SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Diofantiska ekvationer

av

Erik Bergström Björlund

2022 - No K33

Diofantiska ekvationer

Erik Bergström Björlund

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Sofia Tirabassi

2022

Abstract

A diophantine equation is an equation where only integer solutions are sought after. The pythagorean equation, $x^2 + y^2 = z^2$, is a type of diophantine equation where we can find three integers x, y, z that solves the equation. These numbers are called *pythagorean triples*.
An example of a diphantine equation is the *Pell equation*, $x^2 - ny^2 = 1$. The equation has a special connection to the irrational number $\sqrt{2}$, and we will also find a method for generating an infinite number of solutions to the equation.

Sammanfatting

En diofantisk ekvation är en ekvation där endast heltalslösningar eftersöks. Pythagoras ekvation, $x^2 + y^2 = z^2$ är en typ av diofantisk ekvation där vi kan hitta tre tal x, y, z som löser ekvationen. Dessa tal kallas för *pythagoresiska tripletter*.
Ett exempel på en diofantisk ekvation är *Pells ekvation*, $x^2 - ny^2 = 1$. Ekvationen har en speciell koppling till det irrationella talet $\sqrt{2}$, och det ska även visa sig finnas en metod för att generera oändligt många lösningar till ekvationen.

Innehåll

1

Bakgrund och arbetets innehåll

En diofantisk ekvation är en ekvation där endast heltalslösning efterfrågas. Namnet kommer från den grekiske matematikern Diofantos som levde cirka 250 e.Kr

1.0.1 Pythagoras ekvation och pythagoresiska tripletter

En av de kändaste diofantiska ekvationerna, vilken även ligger till stor grund för detta arbete är *Pythagoras ekvation*, $x^2 + y^2 = z^2$. Ekvationen används för att beräkna längden av hypotenusan i en rätvinklig triangel, och är en viktig del av geometri och trigonometri.

Talen x, y, z i ekvationen, vilka fortsättningsvis kommer benämnas som *Pythagoresiska tripletter*, är det som en stor del av detta arbete kommer att avhandla. Vi kommer leta efter och förklara olika tillvägagångssätt att finna sådana tripletter, där avstamp tas från det som beskrivits som den första trigonometriska tabellen, *Plimpton 322*.

Vi fortsätter sedan med att förklara *Euklides formel för pythagoresiska tripletter*, vilken är till för att generera pythagoresiska tripletter med hjälp av godtyckliga tal. Formeln visar sig sedan ha en koppling till både *Diofantus kordametod*, vilket är ett sätt att hitta pythagoresiska tripletter bland de rationella talen med hjälp av en korda dragen i enhetscirkeln, där lutningen på kordan bestämmer värdet på de pythagoresiska tripletterna.

Vi fortsätter sedan vidare en bit och tittar på hur en utveckling av kordametoden kan användas för att hitta lösningar till ekvationer med kubiska termer, där vi med hjälp av tangenten till en kurva kan hitta oändligt många lösningar till ekvationer med kubiska termer.

Den sista metoden för att generera tripletterna är med hjälp av de komplexa talen, närmare bestämt de *Gausiska heltalen*. Här ser vi hur, med användning av det imaginära talet i, kan hitta ytterligare ett sätt att generera pythagoresiska tripletter.

1.0.2 Pells ekvation

Avslutningsvis går vi igenom den diofantiska ekvationen *Pells ekvation*, $x^2 - ny^2 = 1$, en ekvation från 400 f.Kr. Här tittar vi bland annat på hur ekvationen kan användas för att ge en rationell approximering av det irrationella talet $\sqrt{2}$, samt hur vi kan hitta en generell lösning till ekvationen för alla tal n.

2

Pythagoras ekvation

Pythagoras ekvation $x^2 + y^2 = z^2$ används för att räkna ut längden av hypotenusan i en rätvinklig triangel. Ekvationen är namngiven efter den grekiska filosofen Pythagoras, född 570 f.Kr.

Trots att Pythagoras anses vara grundare av ekvationen finns det flertalet bevis för att ekvationen användes innan detta, det första exemplet återfinns på en lertavla från 1750-1790 f.Kr, kallad Plimpton 322 (se Tabell 1).

y	z
119	169
3367	4825
4601	6649
12709	18541
65	97
2291	3541
799	1249
481	769
4961	8161
45	75
1679	2929
161	289
1771	3229
56	106

Tabell 1: Plimpton 322

Lertavlan innehåller inga x-värden, men då varje par y och z insatt i pythagoras ekvation ger ett kvadrattal är listan alltså en uppsättning av 15 *Pythagoresiska trippletter*, vilket är tre tal (x, y, z) som löser pythagoras ekvation.

Exempel 2.1. Vi testar de sista fem tripletterna i tabellen.

z	y	z^2-y^2	$\sqrt{z^2-y^2}$
106	56	8100	90
3229	1771	7290000	2700
289	161	57600	240
2929	1679	5760000	2400
75	45	3600	60

Tabell 2: Test av Plimpton

Då $x^2 = z^2 - y^2$ och $x = \sqrt{z^2-y^2}$ representerar den tredje kolumnen x^2-värden och den fjärde kolumnen x-värden. Vi kan alltså se att tabellen innehåller z och y-värden från pythagoras ekvation.

2.1 Euklides formel

Ett sätt att generera pythagoreiska tripletter bland heltalen är med hjälp av Euklides formel, vilken lyder:

$$x = (u^2 - v^2)w, \quad y = 2uvw, \quad z = (u^2+v^2)w. \tag{1}$$

där u, v, och w är positiva heltal, med $u > v$.
Vi ska nu kontrollera att euklides formel faktiskt genererar pythagoresiska tripletter:

Bevis. Då det är givet att x, y, z är heltal behöver vi endast kontrollera att $x^2+y^2 = z^2$ för alla värden (u, v, w). För att göra det räknar vi först ut x^2 och y^2:

$$x^2 = u^4w^2 - 2u^2v^2w^2 + v^4w^3,$$
$$y^2 = 4u^2v^2w^2.$$

Sätter vi sedan in dessa värden i pythagoras ekvation får vi:

$$\begin{aligned} x^2 + y^2 &= u^4w^2 - 2u^2v^2w^2 + v^4w^2 + 4u^2v^2w^2 \\ &= u^4w^2 + v^4w^2 + 2u^2v^2w^2 \\ &= \left(u^2w + v^2w\right)^2 = z^2. \end{aligned}$$

Därför kan vi tydligt se att $x^2 + y^2 = z^2$. □

2.2 Diophantus kordametod

Euklides formel är ett bra sätt att generera pythagoresiska tripletter bland heltalen. Ett sätt att hitta trippletter bland de rationella talen är med hjälp av Diophantus korda-metod.
Vi väljer tre heltal (a, b, c) med $c \neq 0$ som uppfyller $x^2 + y^2 = z^2$ får vi:

$$a^2 + b^2 = c^2.$$

Delar vi bägge sidor med c^2 får vi:

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1$$

Sedan skriver vi om detta med de rationella variablerna X och Y:

$$X = \left(\frac{a}{c}\right), Y = \left(\frac{b}{c}\right).$$

Med denna omskrivning ser vi att $X^2 + Y^2 = 1$. Alltså är punkten (X, Y) en punkt med rationella koordinater på enhetscirkeln.

Väljer vi nu en punkt $B = (-1, 0)$ och drar en korda från denna med lutningen m kommer den kordan att ha ekvationen $Y = m(X + 1)$. Kordan kommer skära cirkeln i en godtycklig punkt som vi kan benämna C. Vi kan räkna ut koordinaterna för punkten C genom att substituera in kordans ekvation i ekvationen för enhetscirkeln:

$$Y^2 = m^2(X + 1)^2, \quad X^2 + m^2(X + 1)^2 = 1.$$

Utvecklar vi och skriver om uttrycket får vi:

$$(m^2 + 1)X^2 + 2m^2X + m^2 - 1 = 0.$$

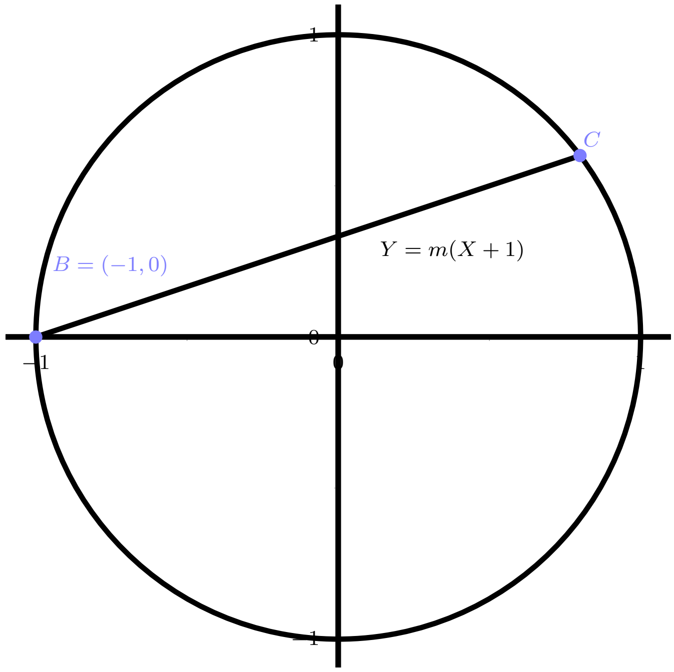
Med hjälp av pq-fomeln kan vi räkna ut X-värdena, och får:

$$X = \frac{-2m^2 \pm \sqrt{4m^4 - 4(m^4 - 1)}}{2m^2 + 2} = \frac{-2m^2 \pm \sqrt{4}}{2m^2 + 2}.$$

Detta ger oss X-värdena:

$$X = -1, \frac{1-m^2}{1+m^2}.$$

X= -1 är ju punkten B, men med hjälp av lösningen X=$\frac{1-m^2}{1+m^2}$ kan vi nu substituera in detta i $Y = m(X+1)$ och få $Y = m\left(\frac{1-m^2}{1+m^2}+1\right) = \frac{2m}{1+m^2}$.
I Figur 1 ser vi den geometriska representationen av vad vi gjorde.



Figur 1: Kordametoden

Detta innebär alltså att vi kan uttrycka den godtyckliga punkten C på enhetscirkeln med koordinaterna $(\frac{1-m^2}{1+m^2}, \frac{2m}{1+m^2})$. Då vi vet att m är ett rationellt tal kan vi välja att uttrycka det som som $m = \frac{v}{u}$, vilket leder till att att punkten C kan skrivas med koordinaterna:

$$C = \left(\frac{1-\frac{v^2}{u^2}}{1+\frac{v^2}{u^2}}, \frac{2\frac{v}{u}}{1+\frac{v^2}{u^2}}\right) = \left(\frac{u^2-v^2}{u^2+v^2}, \frac{2uv}{u^2+v^2}\right).$$

Då koordinaterna i C är rationella kan vi välja att uttrycka punkterna som bråk, exempelvis $\left(\frac{x}{z}, \frac{y}{z}\right)$ och få:

$$\frac{x}{z} = \frac{u^2-v^2}{u^2+v^2}, \quad \frac{y}{z} = \frac{2uv}{u^2+v^2}.$$

Vilket leder till:

$$x = u^2 - v^2, \quad y = 2uv, \quad z = u^2 + v^2.$$

Återgår vi nu till Eukildes formel kan vi se den uppenbara likheten mellan uttrycken, där Euklides formel lyder:

$$x = (u^2 - v^2)w, \quad y = 2uvw, \quad z = (u^2 + v^2)w.$$

Vi har alltså lyckats uttrycka de rationella talen i Diophantus kordametod med hjälp av heltalen från Euklides formel. Skillnaden är termen w i Euklides formel, men då den termen återfinns i både x, y och z kan den förkortas bort.
Det finns även en utveckling av diofantus kordametod för ekvationer av kubiska termer. Denna finns att läsa om i bilaga A

2.3 Pythagoreiska tripletter och gausiska heltal

Vi har än så länge gått igenom olika sätt att hitta pythagoresiska tripletter bland de rationella talen. Fortsätter vi vidare kan vi även hitta pythagoresiska tripletter bland de komplexa talen, närmare bestämt de gausiska heltalen.

2.3.1 Gausiska heltal och primtal

Definition 2.2. Ett gausisk heltal är ett är ett komplext tal $a + bi$ där a och b är heltal.

Ett gausiskt primtal är ett gausiskt heltal $a + bi$ som är irreducibelt, det kan alltså inte delas upp i olika faktorer, bortsett från enhetsfaktorerna $1, -1, i, -1$. För att undersöka om ett gausiskt heltal är prim behöver vi undersöka talets norm:

$$norm(a + bi) = |a + bi|^2 = a^2 + b^2.$$

Om ett gausiskt heltals norm är ett (rationellt) primtal vet vi att det är ett gausisk primtal. Vi kan till exempel se att talet 2 inte är ett gausisk primtal:

$$norm(2) = |2|^2 = 4$$

Där 2 kan faktoriseras som $(1 + i)(1 - i)$.
Det gausiska heltalet (5+2i) är däremot ett gausiskt primtal, då det har normen

$$norm(5 + 2i) = |5 + 2|^2 = 29.$$

Där 29 är ett rationellt primtal.
I fallet där $b = 0$ behöver två saker stämma för att vi kan säga att a är ett gausiskt primtal:

1. a måste vara ett primtal.
2. $|a| \equiv 3 \pmod{4}$, alltså att a kan skriva som $a = 4n + 3$.

Exempel 2.3. Talet 5 är inte ett gausiskt primtal då $5 \equiv 1 \pmod 4$ och har faktoriseringen $(2 + i)(2 - i)$. 7 är däremot ett gausiskt primtal då $7 \equiv 3 \pmod 4$.

2.3.2 Gausiska primtal och pythagoreiska tripletter

Pythagoras ekvation har den komplexa faktoriseringen $x^2 + y^2 = (x - yi)(x + yi)$ där vi har det imaginära talet i med egenskapen $i = \sqrt{-1}$.
Egenskapen kan vi använda för att hitta nya pythagoresiska tripletter, men för att göra det måste vi först definiera och bevisa det som kallas *"två kvadrats-identiteten"* (2), vilken förklarar att *summan av två kvadrater multiplicerat med summan av två kvadrater alltid kommer vara summan av två kvadrater*, dvs:

$$(a_1^2 + b_1^2)(a_2^2 + b_2^2) = (a_1a_2 - b_1b_2)^2 + (a_1b_2 + b_1a_2)^2. \tag{2}$$

Med hjälp av egenskapen för i kan vänsterledet faktoriseras som:

$$(a_1^2 + b_1^2)(a_2^2 + b_2^2) = (a_1 - b_1i)(a_1 + b_1i)(a_2 + b_2i)(a_2 - b_2i).$$

Väljer vi nu att multiplicera ihop den första parentesen med den sista, och den andra parentesen med den tredje får vi:

$$((a_1a_2 - b_1b_2) - i(a_1b_2 + a_2b_1))((a_1a_2 - b_1b_2) + i(a_1b_2 + a_2b_1)) =$$

$$= (a_1a_2 - b_1b_2)^2 + (a_1b_2 + b_1a_2)^2.$$

Med hjälp av identiteten kan vi göra följande antagande: Om det finns två pythagoresiska tripletter (a_1, b_1, c_1) och (a_2, b_2, c_2), måste även $(a_1a_2 - b_1b_2, a_1b_2 + b_1a_1, c_1c_2)$ vara en pythagoresisk triplett.
Beviset följer av identiteten, då vi vet att:

$$a_1^2 + b_1^2 = c_1^2, \quad a_2^2 + b_2^2 = c_2^2.$$

Multiplicerar vi ihop båda ekvationerna får vi:

$$(a_1^2 + b_1^2)(a_2^2 + b_2^2) = (c_1c_2)^2.$$

Enligt identiteten kan detta skrivas som:

$$(a_1a_2 - b_1b_2)^2 + (a_1b_2 + b_1a_2)^2 = (c_1c_2)^2.$$

Vilket visar att $(a_1a_2 - b_1b_2, a_1b_2 + b_1a_1, c_1c_2)$ är en pythagoresisk triplett.

Vidare kan vi hitta ytterligare kopplingar mellan de gausiska heltalen och de pythagoreriska tripletterna. Väljer vi att faktorisera pythagoras ekvation som $z^2 = x^2 + y^2 = (x - yi)(x + yi)$ kan vi säga att, då x och y är relativt prima så är även $x - yi$ och $x + yi$ det. Detta leder till att termerna $x - yi$ och $x + yi$ är kvadrater, eftersom att de är faktorer av kvadraten z^2. Alltså kan vi skriva:

$$x - yi = (u^2 - v^2)$$

Där u och v är reela tal, vilket leder till omskrivningen:

$$x - yi = (u^2 - v^2) - 2uvi$$

Där vi kan ge x och y värden utefter vilken del som är reel och imaginär, alltså får vi:

$$x = u^2 - v^2 \quad y = 2uv.$$

Vi har alltså ännu en gång återkommit till Euklides formula för pythagoresiska tripletter.

3

Pells ekvation

En diofantisk ekvation på formen $x^2 - ny^2 = 1$ där n är ett heltal, kallas för *Pells ekvation*.
Pells ekvation på formen $x^2 - 2y^2 = 1$ kan spåras tillbaka till cirka 400 f.Kr., vilket gör den till en av de äldsta kända ekvationerna inom matematiken.
För att hitta lösningar till Pells ekvation är det viktigt att talet n inte är en heltalskvadrat, då vi i detta fall hamnar i situationen där vi kan faktorisera $x^2 - ny^2 = 1$ som $(x + y\sqrt{n})(x - y\sqrt{n}) = 1$, där $\sqrt{n}$ är ett heltal. Detta leder till att $(x + y\sqrt{n})$ och $(x - y\sqrt{n})$ kommer vara heltal, alltså måste $(x + y\sqrt{n}) = 1$ och $(x - y\sqrt{n}) = 1$, vilket endast inträffar då $(x, y) = (1, 0)$.

3.1 Ekvationen $x^2 - 2y^2 = 1$

3.1.1 Talet $\sqrt{2}$

Pells ekvation då $n = 2$ har en speciellt koppling till talet $\sqrt{2}$. Faktum är att ekvationen $x^2 - 2y^2 = 1$ kan användas för att approximera talet $\sqrt{2}$.

Exempel 3.1. Delar vi ekvationen $x^2 - 2y^2 = 1$ med y^2 får vi:

$$\frac{x^2}{y^2} = 2 + \frac{1}{y^2}.$$

Låter vi sen $y \to \infty$ ser vi att:

$$\lim_{y \to \infty} \left(2 + \frac{1}{y^2}\right) = 2$$

Det betyder alltså att $\sqrt{\frac{x^2}{y^2}} = \frac{x}{y} \to \sqrt{2}$ då y växer. Vi har alltså lyckats skapa en rationell approximering av det irrationella talet $\sqrt{2}$.

3.1.2 Heltalslösningar till $x^2 - 2y^2 = 1$

För att hitta heltalslösningar till ekvationen $x^2 - 2y^2 = 1$ behöver vi först fördjupa oss lite i irrationella tal.
Som känt är ett irrationellt tal ett reelt tal som inte kan skrivas som ett bråk. En annan egenskap av irrationella tal, och något vi kommer ha användning för, är hur vi kan välja att representera dom. Precis som med de gausiska heltalen, där vi kunde dela upp talet i en reel och en imaginär del, kan vi med de irrationella talen dela upp de i en rationell del a och en irrationell del $b\sqrt{n}$, där (a, b) är heltal. För att hitta rationella lösningar till $x^2 - 2y^2 = 1$ kan vi använda oss av Diofantos kordametod, som vi gick igenom i 2.2. När det kommer till att hitta heltalslösningar kan vi använda oss av följande sats:

Definition 3.2. Om (x_1, y_1) och (x_2, y_2) är lösningar till $x^2 - 2y^2 = 1$ så är även (x_3, y_3) det, där x_3 och y_3 definieras av:

$$(x_1 + y_1\sqrt{2})(x_2 + y_2\sqrt{2}) = x_3 + y_3\sqrt{2}.$$

Vi kan bevisa detta genom att samla ihop alla rationella termer för sig, och de irrationella för sig:

$$(x_1 + y_1\sqrt{2})(x_2 + y_2\sqrt{2}) = (x_1x_2 + 2y_1y_2) + (x_1y_2 + x_2y_1)\sqrt{2}.$$

$$x_3 = x_1x_2 + 2y_1y_2, \quad y_3 = x_1y_2 + x_2y_1.$$

Sätter vi sedan in dessa värden i Pells ekvation $(n = 2)$ får vi:

$$(x_1x_2 + 2y_1y_2)^2 - 2(x_1y_2 + x_2y_1)^2 =$$

$$= (x_1x_2^2 + 4x_1x_2y_1y_2 + 4y_1y_2^2) - 2(x_1y_2^2 + 2x_1x_2y_1y_2 + x_2y_1^2) =$$

$$(x_1x_2^2 + 4y_1y_2^2) - 2(x_1y_2^2 + x_2y_1^2) = (x_1^2 - 2y_1^2)(x_2^2 - 2y_2^2) = 1.$$

Då vi utgick ifrån att (x_1, y_1) och (x_2, y_2) var lösningar till ekvationen vet vi att $(x_1^2 - 2y_1^2)(x_2^2 - 2y_2^2) = 1$. Vi har alltså hittat ett sätt att generera heltaltslösningar till Pells ekvation då $n = 2$.
Vi testar att generera en lösning med hjälp av den triviala punkten $(3, 2)$:

Exempel 3.3. Vi väljer $(x_1, y_1) = (x_2, y_2) = (3, 2)$ Vi sätter in värdena i $(x_1 +$

$y_1\sqrt{2})(x_2 + y_2\sqrt{2}) = x_3 + y_3\sqrt{2}$ och får:

$$(3 + 2\sqrt{2})^2 = (9 + 12\sqrt{2} + 8) = 17 + 12\sqrt{2}.$$

Här får vi fram den rationella delen $x_3 = 17$ och den irrationella delen $y_3 = 12$. Fortsätter vi vidare kan vi nu välja $(x_1, y_1) = (17, 12)$ och $(x_2, y_2) = (3, 2)$ och få:

$$(17 + 12\sqrt{2})(3 + 2\sqrt{2}) = (51 + 70\sqrt{2} + 48) = 99 + 70\sqrt{2}.$$

Här får vi fram punkten $(99, 70)$. Vi kan sedan repetera proceduren och få oändligt många heltalslösningar för Pells ekvation då $n = 2$.

3.2 Pells ekvation då $n \neq 2$

Fortsätter vi vidare och tittar på fallet då $n \neq 2$, alltså ekvationen $x^2 - ny^2 = 1$, hittar vi direkt likheter med fallet då $n = 2$. Exakt som med de gausiska heltalen, som kunde definieras som $\mathrm{Z}[i] = \{a + bi : a, b \in \mathrm{Z}\}$, kan vi definiera talet $\mathrm{Z}[\sqrt{n}] = \{x + y\sqrt{n} : x, y \in \mathrm{Z}\}$, det vill säga talet $x + y\sqrt{n}$ där x och y är heltal. Exakt som för fallet då $n = 2$ där vi använde oss av $x + y\sqrt{2}$ för att finna lösningar använder vi oss nu av $\mathrm{Z}[\sqrt{n}]$, där vi även i detta fall kan använda oss av en trivial lösning för att generera oändligt många nya lösningar till ekvationen:

Definition 3.4. Om (x_1, x_2) och (x_2, y_2) är lösningar till ekvationen $x^2 - ny^2 = 1$ så är även (x_3, y_3) det, där $(x_3, y_3) = (x_1x_2 + ny_1y_2, x_1y_2 + y_1x_2)$.

Beviset följer genom faktorisering av Pells ekvation:

$$x^2 - ny^2 = 1 = (x + y\sqrt{n})(x - y\sqrt{n}).$$

Då vi vet att (x_1, x_2) och (y_1, y_2) är lösningar till ekvationen kan detta skrivas som:

$$(x_1^2 - ny_1^2)(x_2^2 - ny_2^2) = (x_1 - y_1\sqrt{n})(x_1 + y_1\sqrt{n})(x_2 - y_2\sqrt{n})(x_2 + y_2\sqrt{n}) = 1.$$

Sorterar vi om termerna får vi:

$$(x_1 + y_1\sqrt{n})(x_2 + y_2\sqrt{n})(x_1 - y_1\sqrt{n})(x_2 - y_2\sqrt{n}) =$$

$$= (x_1x_2 + ny_1y_2 + \sqrt{n}(x_1y_2 + y_1x_2))(x_1x_2 + ny_1y_2 - \sqrt{n}(x_1y_2 + y_1x_2)) =$$

$$= (x_1x_2 + ny_1y_2)^2 - n(x_1y_2 + y_1x_2)^2 = x_3^2 - ny_3^2.$$

Där vi i sista steget når just $(x_3, y_3) = (x_1x_2 + ny_1y_2, x_1y_2 + y_1x_2)$, vilket vi var ute efter. Vi testar då $n = 3$ och $n = 5$:

Exempel 3.5. Vi letar efter lösningar då $n = 3$.
För ekvationen $x^2 - 3y^2 = 1$ hittar vi den minsta lösningen $(x_1, y_2) = (2, 1)$.
Väljer vi sedan $(x_1, y_1) = (x_2, y_2)$ kan vi konstruera lösningen:

$$(x_3, y_3) = (2 \times 2 + 3, 2 + 2) = (7, 4).$$

Forsatt kan denna lösning användas för att hitta oändligt många nya punkter.

Exempel 3.6. Då $n = 5$, alltså, $x^2 - 5y^2 = 1$ hittar vi minsta lösningen först vid $(9, 4)$. Konstruerar vi en ny punkt (x_3, y_3) där $(x_1, y_1) = (x_2, y_2) = (9, 4)$ får vi:

$$(x, y) = (9 \times 9 + 5 \times 4 \times 4, 9 \times 4 + 9 \times 4) = (161, 72).$$

Med denna metod kan vi alltså hitta oändligt många lösningar till Pells ekvation, givet att vi först lyckas hitta minst en lösning med någon annan metod.
Fortsatt är det värt att tillägga att lösningarna för Pells ekvation kan förenklas ytterligare, då vi, i fallet $n = 3$ med minsta lösning $(2, 1)$ kan uttrycka lösningen $(7, 4)$ som $(2 + \sqrt{3})^2$. Fortsatt kan vi generalisera detta till att en godtycklig lösning (x_k, y_k) kan uttryckas som $x_k + y_k\sqrt{n} = (x_1 + y_1\sqrt{n})^k$ till ekvationen $x^2 - ny^2 = 1$, där (x_1, y_1) är en lösning, och k är ett heltal.

A

Kordametod för Kubisk Ekvation

På samma sätt som vi, med Diophantus kordametod, kan använda geometri för att finna lösningar till Pythagoras ekvation bygger Diophantus vidare för ekvationer med kubiska termer, där vi även kan använda oss av geometri för att lösa ekvationer. Ett exempel är ekvationen $y^2 = x^3 - 2$, där vi med hjälp av att dra en tangent i en punkt längst ekvationens graf kan hitta oändligt många rationella lösningar för ekvationen.

För ekvationen $y^2 = x^3 - 2$ kan vi dra en tangent från den triviala heltalslösningen $(x_1, y_1) = (3, 5)$, vilken kommer korsa kurvan i en annan, rationell, punkt. Värt att notera är att ekvationen är symmetrisk, så varje punkt x kommer svara mot två punkter $\pm y$. För enkelhetens skull tittar vi bara på positiva y-värden.

Först påminner vi oss om att ekvationen för en tangent lyder:

$$y - y_1 = f'(x_1)(x - x_1).$$

Vi skriver om ekvationen:

$$y^2 = x^3 - 2, \quad y = \pm, \sqrt{x^3 - 2}.$$

Sedan räknar vi ut $f'(x_1)$, där $x_1 = 3$ och $y_1 = 5$. Då vi valt att endast fokusera på positiva y-värden får vi:

$$f'(x) = y' = \frac{3x^2}{2\sqrt{x^3 - 2}}.$$

Vilket ger:

$$f'(x_1) = \frac{27}{10}.$$

Använder vi sedan detta värde, insatt i ekvationen för en tangent, får vi:

$$(y - 5) = \frac{27}{10}(x - 3).$$

Tangenten till punkten $(3,5)$ på kurvan blir alltså:

$$y = \frac{27x}{10} - \frac{31}{10}.$$

Vi kan nu ersätta kurvans y-värden med tangentens ekvation för att hitta punkterna där tangentens graf och kurvans graf korsas:

$$\left(\frac{27x}{10} - \frac{31}{10}\right)^2 = x^3 - 2.$$

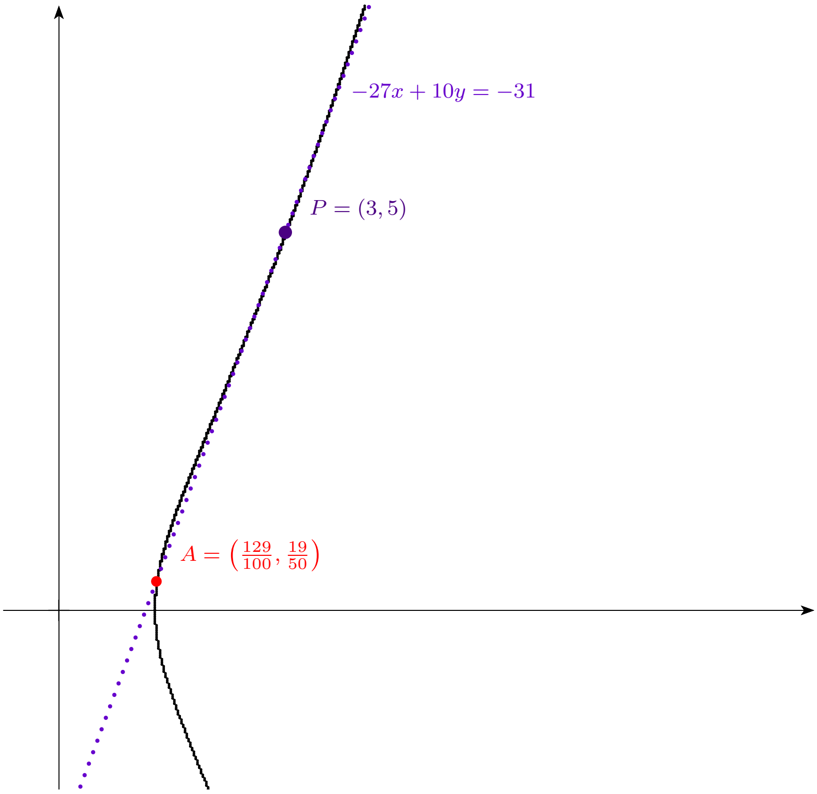
För att lösa ut ett x-värde kan det skrivas som:

$$-x^3 + \frac{729x^2}{100} - \frac{837x}{50} + \frac{1161}{100} = 0.$$

Då $x = 3$ är en rot bryter vi ut $(x-3)$:

$$-x^3 + \frac{729x^2}{100} - \frac{837x}{50} + \frac{1161}{100} = \left(-x^2 + \frac{429x}{100} - \frac{387}{100}\right)(x-3) = 0.$$

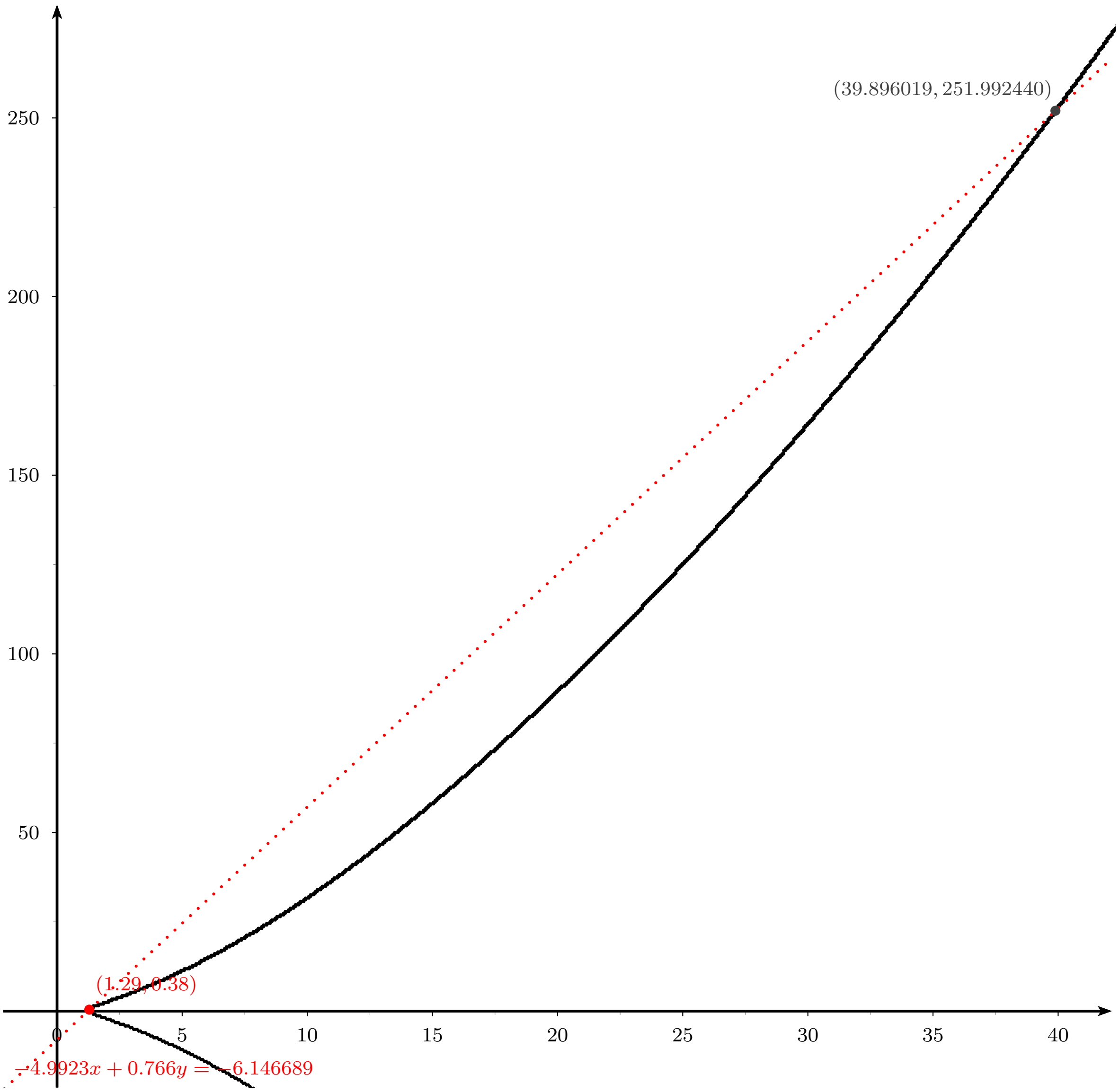
Med pq-formeln kan vi nu lösa ut rötterna ur $-x^2 + \frac{429x}{100} - \frac{387}{100} = 0$, och få dubbelroten $x = 3$, men även roten $x = \frac{129}{100}$, vilket svarar mot $y = \frac{19}{50}$, visuellt representerat i Figur 2 :



Figur 2: Tangent dragen från (3,5)

Fortsatt kan vi nu, med hjälp av den nya punkten $\left(\frac{129}{100}, \frac{19}{50}\right)$, dra ytterligare en tangent, och på så sätt hitta en ny rationell punkt. Figur 3 visar tangenten dragen från $\left(\frac{129}{100}, \frac{19}{50}\right)$.

Faktum är att vi, med hjälp av denna metod, kan hitta oändligt många rationella lösningar till ekvationen. För varje ny punkt vi hittar kan vi sedan dra ytterligare en tangent för att hitta fler punkter på kurvan.



Figur 3: Tangent dragen från $\left(\frac{129}{100}, \frac{19}{50}\right)$

Referenser

[1] J. Stillwell. *Elements of Number Theory.* Springer Science & Business Media, 2003.

[2] G. Everest, T. Ward. *An Introduction to Number Theory.* Springer London, 2005.