Seminar der WE AlZAGK (VAK: 03-404)

Prof. Michael Hortmann, Prof. Jens Gamst, Prof. Eberhard Oeljeklaus

Die Methode von Brouncker und Wallis

Jakob Fisahn,
Matr.Nr.: 2359905,
e-Mail: jakob.fisahn@web.de

Wintersemester 2009/2010

1 Einleitung

Pierre de Fermat stellte im Jahr 1657, wie es bei ihm üblich war, eine "Knobelaufgabe" an seine Kollegen innerhalb der Mathematik in Europa. Er suchte Lösungen (x, y) für die Gleichung $x^2 - Ny^2 = 1$. Da er wohl nicht genau spezifizierte, dass er ganzzahlige Lösungen suchte, bekam er als erstes eine Lösung in Brüchen von den englischen Mathematikern Wallis und Brouncker. Nachdem Fermat klar gemacht hatte, dass er wohl missverstanden worden sei, erhielt er einige Monate später eine Methode, um ganzzahlige Lösungen der Gleichung zu finden.

Wie bei Fermat üblich, hatte er bereits eine Methode zum Lösen des Problems, bevor er die Aufgabe an seine Kollegen stellte. Diese Methode unterschied sich aber nicht wesentlich von der, die Walls und Brouncker fanden, bis auf den Punkt, dass es Fermat möglich war, formal zu beweisen, dass seine Methode immer zu einer Lösung der Gleichung führt.

Im Folgenden werden wir nun die Methode von Wallis und Brouncker nachvollziehen, betrachten aber zunächst die Methode von Bachet zur Lösung der Gleichung $ay-bx = \pm 1$. Diese diente mit Sicherheit als Vorbild für Wallis, Brouncker und Fermat, um ihrerseits ihr Problem zu lösen.

2 Bachet

Man geht davon aus, dass $(x, y) \in \mathbb{N} \times \mathbb{N}$ eine Lösung der Gleichung

$$aY - bX = \pm 1 \quad (*)$$

ist. Es gilt $a, b \in \mathbb{N} : \ a > b > 0 \wedge ggT(a, b) = 1$. Zu aller erst halten wir fest, dass x und y auch teilerfremd sein müssen. Ansonsten wären ay und bx nicht teilerfremd und somit wäre die Differenz nicht gleich ± 1. Als nächstes wird der Trivialfall $b = 1$ bearbeitet. Tritt dieser Fall ein, hat die Gleichung die Form $ay - x = \pm 1$ und die Lösung $x = ay \mp 1$, wobei $y > 0$ beliebig gewählt werden kann.

Das Ziel im allgemeinen Fall ist, die Gleichung durch eine rekursive Methode zum trivialen Fall zu führen, um dann durch Rückeinsetzen die Lösung für die Ursprungsgleichung zu erhalten. Dazu dividiert man a durch b mit Rest und man erhält:

$$a = mb + c \text{ mit } : \ 0 < c < b.$$

Der Rest c ist hier echt größer Null, da a und b nach Vorraussetzung teilerfremd sind und $b > 1$ ist. Des Weiteren setzt man nun

$$x = my + z.$$

Ersetzt man a und x in $(*)$ wie angegeben, gelangt man zu der Gleichung:

$$\pm 1 = ay - bx = (mb + c)y - b(my + z) = cy - bz \Rightarrow bz - cy = \mp 1 (**)$$

Man sucht jetzt also ein neues Lösungspaar (y, z) und für die Gleichung $(**)$. Aus den Voraussetzungen wissen wir, dass $y > 0$ ist. Da x und y teilerfremd sind, ist $z \neq 0$ und $z \neq y$. Außerdem muss z positiv sein. Angenommen z wäre negativ, dann würde folgendes gelten:

$$bz - cy = -1 \Leftrightarrow 0 > z = \frac{-1 + cy}{b} \Leftrightarrow cy < 0$$

Dies ist ein Widerspruch, also ist z positiv. Für das Lösungspaar (y, z) gilt $y, z > 0$ und für die Gleichung $(**)$ gilt $a > b > c > 0$.
Die Lösung (x, y) für $(*)$ erhält man, indem man z in $x = my + z$ einsetzt. Normalerweise ist man nach einem Mal Umformen noch nicht beim Trivialfall angekommen, deswegen muss das Verfahren so oft wiederholt werden, bis man diesen erreicht. Die Lösung des Trivialfalls liefert dann die Lösung der ursprünglichen Gleichung.

3 Brouncker und Wallis

Nun zur Gleichung

$$U^2 - NX^2 = \pm 1 \ . \tag{1}$$

Zur Erinnerung, N ist hier eine positive ganze Zahl, die keine Quadratzahl ist. Wie im vorherigen Kapitel gehen wir davon aus, dass die Gleichung (1) eine Lösung $(u, x) \in \mathbb{N} \times \mathbb{N}$ besitzt. Sei $n \in \mathbb{N}: \ n^2 < N < (n+1)^2$. Der Fall $N = n^2 \pm 1$ wird hier ausgeschlossen, da sich in diesem Fall die Lösung leicht berechnen lässt:

$$u^2 - (n^2 \pm 1)x^2 = \pm 1 \Leftrightarrow x^2 = \frac{u^2 \mp 1}{n^2 \pm 1}$$

Die rechte Gleichung ist genau dann erfüllt, wenn $(u, x) = (n, 1)$. Das heißt insbesondere, dass wir in Zukunft auch davon ausgehen können, dass $x > 1$ ist.

Es gilt nun: $u > nx$.

Beweis:

$$\begin{aligned} u^2 - Nx^2 &= \pm 1 \\ u^2 &= Nx^2 \pm 1 \\ u^2 &> n^2x^2 \text{ (da } x > 1) \quad \Rightarrow \quad u > nx \end{aligned}$$

□

Mit diesem Wissen kann man nun u in Gleichung (1) durch $nx + y$ ($y \in \mathbb{N} : \ y > 0$) ersetzen. Durch Auflösen nach x und y erhält man die Gleichung $(N - n^2)x^2 - 2nxy - y^2 = \mp 1$. Setzt man $A = N - n^2,\ B = n,\ C = 1$, so ist das Tupel (x, y) eine Lösung der Gleichung

$$AX^2 - 2BXY - CY^2 = \mp 1 \ , \tag{2}$$

wobei $A,\ B,\ C$ ihrer Definition nach natürliche Zahlen $\neq 0$ sind. Sie haben die Eigenschaft, dass $B^2 + AC = N$ gilt.

Das Interesse konzentriert sich im Folgenden auf die Eigenschaften der Gleichung (2). In Zukunft wird die linke Seite derselben mit $(A,\ B,\ C)$ (wobei $A,\ B,\ C \in \mathbb{N}$ beliebig) bezeichnen. Zunächst kann man (2) als Funktion $F : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{R},\ (x, y) \longmapsto Ax^2 - 2Bxy - Cy^2$ begreifen. Sei $t := \frac{x}{y}$ und $f(t) := \frac{F(x,y)}{y^2} = A(\frac{x}{y})^2 - 2B\frac{x}{y} - C = At^2 - 2Bt - C$. Es folgt die

Definition: $(A,\ B,\ C)$ heißt *reduziert*, falls $f(t)$ zwei Nullstellen $t_1, t_2 \in \mathbb{R}$ mit $t_1 > 1\ \wedge -1 < t_2 < 0$ besitzt.

Satz: $(A,\ B,\ C)$ ist genau dann reduziert, wenn $|A - C| < 2B$ ist.

Beweis: Als erstes erinnere man sich, dass $A,\ B,\ C \in \mathbb{N}$ ist. Berechnet man nun mit der pq-Formel die Nullstellen des Polynoms $f(t)$, so erhält man:

$$f(t) = 0 \Leftrightarrow t_{1,2} = \frac{B \pm \sqrt{B^2 + AC}}{A}$$

Wegen $C > 0$ ist die eine Nullstelle positiv und die andere negativ. Zuerst betrachten wir nun die negative Nullstelle:

$$\begin{array}{rrcl} & \frac{B - \sqrt{B^2+AC}}{A} & > & -1 \\ \Leftrightarrow & B - \sqrt{B^2 + AC} & > & -A \\ \Leftrightarrow & \sqrt{B^2 + AC} & < & A + B \\ \Leftrightarrow & B^2 + AC & < & A^2 + 2AB + B^2 \\ \Leftrightarrow & A(C - A) & < & 2AB \\ \Leftrightarrow & C - A & < & 2B \end{array}$$

Nun die positive Nullstelle:

$$\begin{array}{rcl} \frac{B+\sqrt{B^2+AC}}{A} & > & 1 \\ \Leftrightarrow \quad \sqrt{B^2+AC} & > & A-B \end{array}$$

Hier muss man nun eine Fallunterscheidung durchführen:
1. Fall: $A - B > 0$

$$\begin{array}{rrcl} \Rightarrow & B^2 + AC & > & A^2 - 2AB + B^2 \\ \Leftrightarrow & AC & > & A^2 - 2AB \\ \Leftrightarrow & C & > & A - 2B \\ \Leftrightarrow & A - C & < & 2B \end{array}$$

2. Fall: $A - B \leq 0$

$$2B = B + B \geq B + A > A \geq A - C$$

□

Um eine klarere Formulierung zu gewährleisten dient Folgendes.
Definition: $(C,\ B,\ A) = F^t$ heißt die *transponierte Form* zu F.
Mit Hilfe des Satzes sieht man sofort: Falls F reduziert ist, so ist auch F^t reduziert. Wegen $N < (n+1)^2$ lässt sich außerdem leicht nachrechnen, dass für $A = N - n^2,\ B = n,\ C = 1$, $(A,\ B,\ C)$ ebenfalls reduziert ist.
Für eine beliebige reduzierte Form $F = (A,\ B,\ C)$ sei m die größte natürliche Zahl echt kleiner als die positive Nullstelle von F. Da diese Nullstelle echt größer 1 ist, ist m mindestens gleich 1.
Definition: Wir nennen $F' = (A',\ B',\ C')$ die von F *abgeleitete Form*. Man erhält sie mit:

$$A' = -(Am^2 - 2Bm - C), \quad B' = Am - B, \quad C' = A \tag{3}$$

Behauptung: m ist die größte ganze Zahl, für die $A' > 0$ ist, außerdem ist $B' > 0$ und F' wieder reduziert.

Beweis der Behauptung: $f(t)$ ist eine nach oben offene Parabel mit einer Nullstelle $t_1 > 1$ und einer Nullstelle $t_2 \in [-1, 0]$. Ist m wie oben definiert, gilt: $f(m) < 0 \Rightarrow -f(m) > 0 \Rightarrow A' > 0$.

Aus den Eigenschaften der Parabel lässt sich auch herleiten, dass $f'(m)$ positiv sein muss. Wäre die Ableitung an der Stelle m negativ, wäre die Steigung von $f(t)$ an der Stelle m negativ. Daraus würde folgen, dass sich zwischen m und t_1 ein Minimum befinden müsste. Wäre dem so, würde aus der Symmetrie der Parabel folgen, dass die zweite Nullstelle echt größer 0 wäre, was nicht sein kann, da $(A,\ B,\ C)$ reduziert ist. D. h.: $0 < f'(m)$ woraus folgt, dass $0 < \frac{f'(m)}{2} = Am - B = B'$.

Es fehlt noch der Beweis für die Behauptung, dass F' ebenfalls reduziert ist, wenn F es ist. $F' = (A',\ B',\ C')$, also ist $f(t') = A't'^2 - 2B't' - C'$. Um zu wissen, wie t' genau aussieht, beachte man nun, dass man F zu $-F'$ umwandeln kann, indem man X und Y mit

$$X = X'm + Y', \qquad Y = X' \tag{4}$$

substituiert. Denn:

$$\begin{aligned} & A(X'm + Y')^2 - 2B(X'm + Y')X' - CX'^2 \\ = {} & (Am^2 - 2Bm - C)X'^2 + 2(Am - B)X'Y' + AY'^2 \\ = {} & -A'X'^2 + 2B'X'Y' + C'Y'^2 \ = \ -F' \end{aligned}$$

Wichtig ist hier den Vorzeichenwechsel zu beachten. Falls $N = B^2 + AC$ gilt, so gilt auch $B'^2 + A'C' = N$, was man durch Einsetzen schnell sieht.

Das heißt $F(X'm + Y', X') = -F'(X', Y')$. Vor dem Beweis des Satzes wurde t als $\frac{x}{y}$ definiert. Daraus folgt, mit Hilfe von (4), für t', dass $t = \frac{mX'+Y'}{X'} = m + \frac{Y'}{X'} = m + \frac{1}{t'} \ \Rightarrow \ t' = \frac{1}{t-m}$. Das bedeutet für die Nullstelle t'_1 von $f(t')$, dass $t'_1 = \frac{1}{t_1-m} > 1$, da $t_1 - m \in]0,1[$. Für die zweite Nullstelle t'_2 gilt: $0 > t'_2 = \frac{1}{t_2-m} > -1$, da $t_2 - m$ echt kleiner -1.

Damit ist gezeigt, dass F' ebenfalls zwei Nullstellen besitzt, die den Kriterien der Reduziertheit genügen, d. h. F' ist ebenfalls reduziert. □

Was wurde also, um sich einen kleinen Überblick zu verschaffen, bis zu diesem Punkt getan?

1. Die Gleichung $U^2 - NX^2 = \pm 1$ wurde mit $u = nx + y$ in die Gleichung $AX^2 - 2BXY - CY^2 = \mp 1$ umgewandelt.

2. Die linke Seite der Gleichung wurde $F = (A,\ B,\ C)$ genannt und es wurde festgestellt, dass sie unter bestimmten Umständen *reduziert* ist.

3. Ist F reduziert, so sind auch $(C,\ B,\ A)$ und $F' = (A',\ B',\ C')$ reduziert. Gilt außerdem $N = B^2 + AC$, so gilt auch $N = B'^2 + A'C'$.

4. Klar ist auch, dass es nur endlich viele Tripel $(A,\ B,\ C)$ positver ganzer Zahlen gibt, für die $N = B^2 + AC$ gilt.

Das Ziel ist es, durch Umformen von F auf eine Gleichung zu kommen, deren Lösung trivial ist, ähnlich wie im ersten Teil dieser Ausarbeitung bei der Gleichung $aY - bX = \pm 1$. Durch den obigen vierten Punkt ist man nun einen Schritt weiter, da er vermuten lässt, dass F und F' sich irgendwann wiederholen, wenn man nur oft genug umformt. Um dem nachzugehen braucht man folgende Überlegung:

Wie schon gesagt, ist $F' = (A',\ B',\ C')$ die von $F = (A,\ B,\ C)$ „abgeleitete Form" (s. (3)). Um den „Rückweg" von F' zu F anzutreten, formt man $(C',\ B',\ A')$ mit

$$C = -(C'm^2 - 2B'm - A'),\ B = C'm - B',\ A = C' \tag{5}$$

zu $(C,\ B,\ A)$ um. Die Rechnung dazu sieht wie folgt aus:

$$\begin{aligned}
& C'X'^2 - 2B'X'Y' - A'Y'^2 = \pm 1 \\
\overset{X'=Xm+Y \wedge Y'=X}{\Rightarrow}\quad & C'(Xm+Y)^2 - 2B'(Xm+Y)X - A'X^2 = \pm 1 \\
\Rightarrow\quad & (C'm^2 - 2B'm - A')X^2 + 2(C'm - B') + C'Y^2 = \pm 1 \\
\overset{\cdot(-1)}{\Rightarrow}\quad & -(C'm^2 - 2B'm - A')X^2 - 2(C'm - B') - C'Y^2 = \mp 1 \\
\Rightarrow\quad & CX^2 - 2BXY - AY^2 = \mp 1
\end{aligned}$$

Somit ist $(C,\ B,\ A)$ die von $(C',\ B',\ A')$ abgeleitete Form und man hat folgenden Kreislauf:

$$F \quad \overset{(4)}{\Rightarrow} \quad F' \quad \overset{\text{transp.}}{\Rightarrow} \quad F'^t \quad \overset{(5)}{\Rightarrow} \quad F^t \quad \overset{\text{transp.}}{\Rightarrow} \quad F$$

Desweiteren gilt, dass m die größte ganze Zahl ist, für die $C'm^2 - 2B'm - A'$ echt kleiner Null ist. Mit Hilfe von (5) kann man nun aus einem beliebigen F' die „Ursprungsform" F gewinnen.

Startet man nun mit einer beliebigen reduzierten Form $F_0 = (A_0,\ B_0\ C_0)$, so bekommt man durch das Prozedere $F_1 = F_0',\ F_2 = F_1'$ und so weiter. Somit ist für alle $i \in \mathbb{N}$ $F_i = (A_i,\ B_i,\ C_i)$ die von $F_{i-1} = (A_{i-1},\ B_{i-1},\ C_{i-1})$ abgeleitete Form. Alle F_i sind reduziert. Außerdem gilt $N = B_i^2 + A_iC_i$ für alle $i \in \mathbb{N}$ und, wie oben schon erwähnt wurde, müssen sich die F_i's irgendwann wiederholen. Man kann also annehmen, dass ein $p \in \mathbb{N}$ mit $p \geq 1$ existiert, sodass $F_{i+p} = F_i$ für ein $i \geq 0$. Für alle i sei nun $G_i = F_i^t = (C_i,\ B_i,\ A_i)$.

G_0 ist nach (5) die i-te abgeleitete Form von G_i, genau so wie G_p die i-te abgeleitete Form von G_{i+p} ist. Aus $F_{i+p} = F_i$ folgt $G_{i+p} = G_i$ und damit ist $G_p = G_0$ und $F_p = F_0$. Hat die Periode eine Länge p, so gilt: $F_{kp} = F_0$.

Wie bei Brouncker und Wallis sei $F_0 = (A = N - n^2,\ B = n,\ C = 1)$. Mit (4) substituiert man F_0 und erhält $-F' = \mp 1$, woraus $F_1 = F' = \pm 1$ folgt. Wird dieses Prozedere bei einer Periodenlänge p fortgesetzt, muss $C_p = 1$ sein, da $F_0 = F_p$. Also ist nach (3) $A_{p-1} = 1$ und somit existiert für die Gleichung $F_{p-1} = X^2 - 2B_{p-1}XY - C_{p-1}Y^2 = 1$ die triviale Lösung $(1, 0)$. Wird die Lösung nun rückwärts in die Substitutionsvorschrift (4) eingesetzt, erhält man eine Lösung $(u,\ x)$ für die Anfangsgleichung (1). Wie erwähnt alterniert bei jeder Umformung das Vorzeichen, d. h. $F_i(X, Y) = \pm(-1)^{i+1}$. Da beim Wechsel von der Gleichung (1) auf (2) ebenfalls ein Vorzeichenwechel stattfindet, löst $(u,\ x)$, je nachdem ob p gerade oder ungerade ist, die Gleichung $U^2 - NX^2 = +1$ oder $U^2 - NX^2 = -1$. Trifft letzteres zu, muss der Prozess bis F_{2p} durchlaufen werden, um eine Lösung für $U^2 - NX^2 = +1$ zu erhalten.

4 Beispiele

4.1 $N = 13$

Im Folgenden wird ausführlich die Berechnung einer Lösung $(u,\ x)$ für die Gleichung $u^2 - 13x^2 = \pm 1$ gezeigt. Zuerst bestimmt man die größte ganze Zahl n kleiner als $\sqrt{13}$. In diesem Fall also 3. Danach kann man $A,\ B$ und C mit $A = N - n^2 = 13 - 9 = 4$, $B = n = 3$ und $C = 1$ berechnen. In der Tabelle sind nun alle folgenden Funktionen aufglistet, die durch Substitution mit $X = X'm + Y'$ und $Y = X'$ entstehen.

i	F_i	t_{pos}	m
0	$4x^2 - 6xy - 1y^2 = \mp 1$	$\approx \frac{6,6}{4}$	1
1	$3x^2 - 2xy - 4y^2 = \pm 1$	$\approx \frac{4,6}{3}$	1
2	$3x^2 - 4xy - 3y^2 = \mp 1$	$\approx \frac{5,6}{3}$	1
3	$4x^2 - 2xy - 3y^2 = \pm 1$	$\approx \frac{4,6}{4}$	1
4	$1x^2 - 6xy - 4y^2 = \mp 1$	$\approx \frac{6,6}{1}$	6

F_4 hat die triviale Lösung $(x^{iv}, y^{iv}) = (1, 0)$. Man unterbricht den Prozess an dieser Stelle, da sich die Funktionen von nun an wiederholen. Indem man die Lösung rückwärts in die Substitutionsvorschift einsetzt, erhält man:

$$
\begin{array}{lrcl}
 & (x^{iv}, y^{iv}) & = & (1,0) \\
\overset{X=X'm+Y' \wedge Y=X'}{\Rightarrow} & (x^{iii}, y^{iii}) & = & (1,1) \\
\Rightarrow & (x^{ii}, y^{ii}) & = & (2,1) \\
\Rightarrow & (x^{i}, y^{i}) & = & (3,2) \\
\Rightarrow & (x, y) & = & (5,3) \\
\overset{u=nx+y}{\Rightarrow} & (u, x) & = & (18,5) \\
 & & & \\
\Rightarrow & 18^2 - 13 \cdot 5^2 & = & 324 - 325 = -1
\end{array}
$$

Möchte man eine Lösung (u, x) für $u^2 - Nx^2 = 1$ generieren, muss man den Prozess, wie im vorherigen Kapitel beschrieben, bis $i = 9$ durchlaufen. Das ist der niedrigste Index nach $i = 4$, bei dem die Funktion F eine triviale Lösung besitzt. Durch Rückwärtseinsetzen von diesem Punkt aus, erhält man eine

Lösung für $u^2 - 13x^2 = 1$:

$$
\begin{array}{rrcl}
 & (x^{ix}, y^{ix}) & = & (1,0) \\
\Rightarrow & & \cdots & \\
\Rightarrow & (x^{v}, y^{v}) & = & (5,3) \\
\overset{m=6}{\Rightarrow} & (x^{iv}, y^{iv}) & = & (33,5) \\
\Rightarrow & & \cdots & \\
\Rightarrow & (x,y) & = & (180,109) \\
\Rightarrow & (u,v) & = & (649,180) \\
\Rightarrow & 649^2 - 13 \cdot 180^2 & = & 421201 - 13 \cdot 32400 \\
 & & = & 421201 - 421200 \\
 & & = & 1
\end{array}
$$

4.2 $N = 61$ und $N = 109$

$N = 61$ und $N = 109$ sind die Beispiele, die Fermat seinen Kollegen vorschlug zu lösen. Dabei vergaß er nicht zu sagen, dass er diese Zahlen auswählte, um ihnen nicht zu viel Arbeit zu bereiten. Dabei sind diese beiden Zahlen eher Beispiele für eine lange Sequenz von Funktionen.

In den folgenden Tabellen sind die jeweiligen $(A_i,\ B_i,\ C_i)$ und die dazugehörigen m_i aufgelistet.

Fängt man von $i = 10$ resp. $i = 14$ aus an, die Lösung zu berechnen, so erhält man jeweils eine Lösung für $u^2 - 61x^2 = -1$, resp. $u^2 - 109x^2 = -1$. Wie in der Einleitung erwähnt suchte Fermat Lösungen für $u^2 - Nx^2 = 1$, dass heißt man muss von $i = 21$, bzw. $i = 29$ rückwärts in die Substitutionsvorschrift einsetzen, um ein Lösungspaar für $u^2 - Nx^2 = 1$ zu erhalten. Nachdem man das getan hat ohne sich zu verrechnen, erhält man für $N = 61$ das Lösungspaar $(u,\ x) = (1766319049,\ 226153980)$ und für $N = 109$ das Paar $(u,\ x) = (158070671986249,\ 15140424455100)$.

i	A_i	B_i	C_i	m_i
0	12	7	1	1
1	3	5	12	4
2	4	7	3	3
3	9	5	4	1
4	5	4	9	2
5	5	6	5	2
6	9	4	5	1
7	4	5	9	3
8	3	7	4	4
9	12	5	3	1
10	1	7	12	1

Abb. 1: $N = 61$

i	A_i	B_i	C_i	m_i
0	9	10	1	2
1	5	8	9	3
2	12	7	5	1
3	7	5	12	2
4	4	9	7	4
5	15	7	4	1
6	3	8	15	6
7	3	10	3	6
8	15	8	3	1
9	4	7	15	4
10	7	9	4	2
11	12	5	7	1
12	5	7	12	3
13	9	8	5	2
14	1	10	9	20

Abb. 2: $N = 109$

Literatur

[1] M. Jacobson, H. Williams: *Solving the Pell Equation*, Springer 2009

[2] A. Weil: *Number Theory*, Boston 1984