x^2 - 1) - (x - 1) = x + 1 \iff x^2 + 2x - 1 = 0 \iff x = -1 \pm \sqrt{2}.$$

  Enbart $x = \sqrt{2} - 1$ ligger inom intervallet.

- Fall $1 \leq x$: Här blir ekvationen

  $$(x^2 - 1) + (x - 1) = x + 1 \iff x^2 - 3 = 0 \iff x = \pm\sqrt{3}.$$

  Bara $\sqrt{3}$ är lösning inom intervallet.

Ekvationen har lösningarna $x = \sqrt{3}$ samt $x = \sqrt{2} - 1$.

Exempel 52. Mathematica kan lösa olikheter. Att lösa olikheten

$$|x - 6| - |x(x+4)| + |(x+2)(x+4)| \leq 5$$

kan man göra med kommandot

```
Reduce[Abs[x - 6] - Abs[(x + 4) x] + Abs[(x + 2) (x + 4)] <= 5, x, Reals]
```

Detta ger att $x \leq -9$, eller att $-\frac{7}{3} \leq x \leq -\frac{3}{2}$.

Föreläsning 6
Modulär aritmetik

Definition 53. Två tal m, n är **kongruenta mod** b, om de ger samma rest vid division med b. Vi skriver det som $m \equiv n \pmod{b}$ (notation som används i kursboken), eller som $m \equiv_b n$.

Exempel 54. Till exempel, 16 är kongruenta med 9 modulo 7. Vi skriver det som $16 \equiv_7 9$. Vi har också att $16 \equiv_7 2$ och $16 \equiv_7 23$.

Relationen $\equiv_b$ är en **ekvivalensrelation**, som innebär att

- $m \equiv_b m$ för alla m
- $m \equiv_b n$ implicerar $n \equiv_b m$,
- $m \equiv_b n$ samt $n \equiv_b k$ ger att $m \equiv_b k$.

Sats 55. *Vi har att $m \equiv_b n$ om och endast om $b \mid (m - n)$.*

Bevis. Vi vet $m = kb + r$, $n = lb + r$. Då gäller $m - n = (k - l)b$, så vi har delbarhet med b. Omvänt, antag $b \mid (m - n)$, så att $(m - n) = kb$. Sätt $n = lb + r$, då gäller $m = m - n + n = kb + lb + r = (k + l)b + r$, så m har också resten r. □

6.1. Räkneregler

Sats 56. *Om $m \equiv_b m'$ och $n \equiv_b n'$, gäller*

$$m + n \equiv_b m' + n', \qquad m - n \equiv_b m' - n', \qquad mn \equiv_b m'n'.$$

Bevis. Använd att $m - m' = kb$ tillsammans med tidigare sats. □

Använder vi denna sats flera gånger, så får vi att $m^k \equiv_b (m')^k$, om $m \equiv_b m'$.
Varning: Man kan inte reducera exponenten med modulo!

Exempel 57. Notera att $2^7 = 128 \equiv_5 3$ som inte är kongruent med $2^2 = 4$ modulo 5, trots att $7 \equiv_5 2$.

6.2. Fermats lilla sats

Sats 58. *Om p är primtal, och a ej delbart med p, gäller:*

$$a^{p-1} \equiv_p 1.$$

Detta kallas för **Fermats lilla sats** och bevisas i en senare kurs. Metoden för beviset bygger på något som kallas *grupper*.

6.3. Tillämpningar

Exempel 59 (Check-summor)**.** Kan det gälla att $149291^2 = 22287802671$? Notera att $149291 \equiv_3 1+1+2+1 \equiv_3 2$, så vänsterledet modulo 3 är 1. Vi har därefter att $22287802671 \equiv 2+2+2+2+1+2+2+1+1 \equiv_3 0$ så högerledet är en multipel av 3.

De båda sidorna kan alltså inte vara lika.

Alternativt kan man också se att sidorna inte är lika genom att beräkna resten vid division med 100.

Problem 60 (Delbarhet med 9)**.** Visa att om heltalet N i bas 10 skrivs (med siffror) som $a_k a_{k-1} \dots a_0$ så är N kongruent med siffersumman $a_k + a_{k-1} + \cdots + a_0$ modulo 9.

Lösning. Vi har att

$$N = \sum_{i=0}^{k} a_i 10^i \equiv_9 \sum_{i=0}^{k} a_i (1)^i = \sum_{i=0}^{k} a_i.$$

Problem 61. Bestäm resten då 2^{1026} delas med 17.

Lösning. Vi har att

$$2^{1026} = 4 \cdot 2^{1024} = 4 \cdot (2^4)^{256} = 4 \cdot 16^{256} \equiv_{17} 4(-1)^{256} = 4,$$

så resten är 4. Alternativt kan man utnyttja att $2^{1024} = (2^{16})^{64}$ och $2^{16} \equiv_{17} 1$ enligt Fermats lilla sats.

Problem 62. Visa att $2^n + 6 \times 9^n$ alltid är delbart med 7.

Problem 63. Visa att $m^2 + 1$ aldrig är delbart med 7.

Problem 64. Visa att $8 \mid 5^{2n} + 7$ för alla $n \in \mathbb{N}$.

Problem 65. Visa att $5 \mid 3^{2n+1} + 2^{2n+1}$ för alla naturliga tal n.

Problem 66. Finn alla heltal x så att $5x \equiv_{11} 4$.

Lösning. Detta problem är ekvivalent med att lösa $5x + 11y = 4$. Eftersom $\mathrm{SGD}(5, 11) = 1$, så finns det lösningar.

Euklides algoritm ger att $11 = 2 \cdot 5 + 1$, så $1 = (-2)5 + 1 \cdot 11$. Det ger oss då att $4 = (-8)5 + 4 \cdot 11$. En partikulärlösning är då $x = -8$, $y = 4$ och allmänna lösningen är

$$x = -8 + 11k, \qquad y = 4 - 5k.$$

De x som löser ekvationen är då de på formen $11k - 8$.

Problem 67. Bestäm resten då $2^{17^{99}}$ delas med 7.

Lösning. Vi vet att $a^6 \equiv_7 1$ (enligt Fermats lilla sats), så det vore bra om vi kan skriva 17^{99} som $6k + r$. Nu, $17^{99} \equiv_6 (-1)^{99} \equiv_6 -1 \equiv_6 5$. Alltså har vi att $17^{99} = 6k + 5$ för något k. Detta ger nu

$$2^{17^{99}} = 2^{6k+5} = 2^5 \cdot (2^6)^k \equiv_7 32 \cdot 1^k \equiv_7 4$$

Så resten är 4.

Problem 68 (Delbarhet med 7)**.** Följande algoritm finns för att avgöra om ett tal n är delbart med 7: Tag sista siffran i n och multiplicera med 2. Subtrahera detta från det tal som fås från n då sista siffran stryks. Om resultatet är delbart med 7, är n också delbart med 7.

Exempel: Tag $n = 4316$. Vi ska då betrakta $431 - 2 \cdot 6 = 419$ istället. Nu, 419 ger oss $41 - 2 \cdot 9 = 23$. Slutligen ser vi att 23 ej är delbart med 7, så 4316 är inte delbart med 7.

Bevisa att denna metod fungerar.

Lösning. Talet n vi börjar med kan skrivas på formen $10k + r$ där $0 \leq r \leq 9$. Talet r är då entalssiffran och k representerar talet som fås av övriga siffror. Översätter vi metoden ovan, så innebär det att vi vill visa följande ekvivalens:

$$10k + r \equiv_7 0 \iff k - 2r \equiv_7 0.$$

Vi börjar med implikationen från vänster till höger:

$$10k + r \equiv_7 0 \implies 3k + r \equiv_7 0 \implies 9k + 3r \equiv_7 0.$$

Tar vi nu skillnaden ledvis av första och sista ekvivalensen, får vi att $k - 2r \equiv_7 0$.

Implikationen åt andra hållet:

$$k - 2r \equiv_7 0 \implies 10(k - 2r) \equiv_7 0 \implies 10k - 20r \equiv_7 0 \implies 10k - 20r + 21r \equiv_7 0.$$

Vi ser då att $10k + r \equiv_7 0$ från sista påståendet.

Problem 69 (Tenta 2024-04-07)**.** Bestäm vilken rest som fås då 5^{31} delas med 26.

Lösning. Vi har att $5^{31} = 5 \cdot 5^{30} = 5 \cdot 25^{15}$ och eftersom $25 \equiv_{26} -1$, får vi $5 \cdot (-1)^{15} = -5$, som är kongruent med 21 modulo 26. Alltså är resten 21.

Problem 70 (Tenta 2024-03-07)**.** Avgör om $121206^2 + 1$ är lika med 14700007507.

Lösning. Man kan antingen jämföra de båda uttrycken modulo 9, eller modulo 100. Räknar man modulo 9, kan man utnyttja egenskapen att ett tals rest modulo 9, är samma som dess siffersumma. Räknar man modulo 100, ser man att vänsterledet är $6^2 + 1 = 37$, men högerledet modulo 100 är 7.

Problem 71 (Tenta 2024-08-13)**.** Beräkna resten då 4^{63} delas med 31.

Lösning. Eftersom 31 är ett primtal, gäller enl. Fermats lilla sats att

$$4^{63} = 4^3(4^{30})^2 \equiv_{31} 4^3 \cdot 1^2 = 64 \equiv_{31} 2.$$

Alternativt, $4^{60} = 2^{120} = (2^5)^{24} = (32)^{24} \equiv_{31} 1^{24} = 1$, där $\equiv_{31}$ indikerar att talen ger samma rest modulo 31.

Problem 72 (Tenta 2024-10-25)**.** Avgöra om den Diofantiska ekvationen $\left(3^{300} - 5^{60}\right) x + 7y = 12$ har lösningar.

Lösning. Den Diofantiska ekvationen $ax + by = c$ heltalslösningar precis då $\text{SGD}(a, b) \mid c$. Vi har att

$$3^{300} - 5^{60} \equiv_7 (3^2)^{150} - (5^2)^{30} \equiv_7 2^{150} - 4^{30} \equiv_7 (2^3)^{50} - (4^3)^{10} \equiv_7 1^{50} - 1^{10} = 0.$$

Alltså gäller $\text{SGD}(3^{300} - 5^{60}, 7) = 7$, och eftersom 12 ej är delbart med 7, så saknar ekvationen lösningar.

Exempel 73. Mathematica kan arbeta med moduloräkning. Till exempel har vi att $7 \mid 3^{300} - 5^{60}$ eftersom kommandot nedan ger 0 som resultat.

```
Mod[3^300 - 5^60, 7]
```

Stora potenser modulo ett tal beräknas effektivt med `PowerMod`:

```
PowerMod[2, 17^99, 7]
```

Kongruensekvationer kan också lösas direkt:

```
Solve[5 x == 4, x, Modulus -> 11]
```

Kommandot `ChineseRemainder` löser system av kongruenser. Till exempel ger

```
ChineseRemainder[{4, 1}, {12, 15}]
```

det minsta icke-negativa talet som är kongruent med 4 modulo 12 och 1 modulo 15.

Föreläsning 7
Komplexa tal på rektangulär form

Vi utökar de reella talen genom att lägga till $i = \sqrt{-1}$. Formellt är i en lösning till ekvationen $x^2 + 1 = 0$ och den andra lösningen är då $-i$.

De **komplexa talen**, $\mathbb{C}$, är då alla tal på formen $a+bi$, där $a, b \in \mathbb{R}$. Addition och multiplikation av komplexa tal följer samma regler som för algebraiska uttryck.

För det komplexa talet $z = a + bi$ har vi att $a = \mathrm{Re}(z)$, **realdelen av** z samt att $b = \mathrm{Im}(z)$, **imaginärdelen av** z.

Konjugatet till ett komplext tal $a + bi$, är $a - bi$. Konjugatet till $z \in \mathbb{C}$ betecknas med $\overline{z}$. För att utföra division av komplexa tal, förläng med nämnarens konjugat.

Sats 74. *Vi har följande egenskaper för konjugatet:*

- $\overline{z + w} = \overline{z} + \overline{w}$
- $\overline{z - w} = \overline{z} - \overline{w}$
- $\overline{zw} = \overline{z} \cdot \overline{w}$
- $\overline{z/w} = \overline{z}/\overline{w}$
- $\overline{(\overline{z})} = z$.

Notera, om $z = a + bi$ gäller $z\overline{z} = a^2 + b^2 \geq 0$.

7.1. Absolutbelopp av komplexa tal

Vi definierar **absolutbeloppet** av $a + bi$ som $|z| = \sqrt{a^2 + b^2}$. Notera att $|z|^2 = z \cdot \overline{z}$.
I det **komplexa talplanet** motsvarar $|z|$ avståndet från (a, b) till origo.

Sats 75. *Vi har att $|zw| = |z| \cdot |w|$. Motsvarande gäller för kvotuttryck.*

Bevis. Vi har att

$$|zw| = \sqrt{zw \cdot \overline{zw}} = \sqrt{z\overline{z}}\sqrt{w\overline{w}} = |z| \cdot |w|.$$

□

Sats 76 (Triangelolikheten)**.** $|z + w| \leq |z| + |w|$.

Bevis. Man kan rita parallellogram, argumentera geometriskt. Alternativt: Samma som att visa

(med $z = a + bi$, $w = c + di$)

$$\begin{aligned}
|z + w|^2 &\leq |z|^2 + 2|z||w| + |w|^2 \\
(a + c)^2 + (b + d)^2 &\leq a^2 + b^2 + c^2 + d^2 + 2\sqrt{a^2 + b^2}\sqrt{c^2 + d^2} \\
a^2 + c^2 + 2ac + b^2 + d^2 + 2bd &\leq a^2 + b^2 + c^2 + d^2 + 2\sqrt{a^2 + b^2}\sqrt{c^2 + d^2} \\
ac + bd &\leq \sqrt{a^2 + b^2}\sqrt{c^2 + d^2} \\
(ac + bd)^2 &\leq (a^2 + b^2)(c^2 + d^2) \\
a^2c^2 + b^2d^2 + 2abcd &\leq a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 \\
0 &\leq a^2d^2 + b^2c^2 - 2abcd \\
0 &\leq (ad - bc)^2.
\end{aligned}$$

□

Problem 77 (Från boken)**.** Finn alla z som uppfyller

$$\left|\frac{z+1}{z+i}\right| = \sqrt{2}.$$

Lösning. Vi skriver om och får

$$|z + 1| = \sqrt{2}|z + i| \iff |z + 1|^2 = 2|z + i|^2.$$

Sätt $z = x + yi$, och vi får $(x + 1)^2 + y^2 = 2(x^2 + (y + 1)^2)$. Omskrivning igen ger

$$x^2 - 2x + y^2 + 4y + 1 = 0 \iff (x - 1)^2 + (y + 2)^2 = 4.$$

Detta beskriver en cirkel med radie 2 och centrum i $(1, -2)$, dvs. en cirkel centrerad i $1 - 2i$.

7.2. Komplexa andragradsekvationer

Problem 78. Lös andragradsekvationen $x^2 - 6x + 34 = 0$.

Lösning. Kvadratkomplettering ger

$$(x - 3)^2 - 9 + 34 = 0 \iff (x - 3)^2 = -25$$

så $x - 3 = \pm 5i$ och $x = 3 \pm 5i$.

Problem 79. Finn z, så att $z^2 = -16 + 30i$.

Lösning. Sätt $z = a + bi$. Genom att jämföra realdel, imaginärdel och absolutbelopp av båda sidor, får vi de tre ekvationerna

$$a^2 - b^2 = -16, \qquad 2ab = 30, \qquad a^2 + b^2 = \sqrt{16^2 + 30^2} = \sqrt{256 + 900} = \sqrt{1156} = 34.$$

Ledvis addition av första och sista ger $2a^2 = 34 - 16 = 18$, så $a = \pm 3$. Insatt i andra ekvationen ger $b = \pm 5$. Lösningar: $z = 3 + 5i$ eller $z = -3 - 5i$.

Problem 80. Lös andragradsekvationen $x^2 - (4 + 2i)x + (11 - 2i) = 0$.

Lösning. Kvadratkomplettering ger

$$\begin{aligned}(x-(2+i))^2 &= (2+i)^2-(11-2i)\\ (x-(2+i))^2 &= 4+4i-1-11+2i\\ (x-(2+i))^2 &= -8+6i.\end{aligned}$$

Vi måste nu lösa

$$(a+bi)^2 = -8+6i.$$

Detta ger (Real, imag, absolutbelopp)

$$a^2-b^2=-8 \qquad 2ab=6, \qquad a^2+b^2=\sqrt{8^2+6^2}=10.$$

Notera att $ab=3$. Addition ledvis ger $2a^2 = 10-8 = 2$ så $a^2=1$. Detta ger lösningarna $(a=1, b=3)$ eller $(a=-1, b=-3)$. Så,

$$x-(2+i)=1+3i \qquad \text{eller} \qquad x-(2+i)=-1-3i,$$

som slutligen ger

$$x=3+4i \qquad \text{eller} \qquad x=1-2i.$$

Problem 81. Lös andragradsekvationen $x^2-(5-2i)x+(21-i)=0$.

Lösning. Kvadratkomplettering ger

$$\begin{aligned}(x-(5/2-i))^2 &= (5/2-i)^2-(21-i)\\ (x-(5/2-i))^2 &= \frac{25}{4}-5i-1-21+i\\ (x-(5/2-i))^2 &= \frac{25-88}{4}-4i\\ (x-(5/2-i))^2 &= \frac{-63-16i}{4}.\end{aligned}$$

Vi måste nu lösa

$$(a+bi)^2 = \frac{-63-16i}{4}.$$

Detta ger (realdel, imaginärdel, absolutbelopp)

$$a^2-b^2=\frac{-63}{4} \qquad 2ab=\frac{-16}{4}, \qquad a^2+b^2=\frac{\sqrt{63^2+16^2}}{4}=\frac{65}{4}.$$

Notera att $ab=-2$. Ledvis addition ger

$$2a^2=\frac{2}{4} \implies a^2=\frac{1}{4},$$

så vi får $a_1=\frac{1}{2}$, $b_1=-4$, eller $a_2=-\frac{1}{2}$, $b_2=4$.
Alltså,

$$x-(5/2-i)=\frac{1}{2}-4i \qquad x-(5/2-i)=-\frac{1}{2}+4i.$$

Detta leder slutligen till de två lösningarna

$$x=3-5i \qquad x=2+3i.$$

Exempel 82. Fler exempel:

- $x^2 - 8x + (16 - 2i) = 0 \quad (x = 5 + i,\ x = 3 - i)$
- $x^2 - (2 - 2i)x + (9 - 2i) \quad (x = 1 + 2i,\ x = 1 - 4i)$.

Exempel 83. I Mathematica skrivs den imaginära enheten som `I`. De vanliga räknesätten fungerar direkt:

```
(3 + 4 I) + (1 - 2 I)
(3 + 4 I)/(1 - 2 I)
Conjugate[3 + 4 I]
Abs[3 + 4 I]
Solve[z^2 - (4 + 2 I) z + (11 - 2 I) == 0, z]
```

Föreläsning 8
Komplexa tal på polär form

Polära koordinater: punkter (x, y) kan beskrivas som $(r\cos(\theta), r\sin(\theta))$. Notera, vi kan använda olika vinklar (upp till multiplar av 2π) för samma punkt. Detta är en viktig egenskap! Radien, r är given av absolutbeloppet. Vinkeln kan beräknas med hjälp av arctan.

8.1. Polära koordinater

Absolutbeloppet betecknas ibland abs(z), och vinkeln betecknas arg(z). Här måste man bestämma sig om man vill ha vinklar mellan 0 och 2π, eller mellan $-\pi$ och π.

Den **komplexa exponentialfunktionen** definieras av

$$e^{i\theta} := \cos(\theta) + i\sin(\theta).$$

Detta visar sig vara en bra definition, eftersom alla regler för exponenter fortsätter gälla (men man måste bevisa detta!). Varför man just ska använda talet e som bas kommer förklaras senare i analysen då man lär sig om Taylorserier. Varje komplext tal kan nu skrivas på **polär form**:

$$r \cdot \cos(\theta) + r \cdot i\sin(\theta) = re^{i\theta}.$$

Exempel 84. Skriv talet $1 + i$ på polär form.

Exempel 85. Skriv talet $-1 + \sqrt{3}i$ på polär form.

Exempel 86. Skriv talet $20e^{i\pi/2}$ på rektangulär form.

8.2. Mer om exponentialfunktionen

Notera att om $z = re^{i\theta}$, gäller det att

$$re^{-i\theta} = r(\cos(-\theta) + i\sin(-\theta)) = r(\cos(\theta) - i\sin(\theta)) = \overline{z}$$

så konjugering är samma som att byta tecken på vinkeln.

Sats 87. *Vi har att*

$$e^{i\alpha+i\beta} = e^{i\alpha}e^{i\beta}.$$

Bevis. Bevisa genom additionslagarna för sinus- och cosinus. Notera att man *inte* kan använda potenslagarna (eftersom vi inte ännu verifierat att de stämmer för komplexa exponenter). Beviset ovan visar att definitionen av $e^{i\alpha}$ är kompatibel med existerande potenslagar. □

Notera att ovanstående nu kan användas för att visa att $(e^{i\alpha})^n = e^{i\alpha n}$, om n är ett heltal.

Exempel 88. Potenslagarna fungerar *inte* alltid som förväntat om man har en negativ bas:

$$-1 = \sqrt{-1} \cdot \sqrt{-1} \stackrel{!}{=} \sqrt{(-1) \cdot (-1)} = \sqrt{1} = 1.$$

I ett av stegen har vi använt en potenslag som inte gäller (inte kan generaliseras till situationen ovan).

Sats 89 (Eulers identiteter)**.** *Vi har*

$$\cos(\theta) = \frac{e^{i\theta} + e^{-i\theta}}{2} \qquad \sin(\theta) = \frac{e^{i\theta} - e^{-i\theta}}{2i}.$$

Speciellt, $e^{\pi i} = -1$.

Sats 90. *Om $z = re^{\alpha i}$ och $w = se^{\beta i}$ så har vi produkten*

$$zw = rse^{(\alpha+\beta)i}.$$

Med andra ord, för tal på polär form så multipliceras absolutbeloppen, och argumenten adderas. Se motsvarande för division.

8.3. De Moivres formel

Upprepar vi multiplikation, får vi potenser: Om $z = re^{\theta i}$ gäller

$$z^n = r^n e^{n\theta i} = r^n(\cos(n\theta) + i\sin(n\theta)).$$

Problem 91. Bestäm $(1+i)^{100}$ på rektangulär form.

Lösning. Vi har $w = 1 + i = \sqrt{2}e^{i\pi/4}$, så

$$w^{100} = \sqrt{2}^{100} e^{25i\pi} = 2^{50} e^{24\pi i + \pi i} = -2^{50}.$$

Problem 92. Visa att $\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta)$.

Lösning. Låt $z = \cos(\theta) + i\sin(\theta)$. Notera att

$$(\cos(\theta) + i\sin(\theta))^3 = (\cos(\theta) + i\sin(\theta))^3.$$

Ena sidan blir $\cos(3\theta) + i\sin(3\theta)$ enligt De Moivres formel, men högerledet kan vi utveckla genom upprepad multiplikation. Vi jämför sedan real- och imaginärdel. Man måste även använda trigonometriska ettan om man vill ha enbart uttryck i $\cos(\theta)$. Svaret blir $4\cos^3(\theta) - 3\cos(\theta)$.

8.4. Binomiska ekvationer

Låt oss lösa $z^n = w$, för komplexa tal w. Vi skriver om $w = r(\cos(\theta) + i\sin(\theta))$, som är kända, samt $z = s(\cos(\gamma) + i\sin(\gamma))$ Vi ser att

$$z^n = s^n(\cos(n\gamma) + i\sin(n\gamma)) = r(\cos(\theta) + i\sin(\theta))$$

så för att dessa ska stämma, måste $s^n = r$ samt

$$n\gamma = \theta + 2\pi k,$$

vilket leder till

$$s = \sqrt[n]{r}, \qquad \gamma = \frac{\theta + 2\pi k}{n} \qquad k \in \mathbb{Z}.$$

Notera att lösningarna ligger symmetriskt i det komplexa talplanet! De bildar en regelbunden n-gon.

Problem 93. Lös ekvationen $z^6 = 64$.

Lösning. Notera, $r = 64$, så $|z| = \sqrt[6]{64} = 2$. Argumentet för 64 är $0 + 2k\pi$, så argumenten för lösningarna är $0/6 + 2k\pi/6$, där $k = 0, \ldots, 5$. Alla lösningar är då

$$2(\cos(0) + i\sin(0)),\ 2(\cos(\pi/3) + i\sin(\pi/3)),\ 2(\cos(2\pi/3) + i\sin(2\pi/3)),$$
$$\ldots,\ 2(\cos(5\pi/3) + i\sin(5\pi/3)).$$

Problem 94. Lös ekvationen $z^3 = 27i$.

Lösning. Notera, $r = 27$, så $|z| = \sqrt[3]{27} = 3$. Argumentet för $27i$ är $\pi/2 + 2k\pi$, så argumenten för lösningarna är $\pi/6 + 2k\pi/3$, där $k = 0, \ldots, 2$. Alla lösningar är då

$$3(\cos(\pi/6) + i\sin(\pi/6)),\ 3(\cos(\pi/6 + 2\pi/3) + i\sin(\pi/6 + 2\pi/3)),$$
$$3(\cos(\pi/6 + 4\pi/3) + i\sin(\pi/6 + 4\pi/3)).$$

Notera då att $(27i)^{\frac{1}{3}}$ inte har ett entydigt värde!
Vi kan inte förvänta oss att komplext tal upphöjt med annat (reellt, eller komplext) tal har ett entydigt värde. Det är bara om det tal vi upphöjer med är ett heltal, som vi får ett entydigt svar!

Problem 95. Ge mening till och beräkna i^i.

Lösning. Vi har att $i = e^{\pi i/2 + 2\pi ki}$, så $i^i = \left(e^{\pi i/2 + 2\pi ki}\right)^i$ vilket blir (om man vill att potenslagarna ska gälla för komplexa tal)

$$e^{-\pi/2 - 2\pi k},$$

ett möjligt värde är då $e^{-\pi/2}$, men egentligen finns det oändligt många "rätta" svar då man varierar k.

Problem 96. Bestäm följande summa:

$$\arctan(3/2) + \arctan(7/4) + \arctan(2/1).$$

Lösning. Vi tillverkar tre komplexa tal som har dessa vinklar som argument:

$$(2 + 3i),\ (4 + 7i) \text{ samt } (1 + 2i).$$

Argumentet för deras produkt är precis den vinkel vi söker. Multiplicerar vi samman de tre talen ovan, får vi det reella talet -65, som har argument π. Alltså är summan ovan π.

Problem 97. Låt vinklarna θ_1, θ_2 och θ_3 vara

$$\theta_1 = \arctan\frac{1}{3}, \quad \theta_2 = \arcsin\frac{2}{\sqrt{5}}, \quad \theta_3 = \arccos\frac{3}{5}.$$

Ge exempel på tre komplexa tal z_1, z_2 och z_3 som uppfyller att $\theta_1 = \arg(z_1)$, $\theta_2 = \arg(z_2)$ samt $\theta_3 = \arg(z_3)$. Beräkna slutligen summan $\theta_1 + \theta_2 + \theta_3$ exakt.

Lösning. Summan blir $3\pi/4$.

Problem 98. Låt $z = 1 + i$ och bestäm $1 + z + z^2 + z^3 + \cdots + z^{19}$.

Lösning. Det är *geometrisk serie*[1] vars summa blir $\frac{z^{20}-1}{z-1}$. Först, $z^{20} = \sqrt{2}^{20} e^{5\pi i} = -1024$. Svaret blir då

$$\frac{-1024 - 1}{1 + i - 1} = \frac{-1025}{i} = 1025i.$$

Problem 99. Bestäm $(\cos(\pi/12) + i\sin(\pi/12))^{124^{124}}$.

Lösning. Notera att

$$\cos(\pi/12) + i\sin(\pi/12) = \exp\left(\frac{2\pi}{24}i\right),$$

och om $n = 24k + r$, gäller

$$(\cos(\pi/12) + i\sin(\pi/12))^n = \exp\left(\frac{2\pi \cdot n}{24}i\right) = \exp(2\pi ik) \cdot \exp\left(\frac{2\pi \cdot r}{24}i\right).$$

Vi vill alltså bestämma 124^{124} mod 24. Först, $124 \equiv_{24} 4$, och

$$4^2 \equiv_{24} 16, \text{ och } 4^3 \equiv_{24} 16.$$

Genom att multiplicera båda sidorna upprepade gånger med 4, får vi därefter att $4^m \equiv_{24} 16$ för alla $m \geq 2$. Alltså gäller det att $124^{124} = 24k + 16$ för något heltal k.
Talet vi söker är då

$$\exp\left(\frac{2\pi \cdot 16}{24}i\right) = \exp\left(\frac{4\pi}{3}i\right) = -\frac{1}{2} - \frac{i\sqrt{3}}{2}.$$

Exempel 100. Vill man lösa ekvationen $z^6 = 64i$, så kan man göra det i Mathematica:

```
Solve[z^6 == 64 I, z]
```

Svaret kan göras om till något mer läsbart med `ExpToTrig`:

```
ExpToTrig[Solve[z^6 == 64 I, z]]
```

Några kommandon som är användbara för polär form är:

```
Abs[-1 + Sqrt[3] I]
Arg[-1 + Sqrt[3] I]
TrigToExp[Cos[t] + I Sin[t]]
ExpToTrig[(Sqrt[2] Exp[I Pi/4])^8]
```

[1] Tas upp igen senare i kursen.

Föreläsning 9
Polynom

Polynom är egentligen (nästan) de enda funktionerna som vi direkt kan studera, då de är uppbyggda av addition och multiplikation.

Definition 101. Ett polynom är ett uttryck på formen $a_n x^n + \cdots + a_1 x + a_0$. Om $a_n \neq 0$ sägs det ha **grad** n, vilket betecknas $\deg(p)$.

Konstanter har generellt grad 0, men det reella talet 0 anses ha grad $-\infty$.

Detta gör att multiplikation av polynom, ger ett resultat vars grad är *summan* av de ingående polynomens grad. (Sats 9.2 i boken)

9.1. Delbarhet av polynom

Vi säger att $q(x)$ delar $p(x)$, om vi kan skriva $p(x) = q(x) \cdot k(x)$ för något polynom $k(x)$. Detta skrivs som $q \mid p$. Notera att nollskilda konstanter delar alla polynom.

Delbarhet är viktigt när man ska undersöka (rationella) funktioner.

Exempel 102. Vi har

$$\frac{x^3 - 4x}{x - 2} = x(x + 2) \text{ då } x \neq 2.$$

9.2. Divisionsalgoritmen för polynom

Sats 103 (Sats 9.4)**.** *Till varje polynom $p(x)$ och nollskilt polynom $q(x)$, finns det* unika *polynom $k(x)$ och $r(x)$ så att*

$$p(x) = k(x)q(x) + r(x), \text{ och } \deg(r(x)) < \deg(q(x)).$$

Beviset kommer nedan, och bygger på divisionsalgoritmen för polynom.

Man kan utföra polynomdivision precis som liggande stolen. Vad är liggande stolen? Jo, det är egentligen upprepad subtraktion! Om vi ska dela 60 med 12, är detta samma som att fråga *Hur många gånger kan vi dra 12 från 60?*

Exempel 104. Utför polynomdivision med $x^5 + 2x^4 + 5x + 2$ delat med $x^2 - x + 1$. Vi ska få $x^3 + 3x^2 + 2x - 1$ som kvot och resten $2x + 3$.

Notera att om $p(x)$ delas med $q(x)$ får vi enligt konstruktion att resten har en grad mindre än $\deg q(x)$, eftersom annars skulle vi fortsätta subtrahera. Vi har också att $p(x) = k(x)q(x) + r(x)$ uppfylls, eftersom vi mer eller mindre har att $p(x) - k(x)q(x) = r(x)$, då $k(x)$ kodar ned vilka multiplar av $q(x)$ vi subtraherat.

Bevis av Sats 9.4. Liggande stolen visar hur vi hittar två polynom, $k(x)$ samt $r(x)$ med de eftersökta egenskaperna. Det räcker då att visa att dessa är unika. Antag

$$p(x) = k(x)q(x) + r(x) = \tilde{k}(x)q(x) + \tilde{r}(x).$$

Ledvis subtraktion ger

$$\Big(k(x) - \tilde{k}(x)\Big)\, q(x) = \tilde{r}(x) - r(x).$$

Men titta nu på graderna! Högerledet har grad strikt mindre än $\deg q(x)$, medan vänsterledet har grad minst $\deg q(x)$ om inte $k(x) = \tilde{k}(x)$. Detta leder sedan till att resterna också är lika. □

9.3. Restsatsen och faktorsatsen

Sats 105 (Sats 9.5)**.** *Låt $p(x)$ vara polynom och $\alpha \in \mathbb{C}$. Då finns $k(x)$ och $r \in \mathbb{C}$ så att*

$$p(x) = (x - \alpha)k(x) + r \text{ där } p(\alpha) = r.$$

Bevis. Enligt tidigare sats finns $k(x)$ och r, och r måste ju ha grad som mest 0, då vi delar med $x - \alpha$. Sätter vi nu in $x = \alpha$ på båda sidor, får vi att $r = p(\alpha)$. □

Sats 106. *Ett polynom $p(x)$ har $\alpha \in \mathbb{C}$ som nollställe om och endast om $(x - \alpha)$ delar $p(x)$.*

Man kan också visa att *alla* icke-konstanta polynom har minst ett (komplext) nollställe — kombinerar man detta med satsen ovan får vi att alla polynom kan faktoriseras (över $\mathbb{C}$) i linjära faktorer (faktorer av grad 1).

Man kan nu visa att ett polynom av grad n som mest kan ha n nollställen (med multiplicitet räknat).

9.4. Blandade polynomproblem

Problem 107. Bestäm resten då polynomet $(x-1)^{20} + x$ delas med $x(x-2)$.

Lösning. Om vi delar det stora polynomet med $x(x-2)$, får vi en rest med grad 1, dvs. på formen $ax + b$. Alltså måste a och b uppfylla

$$(x-1)^{20} + x = x(x-2)k(x) + ax + b, \tag{9.1}$$

där $k(x)$ är kvoten. Vi vill ta reda på a och b utan att beräkna k. Tricket är att sätta in olika värden på x i relationen (9.1) som gör att termen $x(x-2)k(x)$ försvinner, så vi sätter in de nollställen som finns för $x(x-2)$. Insättning av $x = 0$ i (9.1) ger att $(-1)^{20} + 0 = a \cdot 0 + b$. Insättning av $x = 2$ i (9.1) ger att $(2-1)^{20} + 2 = a \cdot 2 + b$. Detta leder oss till ekvationssystemet

$$b = 1 \qquad 1 + 2 = 2a + b,$$

och löser vi ut a och b får vi $a = 1$, $b = 1$. Detta gör att resten vi söker är $x + 1$.

Problem 108. Bestäm resten då $x^{16} + 3x^{10} + 4x^4 + x^2 + 1$ delas med $x^2 + 2$.

Problem 109. Visa att om $x^{100} + 6x^{78} + 44x^{26} + 12x^2 + 2$ delas med $(x^2+1)^2$, så får man en rest på formen $ax^2 + b$, där $a, b \in \mathbb{R}$.

Lösning. Vi kan utföra substitutionen $t = x^2$, då alla potenser av x är jämna.

Problem 110. Antag att $p(x)$ och $q(x)$ är polynom så att $p(n) = q(n)$ för alla heltal $n \geq 1000$. Visa att $p(x)$ och $q(x)$ är samma polynom.

Lösning. Låt $r(x) \coloneqq p(x) - q(x)$. Målet är att visa att $r(x)$ är nollpolynomet. Låt d vara graden på $r(x)$. Eftersom $p(n) = q(n)$ för $n \geq 1000$ så gäller det att $r(n) = 0$ för alla heltal $n \geq 1000$. Alltså är $(x - 1000)$, $(x - 1001)$ och så vidare delare till $r(x)$. Speciellt är då

$$(x - 1000)(x - 1001) \cdots (x - (1000 + d))$$

delare till $r(x)$. Men produkten ovan har större grad än r, så enda möjligheten till delbarhet är om $r(x)$ är nollpolynomet.

Problem 111. Polynomen $p(x) = 3x^3 + 8x^2 - 18x + 5$ och $q(x) = 3x^3 + 5x^2 - 17x + 5$ har en gemensam rot. Hitta den.

Lösning. Om α är den gemensamma roten, så är $(x - \alpha)$ en faktor till båda polynomen. Alltså är $(x - \alpha)$ också en faktor till $p(x) - q(x)$. Nu,

$$p(x) - q(x) = 3x^2 - x = x(3x - 1) = 3x(x - \tfrac{1}{3}).$$

Vi ser[1] att x inte är en faktor till varken p eller q, så det återstår att testa $(3x-1)$. Polynomdivision ger att

$$p(x) = (3x - 1)(x^2 + 3x - 5), \qquad q(x) = (3x - 1)(x^2 + 2x - 5).$$

Den gemensamma roten är då $x = \frac{1}{3}$.

Exempel 112. Mathematica kan beräkna både kvot och rest av polynom. Det finns funktioner för kvot, rest och en funktion som ger båda:

```
PolynomialQuotient[x^10+7x^8-x^5+3x+1,x^2+x+1,x]
PolynomialRemainder[x^10+7x^8-x^5+3x+1,x^2+x+1,x]
PolynomialQuotientRemainder[x^10+7x^8-x^5+3x+1,x^2+x+1,x]
```

Vi får här att

$$x^{10} + 7x^8 - x^5 + 3x + 1 = (x^8 - x^7 + 7x^6 - 6x^5 - x^4 + 6x^3 - 5x^2 - x + 6) \cdot (x^2 + x + 1) + (-2x - 5).$$

Exempel 113. `Factor` försöker faktorisera polynom. Ibland behöver man berätta vilken typ av koefficienter man tillåter i faktoriseringen:

```
Factor[x^3 - 6 x^2 + 11 x - 6]
Factor[x^4 + 1]
Factor[x^4 + 1, Extension -> Sqrt[2]]
Factor[x^4 + 1, Extension -> {I, Sqrt[2]}]
Factor[x^2 + 1, GaussianIntegers -> True]
```

De två sista exemplen visar faktorisering där man tillåter reella respektive komplexa algebraiska tal.

[1] Vi ser $p(0) \neq 0$ och $q(0) \neq 0$.

Föreläsning 10
Polynomekvationer

Sats 114 (Rationella rotsatsen)**.** *Låt $p(x) = a_n x^n + \cdots + a_1 x + a_0$ vara ett polynom med heltalskoefficienter.* Om $\frac{s}{t}$ *är en (förkortad) rationell rot till p, så gäller det att $s \mid a_0$ samt $t \mid a_n$. Speciellt, de enda rationella rötterna till moniska polynom är heltal.*

Bevis. Antag $p(s/t) = 0$. Sätter vi in $x = s/t$ får vi att

$$t^n p(s/t) = a_n s^n + a_{n-1} t s^{n-1} + \cdots + a_1 s t^{n-1} + a_0 t^n = 0.$$

Flyttar vi över $a_0 t^n$ i högerledet, så är vänsterledet en multipel av s, så $s \mid a_0 t^n$, så $s \mid a_0$ eftersom $\mathrm{SGD}(t, s) = 1$. På samma sätt kan vi visa att $t \mid a_n s^n$ och då få att $t \mid a_n$. □

Exempel 115. Vilka möjliga rationella rötter har $2x^3 + x^2 + 2x + 1 = 0$? Jo, de på formen s/t där $t \mid 2$ och $s \mid 1$. Detta leder till att $t = \pm 1$ och ± 2, $s = \pm 1$ vilket ger talen $\pm 1, \pm\frac{1}{2}$. Det visar[1] sig att $-1/2$ är en rot. Utför nu polynomdivision och hitta övriga rötter.

10.1. Algebrans fundamentalsats

Sats 116 (Algebrans fundamentalsats)**.** *Ett polynom med positiv grad och komplexa koefficienter, har minst ett komplext nollställe.*

Vi går inte igenom beviset—man kan inte riktigt uppskatta det på denna nivå.

Eftersom vi har polynomdivision, och sambandet mellan $(x - \alpha) \mid p \iff p(\alpha) = 0$, så kan vi dra slutsatsen: **Ett polynom av grad n, har precis n komplexa rötter, om man räknar dem med multiplicitet.**

Sats 117. *Varje komplext polynom av grad n kan faktoriseras som*

$$c(x - \alpha_1) \cdots (x - \alpha_n),$$

där c är koefficienten för x^n och $\alpha_i \in \mathbb{C}$ är polynomets rötter (samma rot kan förekomma flera gånger).

Antalet gånger en rot förekommer i faktoriseringen ovan kallas för rotens/nollställets **multiplicitet**.

[1] Bara negativa rötter måste kollas, varför?

10.2. Konjugerade rötter

Sats 118. *Om $p(x)$ är ett polynom med reella koefficienter och $\alpha \in \mathbb{C}$ är ett nollställe, så är även $\overline{\alpha}$ ett nollställe.*

Detta innebär att för polynom med reella koefficienter, så kommer icke-reella rötter i konjugerade par.

Bevis. Vi vet $p(\alpha) = 0$, $p(x) = a_n x^n + \cdots a_1 x + a_0$ Betrakta nu $\overline{p(\alpha)}$. Detta är ju å ena sidan noll, eftersom konjugatet av 0 är 0. Å andra sidan

$$\overline{p(\alpha)} = \overline{a_n \alpha^n + \cdots + a_1 \alpha + a_0}$$

men detta blir precis

$$a_n \overline{\alpha}^n + \cdots + a_1 \overline{\alpha} + a_0 = p(\overline{\alpha})$$

så $p(\overline{\alpha}) = 0$. □

Notera: En liknande metod fungerar för polynom med rationella koefficienter: Om $a + b\sqrt{d}$ är en rot, där d inte är en perfekt kvadrat, så måste $a - b\sqrt{d}$ också vara en rot. (Anledningen är att $\sqrt{d}$ inte är ett bråk, så vi måste ha två faktorer som "tar ut varandra".)

10.3. Irreducibla polynom, faktorisering över de reella talen

Sats 119. *Om ett polynom $p(x)$ har enbart reella koefficienter kan det faktoriseras i faktorer på formen $(x - \alpha)$ $\alpha \in \mathbb{R}$ samt $(x^2 - 2ax + (a^2 + b^2))$, med $a, b \in \mathbb{R}$. Detta motsvarar rötterna α samt $a \pm bi$.*

Bevis. För varje reell rot α så har vi en faktor $x - \alpha$ enligt tidigare satser. Nu, vi vet att om $a + bi$ är en rot, så är $a - bi$ också en rot till p. Alltså är

$$(x - a - bi)(x - a + ib) = x^2 - 2ax + (a^2 + b^2)$$

också en faktor. □

Alltså, alla polynom kan skrivas som produkt av linjära faktorer, med komplexa tal.

Polynom med *reella koefficienter* kan skrivas som produkt av linjära och kvadratiska faktorer, där de kvadratiska faktorerna saknar reella rötter.

Definition 120. Låt K vara någon av mängderna $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, och $\mathbb{C}$. Polynom med koefficienter i K som inte kan faktoriseras i mindre polynom[2] där faktorernas koefficienter också finns i K, kallas för **irreducibla över K**.

Som exempel, polynomet $x^2 - 2$ är irreducibelt över $\mathbb{Q}$, men är reducibelt över $\mathbb{R}$ där det kan faktoriseras som $(x - \sqrt{2})(x + \sqrt{2})$. Ett annat exempel, $x^4 + 2x^2 + 1 = (x^2 + 1)^2$ är reducibelt över $\mathbb{R}$, men kan faktoriseras ytterligare över $\mathbb{C}$.

Notera att alla polynom i $\mathbb{R}[x]$ med grad 3 eller mer är reducibla, och alla polynom av grad 2 eller mer i $\mathbb{C}[x]$ är reducibla. (Fundera på varför!)

Problem 121. Polynomet $p(x) = x^5 - 4x^4 + 8x^3 - 12x^2 + 12x - 8$ har $x = 1 + i$ som ett nollställe. Faktorisera polynomet i reella irreducibla faktorer.

[2] mindre grad

Lösning. Vi vet att $(x-1-i)(x-1+i) = x^2-2x+2$ är en (irreducibel) faktor. Vi använder nu polynomdivision och får att

$$p(x) = (x^2-2x+2)(x^3-2x^2+2x-4).$$

Rationella rotsatsen används för att leta rötter till (x^3-2x^2+2x-4). Då det är moniskt, kan bara heltalsrötter finnas. Vi testar med $x = \pm 1, \pm 2, \pm 4$. Vi får att $x = 2$ är en rot, så vi delar med $(x-2)$. Detta ger den slutliga faktoriseringen

$$p(x) = (x^2-2x+2)(x-2)(x^2+2),$$

då (x^2+2) saknar reella rötter.

Fundera på hur man kan *konstruera* problem av typen ovan.

10.4. Samband mellan rötter och koefficienter — Vietas formler

Vi vet att ett moniskt polynom $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ kan faktoriseras som $(x-\alpha_1)\cdots(x-\alpha_n)$. Utvecklar vi högerledet, får vi att

$$\begin{aligned} a_0 &= (-1)^n \alpha_1 \alpha_2 \cdots \alpha_n \\ a_1 &= (-1)^{n-1}\left(\alpha_2 \cdots \alpha_n + \alpha_1\alpha_3\cdots\alpha_n + \cdots + \alpha_1\alpha_2\cdots\alpha_{n-1}\right) \\ &\vdots \\ a_{n-1} &= -(\alpha_1 + \alpha_2 + \cdots + \alpha_n). \end{aligned}$$

Med andra ord, koefficienterna kan uttryckas i termer av rötterna.

Problem 122. Ekvationen $x^5 - 9x^4 + 31x^3 - 51x^2 + 40x - 12 = 0$ har 5 rötter. Fyra av rötterna har produkten 4. Vad är den sista roten?

Lösning. Vi vet att $\alpha_1 \cdots \alpha_5 = (-1)^5(-12) = 12$. Eftersom de fyra första rötterna har produkt 4, måste den sista roten vara 3.

Problem 123. Polynomet $x^3 - x^2 + 3x - 2$ har nollställen α, β, γ. Bestäm $\alpha^2 + \beta^2 + \gamma^2$.

Lösning. Vi vet

$$\alpha + \beta + \gamma = 1, \quad \alpha\beta + \alpha\gamma + \beta\gamma = 3, \qquad \alpha\beta\gamma = 2.$$

Vi vill tillverka uttrycket $\alpha^2 + \beta^2 + \gamma^2$. Kvadrerar vi $(\alpha + \beta + \gamma)$ får vi

$$(\alpha+\beta+\gamma)^2 = \alpha^2 + \beta^2 + \gamma^2 + 2(\alpha\beta + \alpha\gamma + \beta\gamma),$$

så

$$\alpha^2 + \beta^2 + \gamma^2 = (\alpha+\beta+\gamma)^2 - 2(\alpha\beta + \alpha\gamma + \beta\gamma) = 1^2 - 2\cdot 3 = -5.$$

Problem 124. Polynomet $x^{20} - 21x^{19} + \cdots - 39x + 2$ har enbart positiva heltal som nollställen. Bestäm alla rötter till polynomet samt faktorisera det.

Lösning. Enligt rationella rotsatsen, så kan enbart rötterna vara ± 1, ± 2, men det är givet att polynomet bara har positiva rötter. Vidare, produkten av alla rötter är 2 (vi ser det på konstanttermen) så exakt en rot är 2, alla andra är 1. Detta ger att polynomet måste vara $(x-1)^{19}(x-2)$.

Föreläsning 11
Summor, produkter och binomialsatsen

11.1. Summanotation

Summanotation fungerar ungefär som en **for-loop** i programmering. Den generella formeln är att

$$\sum_{k=a}^{b} f(k) \coloneqq f(a) + f(a+1) + \cdots + f(b-1) + f(b).$$

Exempel 125. Som exempel har vi att

$$\sum_{k=1}^{10} k = 1 + 2 + 3 + 4 + \cdots + 10,$$

och

$$\sum_{k=2}^{5} (k^2 + 1) = (2^2 + 1) + (3^2 + 1) + (4^2 + 1) + (5^2 + 1).$$

Notera speciellt,

$$\sum_{k=1}^{n} (a_k + b_k) = \sum_{k=1}^{n} a_k + \sum_{k=1}^{n} b_k \quad \text{och} \quad \sum_{k=1}^{n} C \cdot a_k = C \sum_{k=1}^{n} a_k.$$

Dessa egenskaper motsvarar räkneregler för integraler.

11.2. Produktnotation

På samma sätt definierar vi produktnotationen som

$$\prod_{k=a}^{b} f(k) \coloneqq f(a) \cdot f(a+1) \cdot \cdots \cdot f(b).$$

Som ett viktigt exempel har vi att $n! \coloneqq \prod_{k=1}^{n} k$. Ett annat exempel är

$$\prod_{k=2}^{5} (k^2 + 1) = (2^2 + 1) \cdot (3^2 + 1) \cdot (4^2 + 1) \cdot (5^2 + 1).$$

Exempel 126. Beräkna $\prod_{k=1}^{8} \frac{k+2}{k}$. Vi får

$$\frac{3}{1}\frac{4}{2}\frac{5}{3} \cdots \frac{8}{6}\frac{9}{7}\frac{10}{8} = \frac{9 \cdot 10}{1 \cdot 2} = 45.$$

Exempel 127. Att kunna hantera index i summor och produkter är viktigt. Till exempel kan man flytta index och skriva om uttrycket inuti summan, så att indexet börjar på 0, eller annan valfi startpunkt:

$$\sum_{k=a}^{b} f(k) = \sum_{k=0}^{b-a} f(a+k).$$

Man kan också plocka termer ur en summa (en eller flera av den första eller sista):

$$\sum_{k=0}^{100} f(k) = f(0) + \sum_{k=1}^{100} f(k) = f(100) + \sum_{k=0}^{99} f(k).$$

Det går också bra med mer komplicerade omskrivningar. Till exempel, fundera på varför vi har

$$\sum_{k=1}^{100} f(k) = \sum_{k=1}^{50} f(2k-1) + \sum_{k=1}^{50} f(2k).$$

11.3. Aritmetisk summa

En **aritmetisk talföljd** är tal,

$$a_1, \ldots, a_n$$

så att skillnaden mellan två på varandra följande tal är konstant. Till exempel är talföljden nedan aritmetisk:

$$2, 5, 8, 11, 14, 17.$$

Sats 128. *Om $a_1, \ldots, a_n$ är en aritmetisk talföljd, gäller det att dess summa är $n\frac{a_1+a_n}{2}$. Man tar helt enkelt antalet termer multiplicerat med deras medelvärde.*

Bevis. Antag att talföljden ges av $a_2 = a_1 + k$, $a_3 = a_1 + 2k$, och så vidare tills $a_n = a_1 + (n-1)k$. Om

$$S = a_1 + a_2 + a_3 + \cdots + a_n$$

gäller

$$2S = (a_1 + a_n) + (a_2 + a_{n-1}) + (a_3 + a_{n-2}) + \cdots + (a_n + a_1).$$

Men var och en av de n termerna till höger har värdet $(a_n + a_1)$, så

$$2S = n \cdot (a_n + a_1),$$

och vi är klara. □

Notera: Det är n tal i följden, kurskompendiet har en liten annan indexeringskonvention.

Problem 129 (Från tentan 2024-04-17)**.** Bestäm summan av alla tal i tabellen nedan:

$$\begin{array}{cccccc} 1 & 2 & 3 & 4 & \ldots & 20 \\ 2 & 4 & 6 & 8 & \ldots & 40 \\ 3 & 6 & 9 & 12 & \ldots & 60 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 20 & 40 & 60 & 80 & \ldots & 400. \end{array}$$

Varje rad och kolonn i tabellen utgör en aritmetisk talföljd.

Lösning. Rad nummer k i tabellen har summan $k(1+2+3+\cdots+20) = k \cdot 210$. Om vi summerar detta från rad $k = 1$ till rad $k = 20$ får vi

$$1 \cdot 210 + 2 \cdot 210 + \cdots + 20 \cdot 210 = 210(1 + 2 + 3 + \cdots + 20) = 210^2 = 44100.$$

11.4. Geometrisk summa

Geometrisk följd: I en **geometrisk följd** är kvoten på två varandra följande termer konstant. Ett exempel är

$$3, 6, 12, 24, 48, 96$$

som har den konstanta kvoten $r = 2$. En generell geometrisk summa (med $n + 1$ termer) är på formen

$$S = a + ar + ar^2 + \cdots + ar^n.$$

Notera att $rS = ar + ar^2 + \cdots + ar^n + ar^{n+1} = S + ar^{n+1} - a$. Löser vi ut S, får vi

$$(r-1)S = a\left(r^{n+1} - 1\right) \implies S = a \cdot \frac{r^{n+1} - 1}{r - 1} = a \cdot \frac{1 - r^{n+1}}{1 - r}.$$

där det sista steget bara kan göras om $r \neq 1$.

Exempel 130. Beräkna $\sum_{k=1}^{7}(3k + 1 + 2^k)$.

Vi delar upp det som

$$\sum_{k=1}^{7}(3k+1) + \sum_{k=1}^{7} 2^k.$$

Första summan är $7 \cdot \frac{4+22}{2} = 7 \cdot 13 = 91$, andra summan är geometrisk summa, med $a = 2$ och $r = 2$.

$$\sum_{k=1}^{7} 2^k = 2 \cdot \frac{2^7 - 1}{2 - 1} = 2(128 - 1) = 254.$$

Oändlig geometrisk summa. Kom ihåg att

$$\sum_{k=0}^{n} r^k = 1 + r + r^2 + \cdots + r^n = \frac{1 - r^{n+1}}{1 - r}.$$

Om $-1 < r < 1$, så blir r^{n+1} mindre och mindre då n växer, och kommer godtyckligt nära noll. Vi kan då säga att då $-1 < r < 1$ gäller

$$\sum_{k=0}^{\infty} r^k = \frac{1}{1 - r}.$$

Problem 131. Låt $z = 1 + i$ och bestäm $1 + z + z^2 + z^3 + \cdots + z^{19}$.

Lösning. Det är geometrisk serie—kolla att beviset även funkar för komplexa tal—vars summa blir $\frac{z^{20}-1}{z-1}$. Först, $z^{20} = \sqrt{2}^{20} e^{5\pi i} = -1024$. Svaret blir då

$$\frac{-1024 - 1}{1 + i - 1} = \frac{-1025}{i} = 1025i$$

Problem 132 (Från 2024-10-25)**.** Låt $z = 1 + i \in \mathbb{C}$ och beräkna summan

$$\sum_{k=0}^{16} \left(\frac{z}{\sqrt{2}}\right)^k.$$

Lösning. Formeln för geometrisk summa ger oss att summan är $\frac{(z/\sqrt{2})^{17}-1}{z/\sqrt{2}-1}$. Om $z = 1 + i$ så är $z/\sqrt{2} = e^{i\pi/4}$. Alltså är summan

$$\frac{(e^{i\pi/4})^{17} - 1}{e^{i\pi/4} - 1} = \frac{e^{i\pi/4}(e^{i\pi/4})^{16} - 1}{e^{i\pi/4} - 1}.$$

Eftersom $(e^{i\pi/4})^{16} = 1$, så är täljare och nämnare lika, så summans värde är 1.

Problem 133. På varje heltalspunkt (x, y) med $x, y \geq 0$ placeras ett mynt med värde $\frac{1}{2^{x+y}}$.

(a) Vad är det totala värdet av alla sådana mynt?

(b) Använd resultatet i (a) för att motivera identiteten

$$\sum_{x=0}^{\infty}\sum_{y=0}^{\infty} 2^{-x-y} = \sum_{n=0}^{\infty}(n+1)\cdot 2^{-n}.$$

Tips: Rita ut mynten med deras värden för $0 \leq x, y \leq 4$. Formeln $1 + r + r^2 + r^3 + \cdots = \frac{1}{1-r}$ för $|r| < 1$ får användas.

Lösning. (a) Myntet på koordinat (x, y) har värdet 2^{-x-y} så totala summan är

$$\sum_{x=0}^{\infty}\sum_{y=0}^{\infty} 2^{-x-y} = \sum_{x=0}^{\infty} 2^{-x} \sum_{y=0}^{\infty} \left(\frac{1}{2}\right)^{y}.$$

Den inre summan är en oändlig geometrisk summa, vars värde blir $\frac{1}{1-1/2} = 2$. Det återstår att beräkna

$$2 \cdot \sum_{x=0}^{\infty} 2^{-x} = 2 \cdot 2 = 4$$

då vi har samma summa igen. Totala värdet är alltså 4.

(b) Om vi tittar på antalet icke-negativa heltalskoordinater (x, y) med $x + y = n$, så finns det $n+1$ sådana punkter. Vi kan alltså summera över alla (x, y) diagonal för diagonal. De $(n+1)$ mynten på diagonalen med koordinatsumma n har alla värdet 2^{-n}. Alltså måste vi ha att

$$\sum_{x=0}^{\infty}\sum_{y=0}^{\infty} 2^{-x-y} = \sum_{n=0}^{\infty}(n+1)\cdot 2^{-n},$$

eftersom båda sidor är samma summa; den i högerledet har grupperat koordinater enligt diagonaler.

11.5. Binomialsatsen

Sats 134. *Vi har att*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k},$$

där

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

kallas för ***binomialkoefficienter****.*

Man kan beräkna binomialkoefficienterna via Pascals triangel. Varför detta är möjligt ska vi visa senare på kombinatorikföreläsningen.

Problem 135. Bestäm koefficienten för x^8 i $(2x^4 + x^{-1})^7$.

Lösning. Binomialsatsen ger

$$(2x^4 + x^{-1})^7 = \sum_{k=0}^{7} \binom{7}{k} (2x^4)^k (x^{-1})^{7-k} = \sum_{k=0}^{7} \binom{7}{k} 2^k x^{4k} x^{k-7} = \sum_{k=0}^{7} \binom{7}{k} 2^k x^{5k-7}.$$

Måste välja $5k - 7 = 8$, så $5k = 15$, så $k = 3$. Denna term är

$$\binom{7}{3} 2^3 = 8 \cdot \frac{7 \cdot 6 \cdot 5}{3!} = 8 \cdot 35 = 240 + 40 = 280.$$

Problem 136 (Från 2024-11-20)**.** Bestäm koefficienten för z^9 i polynomet $\left(\frac{1}{16} + (1 + i\sqrt{3})z\right)^{12}$.

Lösning. Enligt binomialsatsen har vi att

$$\left(\frac{1}{16} + (1 + i\sqrt{3})z\right)^{12} = \sum_{k=0}^{12} \binom{12}{k} 16^{-(12-k)} (1 + i\sqrt{3})^k z^k,$$

och vi söker koefficienten som motsvarar $k = 9$. Genom att skriva om $1 + i\sqrt{3}$ på polär form, får vi att koefficienten som sökes är

$$\binom{12}{9} 16^{-3} \left(2 \cdot e^{\pi i/3}\right)^9 = \frac{12 \cdot 11 \cdot 10}{3 \cdot 2 \cdot 1} \cdot \frac{2^9}{2^{12}} \cdot e^{3\pi i} = -\frac{55}{2}.$$

Problem 137 (Från 2025-03-12)**.** Bestäm koefficienten för x^8 i uttrycket $\left(2x^2 + \frac{1}{x}\right)^{10}$. Svaret ska anges som en produkt av heltal.

Lösning. Binomialsatsen ger att

$$\left(2x^2 + \frac{1}{x}\right)^{10} = \sum_{k=0}^{10} \binom{10}{k} (2x^2)^k \cdot x^{-(10-k)} = \sum_{k=0}^{10} 2^k \binom{10}{k} x^{3k-10}.$$

Vi söker den term som motsvarar $k = 6$, så svaret är $2^6 \binom{10}{6} = 64 \cdot \frac{10 \cdot 9 \cdot 8 \cdot 7}{24} = 64 \cdot 30 \cdot 7$.

Exempel 138. Mathematica har kommandon för binomialkoefficienter, summor och produkter:

```
Binomial[10, 3]
Expand[(a + b)^5]
Sum[k^2 + k, {k, 1, n}]
Product[(k + 2)/k, {k, 1, 8}]
```

Exempel 139. Mathematica kan ibland ge slutna formler för oändliga summor. Med alternativet `GenerateConditions` får man också villkoren för konvergens:

```
Sum[(2 - x)^k + x^2 (2/x)^(2 k), {k, 0, Infinity},
    GenerateConditions -> True]
```

För reella x konvergerar summan när $2 < x < 3$.

Föreläsning 12
Induktion

12.1. Summor, produkter och olikheter

Problem 140. Visa att om $n \geq 1$, gäller det att

$$\text{(a) } \sum_{k=1}^{n} k = \frac{n(n+1)}{2} \qquad \text{(b) } \sum_{k=1}^{n}(2k-1) = n^2.$$

Lösning. (a): Först kontrollerar vi basfallet, $n = 1$. Summan är 1 och formeln ger också 1, så vi är klara med basfallet.
Induktionsantagande: Antag att för något $n \geq 1$ har vi

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$$

Vi lägger till $(n+1)$ på båda sidor av denna relation och får

$$\sum_{k=1}^{n+1} k = (n+1) + \frac{n(n+1)}{2}.$$

Högerledet kan nu skrivas om som

$$\sum_{k=1}^{n+1} k = \frac{[n+1]([n+1]+1)}{2}.$$

Således har vi bevisat att om formeln gäller för n, gäller den också för $n+1$. Enligt principen för matematisk induktion är identiteten sann för alla heltal $n \geq 1$.

(b): Först kontrollerar vi basfallet, $n = 1$. Båda sidorna har värdet 1, så basfallet är klart.
Induktionsantagande: Antag att för något $n \geq 1$ har vi

$$\sum_{k=1}^{n}(2k-1) = n^2.$$

Vi lägger till $2(n+1) - 1$ på båda sidor av denna relation och får

$$\sum_{k=1}^{n+1}(2k-1) = 2(n+1) - 1 + n^2.$$

Högerledet kan nu skrivas om som

$$\sum_{k=1}^{n+1}(2k-1) = [n+1]^2.$$

Således har vi bevisat att om formeln gäller för n, gäller den också för $n+1$. Enligt principen för matematisk induktion är identiteten sann för alla heltal $n \geq 1$.

Problem 141. *Formel för geometrisk summa.* Visa att om $r \neq 1$ gäller det att

$$\sum_{j=0}^{n} r^j = \frac{r^{n+1}-1}{r-1}.$$

Lösning. Basfallet $n = 0$: Vänsterledet är bara $r^0 = 1$. Högerledet är också $\frac{r-1}{r-1} = 1$. Antag nu att formeln gäller för ett visst värde av n. Vi vill bevisa att

$$\sum_{j=0}^{n+1} r^j = \frac{r^{n+2}-1}{r-1}.$$

Detta är ekvivalent med att bevisa

$$r^{n+1} + \sum_{j=0}^{n} r^j = \frac{r^{n+2}-1}{r-1},$$

och genom att använda induktionsantagandet kan summan i vänsterledet uttryckas med hjälp av formeln. Således behöver vi bevisa

$$r^{n+1} + \frac{r^{n+1}-1}{r-1} = \frac{r^{n+2}-1}{r-1}.$$

Genom att multiplicera båda sidor med $r-1$ får vi

$$(r-1)r^{n+1} + r^{n+1} - 1 = r^{n+2} - 1,$$

vilket lätt ses vara sant. Därmed gäller formeln ovan för alla $n \geq 0$.

Problem 142. Bevisa att

$$\prod_{j=1}^{n}\left(1+\frac{1}{j^2}\right) \leq n+1.$$

Lösning. Olikheten är sann för $n = 1$, eftersom vi får $3/2 < 2$. Antag att olikheten är sann för något $n \geq 1$. Multiplicera båda sidorna i induktionsantagandet med $1 + (n+1)^{-2}$:

$$\prod_{j=1}^{n+1}\left(1+\frac{1}{j^2}\right) \leq (n+1)(1+(n+1)^{-2}).$$

Utvecklar vi högerledet får vi att

$$\prod_{j=1}^{n+1}\left(1+\frac{1}{j^2}\right) \leq (n+1) + \frac{1}{n+1}.$$

Nu, eftersom $\frac{1}{n+1} < 1$ kan vi dra slutsatsen att högerledet är mindre än $n+2$. Alltså har vi att

$$\prod_{j=1}^{n+1}\left(1+\frac{1}{j^2}\right) < n+2$$

och vi är klara.

Exempel 143. Man kan använda Mathematica för att hitta slutna formler som sedan kan bevisas med induktion:

```
Sum[k, {k, 1, n}]
Sum[2 k - 1, {k, 1, n}]
Sum[k^2 + k, {k, 1, n}]
Sum[k^3, {k, 1, n}]
```

Prova gärna att ändra uttrycket i summan och formulera en egen induktionsuppgift.

12.2. Rekursion

Problem 144. Låt $a_0 = 0$ och $a_n = 2a_{n-1} + n$ för $n \geq 1$. Visa att $a_n = 2^{n+1} - n - 2$.

Lösning. Basfall: För $n = 0$ är $a_0 = 2^{0+1} - 0 - 2 = 2 - 0 - 2 = 0$, vilket stämmer överens med definitionen av a_0.
Induktionsantagande: Antag att $a_k = 2^{k+1} - k - 2$ för något $k \geq 0$. Vi ska visa att detta implicerar att $a_{k+1} = 2^{(k+1)+1} - (k+1) - 2$. Enligt definitionen har vi att

$$\begin{aligned} a_{k+1} &= 2a_k + (k+1) \\ &= 2(2^{k+1} - k - 2) + (k+1) \quad \text{(enligt induktionsantagandet)} \\ &= 2^{k+2} - 2k - 4 + k + 1 \\ &= 2^{k+2} - k - 3 \\ &= 2^{(k+1)+1} - (k+1) - 2. \end{aligned}$$

Detta visar att a_{k+1} är lika med $2^{(k+1)+1} - (k+1) - 2$, vilket slutför induktionssteget.
Enligt principen för matematisk induktion gäller därför att $a_n = 2^{n+1} - n - 2$ för alla $n \geq 0$.

Problem 145. Låt $a_1 = 4$, $a_2 = 16$ och $a_n = 6a_{n-1} - 8a_{n-2}$ för $n \geq 3$. Visa att $a_n = 4^n$ för alla $n \geq 1$.

Lösning. **Basfall:** För $n = 1$ och $n = 2$ så gäller den slutna formeln.
Induktionsantagande: Antag att

$$a_{n-2} = 4^{n-2}, \quad a_{n-1} = 4^{n-1}$$

för något fixt värde på n.
Vi vill nu visa att $a_n = 4^n$. Från rekursionen har vi att

$$a_n = 6a_{n-1} - 8a_{n-2}.$$

Genom att använda induktionsantagandet får vi

$$\begin{aligned} a_n &= 6(4^{n-1}) - 8(4^{n-2}) \\ &= 4^{n-2}(6 \cdot 4 - 8) \\ &= 4^{n-2}4^2 \\ &= 4^n. \end{aligned}$$

Därmed har vi visat att om den slutna formeln gäller för $n-1$ och $n-2$, så gäller den slutna formeln för n också. Tillsammans med de två basfallen kan vi då dra slutsatsen att $a_n = 4^n$ för alla $n \geq 1$.

Problem 146. Låt $a_1 = 1$ och $a_2 = 8$ och $a_n = a_{n-1} + 2a_{n-2}$ när $n \geq 3$. Visa att $a_n = 3 \cdot 2^{n-1} + 2(-1)^n$ för alla $n \geq 1$.

Lösning. Detta bevis kräver två basfall. Formeln säger oss att $a_1 = 3 \cdot 2^0 + 2(-1) = 1$ och $a_2 = 3 \cdot 2^1 + 2 = 8$, vilket överensstämmer med definitionen av a_1 och a_2. Så vi har två basfall.

Induktionsantagande: Antag nu att

$$a_{n-1} = 3 \cdot 2^{(n-1)-1} + 2(-1)^{n-1} \text{ och } a_{n-2} = 3 \cdot 2^{(n-2)-1} + 2(-1)^{n-2}.$$

Med dessa två likheter tillsammans med rekursionen, kan vi dra slutsatsen att

$$a_n = \left(3 \cdot 2^{(n-1)-1} + 2(-1)^{n-1}\right) + 2\left(3 \cdot 2^{(n-2)-1} + 2(-1)^{n-2}\right).$$

Det är nu en fråga om algebra att se att högerledet kan omformuleras till $3 \cdot 2^{n-1} + 2(-1)^n$, och vi är klara.

Problem 147. Låt $a_0 = 0$ och $a_{n+1} = \sqrt{2a_n + 3}$ när $n \geq 0$. Visa att $0 \leq a_n \leq 3$.

Lösning. Basfall: För $n = 0$ har vi $a_0 = 0$, vilket uppfyller olikheten $0 \leq a_0 \leq 3$.

Induktionsantagande: Anta att olikheten gäller för något $k \geq 0$, dvs $0 \leq a_k \leq 3$. Vi vill visa att olikheten också gäller för $k + 1$.

Vi har $a_{k+1} = \sqrt{2a_k + 3}$, och eftersom $a_k \geq 0$ ser vi direkt att $a_{k+1} \geq 0$. Vi har också att

$$a_k \leq 3 \implies 2a_k \leq 6 \implies 2a_k + 3 \leq 9 \implies \sqrt{2a_k + 3} \leq 3.$$

Alltså gäller det att $a_{k+1} \leq 3$. Genom induktion gäller olikheten $0 \leq a_n \leq 3$ för alla $n \geq 0$.

Problem 148. Visa att för Fibonaccitalen gäller det att $\text{SGD}(f_{n+1}, f_n) = 1$. Fibonaccitalen är definierade av att $f_1 = 1$, $f_2 = 1$ samt rekursionen $f_n = f_{n-1} + f_{n-2}$.

Lösning. Först kontrollerar vi att $\text{SGD}(f_1, f_2) = 1$, vilket är sant. Sedan, genom att använda att $\text{SGD}(a + b, b) = \text{SGD}(a, b)$ (som bevisats tidigare) har vi att

$$\text{SGD}(f_{n+1}, f_n) = \text{SGD}(f_n + f_{n-1}, f_n) = \text{SGD}(f_{n-1}, f_n)$$

och det sista uttrycket är 1 genom induktionsantagandet.

Vill man förstå detta bevis ytterligare, så rekommenderas man att beräkna de första 10 Fibonaccitalen samt $\text{SGD}(89, 55)$ med hjälp av Euklides algoritm.

12.3. Delbarhet och talteori

Problem 149. Visa att 3^{n+1} delar $2^{3^n} + 1$.

Lösning. Basfallet $n = 0$ är klart. Antag nu att 3^{n+1} delar $2^{3^n} + 1$ för något $n \geq 0$. Detta innebär att $2^{3^n} + 1 = m3^{n+1}$ för något m (som beror på n), och $2^{3^n} = m3^{n+1} - 1$. Nu är nästa steg

$$\begin{aligned}
2^{3^{n+1}} + 1 &= \left(2^{3^n}\right)^3 + 1 \\
&= \left(m3^{n+1} - 1\right)^3 + 1 \\
&= \left(m3^{n+1}\right)^3 - 3\left(m \cdot 3^{n+1}\right)^2 + 3m \cdot 3^{n+1} - 1 + 1 \\
&= m^3 3^{3(n+1)} - 3m^2 \cdot 3^{2(n+1)} + m3^{n+2} \\
&= 3^{n+2}\left(m^3 3^{2n+1} - 3m^2 \cdot 3^n + m\right),
\end{aligned}$$

och detta är nu en multipel av 3^{n+2}.

12.4. Konstruktioner

Problem 150. Visa att varje heltal $n \geq 8$ kan uttryckas som $n = 3k + 5m$ för några heltal $k, m \geq 0$.

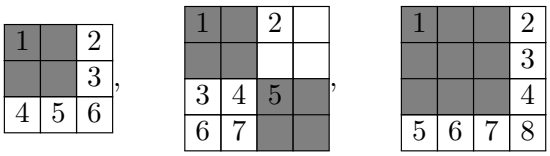
Lösning. Antag att $n > 8$. Vårt induktionsantagande är att vi har ett sådant uttryck för $n - 1$. Det finns två fall att undersöka:

- antingen har $n - 1$ en 5:a i representationen, i så fall tar vi bort den och lägger till två 3:or, vilket ger en giltig representation för n, eller
- $n - 1$ har endast 3:or i representationen. Eftersom $n > 8$ är antalet 3or då minst tre, så kan vi ta bort tre av dem och istället lägga till två 5:or. Detta ger en giltig representation av n.

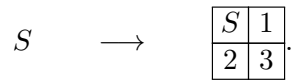
Alternativt kan man visa att påståendet är sant för $n = 8$, $n = 9$ samt $n = 10$. Dessa utgör basfall. Därefter noterar man att om påståendet gäller för n, så gäller det för $n + 3$ då vi till representationen för n kan lägga till en ytterligare 3:a.

Problem 151. Bevisa att vilken kvadrat som helst[1] kan delas upp i ett godtyckligt antal n mindre kvadrater, för varje $n \geq 6$.

Lösning. Vi måste visa att för vilket $n \geq 6$ som helst finns det en kvadrat som är uppdelad i n delkvadrater.
Våra basfall är följande: Det finns kvadrater uppdelade i $n = 6$, $n = 7$ och $n = 8$ delkvadrater:



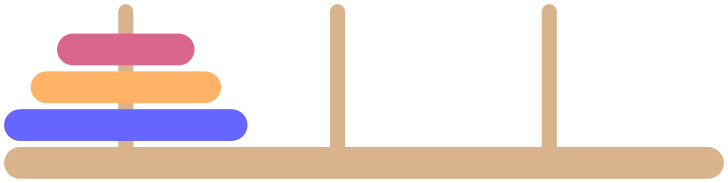
Antag nu att $n > 8$ och att vi kan konstruera en kvadrat S med $(n - 3)$ delkvadrater. Vi kan sedan konstruera en kvadrat med n delkvadrater på följande sätt. Ta S och lägg till tre ytterligare kvadrater av samma storlek, så bildas en större kvadrat:



Detta bevisar att varje antal > 5 delkvadrater kan erhållas—från det första basfallet kan vi erhålla talen $6, 9, 12, 15, \ldots$. Det andra basfallet ger $7, 10, 13, 16, \ldots$ och det sista basfallet ger $8, 11, 14, 17, \ldots$ Dessa sekvenser täcker alla heltal större än 5.

Problem 152. **Tornen i Hanoi** är ett klassiskt problem. Det finns tre pelare, A, B, C, där n guldplattor[2] är placerade på pelare A. Guldplattorna är av olika storlek, där en större platta aldrig ligger ovanpå en mindre, så som i Figur 12.1. Målet är att flytta guldplattorna från en pelare till en annan—alltid en platta i taget—tills att alla guldplattor befinner sig på pelare C. Visa att detta kan göras med $2^n - 1$ drag.

[1] En kub kan delas upp i vilket antal kuber som helst ≥ 47. För hyperkuber är detta fortfarande ett olöst problem, se `https://arxiv.org/pdf/1910.06206.pdf`.
[2] I den klassiska berättelsen är $n = 64$.



Figur 12.1: Tornen i början av proceduren, för $n = 3$.

Lösning. Om $n = 1$ finns det bara en platta, och denna flyttas helt enkelt ett steg. Detta kräver ett drag. Notera att det är egentligen ingen skillnad på pelare B och pelare C. Om hela stapeln med plattor kan flyttas från A till C, så finns en motsvarande serie drag som fungerar för att flytta hela stapeln från A till B. Vi använder nu induktion, och antar att vi kan flytta en stapel med $n-1$ plattor från en pelare till en annan, användandes $2^{n-1}-1$ drag. För att nu flytta n plattor från A till C, använd induktionsantagandet för att flytta de översta $n-1$ plattorna till pelare B, därefter flytta den största plattan från A till C. Slutligen flyttas nu de återstående $n-1$ plattorna från B till C, igen med induktionsantagandet. Totalt har vi använt

$$(2^{n-1}-1)+1+(2^{n-1}-1) = 2^n - 1$$

drag, vilket visar att formeln även fungerar för n plattor.

Problem 153. Visa att för varje heltal $n \geq 3$ kan vi hitta positiva heltal $a_1, \ldots, a_n$ så att

$$n = \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n}.$$

Problem 154. Visa att om x är ett reellt tal så att $x + x^{-1} \in \mathbb{Z}$, så gäller det att $x^n + x^{-n} \in \mathbb{Z}$ för alla $n \geq 0$.

12.5. Analys

Problem 155. Visa att för alla $n \geq 0$ har vi

$$\int_0^\infty x^n e^{-x} dx = n!.$$

Lösning. Basfallet $n = 0$ är $\int_0^\infty e^{-x}dx = [-e^{-x}]_0^\infty = 1$, vilket överensstämmer med $0!$.
Anta nu att $\int_0^\infty x^n e^{-x}dx = n!$. Vi har att för $n \geq 1$, så

$$\begin{aligned}
\int_0^\infty x^{n+1}e^{-x}dx &= \text{(Genom partiell integration)} \\
&= \left[x^{n+1}(-e^{-x})\right]_0^\infty - \int_0^\infty (n+1)x^n(-e^{-x})dx \\
&= 0 + (n+1)\int_0^\infty x^n e^{-x}dx \\
&= 0 + (n+1)n!
\end{aligned}$$

där vi i det sista steget använde induktionsantagandet. Eftersom $(n+1)! = (n+1)n!$, är vi klara.

Föreläsning 13
Kombinatorik

13.1. Oberoende val och multiplikationsprincipen

Om vi har två oberoende val (val där resultatet av första valet inte påverkar det andra) så multipliceras antalen ihop.

Exempel 156. Hur många ord kan bildas av bokstäverna ABCD av längd 5, där samma bokstav får förekomma flera gånger?

13.1.1. Ordnat urval och permutationer

Antal sätt att ordna (olika) bokstäver till ett ord utan repetition.
Att placera n personer i ett led kan göras på $n!$.

13.1.2. Oordnat urval, delmängder, binomialkoefficienter

Binomialkoefficienten på återseende.

Sats 157. *Antalet sätt att bland n personer välja en grupp av k personer ges av*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Bevis. Vi ställer de n personerna på led. Det finns $n!$ sådana sätt. De k första utgör gruppen. Dock dubbelräknar vi—varje val av omkastning av de k första personerna resulterar i samma val. På samma sätt får vi samma val om vi sorterar om de $n-k$ sista personerna. □

Kopplingen mellan Pascals triangel och binomialkoefficienter följer av följande identiteter:

- $\binom{n}{0} = \binom{n}{n} = 1$
- $\binom{n}{k} = \binom{n}{n-k}$
- $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ (ett element markerat, med eller inte).

Exempel 158. Hur många binära ord av längd 8 finns det med exakt tre stycken ettor?

Lösning. Det ges av $\binom{8}{3}$ då vi bland 8 positioner ska välja 3.

Sats 159. *Om man har $n = k_1 + k_2 + k_3 + \cdots + k_\ell$ bokstäver totalt, k_1 stycken* `A`*, k_2 stycken* `B` *och så vidare, så kan man totalt bilda*

$$\frac{n!}{k_1!k_2!\cdots k_\ell!}$$

antal ord av dessa.

Detta är samma som om vi har n personer, som ska delas upp i grupper av storlek k_1, k_2, k_3 och så vidare, där grupperna har namn—Grupp A, Grupp B, Grupp C, etc.

13.2. Kombinatoriska uträkningar

Problem 160. Hur många olika ord kan skapas genom att omarrangera bokstäverna i `KÖKKENMÖDDING`[1]?

Lösning. Det finns 3 stycken `K`, 2 stycken `Ö`, 2 stycken `N`, 2 stycken `D` och 13 bokstäver totalt. Antal ord som kan bildas är då $\frac{13!}{3!2!2!2!}$.

Problem 161. Du skapar en 4-siffrig PIN-kod. Hur många valmöjligheter finns det i följande fall?

(a) Utan begränsning.

(b) Ingen siffra upprepas.

(c) Ingen siffra upprepas, tredje siffran är 0.

(d) Ingen siffra upprepas, och de måste förekomma i stigande ordning.

(e) Ingen siffra upprepas, och 2 och 5 måste vara med.

Lösning. (a) Det finns 4 oberoende val, så 10^4.

(b) $10 \cdot 9 \cdot 8 \cdot 7$.

(c) Välj de återstående tre: $9 \cdot 8 \cdot 7$.

(d) $\binom{10}{4}$.

(e) Välj två ytterligare siffror[2] och räkna alla permutationer: $\binom{8}{2} \times 4!$.

Problem 162. På hur många sätt kan 8 personer skapa 4 par?

Lösning. Det är lättare att betrakta paren som märkta. Vi väljer först 2 personer för att bilda par A, sedan 2 andra personer för att bilda par B och så vidare. Antalet sätt att skapa *märkta* par är

$$\frac{8!}{2!2!2!2!} = \frac{8!}{2^4}.$$

Dock producerar alla permutationer av de 4 par-namnen (ABCD) samma uppsättning par, så vi måste dela resultatet med 4!. Svaret är därför $\frac{8!}{4! \times 2^4}$.

[1] En kökkenmödding är en avfallshög från den senare delen av äldre stenåldern

[2] Dessa måste väljas på ett oordnat sätt, eftersom vi senare räknar alla 4! permutationer av de oordnade siffrorna.

Problem 163. Hur många ord kan du skapa av längd 6, från bokstäverna `a`, `b`, `c` och `d` om

- du måste inkludera varje bokstav minst en gång, och
- `a` måste förekomma exakt en gång.

Lösning. Vi behöver bara bestämma vilka två ytterligare bokstäver som ska läggas till i `abcd`.

- De två tillagda bokstäverna är olika. Därmed är bokstäverna en av `abbccd`, `abbcdd` eller `abccdd`. För att beräkna antalet ord vi kan göra från `abbccd`, använder vi en multinomialkoefficient, $\frac{6!}{2!2!1!1!}$.
- Vi lägger till samma bokstav två gånger. Detta ger `abbbcd`, `abcccd` eller `abcddd`, och varje av dessa alternativ ger $\frac{6!}{3!1!1!1!}$ ord.

Genom att summera allt, finns det totalt

$$3\frac{6!}{(2!)^2} + 3\frac{6!}{3!}$$

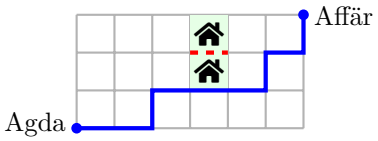
ord som uppfyller kraven.

Exempel 164. Samma problem kan modelleras direkt i Mathematica genom att först skapa alla ord och sedan filtrera:

```
words = Tuples[{"a", "b", "c", "d"}, 6];
good = Select[words,
  Count[#, "a"] == 1 && ContainsAll[#, {"a", "b", "c", "d"}] &
];
Length[good]
```

Detta är inte den effektivaste metoden, men den ligger nära problemformuleringen.

Problem 165 (Från 2025-08-12)**.** Agda bor i ett kvarter i ett rutnät med gator. Hon vill promenera från sitt hem till affären, genom att gå tre sträckor norrut och sex sträckor österut. Hon måste alltså gå 9 sträckor totalt. I figuren är en sådan promenad markerad.



(a) Hur många olika promenader totalt kan Agda gå, med tre sträckor norr och sex sträckor öster?

(b) Ester och Gerd är grannar med en gemensam gata. Agda vill inte promenera på just denna sträcka mellan husen eftersom då Esters pudel har för vana att skälla så förfärligt om hon går där. På hur många sätt kan Agda ta sig till affären utan att gå mellan de två husen i figuren?

Lösning. (a) Agda ska gå 9 sträckor, och tre av dessa ska vara i nordlig riktning. Detta ger totalt $\binom{9}{3} = 84$ olika promenader.

(b) Först räknar vi ut antalet promenader som passerar Ester och Gerds hus. En sådan promenad består av tre delar:

- 5 sträckor (2 norr, 3 öster),
- en sträcka österut, mellan husen,
- 3 sträckor (1 norr, 2 öster).

Första delen kan väljas på $\binom{5}{2} = 10$ sätt och den sista delen har $\binom{3}{1} = 3$ sätt. Totalt finns då 30 promenader som passerar den arga pudeln. Vi kan då konstatera att Agda har $84-30 = 54$ pudelfria promenader att välja bland.

Problem 166 (Från 2024-04-17)**.** *I denna fråga ska samtliga svar anges som heltal eller produkter av heltal. Inget svar är större än 1500. Alla svar ska motiveras.*

Vi har sju personer. Tre av dessa ska få en rolig hatt. Fyra av dessa ska få en rolig halsduk. Samma person kan få både hatt och halsduk och det är ingen skillnad på hattarna, och ingen skillnad på halsdukarna.

(a) På hur många sätt kan de tre personerna med rolig hatt utses?

(b) På hur många sätt kan både hattar och halsdukar fördelas?

(c) Om exakt två personer ska få både hatt och halsduk när accessoarerna fördelas, på hur många sätt kan då alla hattar och halsdukar fördelas?

Lösning. (a) Bland de 7 ska tre hatt-personer väljas: $\binom{7}{3} = \frac{7\cdot 6\cdot 5}{3!} = 35$ sätt.

(b) Vi delar ut halsdukarna oberoende av hatt-utdelningen, så multiplikationsprincipen ger $\binom{7}{3}\binom{7}{4} = 35^2 = 1225$ antal sätt.

(c) Vi väljer först 2 personer som får båda accessoarerna: $\binom{7}{2} = 21$ sätt. Bland de 5 som är kvar, ska en till få hatt, vilket går på $\binom{5}{1} = 5$ sätt. Slutligen ska två av de 4 kvarvarande personerna få halsdukar, och det finns $\binom{4}{2} = 6$ val för dessa. Eftersom antalet val vid varje steg är oberoende av valen dessförinnan, så finns det enligt multiplikationsprincipen totalt $21 \cdot 5 \cdot 6 = 630$ olika sätt.

13.3. Blandade problem

Problem 167. Du har 8 personer tillgängliga. Beräkna antalet sätt

(a) att välja 6 av dem och ordna dem i en kö.

(b) att välja 6 av dem och placera dem i köer som heter A och B, med 3 personer i varje.

(c) att välja 6 av dem och placera dem i två lika stora köer.

(d) att välja 6 av dem för att bilda en grupp.

(e) att välja 6 av dem och placera dem i grupper som heter A och B, med 3 i varje.

(f) att välja 6 av dem och bilda två lika stora grupper.

(g) att välja 6 av dem och bilda tre lika stora grupper.

Lösning. (a) Det finns $8 \times 7 \times \cdots \times 3$ sätt.

(b) Det finns $(8 \times 7 \times 6) \times (5 \times 4 \times 3)$ sätt.

(c) Det finns $\frac{1}{2}(8 \times 7 \times \cdots \times 3)$ sätt, eftersom två par av köer (abc, def) och (def, abc) betraktas som lika konfigurationer.

(d) Det finns $\binom{8}{6}$ sätt.

(e) Vi väljer först 6 personer och väljer sedan 3 av dem att vara i grupp A: $\binom{8}{6}\binom{6}{3}$ sätt.

(f) Det finns $\frac{1}{2}\binom{8}{6}\binom{6}{3}$ sätt.

(g) Det finns $\binom{8}{6}\frac{1}{3!}\frac{6!}{2!2!2!}$ sätt.

Problem 168. Du har 8 röda bollar tillgängliga[3]. Beräkna antalet sätt

(a) att välja 6 av dem och ordna dem i en rad.

(b) att välja 6 av dem för att bilda en grupp.

(c) att välja 6 av dem och ge dem till tre personer, några kanske inte får några. (Överkurs)

(d) att välja 6 av dem och ge dem till tre personer, varje person får åtminstone en. (Överkurs)

(e) att välja 6 av dem och bilda tre icke-tomma grupper.

(f) att välja 6 av dem och dela upp dem i högar.

Lösning. (a) Det finns endast ett sätt.

(b) Det finns endast ett sätt.

(c) Det finns $\binom{6+2}{2}$ sätt.

(d) Det finns $\binom{3+2}{2}$ sätt.

(e) Detta är detsamma som att räkna heltalspartitioner av 6 i 3 delar. Vi får tre sätt, $4+1+1$, $3+2+1$ och $2+2+2$.

(f) Samma som föregående fråga, men vi kan ha så många högar som vi vill. Vi får 11 sätt,

6	5+1	4+2	3+3
4+1+1	3+2+1	2+2+2	3+1+1+1
2+2+1+1	2+1+1+1+1	1+1+1+1+1+1.	

13.4. Kombinatoriska resonemang

Kombinatoriska bevis behöver inte innehålla beräkningar, utan man kan bevisa identiteter genom att tolka båda sidor av en identitet, och konstatera att de "berättar" samma historia.

Problem 169 (Lite svårare variant av problem från tentan 2023-05-10)**.** Visa att om $1 \leq k \leq n$, då är $k\binom{n}{k} = n\binom{n-1}{k-1}$. Använd antingen ett kombinatoriskt argument eller algebraisk manipulation.

[3]Dessa är identiska!

Lösning. **På vänster sida** väljer vi en grupp av k personer bland n personer, och i denna grupp ger vi en av personerna ett äpple.

På höger sida ger vi först ett äpple till en av de n personerna. Bland de återstående $n-1$ personerna väljer vi ytterligare $k-1$ personer, som ansluter sig till äpple-personen för att bilda en grupp med totalt k personer.

Båda sidor räknar därför antalet sätt att välja k personer bland n personer och sedan säkerställa att en av de k valda har ett äpple.

Problem 170. Bevisa att

$$\binom{n+2}{k} = \binom{n}{k} + 2\binom{n}{k-1} + \binom{n}{k-2}.$$

Lösning. Det finns åtminstone tre möjliga tillvägagångssätt. Ett rent algebraiskt bevis, genom att manipulera uttryck med fakulteter. En andra metod är att använda induktion över n, med hjälp av $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$.

Den tredje lösningen är att använda ett kombinatoriskt argument: På vänster sida har vi $n+2$ personer, n studenter och lärarna Svante och Per. Vi väljer k bland dessa. På höger sida överväger vi de möjliga val där det inte finns några lärare bland de k valda, exakt en lärare, eller båda lärarna närvarande.

Problem 171 (Ett svårare exempel)**.** Bevisa att

$$2n \cdot 3^{n-1} = \sum_{k=1}^{n} k \cdot 2^k \binom{n}{k}.$$

Lösning. **Vänster sida.** Det finns n personer på en restaurang som väljer bland tre viner, A, B och C, där B och C är alkoholfria. En person väljs dessutom till förare och har därför bara två vin-alternativ. Därför är tolkningen för vänster sida

$$\underbrace{n}_{\text{Förare}} \times \underbrace{2}_{\text{Förarens vinval}} \times \underbrace{3^{n-1}}_{\text{Återstående vinval}}.$$

Höger sida. Vi summerar över antalet personer, k, som väljer antingen B eller C. De som inte väljs här måste därmed ta vin A. De "nyktra" personerna kan därmed väljas på $\binom{n}{k}$ sätt, och föraren måste väljas bland dessa k personer. Slutligen bestämmer de k nyktra personerna (inklusive föraren) sig för B eller C. Tolkningen är därför

$$\sum_{k=1}^{n} \underbrace{\binom{n}{k}}_{\text{Personer som väljer } B/C} \times \underbrace{k}_{\text{Förare}} \times \underbrace{2^k}_{\text{Val av } B/C}.$$

På båda sidor ser vi att samma historia berättas.

Lösning II: Börja med $(2x+y)^n$, utveckla med binomialidentiteten och ta derivatan med avseende på x. Sätt sedan $x = y = 1$.

Föreläsning 14
Satslogik och mängdlära

Satslogik handlar om påståenden; det är fraser som har sanningsvärde, sant eller falskt.

- 13 är primtal
- Alla jämna tal är summan av två udda tal.
- a är en rot till polynomet $P(x)$.

Det sista är en **öppen utsaga** vars sanningsvärde beror på parametrarna.

14.1. Logiska konnektiver

Utsagor betecknas med stora bokstäver, $P, Q, R, S, \ldots$. Vi kan **negera** en utsaga och få en ny utsaga, $\neg P$.
Vi kan kombinera utsagor.

- **Konjunktion/och**, $P \wedge Q$
- **Disjunktion/eller**, $P \vee Q$ (det ena, det andra eller båda).

Kalle vill ha te eller Kalle vill ha kaffe är då sann om Kalle vill ha minst en av dryckerna.

14.2. Sanningstabeller

Vi kan undersöka större uttryck via **sanningstabeller**. Till exempel de för $\wedge$ och $\vee$.
Ekvivalens, $P \iff Q$ innebär att P är sann precis då Q är sann.

P	Q	$P \implies Q$	$Q \implies P$	$P \iff Q$	$(P \implies Q) \wedge (Q \implies P)$
T	T	T	T	T	T
T	F	F	T	F	F
F	T	T	F	F	F
F	F	T	T	T	T

14.3. Kontraposition

Sanningstabellen för $P \implies Q$ är samma som den för $\neg Q \implies \neg P$.

Till exempel, tar vi $x \in \mathbb{Z}$:

$$\begin{aligned} P = &\ x^2 \text{ är jämnt} \\ Q = &\ x \text{ är jämnt} \end{aligned}$$

Vi vill visa $P \implies Q$. Men istället visar vi $\neg Q \implies \neg P$, dvs, x udda medför att x^2 är udda. Det senare är enkelt att visa.

14.4. Motsägelsebevis

Ofta vill vi visa att $P \implies Q$. Då kan man istället visa $P \wedge (\neg Q) \implies F$, dvs. vi antar P och $\neg Q$, och visar att detta leder till motsägelse.

14.5. Kvantifikatorer

Utsagor kan ibland vara öppna, dvs, bero på en eller flera parametrar. Vi kan skriva en sådan utsaga som $P(x)$. Man kan då bilda

$$\forall x \in A : P(x) \text{ utläses “För varje } x \in A \text{ gäller } P(x)\text{”}$$

som nu är sluten.

- $\forall x \in \mathbb{R} : x^2 \geq 0$.
- $\forall x, y \in \mathbb{C} : x^2 - y^2 = (x - y)(x + y)$.
- $\forall T \in$ trianglar : summan av två av sidlängderna i T överstiger den tredje sidlängden.

Vi har också existens-kvantifikatorn:

$$\exists x \in A : P(x)$$

Till exempel, $\exists x \in \mathbb{R} : x^7 + 5x + 21 = 0$.

Exempel 172. Vi kan kombinera kvantifikatorer. Notera att ordning spelar roll!

$$\forall a \in \mathbb{R}\ \exists x \in \mathbb{R} : x^3 + ax + 1 = 0.$$

Detta är ett sant påstående, men påståendet

$$\exists x \in \mathbb{R}\ \forall a \in \mathbb{R} : x^3 + ax + 1 = 0$$

är inte alls sant. Det finns inte ett x som är gemensamt nollställe till alla möjliga polynom $x^3 + ax + 1$.

14.5.1. Omskrivningar med kvantifikatorer

Vi har

- $\neg\forall x : P(x)$ är ekvivalent med $\exists x : \neg P(x)$.
- $\neg\exists x : P(x)$ är ekvivalent med $\forall x : \neg P(x)$.
- $\forall x : P(x) \wedge Q(x)$ är ekvivalent med $\forall x : P(x) \wedge \forall x : Q(x)$.
- $\exists x : P(x) \vee Q(x)$ är ekvivalent med $\exists x : P(x) \vee \exists x : Q(x)$.

Notera dock att

$$\exists x : P(x) \wedge Q(x)$$

inte kan brytas upp; vi måste ju ha att $P(x)$ och $Q(x)$ är sanna samtidigt för *samma* värde på x.

Exempel 173. Påståendet

$$\exists x : x^2 - 4 = 0 \wedge x^3 - 8 = 0$$

är sant, då $x = 2$ löser båda ekvationerna (samtidigt!).

14.6. Övningar och exempel

Problem 174. Visa (via sanningstabeller) att $\wedge, \vee$ och $\iff$ är associativa operatorer. Dvs., visa att

$$P \wedge (Q \wedge R) = (P \wedge Q) \wedge R$$

så att vi med gott samvete kan skriva $P \wedge Q \wedge R$.

Problem 175. Ge exempel på ett polynom $f(x, y)$ så att följande utsaga är sann:

$$(\exists x\ \forall y\ f(x, y) = y) \wedge \Big(\exists x\ \forall y\ f(x, y) = (y^2 + 1)\Big)$$

Motivera svaret!

Man kan ta $f(x, y) = y(1 - x) + (y^2 + 1)x$, så för $x = 0$ får man y och för $x = 1$ får man $y^2 + 1$.

Problem 176. Visa de distributiva lagarna

$$(P \wedge Q) \vee R = (P \vee R) \wedge (Q \vee R) \text{ och } (P \vee Q) \wedge R = (P \wedge R) \vee (Q \wedge R).$$

Problem 177. Visa att implikation inte är associativ, dvs. $(P \implies Q) \implies R$ inte är samma som $P \implies (Q \implies R)$.

Lösning. Tag $P = F$, $Q = F$, $R = F$. Då blir sanningsvärdet av första falskt. Sanningsvärdet av det andra blir sant.

14.7. Mängdlära

Vi har mängder, $\mathbb{N}$, $\mathbb{Z}_+$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\emptyset$. Att tillhöra en mängd skrivs $x \in A$. Att inte tillhöra skrivs $x \notin A$. Vi använder måsvingar för att beskriva mängder. Element kan inte förekomma flera gånger (eller, räknas inte flera gånger).

14.8. Mängdbyggarnotation

$$\{x \in A : P(x)\} \quad \text{alternativt:} \quad \{x \in A \mid P(x)\},$$

för något påstående P.

Exempel 178. Som exempel,

$$\{x \in \mathbb{R} : (x^2 - 4)(x^2 - 9) = 0 \wedge x \geq 0\} = \{2, 3\}.$$

Vi kan definiera primtalen som mängden

$$P = \{x \in \mathbb{N} : x \geq 2 \wedge (\neg \exists y \in \mathbb{N} : 1 < y < x \wedge y \mid x)\}.$$

Det finns många andra sätt. Till exempel,

$$P = \{x \in \mathbb{N} : x \geq 2 \wedge (\forall y \in \mathbb{N} : y \mid x \implies y = 1 \vee y = x)\}.$$

14.8.1. Mängdrelationer

Vi har mängdrelationer $A \subseteq B$, $A \subset B$ (äkta delmängd)

14.8.2. Mängdoperationer

Vi har union, $\cup$, snitt, $\cap$.
Om vi har ett fördefinierat universum, har vi **komplement**, A^c. Vi har även relativt komplement, (set minus):

$$A \setminus B = \{x \in A : x \notin B\}.$$

14.9. De Morgans lagar, och räkneoperationer på mängder

Snitt och union är symmetriska och distributiva

$$(A \cap B) \cap C = A \cap (B \cap C).$$

De Morgans lagar:

$$(A \cup B)^c = A^c \cap B^c \qquad (A \cap B)^c = A^c \cup B^c.$$

Jämför med motsvarande för satslogik!

Distributiva lagarna:

Problem 179. Visa de distributiva lagarna

$$(P \cap Q) \cup R = (P \cup R) \cap (Q \cup R) \quad \text{och} \quad (P \cup Q) \cap R = (P \cap R) \cup (Q \cap R).$$

Notera att motsvarande gäller inom satslogiken!

14.10. Inklusion–exklusion

Visa fallet med 3 element, och visa att varje element räknas exakt en gång i unionen.
Ofta två varianter, antingen vill man ha

$$|A \cup B \cup C| \text{ eller } |(A \cup B \cup C)^c|.$$

Problem 180. Hur många tal från $\{1, \ldots, 100\}$ *är* delbara med antingen 3, 5 eller 11?

Lösning. Vi räknar. Enkel division berättar för oss att det finns

- 33 tal som är delbara med 3,
- 20 tal som är delbara med 5, och
- 9 tal som är delbara med 11.

Dessutom finns det

- 6 tal som är delbara med både 3 och 5,
- 3 tal som är delbara med både 3 och 11,
- 1 tal som är delbart både med 5 och 11.

Slutligen är inget tal delbart med alla tre. Därför får vi

$$33 + 20 + 9 - (6 + 3 + 1) = 62 - 10 = 52.$$

Problem 181 (Del av tentan 2023-08-10)**.** Bland 1260 ord, så finns det 120 ord där `aa` förekommer, 120 ord där `bb` förekommer och 24 ord där både `aa` och `bb` förekommer. Hur många av orden uppfyller att varken `aa` eller `bb` förekommer?
(Notera att bland de 120 ord som innehåller `aa`, så får `bb` också förekomma, och vice versa för de ord som innehåller `bb`.)

Lösning. Vi använder inklusion-exklusion: Låt U vara alla ord, låt A vara orden med `aa` och B orden med `bb`. Vi söker $|(A \cup B)^c| = |U| - |A| - |B| + |A \cap B|$ (rita Venn-diagram) som för oss blir

$$1260 - 120 - 120 + 24 = 1044.$$

Problem 182 (Från övningstenta vårterminen 2023)**.** Bokstäverna `ABCDE` skrivs ned i omkastad ordning så att ett ord bildas.

(a) Hur många ord kan bildas på detta sätt?

(b) Hur många av orden har `E` sist?

(c) Hur många av orden har varken `A` först eller `E` sist?

Alla svar ska anges med heltal.

Lösning. (a) Det finns $5! = 120$ sådana ord.

(b) Det finns $4!$ sådana ord, vi placerar först ut `E`, på 1 sätt, resten placeras på $4!$ sätt.

(c) Antal ord *med* `A` först är också 4!. Antal ord med `A` först och `E` sist är 3! (då bara 3 bokstäver måste välja plats). Inklusion-exklusion ger oss nu

$$5! - 2 \cdot 4! + 3! = 120 - 48 + 6 = 78.$$

Exempel 183. Man kan också modellera frågan direkt genom att skapa alla permutationer och sedan räkna:

```
words = Permutations[{"A", "B", "C", "D", "E"}];

Length[words]
Count[words, w_ /; Last[w] == "E"]
Count[words, w_ /; First[w] != "A" && Last[w] != "E"]
```

Problem 184 (Från 2024-08-13)**.** Bokstäverna `P`, `E`, `N`, `N`, `A`, `N` kan man sätta samman och bilda kombinationer med 6 bokstäver (ord). Hur många ord

(a) kan skapas totalt?

(b) uppfyller att `P` står direkt till vänster om `E`?

(c) uppfyller att `P` står först eller `N` står sist (eller båda)?

Svaren ska anges med heltal. Inget svar överstiger 300.

Lösning. (a) Ordet innehåller 6 bokstäver, men vi har att `NNN` är tre lika bokstäver så totala antalet ord är $\frac{6!}{3!} = 6!/6 = 5! = 120$.

(b) Vi betraktar `PE` som om det vore en bokstav som kan placeras ut. Detta ger $\frac{5!}{3!} = 20$ olika sådana ord.

(c) Antal ord där `P` står först är $5!/3! = 20$, då vi måste bilda ord genom att kasta om `ENNAN`. Liknande, antal ord där `N` står sist är $5!/2! = 60$, då vi måste bilda ord genom att kasta om `PENNA`. Slutligen, antal ord där `P` står först och `N` står sist fås genom omkastning av `ENNA`, vilket ger $4!/2! = 12$ ord. Inklusion-exklusion ger nu att totala antalet ord vi söker är

$$20 + 60 - 12 = 68$$

då vi bland de $20 + 60$ orden med antingen `P` först eller `N` sist, dubbelräknar de 12 ord som uppfyller båda kraven.

Problem 185. Det finns fem personer med olika längd. På hur många sätt kan de stå i en rad så att det inte finns tre på varandra följande personer med ökande längd?

Lösning. Först numrera platserna i raden som 12345. Låt A vara händelsen att personerna på platserna 123 är i längdordning, B vara händelsen att 234 är i ordning och C händelsen att 345 är i ordning.

Vi söker $5! - |A \cup B \cup C|$ där den sista termen beräknas via inklusions-exklusionsprincipen. Observera att $|A| = |B| = |C| = \binom{5}{3}2!$ eftersom vi väljer tre av de fem personerna för att vara i ordning, och sedan placera de två återstående personerna på de två möjliga sätten på de sista två platserna. På samma sätt följer det att $|A \cap B| = |B \cap C| = \binom{5}{4}$. Emellertid är $|A \cap C| = 1$ och $|A \cap B \cap C| = 1$ eftersom det betyder att personerna på alla fem platserna måste vara i ökande ordning. Därför finns det

$$5! - 3\binom{5}{3} \cdot 2! + \left[2\binom{5}{4} + 1\right] - 1$$

olika giltiga rader av personer.

Föreläsning 15
Tentamensrepetition

Saker man bör kunna. Ej komplett lista.

- Primtal och delbarhet, största gemensamma delare.
- Moduloräkning, Fermats lilla sats.
- Aritmetisk och geometrisk summa.
- Lösa diofantiska ekvationer och avgöra när de saknar lösning.
- Kunna hantera komplexa tal på polär form.
- Kunna lösa andragradsekvationer med komplexa koefficienter.
- Kunna hantera olikheter och ekvationer med absolutbelopp.
- Rationella rotsatsen.
- Enklare induktionsbevis.
- Kombinatoriska resonemang, binomialtal, inklusion–exklusion.
- Kunna förstå symboler från logik, sanningstabeller.
- Mängder och dess räkneoperationer. Mängdbyggarnotation.

Problem 186. (a) Bestäm SGD$(312, 221)$.

(b) Beräkna resten då 3^{3002} delas med 31.

(c) Låt $A = \{1, 2, 3\}$ $B = \{2, 3, 4\}$, $C = \{3, 4, 5\}$. Bestäm

$$(A \setminus B) \cup (B \cap C).$$

Lösning. (a) Euklides ger

$$\begin{aligned} 312 &= 221 + 91 \\ 221 &= 2 \cdot 91 + 39 \\ 91 &= 2 \cdot 39 + 13 \\ 39 &= 3 \cdot 13 + 0 \end{aligned}$$

så största gemensamma delare är 13.

(b) Vi har att $3^{3002} = 3^2 \cdot 3^{3000} = 9 \cdot (3^{30})^{100}$. Nu, Fermats lilla sats säger att 3^{30} mod 31 är 1, (eftersom 31 är primtal) så vi får resten 9.

(c) $A \setminus B = \{1\}$, $B \cap C = \{3, 4\}$ så deras union blir $\{1, 3, 4\}$.

Problem 187. En av rötterna till $z^4 - 6z^3 + 12z^2 - 12z + 20 = 0$ är $z = 3 + i$. Bestäm de övriga rötterna.

Lösning. Eftersom koefficienterna är reella är $z = 3 - i$ också en rot. Detta ger att

$$(z - 3 - i)(z - 3 + i) = z^2 - 6z + 10$$

är en faktor. Polynomdivision ger nu att

$$z^4 - 6z^3 + 12z^2 - 12z + 20 = (z^2 + 2)(z^2 - 6z + 10)$$

och de två sista rötterna är $\pm i\sqrt{2}$.

Problem 188. Lös olikheten

$$|(x - 2)(x - 3)| \geq 4(x + 4).$$

Lösning. Vi delar upp i två fall, beroende på om det inuti absolutbeloppet är positivt eller negativt. **Fall** $2 \leq x \leq 3$**:** Detta ger

$$-(x - 2)(x - 3) \geq 4(x + 4) \iff 0 \geq x^2 - x + 22 \iff 0 \geq \left(x - \frac{1}{2}\right)^2 + 22 - \frac{1}{4}.$$

Det finns inget värde på x som gör att detta är sant, då högerledet alltid är positivt.
Fall $x < 2$ **eller** $x > 3$**:** Vi får

$$(x - 2)(x - 3) \geq 4(x + 4) \iff x^2 - 9x - 10 \geq 0 \iff (x + 1)(x - 10) \geq 0.$$

Denna olikhet gäller om $x \leq -1$ eller $x \geq 10$. För båda dessa möjligheter uppfyller vi Fall 2s krav, så lösningen ges då av $x \leq -1$ eller $x \geq 10$.

Problem 189. Bestäm det minsta positiva heltal a så att de båda Diofantiska ekvationerna

$$104x - 136y = a \qquad \text{och} \qquad 60x + 84y = a$$

har lösningar.

Lösning. Vi vet att den första Diofantiska ekvationen har lösning om SGD$(104, 136)$ är en delare till a. Samtidigt måste vi ha att SGD$(60, 84)$ ska dela a för att den andra ekvationen ska kunna lösas.
Vi finner med Euklides algoritm att SGD$(104, 136) = 8$, samt SGD$(60, 84) = 12$. Talet a måste då vara den minsta gemensamma multipeln av 8 och 12, så $a = 24$.

Problem 190. Ekvationen

$$x^3 - ax^2 + bx - 2 = 0$$

har rötterna $x = 2 + \sqrt{2}$ samt $x = 2 - \sqrt{2}$. Bestäm talen a och b.

Lösning. Vi vet att

$$(x-2-\sqrt{2})(x-2+\sqrt{2}) = x^2-4x+2$$

är en faktor till polynomet i ekvationens vänsterled. Om r är polynomets tredje nollställe, så gäller det alltså att

$$(x^2-4x+2)(x-r) = x^3-ax^2+bx-2.$$

Detta leder till

$$x^3-(4+r)x^2+(4r+2)x-2r = x^3-ax^2+bx-2.$$

Jämför vi konstanttermerna, ser vi att $r=1$. Detta leder direkt till att ekvationen är

$$x^3-5x^2+6x-2=0$$

så $a=5$ och $b=6$.
Alternativt kan man direkt använda Vietas formler som säger att produkten av rötterna ger konstanttermen (med ett tecken), Alltså, $r(2-\sqrt{2})(2+\sqrt{2})=2$, vilket nu ger att $r=1$.

Problem 191. Låt $A=\{1,2,3,5,6,8,9,11,13\}$. Lista elementen i följande mängd:

$$B=\{x\in A : (\exists y\in A : y\neq x \wedge \mathrm{SGD}(x,y)\neq 1)\}.$$

Lösning. Vi vill ha alla element x i A, som har egenskapen att det finns ett annat element y i A, så att x och y har en största gemensamma delare som inte är 1.

- Vi har att $1\notin B$, då $\mathrm{SGD}(1,y)=1$ alltid.
- Vi har att $2\in B$, då det finns $6\in A$ och $\mathrm{SGD}(2,6)=2$.
- Vi har att $3\in B$, då det finns $6\in A$ och $\mathrm{SGD}(3,6)=3$.
- Vi har att $5\notin B$, då det inte finns $y\in A$ där $\mathrm{SGD}(5,y)\neq 1$.
- Vi har att $6\in B$, då det finns $3\in A$ och $\mathrm{SGD}(6,3)=3$.
- Vi har att $8\in B$, då det finns $2\in A$ och $\mathrm{SGD}(8,2)=2$.
- Vi har att $9\in B$, då det finns $3\in A$ och $\mathrm{SGD}(9,3)=3$.
- Vi har att $11\notin B$, då det inte finns $y\in A$ där $\mathrm{SGD}(11,y)\neq 1$.
- Vi har att $13\notin B$, då det inte finns $y\in A$ där $\mathrm{SGD}(13,y)\neq 1$.

Alltså är $B=\{2,3,6,8,9\}$.

Problem 192. Låt $M=\{\{1,2,3\},\{2,3,4\},\{3,5,6\},\{4,5\},\{1\},\{2,3\},\{1,2,4,5\}\}$. Bestäm elementen i följande mängd:

$$\{X\in M : (\exists Y\in M : |X\setminus Y|=1)\}.$$

Lösning. Vi har att

- $\{1,2,3\}$ ingår, då vi kan ta $Y=\{2,3\}$.
- $\{2,3,4\}$ ingår, då vi kan ta $Y=\{2,3\}$.
- $\{3,5,6\}$ ingår inte, då det inte finns lämpligt Y.

- $\{4, 5\}$ ingår, vi kan ta $Y = \{2, 3, 4\}$.
- $\{1\}$ ingår, vi kan ta $Y = \{2, 3\}$.
- $\{2, 3\}$ ingår, vi kan ta $Y = \{3, 5, 6\}$.
- $\{1, 2, 4, 5\}$ ingår inte, då det inte finns lämpligt Y.

Problem 193. En rekursivt definierad talföljd definieras av

$$a_1 = 1 \text{ samt } a_{n+1} = 2a_n - n + 1 \text{ för } n \geq 1.$$

Visa att $a_n = n$ för alla heltal $n \geq 1$.

Lösning. Den slutna formeln säger att $a_1 = 1$, vilket stämmer med definitionen. Detta är vårt basfall. Antag nu att $a_k = k$ för något fixt $k \geq 1$. Rekursionsformeln säger att

$$a_{k+1} = 2a_k - k + 1,$$

som nu kan skrivas om med antagandet till

$$a_{k+1} = 2k - k + 1 = k + 1.$$

Så vi har alltså visat implikationen $a_k = k \implies a_{k+1} = k + 1$. Tillsammans med basfallet ger induktionsprincipen att den slutna formeln gäller för alla $n \geq 1$.

Problem 194. Antag att $\text{SGD}(a, b) = 2$. Bevisa att $\text{SGD}(a^k, b^k) = 2^k$ för varje positivt heltal k.

Lösning. Vi vet att $2 \mid a$ samt $2 \mid b$, så $a = 2a'$ samt $b = 2b'$. Detta ger att

$$a^k = 2^k(a')^k \qquad b^k = 2^k(b')^k.$$

Vi ser då direkt att 2^k är en gemensam delare till a^k och b^k. Det återstår att visa att detta är den största gemensamma delaren.

Nu, minst ett av talen a' och b' är udda annars hade $\text{SGD}(a, b)$ varit minst 4. Alltså är 2^k största potensen av 2 som delar både a^k och b^k.

Om vi nu har ett udda primtal $p \geq 3$ som delar a^k och b^k, så måste detta primtal dela a och b (enl. sats). Då måste p vara gemensam delare till a och b, vilket motsäger förutsättningen $\text{SGD}(a, b) = 2$. Detta visar att $\text{SGD}(a^k, b^k)$ bara kan vara en tvåpotens vilket vi redan behandlat.

Vi är nu klara med beviset.

En alternativ lösning utgår från aritmetikens fundamentalsats, och betraktar primtalsfaktoriseringen av a och b.

Problem 195. Visa följande kombinatoriska identitet för alla heltal $n \geq 5$:

$$\binom{n}{5}\binom{5}{3}3! = n(n-1)(n-2)\binom{n-3}{2}.$$

Bevis. Algebraiskt bevis: Sätt in definitionen av binomialkoefficienter $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ och utveckla.
Kombinatoriskt bevis: Vänsterledet tolkas som följande. Vi har n personer. Bland dessa väljer vi 5— $\binom{n}{5}$ val. Bland de 5 väljs tre ut—$\binom{5}{3}$—som ska tilldelas rollerna A, B och C. Tilldelningen av roller kan ske på 3! sätt.
Högerledet är nu samma men valen görs i annan ordning. Först väljer vi vem som ska ha roll A, därefter roll B och slutligen en person som ska ha roll C. Bland de $n-3$ återstående personerna väljs nu ut två ytterligare så att roll-personerna plus de två extra bildar en grupp med 5 personer. □

Problem 196. Vi har 9 personer—två matematiker, två fysiker, och fem mixologer.

(a) På hur många sätt kan 5 personer väljas ut till en grupp?

(b) På hur många sätt kan 5 väljas så att båda matematikerna ingår i gruppen?

(c) På hur många sätt kan 5 väljas så att vi har maximalt en matematiker och maximalt en fysiker bland de valda?

Lösning. (a) Det finns $\binom{9}{5} = \frac{9\cdot8\cdot7\cdot6}{4\cdot3\cdot2} = 9\cdot7\cdot2 = 126$ sådana val.

(b) Om båda matematikerna ingår, så behövs 3 till väljas bland övriga 7. Detta ger $\binom{7}{3} = 35$ val.

(c) Vi förbjuder fallen med två matematiker, och fallen med två fysiker. Inklusion-exklusion ger

$$\binom{9}{5} - \binom{7}{3} - \binom{7}{3} + \binom{5}{1} = 126 - 70 + 5 = 61$$

antal sådana val.

Alternativt kan man dela upp i fyra icke överlappande fall:

- Bara mixologer: 1
- En matematiker och fyra mixologer: $2\binom{5}{4} = 10$.
- En fysiker och fyra mixologer: $2\binom{5}{4} = 10$.
- En matematiker, en fysiker samt tre mixologer: $2\cdot2\cdot\binom{5}{3} = 40$.

Igen får vi totalt 61 val.

Problem 197. Bokstäverna i namnet `amanda` kastas om.

(a) Hur många ord kan bildas totalt?

(b) Hur många ord har att de första två a:na i ordet förekommer på plats 2 och 3?

(c) Hur många ord har att inga två a:n står bredvid varandra?

Lösning. För första frågan är svaret $\frac{6!}{3!} = 120$, då vi har 6 bokstäver varav tre är lika.

För andra frågan, då placerar vi ut `aa` på plats 2 och 3. Det tredje `a`:et kan då vara på plats 4, 5 eller 6. Detta ger $3 \cdot 3! = 18$ olika sådana ord, då de tre övriga bokstäverna har 3! sätt att placeras ut på.

För tredje frågan, vi räknar de förbjudna fallen och delar upp beroende på var första instansen av `aa` förekommer.

- Plats 1 och 2: $4 \cdot 3! = 24$ (fyra platser för tredje `a`:et samt de tre övriga.
- Plats 2 och 3: $3 \cdot 3! = 18$, enligt fråga (b).
- Plats 3 och 4: $(1 + 2) \cdot 3! = 18$ (det tredje A:et kan vara på plats 1, 5 eller 6).
- Plats 4 och 5: $(2 + 1) \cdot 3! = 18$.
- Plats 5 och 6: $3 \cdot 3! = 18$.

Totalt är det då $24 + 4 \cdot 18 = 96$ förbjudna ord. Detta ger $120 - 96 = 24$ ord utan att `aa` förekommer:

`amanda`, `amanad`, `amadna`, `amadan`, `amnada`, `amdana`,
`anmada`, `anamda`, `anamad`, `anadma`, `anadam`, `andama`,
`admana`, `adamna`, `adaman`, `adanma`, `adanam`, `adnama`,
`manada`, `madana`, `namada`, `nadama`, `damana`, `danama`.

Alternativt konstaterar man att det bara finns 4 olika sätt att placera ut `a`:na så att de inte är bredvid varandra:

`a.a.a.` `a.a..a` `a..a.a` `.a.a.a`

och det finns sedan $3! = 6$ sätt att placera ut övriga bokstäver.

Problem 198. Bestäm summan

$$\sum_{m=0}^{7} \sum_{k=0}^{7} 2^{m+k}.$$

Svaret får innehålla heltal kombinerade med de fyra räknesätten samt potenser.

Lösning. Vi börjar med den inre summan:

$$\sum_{k=0}^{7} 2^{m+k} = 2^m \sum_{k=0}^{7} 2^k = 2^m \frac{2^8 - 1}{2 - 1} = 255 \cdot 2^m.$$

Vi vill alltså finna

$$\sum_{m=0}^{7} 255 \cdot 2^m = 255 \sum_{m=0}^{7} 2^m = 255 \frac{2^8 - 1}{2 - 1} = 255^2.$$

Problem 199. Bokstäverna i ordet `TENTADAG` kan kastas om och bilda ord.

(a) Hur många ord totalt kan bildas?

(b) Hur många kan bildas där båda `A` står intill varandra?

(c) Hur många ord kan bildas där två lika bokstäver inte står intill varandra?

Svaren får anges innehållandes fakulteter och binomialtal.

Lösning. (a) Ordet innehåller 8 bokstäver, men `AA` och `TT` är dubbletter så totala antalet ord är $\frac{8!}{2!2!} = \frac{8!}{4} = 2 \cdot 7!$.

(b) Vi betraktar `AA` som om det vore en bokstav som kan placeras ut. Detta ger $\frac{7!}{2!}$ olika sådana ord.

(c) Samma resonemang som i (b) visar att antalet ord där `TT` förekommer, är $\frac{7!}{2}$. Antalet ord där *både* `AA` och `TT` förekommer är 6!, då vi nu har de 6 symbolerna

$$\texttt{AA}, \texttt{N}, \texttt{TT}, \texttt{D}, \texttt{G}, \texttt{E}$$

att permutera.

Totala antalet ord där två lika bokstäver inte står intill varandra ges nu med hjälp av inklusion-exklusion:

$$2 \cdot 7! - \frac{7!}{2} - \frac{7!}{2} + 6! = 7! + 6!.$$

Problem 200. Bokstäverna `ABCDDEE` kastas om och bildar ord med 7 bokstäver.

(a) Hur många ord kan totalt bildas?

(b) Hur många ord kan bildas där `A` står först och `B` står på andra plats?

(c) Hur många ord kan bildas där minst en av bokstäverna `A` och `B` står på sin ursprungliga plats (dvs. plats 1 och 2)?

Svaren ska vara fullt uträknade.

Lösning. (a) Det är 7 olika bokstäver, med två `D` och två stycken `E` så vi har $\frac{7!}{2!\cdot 2!} = 7 \cdot 6 \cdot 5 \cdot 3 \cdot 2 = 42 \cdot 30 = 1260$ ord.

(b) Vi har bokstäverna `CDDEE` kvar att kasta om, vilket ger $\frac{5!}{4} = 30$ ord.

(c) Låt A vara mängden ord där `A` är på plats 1, B vara mängden ord där `B` är på plats 2. Vi vill beräkna $|A \cup B|$. Vi har att $|A|$ ges av antal ord som kan bildas av `BCDDEE`, så $\frac{6!}{4} = 180$. På samma sätt får man att $|B| = 180$. Enligt fråga (b) gäller $|A \cap B| = 30$.

Inklusion-exklusion ger nu

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Högerledet blir $2 \cdot 180 - 30 = 330$ som då är svaret på frågan.

Problem 201. Beräkna

$$\arg(1 + 3i) + \arg(1 - 2i) + \arg(4 + 3i).$$

Lösning. Eftersom $\arg(zw) = \arg(z) + \arg(w)$ gäller det att summan ges av argumentet av

$$(1 + 3i)(1 - 2i)(4 + 3i) = (7 + i)(4 + 3i) = 25 + 25i.$$

Detta tal har argument $\frac{\pi}{4}$.

Problem 202. Bestäm den sista siffran i talet $2^{2024} + 3^{2024} + 5^{2024}$.

Problem 203. Lös ekvationen $|2x - 4| + |x - 3| = x$.

Lösning. Uttrycken inom absolutbeloppen byter tecken vid $x = 2$ och $x = 3$, respektive. Vi delar upp i tre fall.

- Fall $x < 2$: Här blir ekvationen

$$-(2x - 4) - (x - 3) = x \iff 7 = 4x \iff x = \frac{7}{4}.$$

  Denna lösning uppfyller villkoret i fallet.

- Fall $2 \leq x < 3$: Här blir ekvationen

$$(2x - 4) - (x - 3) = x \iff x - 1 = x \iff -1 = 0.$$

  Det saknas lösningar i detta fall.

- Fall $3 \leq x$: Här blir ekvationen

$$(2x - 4) + (x - 3) = x \iff 3x - 7 = x \iff 2x = 7 \iff x = \frac{7}{2}.$$

  Eftersom $7/2 > 3$ så är även detta en lösning.

Ekvationen har lösningarna $x = 7/4$ samt $x = 7/2$.

Problem 204. (a) Låt $P(x)$ vara ett polynom. Visa att om både α och $-\alpha$ är nollställen till $P(x)$, så är α nollställe till båda polynomen $P(x) + P(-x)$ och $P(x) - P(-x)$.

(b) Det finns ett tal $\alpha \in \mathbb{C}$ så att $P(x) = x^4 - 2x^3 + 9x^2 - 14x + 14$ har både α och $-\alpha$ som nollställen. Faktorisera P över $\mathbb{C}$.

Lösning. (a) Vi har att $P(\alpha) \pm P(-\alpha) = 0 \pm 0 = 0$ så α är ett nollställe till $P(x) \pm P(-x)$.

(b) Enligt (a) så måste α vara nollställe till

$$P(x) - P(-x) = \Big(x^4 - 2x^3 + 9x^2 - 14x + 14\Big) - \Big(x^4 + 2x^3 + 9x^2 + 14x + 14\Big) = -4x^3 - 28x.$$

Vi ser att $P(0) \neq 0$ så $\alpha \neq 0$. Alltså måste α vara ett nollställe till $x^2 + 7$, så $\alpha = \pm i\sqrt{7}$. Då måste $x^2 + 7$ vara en faktor till $P(x)$ och polynomdivision ger

$$P(x) = (x^2 + 7)(x^2 - 2x + 2).$$

Formeln för andragradsekvationer ger att de två sista rötterna är $1 \pm i$, så

$$P(x) = (x - i\sqrt{7})(x + i\sqrt{7})(x - 1 - i)(x - 1 + i).$$

Problem 205. Låt $z = e^{i\frac{\pi}{42}}$ och definiera talföljden $a_n = \mathrm{Re}(z^n)$ för $n = 1, 2, 3, \ldots$.

1. Beräkna a_{21}.
2. Visa att $a_{n+2} = 2 \cdot a_1 \cdot a_{n+1} - a_n$ för alla $n \geq 1$.

Tips: $\cos(u + v) = \cos u \cos v - \sin u \sin v$, $\sin(u + v) = \sin u \cos v + \cos u \sin v$.

Lösning. Låt $\theta = \frac{\pi}{42}$. Vi har enligt de Moivres formel att $a_n = \mathrm{Re}(e^{i\theta n}) = \cos(n\theta)$. Alltså gäller det att $a_{21} = \cos(21 \cdot \pi/42) = \cos(\pi/2) = 0$.
För att visa $a_{n+2} = 2 \cdot a_1 a_{n+1} - a_n$ för alla $n \geq 1$, måste vi visa

$$\cos((n+2)\theta) = 2\cos(\theta)\cos((n+1)\theta) - \cos(n\theta). \tag{15.1}$$

Additionsformeln för cosinus ger oss

$$\begin{aligned}\cos\left((n+2)\theta\right) &= \cos(2\theta)\cos(n\theta) - \sin(2\theta)\sin(n\theta)\\ \cos\left((n+1)\theta\right) &= \cos(\theta)\cos(n\theta) - \sin(\theta)\sin(n\theta).\end{aligned}$$

Vi får då att vänsterled och högerled i (15.1) blir

$$\begin{aligned}\mathrm{VL} &= \cos(2\theta)\cos(n\theta) - \sin(2\theta)\sin(n\theta),\\ \mathrm{HL} &= 2\cos(\theta)\left(\cos(\theta)\cos(n\theta) - \sin(\theta)\sin(n\theta)\right) - \cos(n\theta)\\ &= \underline{\left(2\cos^2(\theta) - 1\right)}\cos(n\theta) - \underline{2\cos(\theta)\sin(\theta)}\sin(n\theta).\end{aligned}$$

Formlerna för dubbla vinkeln,

$$\cos(2\theta) = 2\cos^2(\theta) - 1 \text{ samt } \sin(2\theta) = 2\cos(\theta)\sin(\theta),$$

visar nu att VL = HL och vi är klara.

Problem 206. Betrakta mängden nedan:

$$A = \{12x + 4 : x \in \mathbb{Z}\} \cap \{15y + 1 : y \in \mathbb{Z}\}.$$

Bestäm heltal a och b så att $A = \{az + b : z \in \mathbb{Z}\}$.

Lösning. Vi ska bestämma mängden

$$A = \{12x + 4 : x \in \mathbb{Z}\} \cap \{15y + 1 : y \in \mathbb{Z}\}.$$

Det innebär att vi letar efter heltal som kan skrivas både på formen $12x + 4$ och $15y + 1$, alltså att ekvationen

$$12x + 4 = 15y + 1$$

har heltalslösningar x, y. Detta kan skrivas om som

$$12x - 15y = -3.$$

Vi söker den allmänna lösningen till denna diofantiska ekvation. Division med 3 ger oss $4x - 5y = -1$, och en partikulärlösning är $x = y = 1$. Därmed fås den allmänna lösningen:

$$x = 1 + 5z, \quad y = 1 + 4z, \qquad z \in \mathbb{Z}.$$

Vi sätter då in detta uttryck för x i $12x + 4$ och får $12(1 + 5z) + 4 = 60z + 16$. Vi har alltså att

$$A = \{60z + 16 : z \in \mathbb{Z}\}.$$

Problem 207. Låt $p(x) = x^3 + bx^2 + 10x + 4$ vara ett polynom där $b \in \mathbb{Z}$.

(a) Enligt rationella rotsatsen, vilka möjliga rationella nollställen kan $p(x)$ ha?

(b) Bestäm alla värden på b som gör att ekvationen $p(x) = 0$ har en heltalsrot.

(c) För $b = 6$, lös ekvationen $p(x) = 0$.

Lösning. (a) Satsen säger att vi bara kan ha heltalsrötterna $\pm 1, \pm 2, \pm 4$ då dessa är konstanttermens delare, och polynomet är moniskt.

(b) Om $x = -1$ är ett nollställe, så ger detta att $p(-1) = 0$. Detta ger i sin tur att $b = 7$. På samma sätt ger $p(-2) = 0$ att $b = 6$, $p(1) = 0$ att $b = -15$ och $p(2) = 0$ att $b = -8$. Slutligen ger $p(-4) = 0$ att $b = 25/4$ och $p(4) = 0$ att $b = -27/4$, men dessa är inte heltal. Alltså är $b = 7, 6, -15, -8$ de värden vi söker.

(c) Vi vet att för $b = 6$, så är $(x+2)$ en faktor till polynomet. Polynomdivision följt av pq-formeln ger oss

$$p(x) = (x + 2)(x^2 + 4x + 2) \implies p(x) = (x + 2)(x + 2 - \sqrt{2})(x + 2 + \sqrt{2}).$$

Problem 208. Låt $S = a_1 + a_2 + a_3 + \cdots a_{2n}$ vara en aritmetisk summa med ett jämnt antal termer. Sätt

$$S_1 = a_1 + a_3 + a_5 + \cdots + a_{2n-1}, \quad S_2 = a_2 + a_4 + a_6 + \cdots + a_{2n}.$$

(a) Visa att S_1 och S_2 också är aritmetiska summor.

(b) Visa att

$$\frac{S_2 - S_1}{n} = a_2 - a_1.$$

Appendix
Det matematiska språket

A.0.1. Mängdnotation

De mängder av tal vi kommer arbeta med är $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. I denna kurs gäller det att $0 \in \mathbb{N}$.

A.0.2. Uttryck, ekvation, identitet, påstående

Notera att alla identiteter är (sanna) påståenden. Ekvationer är också påståenden, som antingen är sanna eller falska (sanningsvärdet beror på variablerna som ingår).

A.0.3. Lemma, sats, bevis

Ett **lemma** är ungefär som en sats, men man använder oftast lemman för mindre resultat som sedan används för att bevisa den huvudsakliga satsen.

En **förmodan** är ett påstående som man tror är sant, men man har inte hittat ett bevis (eller motexempel) ännu. En känd förmodan är till exempel *Collatz conjecture*[1].

En **definition** är då man inför ett nytt begrepp, ord eller objekt. Till exempel definierade vi att symbolen $\mathbb{N}$ betyder mängden av naturliga tal. Naturliga tal i sin tur definieras som talen $0, 1, 2, 3, \ldots$.

Ett **axiom** är en sanning som vi tar för givet, som ligger till grund för resten av vår matematiska teori. Till exempel, i modeller för de naturliga talen, brukar man till exempel ha axiomet att 0 är ett naturligt tal, samt axiomet att efter varje naturligt tal n finns ett (annat) naturligt tal, $n + 1$. Det finns flera andra axiom som tillkommer men vi kommer inte dyka ner på det djupet i denna kurs.

A.0.4. Implikation och ekvivalens

Likhet mellan påståenden (samma sanningsvärde) kallas för ekvivalens, och vi använder $\iff$.

Vi har även implikation, $\implies$. Implikation kan uttryckas i text på flera sätt. *Detta ger att*, eller *Vilket leder till*.

[1] `https://en.wikipedia.org/wiki/Collatz_conjecture`