Extramaterial till Algebra och kombinatorik

1 Falsk induktion

Till skillnad från andra typer av induktion[1] har matematisk induktion den fördelen att man kan vara helt säker på att det man bevisat med denna induktion är helt säkert. Å andra sidan måste man speciellt inom matematik var misstänksam mot andra sorters induktion då de förvånansvärt ofta leder till felaktiga resultat. Vi ska ge två exempel på detta.

41 är ett primtal[2]. Om vi lägger 2 till 41 får vi också ett primtal 43. Om vi lägger 4 till 43 får vi återigen ett primtal 47. Fortsätter vi får vi

$$\begin{aligned}
41 &+ 2 &&= 43\\
43 &+ 4 &&= 47\\
47 &+ 6 &&= 53\\
53 &+ 8 &&= 61\\
61 &+ 10 &&= 71\\
71 &+ 12 &&= 83\\
83 &+ 14 &&= 97\\
97 &+ 16 &&= 113\\
113 &+ 18 &&= 131\\
131 &+ 20 &&= 151
\end{aligned}$$

och de är alla primtal. Får vi alltid primtal på det sättet? Ja, om vi fortsätter och kontrollerar om de är primtal (vilket blir tuffare och tuffare förstås) kommer man ända upp till 1681 innan man hittar ett tal som inte är primtal.

Övning: i) Visa att 1681 inte är ett primtal.

ii) (Lång!) Visa att alla tal innan 1681 är det.

Vi har alltså ett exempel på ett påstående ("Man får alltid primtal på detta sätt.") som är sant i de 40 första fallen men som är fel för det 41:a.

Ett ännu mer imponerande exempel fordrar lite mer motivation. Vi har sett man kan definiera *Fibonacciföljden* genom en "tvåstegsrekursion";[3] $a_1 = 1$, $a_2 = 1$ och $a_{n+2} = a_{n+1} + a_n$ för $n > 0$ vilket ger följden $1, 1, 2, 3, 5, 7, \ldots$. Man kan naturligtvis börja med andra startvärden t ex $a_1 = 3$ och $a_2 = 4$ men samma rekursionsregel vilket ger $3, 4, 7, 11, 18, 29, \ldots$.

Låt oss ha denna följd i minne medan vi betraktar ett annat sätt att få en följd av heltal:

$$\begin{aligned}
\left(\tfrac{1+\sqrt{5}}{2}\right)^2 &\approx 2,61803 \text{ avr.: } 3\\
\left(\tfrac{1+\sqrt{5}}{2}\right)^3 &\approx 4,23607 \text{ avr.: } 4\\
\left(\tfrac{1+\sqrt{5}}{2}\right)^4 &\approx 6,8541 \text{ avr.: } 7\\
\left(\tfrac{1+\sqrt{5}}{2}\right)^5 &\approx 11,0902 \text{ avr.: } 11\\
\left(\tfrac{1+\sqrt{5}}{2}\right)^6 &\approx 17,9443 \text{ avr.: } 17\\
\left(\tfrac{1+\sqrt{5}}{2}\right)^7 &\approx 29,0344 \text{ avr.: } 29
\end{aligned}$$

Här har vi tagit ett fixt tal $(1+\sqrt{5})/2$, upphöjt till högre och högre potenser och sedan avrundat till närmaste heltal. Vi ser att vi verkar få samma följd som i den modifierade Fibonacciföljden ovan (med startvärden 3 och 4). Man kan faktiskt visa att dessa två följder verkligen är desamma.

[1] Dvs slutledningar från tidigare kända fakta.

[2] Dvs ett heltal ≥ 2 som inte är produkten av två strikt mindre heltal.

[3] Den korrekta benämningen är "andra ordningens rekursion"

Här har vi alltså ett exempel på en följd som först ges en ganska besynnerlig definition; som avrundningen av potenser av ett tal, och som sedan visar sig kunna definieras genom en enkel andra ordningens induktion.

Vi kan vända lite på sambandet mellan dessa två följder genom att säga att a_n är nära $\left((1+\sqrt{5})/2\right)^{n+1}$ så att a_{n+1}/a_n borde vara nära $(1+\sqrt{5})/2$. Till exempel är $29/18 \approx 1,61111$ med $(1+\sqrt{5})/2 \approx 1,61803$.

Övning: Undersök kvoten a_{n+1}/a_n för större n.

Vi ska nu gå lite baklänges och definiera en följd a_n av heltal och vi ska försöka se till ett kvoterna a_{n+1}/a_n kommer nära varandra. För detta börjar vi med att fixera de två första värdena och vi väljer helt omotiverat $a_1 = 8$ och $a_2 = 55$. Vi vill sedan att a_3 ska vara ett heltal sådant att a_3/a_2 är nära a_2/a_1 och närmare bestämt så väljer vi a_3 som det minsta heltal så att $a_3/a_2 > a_2/a_1$ dvs $a_3 > a_2^2/a_1 = 55^2/8 = 378,125$ så att $a_3 = 379$. Sedan väljer vi a_4 som det minsta heltal så att $a_4/a_3 > a_3/a_2$ dvs så att $a_4 > a_3^2/a_2 \approx 2611,65$ dvs $a_3 = 2612$. Vi fortsätter och får följden

$$8, 55, 379, 2612, 18002, 124071, 855106, 5893451, 40618081, 279942687, 1929384798,$$
$$13297456486, 91647010581, 631637678776, 4353291555505, 30003193292641, \ldots$$

Man kan nu fråga sig om det som med förra exemplet finns någon rekursionsformel som definierar denna följd. Om vi försöker med en andra ordningens är det lätt att se att det inte går och även att det finns en tredje ordningens formel. Om man däremot går ett steg vidare så hittar man en fjärde ordningens formel som verkar fungera nämligen

$$a_{n+4} = 6a_{n+3} + 7a_{n+2} - 5a_{n+1} - 6a_n,$$

så att till att börja med

$$\begin{aligned} 18002 &= 6 \cdot 2612 + 7 \cdot 379 - 5 \cdot 55 - 6 \cdot 8 \\ &\text{och} \\ 124071 &= 6 \cdot 18002 + 7 \cdot 2612 - 5 \cdot 379 - 6 \cdot 55. \end{aligned}$$

Om man kontrollerar om denna relation är uppfylld längre upp i följden så ser det ut som om det är sant. Närmare bestämt är relationen sann för de första 11 056 termerna vilket verkar mycket övertygande. Dock är detta en illusion ty det är inte sant för nästa term!

2 Diofantiska ekvationer

De ekvationer vi ska behandla är av typen

$$ax + by = c$$

där a, b, c är givna heltal och man bara är intresserad av heltalslösningar, d.v.s. x och y ska vara heltal. Vissa sådana ekvationer saknar lösningar.

Exempel: Ekvationen $35x + 55y = 102$ har ingen lösning. Oavsett vilka värden man ger x och y kommer VL att vara delbart med 5. Men 102 är inte delbart med 5.

Ett nödvändigt villkor för att det ska finnas en lösning är alltså att SGD(a, b) delar c. Om detta villkor är uppfyllt kan man dividera bägge sidor av ekvationen med SGD(a, b) utan att ändra lösningsmängden. Om man gör denna division kommer SGD av koefficienterna i VL att bli 1. I fortsättningen antar vi att SGD$(a, b) = 1$. Vi ska se att i detta fall har ekvationen alltid oändligt många lösningar. Antag att vi har hittat en lösning $x = x_0, y = y_0$. Om $x = x_1, y = y_1$ är en annan lösning gäller alltså att $ax_0 + by_0 = c$ och $ax_1 + by_1 = c$. Detta ger att $a(x_1 - x_0) + b(y_1 - y_0) = 0$. Vi får alltså den nya lösningen (x_1, y_1) genom att till den gamla (x_0, y_0) addera $(x_1 - x_0, y_1 - y_0)$,

som är en lösning till ekvationen $ax + by = 0$. Omvänt, om (x_0, y_0) är en lösning till ekvationen $ax+by = c$ och (x', y') är en lösning till ekvationen $ax+by = 0$, så kommer (x_0+x', y_0+y') att vara en lösning till ekvationen $ax+by = c$, för $a(x_0+x')+b(y_0+y') = (ax_0+by_0)+(ax'+by') = c+0 = c$. Vi kan alltså ta reda på ALLA lösningar till ekvationen $ax+by = c$ genom att hitta *en* lösning (en partikulärlösning) till denna ekvation och till denna lösning addera *alla* lösningar till motsvarande "homogena" ekvation $ax + by = 0$. Ibland kan man se en partikulärlösning utan räkning. T.ex. har ekvationen $7x + 34y = 1$ lösningen $x = 5, y = -1$ och ekvationen $34x + 37y = 3$ lösningen $x = -1, y = 1$. En metod som alltid fungerar är att hitta en lösning till $ax + by = 1$ genom Euklides algoritm baklänges (se boken) och sedan multiplicera denna lösning med c.

Exempel: Betrakta ekvationen $34x+37y = 3$ och hjälpekvationen $34x+37y = 1$. Vi bestämmer SGD$(34, 37)$ med Euklides algoritm.

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

Den sista likheten ger $1 = 34-11\cdot 3$ och den första ger $3 = 37-34$, vilket ger $1 = 34-11(37-34) = 12 \cdot 34 - 11 \cdot 37$. Hjälpekvationen har alltså en lösning $x = 12, y = -11$, så den ursprungliga ekvationen har en lösning $x = 36 = 3 \cdot 12, y = -33 = 3 \cdot (-11)$.

Det återstår att bestämma den allmänna lösningen till $ax + by = 0$ där SGD$(a, b) = 1$. Om $ax = -by$ och SGD$(a, b) = 1$ måste a dela y (se nedan), så $y = ka$ för något heltal k. Detta ger $x = -kb$, så den allmänna lösningen till $ax+by = 0$ blir $x = -kb, y = ka$, där k är ett godtyckligt heltal.

Exempel: Ekvationen $34x + 37y = 0$ har allmänna lösningen $x = -37k, y = 34k$, så ekvationen $34x + 37y = 3$ har allmän lösning $x = 36 - 37k, y = -33 + 34k$, där k är ett godtyckligt heltal.

I resonemanget ovan användes följande: Om $ax = -by$ för några heltal a, x, b, y och SGD$(a, b) =$ 1, så måste a dela y. Det kan inses på följande sätt. Gör en primfaktoruppdelning av a, x, b, y. Eftersom primfaktoruppdelningen av ett heltal är unik bortsett från ordningen av faktorerna och tecken på dem, så måste precis samma faktorer ingå i ax som i by. Men a och b har inga gemensamma primfaktorer eftersom SGD$(a, b) = 1$, så alla primfaktorer i a måste finnas i y, d.v.s. a delar y. Alternativt kan man resonera så här: Eftersom SGD$(a, b) = 1$ finns tal m och n så $ma + nb = 1$. Detta ger $may + nby = y$. Eftersom a delar både may och nby (a delar ju by), så delar a summan, d.v.s. a delar y.

Anmärkning: Observera likheten i resonemanget ovan med det för lösning av linjära differentialekvationer. För att lösa t.ex. ekvationen $y'' + 3y' + 4y = x$ bestämmer man först *en* lösning (en partikulärlösning), och adderar till den den allmänna lösningen till den homogena ekvationen $y'' + 3y' + 4y = 0$. På motsvarande sätt kan man lösa linjära ekvationssystem $AX = B$. Man kan först bestämma EN lösning och till den addera ALLA lösningar till $AX = 0$. (För linjära ekvationssystem brukar man inte göra så, eftersom det är lika lätt att direkt lösa det inhomogena ekvationssystemet.)

3 Något om algebraiska ekvationer

Vi betraktar i det följande endast polynom med reella koefficienter. En ekvation

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0 \tag{3.1}$$

av grad n med koefficienter $a_k \in \mathbf{R}$ har som bekant högst n rötter i $\mathbf{C}$ (visas med faktorsatsen). Algebrans fundamentalsats säger att det för varje ekvation (3.1) existerar åtminstone en rot. Bevis för denna sats (det finns flera alternativa sådana) kräver någon form av användning av resultat från analysen, t.ex. att varje ekvation av udda grad har en rot. Med upprepad användning av fundamentalsatsen tillsammans med faktorsatsen erhåller vi:

Sats 3.2 *Varje ekvation av grad n med reella koefficienter har exakt n komplexa rötter, varvid rötterna räknas med sin multiplicitet.*

Om (3.1) har rötterna $c_1, c_2, \ldots, c_n$, så har vi

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = a_n(x - c_1)(x - c_2)\ldots(x - c_n). \tag{3.3}$$

Att en rot c har multiplicitet m innebär att faktorn $(x - c)$ förekommer precis m gånger i (3.3).

En enkel men intressant observation är att ickereella rötter uppträder i par:

Sats 3.4 *Om z är en rot till (3.1), så är även $\overline{z}$ en rot.*

BEVIS: Vi vet att för komplexkonjugering gäller att $\overline{z + w} = \overline{z} + \overline{w}$ och $\overline{zw} = \overline{z} \cdot \overline{w}$. För ett polynom $f(x)$ med reella koefficienter får vi därför att $f(\overline{z}) = \overline{f(z)}$ (verifiera detta!). Om $f(z) = 0$, så är därmed även $f(\overline{z}) = 0$. □

En konsekvens av denna sats är att om ett polynom med reella koefficienter är irreducibelt i $\mathbf{R}[x]$, så är det av grad 1 eller 2.

Ett mycket användbart resultat är följande nödvändiga villkor för existens av rationella rötter:

Sats 3.5 *Antag att (3.1) har heltalskoefficienter, dvs. $a_0, \ldots, a_n \in \mathbf{Z}$. Om (3.1) har en rationell rot p/q, där p och q är relativt prima heltal, så gäller att $p|a_0$ och $q|a_n$.*

Speciellt följer att om $a_n = 1$, så måste alla rationella rötter vara heltal.

BEVIS: Vi sätter in p/q i (1), och får efter förlängning med q^n att

$$a_n p^n + a_{n-1}p^{n-1}q + \ldots + a_1 pq^{n-1} + a_0 q^n = 0.$$

Alla termer utom den sista är delbara med p, och därför måste även $a_0 q^n$ vara delbar med p. Eftersom $\mathrm{SGD}(p, q) = 1$, måste p dela a_0. På motsvarande sätt erhålles att q delar a_n. □