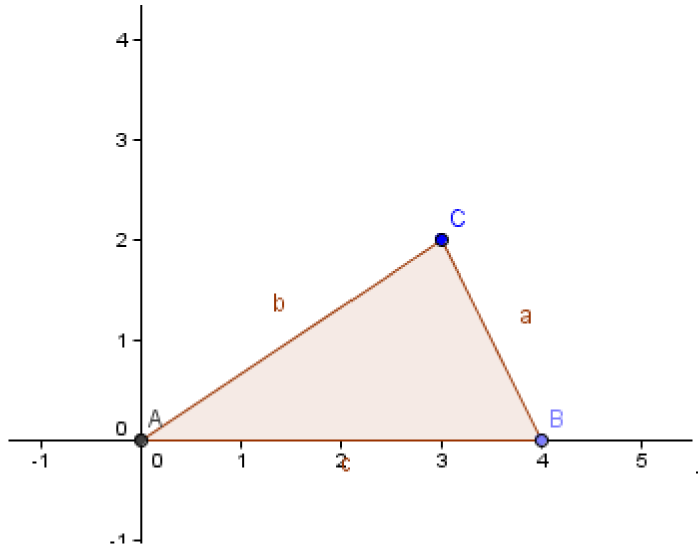
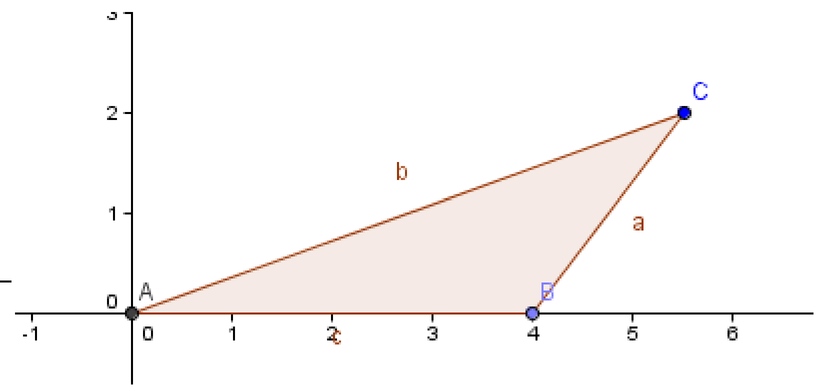
Her er et spørgsmål, du måske aldrig har overvejet: kan man finde to trekanter med samme areal?

Det er ret let at svare på: arealet af en trekant, husker vi fra vor kære folkeskole, findes ved at gange højden med grundlinien og gange med ½. Her kan man se, at arealet af en trekant kun er bestemt af højden og grundlinien. Man kan sagtens to forskellige trekanter, der har samme højde og grundlinie, se bare her:



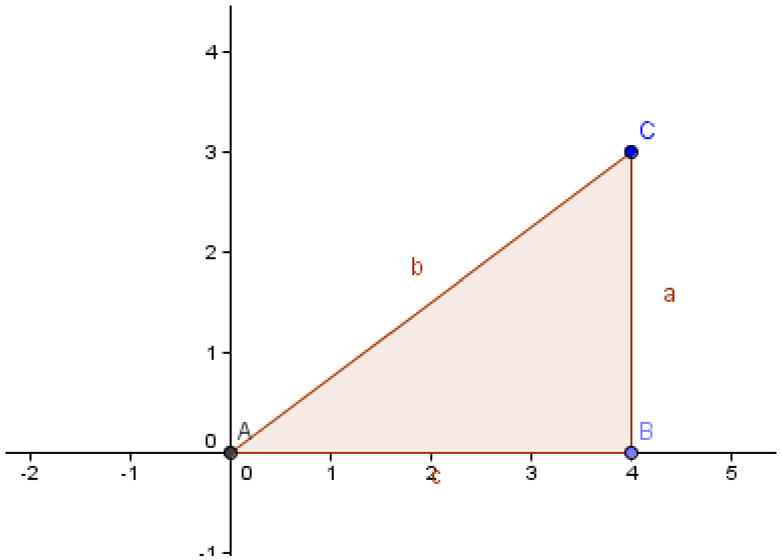


Disse to trekanter har tydeligvis samme grundlinie (4) og samme højde (2), så derfor har de samme areal: ½*4*2 = 4.

Her er et spørgsmål, du sikkert aldrig har overvejet: kan man finde to *retvinklede* trekanter med samme areal?

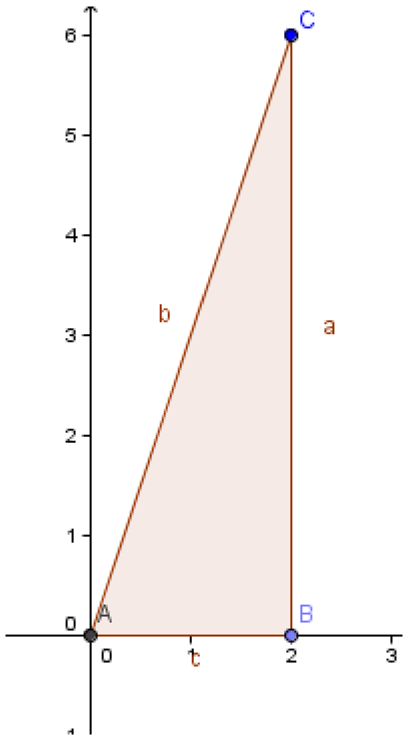
Det er et (lidt) mere kompliceret problem. Når trekanterne skal være retvinklede, bliver den ene katete automatisk grundlinien og den anden katete højden. Pludselig har vi ikke den frihed, jeg havde lige før. Jeg skal i stedet for ændre på længden af begge kateterne, så arealet ender med at være det samme.

Lad os tage et hyggeligt eksempel, den klassiske (3,4,5)-trekant – altså den retvinklede trekant med kateter 3 og 4 og hypotenuse 5. (En hurtig gang Pythagoras efterviser, at den rent faktisk er retvinklet: $3^2 + 4^2 = 9 + 16 = 25 = 5^2$).



Arealet af denne trekant er ½*3*4 = 6.

Nu er det ikke så svært at få en idé – vi kan f.eks. fordoble længden af den ene katete (til 6) og halvere længden af den anden (2).



Så bliver arealet nemlig igen ½*6*2 = 6.

Så vi har løst problemet – to retvinklede trekanter med samme areal.

Her er et spørgsmål, du helt sikkert aldrig har overvejet: kan man finde to retvinklede trekanter med samme areal *og hvor alle siderne kan skrives som brøker eller hele tal*?

Ifølge Pythagoras bliver hypotenusen af den trekant fra før med kateterne 6 og 2 lig med $\sqrt{6^2+2^2}=\sqrt{40}$. Det er sådan set fint nok, men $\sqrt{40}$ er et såkaldt irrationelt tal – det kan ikke skrives som en brøk. Der findes ganske enkelt ikke to hele tal p og q, så $\sqrt{40}=\frac{p}{q}$. Hvis vi altså stiller det krav, at hypotenusen også skal kunne skrives som en brøk, har vi stillet os selv et problem, vi endnu ikke har løst. Kan det lade sig gøre?

Svaret er ja. Og det er overhovedet ikke simpelt.

Det er også et vigtigt problem, fordi det er et skridt på vejen til at kunne angribe det uløste problem indenfor talteori, der hedder ”problemet om de kongruente tal”, som lyder i sin enkelthed ”Givet et helt tal n, kan man så finde en retvinklet trekant, hvor alle sider kan skrives som brøker eller hele tal, som har arealet n?”. Dette problem blev præsenteret for Phimurerlogen af den anerkendte matematiker John Coates i Cambridge sidste år, og det er farligt svært. Det siges, at det er et sværere problem end Fermats Sidste Sætning, et verdensberømt problem, der forblev uløst i 400 år, før et matematisk bevis på små 200 sider blev produceret af Andrew Wiles (en tidligere studerende under John Coates.)

Phimurerlogen har udviklet en metode til at kunne finde flere retvinklede trekanter med rationale sider, der har samme areal. Metoden giver voldsomt præcise resultater, der er helt umulige at gætte sig til. For eksempel er en trekant med følgende sider retvinklet og har arealet 6 (præcist!). Regn selv efter…

$$a = \frac{1470411759186146228788346097638447378632385096234322169830177025825102284298993193835265538073984 01}{1784698080054269335747720824248147353187892880150466352162930585411147359826919611981868268719674 4}$$

$$b = \frac{2141637696065123202897264989097776823825471456180559622595516702493376831792303534378241922463609280}{1470411759186146228788346097638447378632385096234322169830177025825102284298993193835265538073984 01}$$

$$c = \frac{38282870627598124058027263436473454071542681489924701820314936041279368382419444429672863024221282048102305307683054675504581663755927841276758115720421459124252933383997224284932627368440701447 6801}{2624241043508735806564471796442764583007444503849646529252803997087695760054570338847086856407020937797372118475283668490211997266741927258121078271360078372644731911901935335689270712466278006344}$$

Hypotenusen c er en brøk med ca. 200 cifre i både tæller og nævner! De er i øvrigt alle uforkortelige – de kan ikke skrives pænere. Hvordan i alverden kommer man frem til sådan et resultat? Jeg vil i det følgende dokumentere Phimurerlogens arbejdsproces.

TRIN 1:**En parametricering af alle rationale retvinklede trekanter**

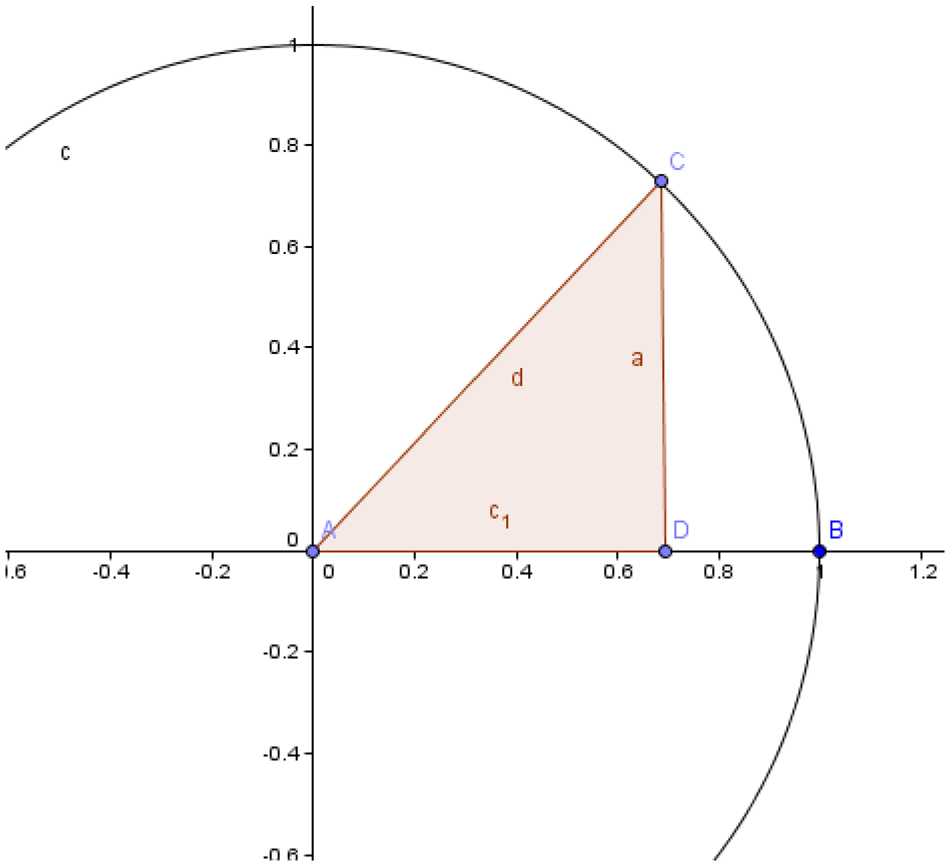
Hvis der er noget,matematikere godt kan lide at gøre, så er det at opfinde svære ord og symboler til at beskrive ting. ”Parametricering” er et eksempel på et sådant ord. Et andet begreb er et, Phimurerlogen selv indførte, nemlig *RRTer*, der står for ”rationale retvinklede trekanter” – netop den slags retvinklede trekanter med heltallige eller brøk-sider, vi snakker om her.

Phimurernes første problem var nemlig overhovedet at kunne skelne RRTer fra alle andre retvinklede trekanter. Trekanten med kateterne 3 og 4 er en RRT, mens trekanten med kateterne 6 og 2 ikke er det. Hvordan kender man forskel?

Ideen bestod i at udnytte det begreb, som alle gymnasieelever kommer igennem i løbet af 1.g, nemlig *forstørrelsesfaktoren.* Man kan kort sagt gange alle siderne i et trekant med det samme tal F (forstørrelsesfaktoren) uden at det ændrer på vinklerne. Det betyder, at så længe man bruger en brøk som en forstørrelsesfaktor på en RRT, får man en ny RRT. (Fordi den rette vinkel bliver ved med at være ret, og eftersom to brøker ganget sammen stadig giver en brøk, ender trekanterne med at have tre sider, der kan skrives som brøker.) Den nye RRT har dog ikke det samme areal som den første. Den skarpe læser kan se, at hvis en trekant med areal T bliver ganget op med forstørrelsesfaktoren F, bliver det nye areal $F^2 \cdot T$.

Eftersom man frit kan gange RRTer op med rationale forstørrelsesfaktorer, er det nok at kigge på RRTer med hypotenuse 1. (Så kan vi få alle andre RRTer ved bare at skalere med den ønskede hypotenuselængde.)

Nu er det gode ved retvinklede trekanter med hypotenusen 1, at de alle sammen passer perfekt ind i en enhedscirkel:



Det endnu mere smarte er, at kateternes længde netop er punktet C's koordinater. Hvis punktet C altså har rationale koordinater, har vi automatisk en RRT! Og vi har endda samtlige RRTer med hypotenuselængde 1 (og dermed, via skalering, alle andre RRTer også) hvis vi kan finde en måde at finde samtlige rationale punkter på enhedscirklen.

Det, vi gjorde, var at erkende, at en ret linie med forskriften $y = ax + b$, når den skærer enhedscirklen $x^2 + y^2 = 1$, giver anledning til en andengradsligning. Vi beviste, at en andengradsligning med rationale koefficienter og d>0 har enten to rationale løsninger eller to irrationale løsninger. Hvis vi altså valgte *a* og *b* i liniens ligning som rationale tal , og sørgede for at tvinge den ene af de to løsninger til at være et rationalt tal, måtte den anden løsning også være det. Og eftersom løsningerne jo angav x-værdier til skæringspunkter mellem linie og enhedscirkel – og dermed altså punkter, der ligger på enhedscirklen – kunne man ved at variere hældningen *a* gennem alle mulige rationale tal, der giver d>0, finde alle rationale punkter på cirklen! (Eftersom hældningen er rational, vil y-værdien til dette skæringspunkt ligeledes være rational.)

Ved at vælge en linie, der altid skar igennem (-1,0) og alle rationale hældninger mellem 0 og 1 rammer man hele den del af enhedscirklen, der ligger i 1.kvadrant, som er de interessante punkter. Med almindelig geometri finder man ud af i sidste ende, at:

SÆTNING 1

Hvis (a,b,c) er sider i en RRT, findes der rationale tal p og q, således at

$$a = p^2 - q^2$$

$$b = 2pq$$

$$c = p^2 + q^2$$

Altså kan man beskrive alle RRTer ved hjælp af to tal, p og q, i stedet for de tre tal (a,b,c). At problemet hermed bliver todimensionelt, giver anledning til at forvente, at man kan tegne en kurve i et almindeligt (x,y)-koordinatsystem, der siger noget interessant om problemet.

TRIN TO: At finde en kurve, der passer.

Efter nogle falske starter fandt vi endelig en naturlig måde at konstruere netop sådan en kurve. Hvis man fastholder *q* i formlerne fra sætning 1 (lad os kalde den N) og lader *p* variere frit (og omdøber den til x, så vi husker, at det er vores frie variabel), får vi altså trekanter med kateterne $x^2 - N^2$ og $2xN$. Det er ikke svært at se, at arealet af sådan en trekant bliver

$$N(x^3 - N^2x)$$

Hvis vi ønsker at beskrive alle trekanter med et fast areal, kan vi faktisk opnå det ved at skalere trekanten ned med en skalafaktor, der er variabel og afhængig af x (den kalder vi af præcist disse grunde for y), som opfylder, at

$$y^2 = x^3 - N^2x$$

Vi skalerer altså trekanten ned, så siderne bliver

$$a = \frac{x^2 - N^2}{y}$$

$$b = \frac{2xN}{y}$$

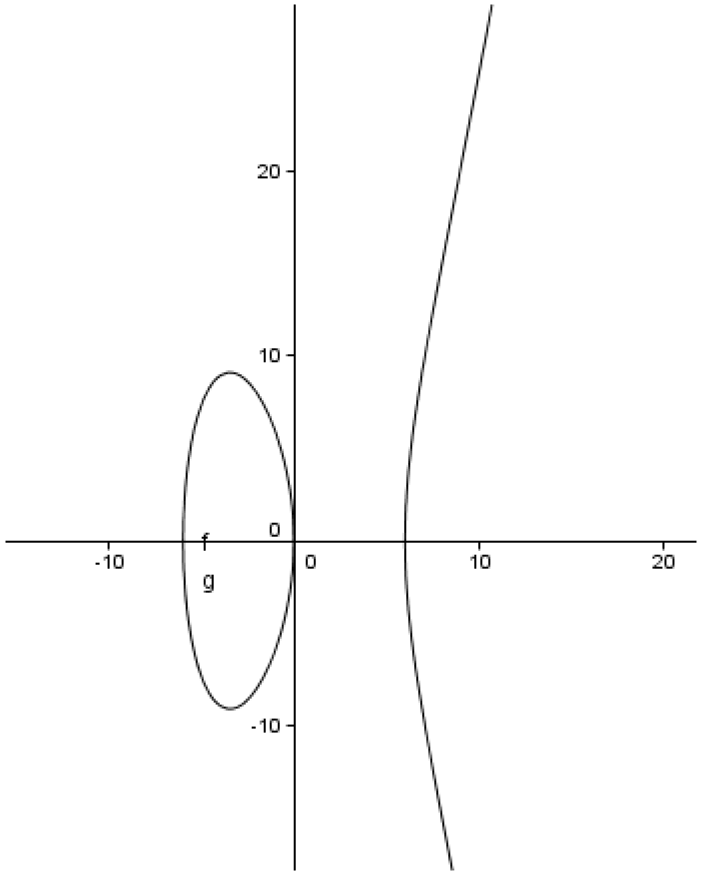
$$c = \frac{x^2 + N^2}{y}$$

Så bliver arealet af trekanten netop

$$\frac{N(x^3 - N^2x)}{y^2} = N$$

Vi kan altså konstatere, at så længe sammenhængen $y^2 = x^3 - N^2x$ er opfyldt, kan vi bruge de ovenstående formler til at lave retvinklede trekanter med areal N. Der er kun ét problem… for at vi skal ende med at have en RRT, skal a,b og c jo være rationale tal, og det bliver de kun, hvis x og y (og N) er rationale. Sammenhængen $y^2 = x^3 - N^2x$ giver selvfølgelig ikke kun rationale koordinater, så problemet er altså endt med at skulle finde rationale punkter på den kurve, der beskriver denne sammenhæng.

For at illustrere problemet, tegner jeg lige grafen for $y^2 = x^3 - N^2x$, når arealet N skal være 6:



Det er en lidt løjerlig sag. Det bliver ikke bedre af, at vi fra et gammelt bevis af Fermat, som vi læste i starten af året, allerede godt ved, at der findes kurver af denne type (som i øvrigt hedder *elliptiske kurver*) som slet ikke har et eneste rationelt punkt overhovedet!

TRIN TRE: PROCESSEN TIL AT SKABE NYE RATIONALE PUNKTER UD FRA ET GAMMELT

En utrolig vigtig erkendelse, som vi fik efter lange studier af elliptiske kurvers egenskaber (vi ved rigtigt meget om dem!) er, at hvis man har givet et rationelt punkt på kurven, kan man finde et nyt rationelt punkt på kurven via en metode, der minder en del om tricket med enhedscirklen fra før. Isolerer man y i sammenhængen, får man nemlig (i den positive halvdel)

$$y = \sqrt{x^3 - N^2 x}$$

Differentierer man den, får man

$$\frac{dy}{dx} = \frac{3x^2 - N^2}{2\sqrt{x^3 - N^2 x}} = \frac{3x^2 - N^2}{2y}$$

Altså bliver hældningen til tangenten til kurven i et rationalt punkt (x,y) selv et rationalt tal. En skæring mellem denne tangent og den elliptiske kurve vil – af samme grunde som ovenfor – være et nyt rationelt punkt!

I princippet er man færdige her, hvis det ikke var fordi, at man løber panden mod en tredjegradsligning af helt ufattelig voldsom kompleksitet. Prøv selv.

Vi fik endelig kontrol over ligningen ved at skrive den helt ud og eksplicit opskrive koefficienterne til 2.gradsleddet, 1. Gradsleddet og 0.gradsleddet (og vi sørgede selvfølgelig for, at den ledende koefficient var 1. Man rydder vel op efter sig selv.). Eftersom vi kendte en dobbeltrod til polynomiet i forvejen (røringspunktet mellem tangenten og kurven), vidste vi også, at det samme polynomium kunne skrives som $(x - x_o)^2(x - x_1)$, hvor x_o var tangentens røringspunkt og x_1 det nye, ukendte skæringspunkt. Ved at skrive de (meget simplere) koefficienter ud her kunne vi direkte stille tre ligninger op ved at sammenholde koefficienter én for én og isolere x_1. Dette gav en (hysterisk grim) formel for bestemmelse af et nyt rationelt punkt på den elliptiske kurve.

Endelig kunne vi regne nye RRTer ud med det samme areal som (3,4,5)-trekanten. Ved at udtrykke x og y ved a,b og c oversætter man trekanten til punktet (12,36) på den elliptiske kurve $y^2 = x^3 - 36x$. Ved at konstruere tangenten i det punkt udregnes så et nyt skæringspunkt, som oversættes tilbage til nye værdier af a,b og c. Ved at gentage denne proces sølle 4 gange får man den vildeste brøk, som TI-interactive kan håndtere (og ingen af os er særligt motiveret til at regne videre i hånden), nemlig de ovenstående, sindssyge brøker. Så vidt jeg ved, er det første gang, at lige netop den trekant med arealet 6 har set dagens lys. Det er da meget sjovt.

TRIN FIRE: Videre i teksten

Vores arbejde består nu i at undersøge problemet om de kongruente tal lidt nærmere. Som vi har set, er problemet det samme som at spørge, på hvilket elliptiske kurver på formen $y^2 = x^3 - N^2x$ har rationale punkter på sig. Hertil kan det være væsentligt at kigge på en sætning fra 1922 af Mordell, der siger, at alle rationale punkter på en elliptisk kurve er en linearkombination af et elementer fra en fast endelig mængde af punkter R (ved brug af en komposition på den elliptiske kurve, der skaber en gruppestruktur.) Opgaven er så at bestemme størrelsen af en sådan mængde (og finde ud af, hvornår den mængde indeholder mere end 0 elementer.) Hvis det lyder svært, så er det det også.

/Phimurerlogen, april 2010.