Sitzungsberichte

der

mathematisch-naturwissenschaftlichen Klasse

der

Bayerischen Akademie der Wissenschaften zu München

Jahrgang 1948

München 1949
Verlag der Bayerischen Akademie der Wissenschaften
In Kommission beim Biederstein Verlag München

Über die Gleichung $X^2 - DY^2 = \pm c \cdot (2^{31} - 1)$, wo c möglichst klein.

Von **Wilhelm Patz** in Bruckdorf bei Halle.

Vorgelegt von Herrn O. Perron 9. Januar 1948.

Vorbemerkung von Herrn Perron.

Die Zahl $p = 2^{31} - 1$ ist bekanntlich Primzahl. Da sie außerdem $\equiv 1 \pmod 3$ ist, also $\left(\frac{-3}{p}\right) = 1$, so kann man leicht schließen, daß sie sich in der Form $x^2 + 3y^2$ darstellen läßt.[1] Da auch $\left(\frac{-5}{p}\right) = 1$, $\left(\frac{13}{p}\right) = 1$, so läßt sich in ähnlicher Weise schließen, daß durch die Formen $x^2 + 5y^2$, $x^2 - 13y^2$ ebenfalls die Zahl p oder ein kleines Multiplum von ihr sich darstellen läßt.[2] Umgekehrt, wenn solche Darstellungen vorliegen, kann man sie benutzen, um den Nachweis, daß p Primzahl ist, abzukürzen. Da mir nun solche Darstellungen nicht bekannt waren, habe ich Herrn Patz, der sich bereits als Meister im Umgang mit Kettenbrüchen[3] und in der Auflösung der Diophantischen Gleichung $x^2 - Dy^2 = Q$ bewährt hat, aufgefordert, die erwähnten Darstellungen zu suchen. Nach kurzer Zeit schickte er mir die unten abgedruckte Note mit den Resultaten

$$46\,162^2 + 3 \cdot 2\,349^2 = 2^{31} - 1,$$
$$64\,557^2 + 5 \cdot 5\,047^2 = 2 \cdot (2^{31} - 1),$$
$$179\,721^2 - 13 \cdot 51\,476^2 = -(2^{31} - 1).$$

Die Methode ist mir nicht ganz klar geworden, und Herr Patz spricht überhaupt seine eigene Sprache, die sich mit der Sprache der Mathematiker nur teilweise deckt. Aber der durch-

[1] Nach Kap. II, Satz 25 meines Buches: Die Lehre von den Kettenbrüchen. Leipzig und Berlin 1913, zweite Auflage 1929.

[2] In der Form $x^2 + 5y^2$ ist die Zahl p selbst natürlich nicht darstellbar, da $x^2 + 5y^2$ nie $\equiv -1 \pmod 4$ ist.

[3] Dafür zeugt sein Buch: Wilhelm Patz, Tafel der regelmäßigen Kettenbrüche für Quadratwurzeln aus den natürlichen Zahlen von 1–10000. Leipzig 1941.

schlagende Erfolg läßt es angebracht erscheinen, die Note in der Originalfassung abzudrucken, damit vielleicht andere hinter das Geheimnis kommen. Zum Verständnis der Bezeichnungsweise möchte ich nur folgendes vorausschicken.

Sind D, P_0, Q_0 ganze Zahlen, dabei D kein Quadrat, und ist $D - P_0^2 \equiv 0 \pmod{Q_0}$, so kann man formal eine kettenbruchartige Entwicklung durchführen

$$\frac{\sqrt{D}+P_0}{Q_0} = b_0 + \frac{Q_1}{\sqrt{D}+P_1}, \quad \frac{\sqrt{D}+P_1}{Q_1} = b_1 + \frac{Q_2}{\sqrt{D}+P_2}, \ldots,$$

wobei $b_0, b_1, \ldots$ beliebige ganze Zahlen sein können. Die P_n, Q_n berechnen sich dann aus den Rekursionsformeln

$$P_n + P_{n+1} = b_n Q_n, \quad D + P_n P_{n+1} = b_n Q_n P_{n+1} + Q_n Q_{n+1},$$

aus denen man noch einige bequemere herleiten kann, und sind wieder ganze Zahlen, wobei $D - P_n^2 \equiv 0 \pmod{Q_n}$ ist. Herr Patz schreibt das so:

$$\frac{\sqrt{D}+P_0}{Q_0} = \begin{matrix} P_0 \\ Q_0 \\ b_0 \end{matrix}\begin{pmatrix} P_1 & P_2 & P_3 \ldots \\ Q_1 & Q_2 & Q_3 \ldots \\ b_1 & b_2 & b_3 \ldots \end{pmatrix}.$$

Betrachtet man nun den Kettenbruch

$$b_0 + \frac{1}{|}\,\frac{1}{b_1} + \frac{1}{|}\,\frac{1}{b_2} + \frac{1}{|}\,\frac{1}{b_3} + \cdots$$

und bezeichnet seine Näherungsbrüche mit $\frac{A_0}{B_0}, \frac{A_1}{B_1}, \ldots$, so gilt die Formel

$$\frac{\sqrt{D}+P_0}{Q_0} = \frac{A_{n-1}(\sqrt{D}+P_n)+A_{n-2}Q_n}{B_{n-1}(\sqrt{D}+P_n)+B_{n-2}Q_n},$$

und folglich ist

$$B_{n-1}D + P_0(B_{n-1}P_n + B_{n-2}Q_n) = Q_0(A_{n-1}P_n + A_{n-2}Q_n),$$
$$P_0 B_{n-1} + B_{n-1}P_n + B_{n-2}Q_n = Q_0 A_{n-1},$$

woraus leicht folgt:

$$(Q_0 A_{n-1} - P_0 B_{n-1})^2 - D B_{n-1}^2 = (-1)^n Q_0 Q_n.$$

Wenn also einmal $Q_n = 1$ wird, so kommt

$$(Q_0 A_{n-1} - P_0 B_{n-1})^2 - D B_{n-1}^2 = (-1)^n Q_0,$$

und die Gleichung $x^2 - Dy^2 = \pm Q_0$ ist für eines der beiden Vorzeichen gelöst.

Ist D positiv, $Q_0 = 1$ und wählt man für b_n stets die größte in $\frac{\sqrt{D} + P_n}{Q_n}$ enthaltene ganze Zahl, so muß bekanntlich stets einmal $Q_n = 1$ kommen; das ist die bekannte Auflösungsmethode der Pellschen Gleichung. Aber wie Herr Patz es anstellt, daß er auch sonst scheinbar spielend auf $Q_n = 1$ kommt, ist nicht ersichtlich; diesbezügliche Fragen läßt er ohne klare Antwort. So weiß ich nicht, ob eine systematische Methode oder eine wunderbare Intuition vorliegt. Dabei kommt er auch bei negativem $D = -3$ zum Ziel, wo der gewonnene reelle Kettenbruch doch unmöglich etwas mit der imaginären Zahl $\frac{\sqrt{-3} + P_0}{Q_0}$ zu tun hat. Für $D = -5$ kommt er nicht auf $Q_n = 1$ und gibt auch einen Grund dafür an, daß das nicht möglich ist (einfacher erkennt man es aus der obigen Fußnote 2). Er kommt aber auf $Q_n = 2$ und findet damit das zweite der oben mitgeteilten Resultate. Perron

Beispiel 1.

Es soll ein quadratischer Teiler von $2^{31} - 1$ der Form

$$x^2 + 3y^2 = 2147\,483\,647$$

gesucht werden. Es sollen also die Werte x und y ermittelt werden.

Zu diesem Zweck ist die Lösung der Kongruenz

$$X^2 \equiv -3 \pmod{2^{31} - 1}$$

zu suchen. Da die Zahl $2^{31} - 1 = 2147\,483\,647$ der Form $4n + 3$ ist, so setze man $n = 536\,870\,911$ und ferner $n + 1 = 536\,870\,912$ und

$$X \equiv 3^{536\,870\,912} \pmod{2^{31} - 1}.$$

Nach 38 Potenzierungen und Divisionen durch 2147 483 647 findet man den gesuchten Wert $X = 1268\,011\,823$ und damit auch gleichzeitig den komplementären Wert $(2^{31} - 1) - X = 879\,471\,824$. Beide befriedigen die Kongruenz

$$X^2 \equiv -3 \pmod{2^{31} - 1}.$$

Der erste Wert gibt

$$1268\,011\,823^2 : 2147\,483\,647 = 748\,715\,356 \text{ Rest } -3,$$

der zweite Wert gibt

$$879\,471\,824^2 : 2147\,483\,647 = 360\,175\,357 \text{ Rest } -3.$$

Nun hätten wir anzusetzen:

$$\frac{\sqrt{-3} - 879\,471\,824}{2147\,483\,647} \text{ oder } \frac{\sqrt{-3} - 1268\,011\,823}{2147\,483\,647}.$$

Nehmen wir den letzteren Wert und entwickeln den K.-Bruch, so erhalten wir nacheinander die folgenden vollständigen Quotienten:

−1268 011 823	1268 011 823	519 296 467	159 121 110		
2147 483 647	748 715 356	360 175 357	70 297 779		
0	1	1	2		
18 525 552	3 879 453	796 689	179 016	23 367	2 319
4 882 033	3 082 764	205 891	155 649	3 508	1 533
3	1	3	1	6	1
786	383	19			
403	364	1			
1	1	38^{+}.			

Wir haben also den K.-Bruch gewonnen

$$(1, 1, 2, 3, 1, 3, 1, 6, 1, 1, 1, 38, \ldots\ldots).$$

Die Periode der vollständigen Quotienten der Entwicklung hat nun den Teilquotienten $Q = 1$, der unter $P = 19$ steht. Und hier betone ich ausdrücklich, daß dies von großer Bedeutung ist. Es ist eben nicht einerlei, welche Zahl Q als Zentrum der vollständigen Quotienten erscheint. Dies wird sich nämlich in seiner vollen Bedeutung beim Beispiel 2 zeigen, welches ich nach Erledigung dieses vorliegenden zeigen werde. Ebenso zeigt sich auch, welche Bedeutung es hat, wenn $Q = 1$ als Teilquotient erscheint, bei dem dann folgenden dritten Beispiel und welche Folgerungen daraus gezogen werden können.

Wir kehren zu unserem Beispiel zurück und weil wir wissen, daß $Q = 1$ vorgekommen ist, so können wir den K.-Bruch in folgender Anordnung schreiben:

$$\frac{38}{2}\,(1, 1, 1, 6, 1, 3, 1, 3, 2, 1, 1,)$$
$$= 19\,(1, 1, 1, 6, 1, 3, 1, 3, 2, 1, 1,).$$

Hieraus erhalten wir den N.-Wert

$$\frac{A_{n-1}}{B_{n-1}} = \frac{46\,162}{2\,349}. \quad (n - 1 = 11)$$

Wir hätten in der weiteren Entwicklung in der Periode der vollständigen Quotienten die beiden Teilquotienten

$$P_n = P_0 = 1268\,011\,823 \text{ und } Q_n = Q_0 = 2147\,483\,647$$

erhalten und machen deshalb beim Aufrollen des K.-Bruches beim $n-1$ ten Gliede halt (genau wie beim Auflösen der Pellschen Gleichung) und erhalten so den eben genannten N.-Wert

$$\frac{A_{n-1}}{B_{n-1}} = \frac{46\,162}{2\,349}.$$

Mit den Werten $X = 46\,162$ und $Y = 2\,349$ wird die Gleichung

$$X^2 + 3 \cdot Y^2 = 2147\,483\,647,$$

oder

$$46\,162^2 + 3 \cdot 2\,349^2 = 2^{31} - 1$$

befriedigt.

Die andere Entwicklung

$$\frac{\sqrt{-3} - 879\,471\,824}{2147\,483\,647} \text{ gibt}$$

$$\begin{array}{r|cccc} -879\,471\,824 & 879\,471\,824 & 159\,121\,110 & \ldots\ldots \\ 2147\,483\,647 & 360\,175\,357 & 70\,297\,779 & \ldots\ldots \\ 0 & 2 & 2 & \ldots\ldots \end{array}.$$

Die nun folgenden vollständigen Quotienten wiederholen sich nun genau in derselben Reihenfolge wie bei der ersten Entwicklung. Und wenn wir die beiden K.-Brüche in ihrer Reihenfolge gegenüberstellen, wie sie aufgerollt werden sollen, also

I. 19 (1, 1, 1, 6, 1, 3, 1, 3, 2, 1, 1,)

II. 19 (1, 1, 1, 6, 1, 3, 1, 3, 2, 2,),

so sieht man sofort, daß beide N.-Werte gleich werden müssen, da der unterste K.-Bruch II mit gerader Gliederzahl seiner primitiven Periode nach der Theorie der K.-Bruchlehre nur die Abkürzungsform des obersten K.-Bruches I mit seiner ungeraden Gliederzahl ist.

Somit ist die Zerlegung durch die Form

$$X^2 + 3 \cdot Y^2 = 2^{31} - 1$$

nur auf eine Art möglich.

Beispiel 2.

Es soll

$$X^2 \equiv -5 \pmod{2^{31} - 1}$$

aufgelöst werden und eventuell die Gleichung

$$X^2 + 5 \cdot Y^2 = 2^{31} - 1$$

befriedigt werden.

Wir suchen hier wie bei Beispiel 1 den verbleibenden Rest von

$$5^{536\,870\,912} : 2147\,483\,647.$$

Durch 38 Potenzierungen und gleichzeitige Division mit $2^{31} - 1$ finden wir

$$X \equiv 2041\,534\,867 \pmod{2^{31} - 1}$$

oder den Komplementärwert

$$X \equiv 105\,948\,780 \pmod{2^{31} - 1}.$$

Hieraus wird

$2041\,534\,867^2 : 2147\,483\,647 = 1940\,813\,202$ Rest -5, oder
$105\,948\,780^2 : 2147\,483\,647 = 5\,227\,115$ Rest -5.

Weiter setzen wir an:

$$\frac{\sqrt{-5} - 2041\,534\,867}{2147\,483\,647} =$$

$$= \frac{-2041\,534\,867}{2147\,483\,647} \quad \begin{matrix} 2041\,534\,867 & 100\,721\,665 & 1\,406\,480 \\ 1940\,813\,202 & 5\,227\,115 & 378\,447 \\ 1 & 19 & 3 \end{matrix}$$

$$\begin{matrix} 271\,139 & 76\,881 & 16\,027 & 7\,585 & 770 & 74 & 11 \\ 194\,258 & 30\,427 & 8\,442 & 6\,815 & 87 & 63 & 2 \\ 1 & 2 & 1 & 1 & 8 & 1 & 5 \end{matrix} \quad \begin{matrix} 1 \\ 3 \\ 1 \end{matrix}$$

$$\begin{matrix} 2\ 1\ \ldots\ldots \\ 3\ 2\ \ldots\ldots \\ 1\ 5\ \ldots\ldots \end{matrix}.$$

Wir brauchen nicht weiter zu gehen. Bei den vollständigen Quotienten $\begin{pmatrix} 1 \\ 3 \\ 1 \end{pmatrix}$, oder eigentlich davor, machen wir halt.

Wir schreiben auch hier den K.-Bruch in umgekehrter Folge wie oben bei Beispiel 1 in der Anordnung, die uns den N.-Wert $\frac{A_{n-1}}{B_{n-1}}$ geben muß, und erhalten:

$$(5,\ 1,\ 8,\ 1,\ 1,\ 2,\ 1,\ 3,\ 19,\ 1,)$$

Wir rollen diesen K.-Bruch auf und erhalten

$$\frac{A_{n-1}}{B_{n-1}} = \frac{5\,047}{29\,755}. \qquad (n - 1 = 10)$$

Mit den beiden Werten $X = 5\,047$ und $Y = 29\,755$ befriedigen wir die Gleichung

$$3X^2 + 2XY + 2Y^2 = 2^{31} - 1,$$

oder, was dasselbe ist,

$$(X + 2Y)^2 + 5X^2 = 2 \cdot (2^{31} - 1).$$

Wir haben in der Entwicklung der vollständigen Quotienten den Teilquotienten $Q = 1$ nicht erhalten und können ihn auch nicht erhalten, weil ja die Form $t^2 + 5 \cdot u^2$ nur die beiden quadratischen Teiler der Form (1, 1, 6) und (2, 1, 3) oder die hierzu äquivalenten (6, 1, 1) und (3, 1, 2,) hat. Zu dieser letzteren sind wir durch unsere K.-Bruchentwicklung gelangt und es hätte jedes weitere Suchen nach einem eventuellen Erscheinen des Teilquotienten $Q = 1$ keinen Erfolg. Hätte man ihn gefunden, so wäre selbstverständlich

$$X^2 + 5 \cdot Y^2 = 2147\,483\,647,$$

was leider aber niemals geschehen kann. Wir setzen

$$3X^2 + 2XY + 2Y^2 = 2147\,483\,647, \text{ oder}$$

$$3 \cdot 5\,047^2 + 2 \cdot 5\,047 \cdot 29\,755 + 2 \cdot 29\,755^2 = 2^{31} - 1.$$

Die Möglichkeit einer anderen Lösung für X und Y aus der Entwicklung

$$\frac{\sqrt{-5} - 105\,948\,780}{2147\,483\,647}$$

lasse ich mit Absicht offen.

Beispiel 3.

Die Gleichung $X^2 - 13 \cdot Y^2 = 2147\,483\,647$ aufzulösen. Wieder ist von der Kongruenz

$$X^2 \equiv 13 \pmod{2^{31} - 1}$$

auszugehen. Wir suchen die Lösungen derselben.

Setzen wir wie bei den beiden vorhergehenden Beispielen

$$13^{536\,870\,912} : 2147\,483\,647$$

und bestimmen den Rest, so finden wir nach 38 Potenzierungen und Divisionen mit 2147 483 647

$$909\,664\,331^2 : 2147\,483\,647 = 385\,329\,684 \text{ Rest } 13, \text{ oder}$$
$$1237\,819\,316^2 : 2147\,483\,647 = 713\,484\,669 \text{ Rest } 13.$$

Wir entwickeln die obere Zeile in einen K.-Bruch, also

$$\frac{\sqrt{13} - 909\,664\,331}{2147\,483\,647} =$$

$$= \begin{array}{rcl} -909\,664\,331 & \Big(& 909\,664\,331 \quad 139\,004\,963 \quad 38\,714\,845 \\ 2147\,483\,647 & \Big(& 385\,329\,684 \quad 50\,145\,059 \quad 29\,890\,068 \\ 0 & & 2 \qquad\quad 2 \qquad\quad 1 \end{array}$$

$$\begin{array}{rcl} 8\,824\,779 \quad 1\,008\,466 \quad 227\,788 \quad 94\,859 \quad 27\,167 \quad 5\,361 & & \\ 2\,605\,437 \quad 390\,339 \quad 132\,929 \quad 67\,692 \quad 10\,903 \quad 2\,636 & & \\ 3 \qquad 2 \qquad 1 \qquad 1 \qquad 2 \qquad 2 & & \\ 89 \quad 5 \quad 3 \quad \ldots\ldots & \Big) & \\ 3 \quad 4 \quad 1 \quad \ldots\ldots & \Big) & \\ 28 \quad 2 \quad 6^{+} \ldots\ldots & \Big) & . \end{array}$$

Schreibt man wieder nach bekannter Manier den K.-Bruch

$$3\ (2, 28, 2, 2, 1, 1, 2, 3, 1, 2, 2,)$$

und rollt ihn auf, so wird

$$\frac{A_{n-1}}{B_{n-1}} = \frac{179\,721}{51\,476}. \qquad (n - 1 = 11)$$

Mit diesem Wert, der hervorgegangen ist aus einem K.-Bruch mit ungerader Anzahl der Teilnenner der primitiven Periode, wird man die Gleichungen

$$X = 179\,721, \quad Y = 51\,476,$$

$$X^2 - 13 \cdot Y^2 = -2147\,483\,647$$

befriedigen. Man müßte somit zwei Perioden des K. Bruches aufrollen, um einen positiven Wert $+ 2147\,483\,647 = + 2^{31} - 1$ zu erhalten.

Wir haben bei der Entwicklung in der Periode der vollständigen Quotienten den Teilquotienten $Q = 1$ erhalten, und darum können alle erweiterten Anwendungen stattfinden, die die Theorie über positive Determinanten einer binären quadratischen Form mit sich bringt.

Erstens erhalten wir unendlich viele Lösungen der Gleichung

$$X^2 - 13 \cdot Y^2 = \left| 2147\,483\,647 \right|,$$

zweitens ebenso viele der Gleichung

$$X^2 - 13 \cdot Y^2 = \left| 2147\,483\,647 \right|^n,$$

und drittens können wir die Formel anwenden

$$\frac{Z_{n-1}\, t \pm 13 \cdot N_{n-1}\, u}{Z_{n-1}\, u \pm N_{n-1}\, t} = \frac{Z_n}{N_n},$$

wo

$$\frac{Z_{n-1}}{N_{n-1}} = \frac{A_{n-1}}{B_{n-1}} = \frac{179\,721}{51\,476}$$

ist und die Werte t und u aus der Gleichung $t^2 - 13 \cdot u^2 = \pm 1$ zu entnehmen sind. In diesem Falle ist $t = 18$ und $u = 5$.

Setzen wir entsprechend der Formel die genannten Werte ein, so erhalten wir vorerst die zwei Werte

$$\frac{Z_0}{N_0} = \frac{110\,962}{27\,963} \text{ und } \frac{Z_2}{N_2} = \frac{6\,580\,918}{1\,825\,173},$$

die beide die Gleichung

$$X^2 - 13 \cdot Y^2 = + 2147\,483\,647$$

befriedigen.

Hiermit sei die weitere Rechnung, oder das Problem, die Primzahl $2^{31} - 1$ in ihre quadratischen Teiler zu zerlegen, fürs erste als hinreichend zu betrachten. Es sei denn, daß noch andere Werte erwünscht sind mit einer Zerlegung, in welcher D eine Primzahl der hier nicht vorliegenden Art ist, unter der Voraussetzung natürlich, daß D quadratischer Rest des Moduls $2^{31} - 1$ ist.