Uppgifter och Lösningar till Pass 1: Primtal

• MatteGym • Malmö Universitet • VT 2022 •

https://mattegym.uni.mau.se

Jonathan Nilsson och Magnus Jakobsson

Senast uppdaterad 8 mars 2022

Primtal och delbarhet - Introduktion

Vi säger att "5 delar 30", eftersom 30 kan delas in i 5 stycken lika stora heltalsdelar. Symbolisk skriver vi detta som $5|30$. Att $5|30$ är alltså ett påstående till skillnad från $\frac{5}{30}$ som är ett tal. Mer allmänt:

Definition. *Låt a och b vara två heltal. Vi skriver $a|b$ om $b = a \cdot c$ för något heltal c.*

Med ord kan man säga att "a delar b" eller att "a är en delare till b" eller att "a är en faktor i b" eller att "b är en multipel av a". Alla dessa uttryck betyder samma sak.

Enligt definitionen gäller alltså $5|30$ eftersom det finns ett tal c (nämligen 6) så att $30 = 5 \cdot c$. Det finns även fler tal som delar 30, här är en lista på alla:

$$-30, -15, -10, -6, -5, -3, -2, -1, 1, 2, 3, 5, 6, 10, 15, 30.$$

Ett **primtal** är ett heltal större än 1 som inte kan skrivas som en produkt av två mindre positiva heltal. De första primtalen är $2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$

Heltal större än 1 som inte är primtal kallas för **sammansatta tal**. Dessa kan skrivas som en produkt av primtal, t.ex. är talet 12 produkten av tre primtal: $12 = 2 \cdot 2 \cdot 3$. När samma primtal förekommer flera gånger skriver man ofta detta med hjälp av exponenter:

$$12 = 2^2 \cdot 3 \qquad\qquad 600 = 2^3 \cdot 3 \cdot 5^2.$$

Att på detta vis skriva ett tal som en produkt av primtal kallas att primtalsfaktorisera talet.

Den **största gemensamma delaren** till heltalen m och n är det största heltalet d med egenskapen att $d|m$ och $d|n$. Vi skriver $d = \gcd(m, n)$ för detta tal (från eng. greatest common divisor). Exempelvis har vi $\gcd(30, 42) = 6$ och $gcd(1000, 54321) = 1$.

Diofantiska ekvationer

En diofantisk ekvation är en ekvation där man endast accepterar lösningar som **heltal**.

Exempelvis har den diofantiska ekvationen $x^2 = 4$ två lösningar, $x = \pm 2$, men den diofantiska ekvationen $x^2 = 5$ saknar lösningar eftersom inga heltal x uppfyller ekvationen.

Den diofantiska ekvationen $y^2 = x^3 - x + 1$ beror på två variabler, så lösningar består av heltalspar (x, y) som uppfyller ekvationen. Exempevis är $(x, y) = (1, 1)$ en lösning, och $(x, y) = (3, 5)$ är en annan.

Förberedelseuppgifter med lösningar

1. Basen och höjden i en rektangel ska vara heltal (mätt i cm). Om rektangelns area ska bli $6cm^2$ finns det fyra olika möjliga rektanglar (1×6, 2×3, 3×2, och 6×1). Hur många olika rektanglar finns det om arean ska bli...

   (a) $\ldots 32cm^2$?

   (b) $\ldots 2310cm^2$?

   (c) $\ldots 72cm^2$?

   (d) $\ldots n\ \mathrm{cm}^2$. Försök alltså hitta en allmän formel för antalet rektanglar utifrån primtalsfaktoriseringen för n.

   Lösning: Vi löser sista deluppgiften. Antag att primtalsfaktoriseringen av n ges av

   $$n = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$$

   där $p_1, p_2, \ldots, p_k$ är olika primtal och exponenterna är positiva heltal. Varje positivt heltal d som är en faktor i n kommer att motsvara en rektangel av storlek $d \times \frac{n}{d}$, så vi får svaret genom att hitta antalet sådana faktorer. En faktor till n har formen

   $$d = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

   där $0 \leq a_k \leq m_k$. När vi väljer en faktor har vi alltså totalt $m_k + 1$ möjligheter för talet a_k, och eftersom dessa val är oberoende av varandra får vi totalt

   $$(m_1 + 1)(m_2 + 1) \cdots (m_k + 1)$$

   stycken faktorer. Med denna formel för antalet delare får vi direkt svaren på de övriga deluppgifterna. Eftersom $32 = 2^5$ får vi $(5 + 1) = 6$ olika rektanglar med area $32cm^2$. Vi har $2310 = 2^1 \cdot 3^1 \cdot 5^1 \cdot 7^1 \cdot 11^1$ så antalet rektanglar med area $2310cm^2$ är $(1+1)(1+1)(1+1)(1+1)(1+1) = 32$. Slutligen är $72 = 2^3 \cdot 3^2$ så antalet rektanglar med area $72cm^2$ är $(3 + 1)(2 + 1) = 12$.

2. Gäller $5|0$? Gäller $0|5$? Gäller $0|0$?
   Tips: Använd definitionen av delbarhet!
   Lösning: Enligt definitionen har vi att
   Fem delar noll eftersom $0 = 5 \cdot 0$.
   Noll delar inte fem eftersom inget tal gånger 0 blir 5.
   Noll delar noll eftersom $0 \cdot 17 = 0$ (till exempel)

3. (a) Beräkna $\gcd(120, 18)$ genom att primtalsfaktorisera talen.

   (b) Beräkna $\gcd(1000000000, 246648060)$ med huvudräkning.

   Lösning: På uppgift (a) kan vi skriva $120 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5$ och $18 = 2 \cdot 3 \cdot 3$. En gemensam faktor måste därför innehålla en primtalsfaktor 2 och en primtalsfaktor 3, så $\gcd(210, 18) = 6$. På uppgift (b) noterar vi att $1000000000 = 10^9 = 2^9 \cdot 5^9$, så de enda primtalen som delar detta tal är 2 och 5. Vi har $246648060 = 24664806 \cdot 2 \cdot 5 = 12332403 \cdot 2 \cdot 2 \cdot 5$, och faktorn 12332403 är inte delbar med 2 eller 5, så den största gemensamma delaren är $2 \cdot 2 \cdot 5 = 20$.

4. Primtalsfaktorisera talet 2022. Vilket är nästa primtalsår? Och vilket är nästa efter det?
   Lösning: Man kan testa om ett tal n är ett primtal genom att testa om n är delbart med något av primtalen $2, 3, 5, 7, 11$ o.s.v upp till $\sqrt{n}$. Ganska snabbt ser vi att

$2022 = 2 \cdot 1011 = 2 \cdot 3 \cdot 337$. Genom testa ser man att 337 inte är delbart med primtalen $2, 3, 5, 7, 11, 13, 17, 19$. Därför är 337 ett primtal och vi är klara med faktoriseringen. På samma vis ser man att nästa två primtalsår är 2027 och 2029, ett par av såkallade *tvillingprimtal*. En känd fråga inom talteori är huruvida det finns oändligt många tvillingprimtal eller inte, de flesta matematiker tror detta, men inget bevis finns ännu, läs mer på `https://en.wikipedia.org/wiki/Twin_prime`.

5. En banan kostar 7kr och ett äpple kostar 5kr. Jag handlar bananer och äpplen för 47 kr.

   (a) Hur många bananer/äpplen har jag köpt? Finns det flera möjligheter?

   (b) Hitta *alla* lösningar till den diofantiska ekvationen $7x + 5y = 47$.

   Lösning: Talen är så små att man ganska snabbt kan gissa lösningar, men jag visar ändå en mer systematisk metod som fungerar för alla linjära diofantiska ekvationer (ekvationer på formen $ax + by = c$, där a, b, c är givna heltal där $\gcd(a, b)$ delar c). Denna metod lärs ofta ut på en första kurs i diskret matematik eller algebra. Vi löser först (b). Vi använder Euklides algoritm för att skriva 1 som en kombination av 5 och 7: Vi har $7 = 5 + 2$ och $5 = 2 \cdot 2 + 1$. Alltså är $1 = 5 - 2 \cdot 2 = 5 - 2 \cdot (7 - 5) = (-2) \cdot 7 + 3 \cdot 5$. Multiplicerar vi med 47 får vi $(-94) \cdot 7 + (141) \cdot 5 = 47$, alltså är $(x, y) = (-94, 141)$ *en* lösning till den diofantiska ekvationen $7x + 5y = 47$. Vi adderar och subtraherar en multipel $5 \cdot 7 \cdot k$ till sambandet ovan och förenklar:

   $$(-94) \cdot 7 + (141) \cdot 5 = 47$$

   $$\Leftrightarrow ((-94) \cdot 7 + 5 \cdot 7 \cdot k) + ((141) \cdot 5 - 5 \cdot 7 \cdot k) = 47$$
   $$\Leftrightarrow (-94 + 5k) \cdot 7 + (141 - 7k) \cdot 5 = 47.$$

   För varje heltal k är alltså $(x, y) = (-94 + 5k, 141 - 7k)$ en lösning till den givna diofantiska ekvationen. Vi kan nu använda detta för att lösa (a) (egentligen är det väl enklare att gissa lösningarna, men vår metod fungerar även för större tal). I uppgift (a) måste $x \geq 0$ och $y \geq 0$. Vi har

   $$x \geq 0 \Leftrightarrow -94 + 5k \geq 0 \Leftrightarrow 5k \geq 94 \Leftrightarrow k \geq 19$$

   (den sista ekvivalensen eftersom k är ett heltal). Analogt:

   $$y \geq 0 \Leftrightarrow 141 - 7k \geq 0 \Leftrightarrow 141 \geq 7k \Leftrightarrow k \leq 20.$$

   Vi ska alltså ha $19 \leq k \leq 20$, alltså $k = 19$ eller $k = 20$. Insättning i vår lösningsformel $(x, y) = (-94 + 5k, 141 - 7k)$ ger två lösningar: $(x, y) = (1, 8)$ respektive $(x, y) = (6, 1)$. Det vill säga vi har köpt antingen en banan och åtta äpplen, eller sex bananer och ett äpple.

   Läs mer om den allmänna lösningsmetoden på
   `https://sv.wikipedia.org/wiki/Linj%C3%A4r_diofantisk_ekvation`
   `https://sv.wikipedia.org/wiki/Euklides_algoritm`

Gruppuppgifter med lösningar

1. 100 släckta grödlampor numrerade 1 till 100 står på en rad. När man trycker på en lampknapp skiftas lampan mellan tänd och släckt. 100 personer går in i rummet i tur och ordning. Person 1 trycker på alla lampknappar, person 2 trycker på varannan lampknapp (alltså knapp $2, 4, 6, \ldots$), person 3 trycker på var tredje lampknapp (alltså knapp $3, 6, 9, \ldots$) och så vidare. Vilka lampor är tända när alla hundra personer har passerat?

Tända och släckta lampor efter att person nummer 3 passerat.

Lösning: Vi undersöker om lampa nummer n är tänd eller släckt. Person nummer k klickar på lampknapp n om och endast om $k|n$, lampan kommer alltså att vara tänd om n har ett udda antal delare. Låt $n = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ vara talets primtalsfaktorisering. Enligt förberedelseuppgift 1 är antalet (positiva) delare till n lika med $(m_1+1)(m_2+1)\cdots(m_k+1)$. För att detta ska vara ett udda tal måste alla faktorerna vara udda, alltså är talen m_i jämna. Om $m_i = 2n_i$ får vi

$$n = p_1^{2n_1} p_2^{2n_2} \cdots p_k^{2n_k} = n = (p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k})^2,$$

n är alltså kvadraten av något tal. Alltså kommer lamporna motsvarande kvadrattal att vara tända; lampa $1, 4, 9, 16, 25, 36, 49, 64, 81, 100$. Givetvis fungerar samma argument om vi hade haft ännu fler lampor.
Alternativ lösning: Ett klurigare sätt att lösa uppgiften är med ett symmetriargument - om person nummer d klickar på lampknapp nummer n så kommer även person nummer $\frac{n}{d}$ att klicka på knappen. Alltså kommer i princip alla lampor att bli släckta i slutändan eftersom varje tändare har en motsvarande släckare. Enda undantaget är om person d och $\frac{n}{d}$ är samma person, vilket händer när $n = d^2$ alltså när n är ett kvadrattal.

2. I USA finns en art cikador som har en ovanlig livscykel. De tillbringar mest tid i dvala under jord, men exakt vart sjuttonde år tar de sig fram ur jorden för att föröka sig, gigantiska svärmar cikador kan ses sådana år.

   (a) Benjamin Franklin skrev i sin dagbok att han bevittnade en sådan Cikada-invasion år 1732. Vilket är nästa år då dessa cikador återkommer? (alltså efter 2022)

   (b) Det finns en annan art Cikador som svärmar vart trettonde år istället, de sågs sist 2015. Vilket blir nästa år som dessa två cikada-arter kommer att svärma samtidigt?

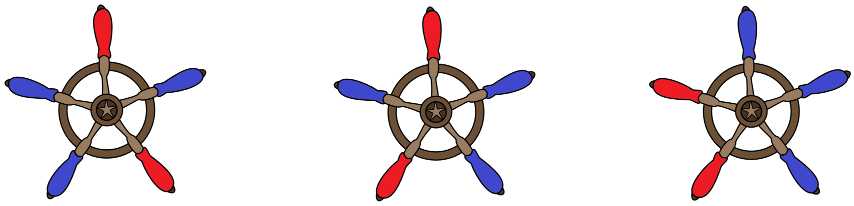
   (c) Både 13 och 17 är primtal, och biologer misstänker att detta inte är en slump. Fundera över vilka evolutionära fördelar som kan finnas med att det just är primtal!

Lösning: Genom att successivt addera multiplar av 17 ser vi att $1732+18\cdot 17 = 2038$ är nästa cikada-år för svärmen u ippgift (a). I (b) uppgiften ser vi att den andra arten cikador kommer fram år $2015, 2028, 2041 \ldots$. Om vi utgår från år 2041 kommer dessa cikador fram på alla år på form $2041+13y$, medans den första stammen kommer fram på år av form $2038+17x$, där x och y är heltal. År där båda kommer fram motsvarar alltså lösningar till den diofantiska ekvationen $2038+17x = 2041+13y$ vilken är ekvivalen med $17x-13y = 3$. Vi kan lösa denna på samma sätt som första förberedelseuppgiften. Med Euklides algoritm blir $17 = 13+4$ och $13 = 3\cdot 4+1$, ur dessa kan vi lösa ut $1 = 13-3\cdot 4 = 13-3\cdot(17-13) = -3\cdot 17+4\cdot 13$. Multiplicerar vi med 3 får vi $3 = (-9)\cdot 17+12\cdot 13$. Jämförelse med vår diofantiska ekvation visar att $(x,y) = (-9,-12)$ är en lösning. $x = -9$ motsvarar årtalet $2038+17x = 1885$, detta var alltså ett år då båda cikadorna kom fram. Eftersom $13\cdot 17 = 221$ är det minsta talet delbart med både 13 och 17 så kommer alla år på formen $1885+k\cdot 221$ att vara årtal då båda cikadastammarna svärmar - nästa gång blir alltså år $1885+221 = 2106$.

Det finns flera teorier till varför det just har utvecklats cikador som svärmar primtalsperiodiskt. Exempelvis gör detta att det är väldigt sällsynt att flera svärmar dyker upp samma år vilken minskar konkurrens om resurser. En annan teori är att någon art som äter cikador skulle kunna synkronisera sin livscykel med cikadorna för att periodiskt få sitt näringstillskott genom att periodiskt dyka upp på år som delar cikada-perioden, men denna strategi fungerar ej när cikada-perioden är primtal. Detta är kanske mer biologi än matematik men kan ändå vara intressant, du kan läsa mer på `https://en.wikipedia.org/wiki/Periodical_cicadas`

3. *(Svår extrauppgift).* Man vill färga pinnarna på ett hjul med röd eller blå färg. Två färgade hjul räknas som lika om man kan rotera det ena och få det andra. Hur många *olika* färgade hjul med fem pinnar finns det? Med 6 pinnar? Med p pinnar där p är ett primtal? Använd detta för att bevisa **Fermats lilla sats**: Om a är ett heltal och p ett primtal så är $a^p - a$ delbart med p.



Tre färgningar av ett hjul med fem pinnar. De två vänstra hjulen räknas som samma eftersom man kan rotera det vänstra $2/5$ varv moturs och få det mellersta. Den högra färgningen är däremot verkligen annorlunda än de första två.

Lösning: Se mig lösa hela uppgiften på en kurs i diskret matematik på Chalmers år 2020:

`https://youtu.be/RnQEwADe8ZA?t=566`

Genom att dela upp i fall beroende på hur många röda pinnar man vill ha ser man ganska snabbt att det finns totalt 8 färgade hjul med 5 pinnar, och med 6 pinnar får vi 14 stycken. Låt oss försöka hitta en mer systematisk lösningsmetod för ett hjul med p pinnar där p är ett primtal. Med p pinnar och två färger finns det 2^p sätt att färga hjulet om man inte tar hänsyn till rotationer (två val av färg för varje pinne). Om vi antar att hjulet inte är enfärgat så har vi $2^p - 2$ sådana hjul. Om vi tar hänsyn till rotationer så ser vi dock att vi här har räknat varje hjul precis p gånger, så det totala antalet olika hjul (ej enfärgade) är $\frac{2^p-2}{p}$. Nu kanske man ser kopplingen till Fermats lilla sats: Om vi istället använder a stycken färger blir antalet olika möjliga hjul (ej enfärgade) lika med $\frac{a^p-a}{p}$. Eftersom detta är antalet sätt att färga hjul måste detta tal vara ett heltal, alltså är $a^p - a$ delbart med p. Detta fungerar faktiskt som bevis för Fermats lilla sats, det är vad som kallas ett kombinatoriskt bevis. Känner man till modulo-räkning så kan det nämnas att Fermats lilla sats vanligare uttrycks som $a^p \equiv a \mod p$, när a är ett heltal och p är ett primtal.