Pythagoreische Zahlentripel

und die 4 Primzahltypen modulo 8 nach Georg Glöckler

Peter Baum*

1 Zahlentripel

Bekanntlich gewinnt man alle pythagoreischen Zahlentripel (x, y, z) mit $x^2+y^2 = z^2$ und $x, y, z \in \mathbb{N}$ wegen der Identität

$$\left(a^2 - b^2\right)^2 + (2ab)^2 = \left(a^2 + b^2\right)^2$$

durch die Formeln

$$x = a^2 - b^2 \qquad y = 2ab \qquad z = a^2 + b^2$$

mit $a > b > 0$.

Man nennt (x, y, z) ein primitives Zahlentripel, wenn x und y teilerfremd sind. Dies ist offenbar nur dann der Fall, wenn auch a und b teilerfremd und zudem nicht beide ungerade sind.

In der Tabelle 1 sind die ersten primitiven Tripel nach der Größe von $z = a^2+b^2$ gelistet. In weiteren Spalten sind die Summe $x+y$ und der Betrag der Differenz $x-y$ notiert. Die letzten vier Spalten enthalten die Primzahlen, geordnet in den vier Restklassen modulo 8.

Im Nachlass von Georg Glöckler befinden sich viele ähnliche Tabellen, unter den verschiedensten Gesichtspunkten untersucht. Dabei fielen ihm folgende Phänomene auf:

- In der Spalte z erscheinen nur die Primzahlen $p \equiv 1$ und $p \equiv 5 \bmod 8$ als Summe zweier Quadratzahlen, es fehlen die Primzahlen $p \equiv 3$ und $p \equiv 7 \bmod 8$.
- In den Spalten $x + y$ und $x - y$ erscheinen nur die Primzahlen $p \equiv 1$ und $p \equiv 7 \bmod 8$, es fehlen die Primzahlen $p \equiv 3$ und $p \equiv 5 \bmod 8$.
- Die Primzahlen $p \equiv 1 \bmod 8$ kommen in allen drei Spalten vor.

*p.baum@posteo.de 09.03.2020

Die Ähnlichkeit der Spalten $x+y$ und $x-y$ hat einen einfachen Grund: Es ist

$$x+y = a^2 - b^2 + 2ab \qquad x-y = \left(a^2 - b^2\right) - 2ab$$
$$x+y = (a+b)^2 - 2b^2 \qquad x-y = (a-b)^2 - 2b^2$$

das heißt, die Zahlen in beiden Spalten werden durch dieselbe quadratische Form

$$u^2 - 2v^2 = p$$

dargestellt.

Dies ist eine sogenannte Pellsche Gleichung. In dem Artikel „Die Pellsche Gleichung und Kettenbruchentwicklungen“[1] hat Georg Glöckler, ausgehend von pythagoreischen Zahlentripel, die Pellsche Gleichung $u^2-2v^2 = \pm 1$ untersucht und auf S. 6 rein empirisch festgestellt:

> „Diejenigen pythagoräischen Zahlentripel, deren Basiswerte sich nur um 1 unterscheiden, vermitteln gleichzeitig die möglichen Lösungen der Pellschen Gleichung.“

Dies folgt so: Wegen

$$z-y = (a-b)^2 \qquad z-x = 2b^2$$

ist

$$(z-y)-(z-x) = x-y$$
$$(a-b)^2 - 2b^2 = x-y$$

und daher sind $u = \sqrt{z-y}$ und $v = \sqrt{\frac{1}{2}(z-x)}$ die Lösungen der Pellschen Gleichung $u^2 - 2v^2 = \pm 1$, falls $x-y = \pm 1$ ist.

[1] Mathematisch-Physikalische Korrespondenz Nr. 210, Michaeli 2002

Pythagoreische Tripel und Primzahlen

		x	y	z	x + y	x - y	Modulo 8			
a	b	$a^2 - b^2$	2ab	$a^2 + b^2$	$a^2 - b^2 + 2ab$	$a^2 - b^2 - 2ab$	≡ 1	≡ 3	≡ 5	≡ 7
2	1	3	4	5	7	1	1	3	5	7
3	2	5	12	13	17	7	17	11	13	23
4	1	15	8	17	23	7	41	19	29	31
4	3	7	24	25	31	17	73	43	37	47
5	2	21	20	29	41	1	89	59	53	71
6	1	35	12	37	47	23	97	67	61	79
5	4	9	40	41	49	31	113	83	101	103
7	2	45	28	53	73	17	137	107	109	127
6	5	11	60	61	71	49	193	131	149	151
7	4	33	56	65	89	23	233	139	157	167
8	1	63	16	65	79	47	241	163	173	191
8	3	55	48	73	103	7	257	179	181	199
7	6	13	84	85	97	71	281	211	197	223
9	2	77	36	85	113	41	313	227	229	239
8	5	39	80	89	119	41	337	251	269	263
9	4	65	72	97	137	7	353	283	277	271
10	1	99	20	101	119	79	401	307	293	311
10	3	91	60	109	151	31	409	331	317	359
8	7	15	112	113	127	97	433	347	349	367
11	2	117	44	125	161	73	449	379	373	383
11	4	105	88	137	193	17	457	419	389	431
9	8	17	144	145	161	127		443	397	439
12	1	143	24	145	167	119		467	421	463
10	7	51	140	149	191	89			461	
11	6	85	132	157	217	47				
12	5	119	120	169	239	1				
13	2	165	52	173	217	113				
10	9	19	180	181	199	161				
11	8	57	176	185	233	119				
13	4	153	104	185	257	49				
12	7	95	168	193	263	73				
14	1	195	28	197	223	167				
13	6	133	156	205	289	23				
14	3	187	84	205	271	103				
11	10	21	220	221	241	199				
14	5	171	140	221	311	31				
15	2	221	60	229	281	161				
13	8	105	208	233	313	103				
15	4	209	120	241	329	89				
14	7	147	196	245	343	49				
16	1	255	32	257	287	223				
15	6	189	180	261	369	9				
12	11	23	264	265	287	241				
16	3	247	96	265	343	151				
13	10	69	260	269	329	191				
14	9	115	252	277	367	137				
16	5	231	160	281	391	71				
15	8	161	240	289	401	79				
16	7	207	224	305	431	17				
13	12	25	312	313	337	287				
14	11	75	308	317	383	233				

Tabelle 1: Pythagoreische Zahlentripel und Primzahlen

2 Primzahltypen

Die Verteilung der Primzahlen in Tabelle 1 führte Georg Glöckler zu der Unterscheidung der Primzahlen nach ihren Resten modulo 8 in die vier Typen

$$u = 8n + 1 \qquad q = 8n + 3 \qquad p = 8n + 5 \qquad r = 8n + 7$$

und er kommt zu dem Ergebnis, dass diese vier Typen durch die quadratischen Formen

$$r = x^2 - 2y^2 \qquad p = x^2 + y^2 \qquad q = x^2 + 2y^2 \tag{1}$$

und

$$u = x_1^2 + y_1^2 = x_2^2 + 2y_2^2 = x_3^2 - 2y_3^2$$

mit natürlichen Zahlen x und y dargestellt werden können.

Während die Typen r, p und q nur jeweils eine der drei Darstellungen gestatten, was noch zu zeigen ist, gibt es für jede der drei Darstellungen jeweils natürliche Zahlen x und y, die jede Primzahl vom Typus u liefert. Glöckler nennt diesen Typus daher universell.

Der Satz von Fermat besagt u.a., dass es zu jeder Zahl $z = 4n + 1$ genau zwei Zahlen x und y mit $z = x^2 + y^2$ gibt, also auch für die Primzahlen

$$u = 4\,(2n) + 1 = 8n + 1 \qquad \text{und} \qquad p = 4\,(2n + 1) + 1 = 8n + 5\,.$$

Wir wollen nun zeigen, dass die Formeln (1) in der Tat für die Typen r, p und q charakteristisch sind. Hierzu stellen wir zunächst fest, dass das Quadrat z^2 einer ungeraden Zahl $z = 2n + 1$ stets zur Restklasse 1 modulo 8 gehört:

$$\begin{aligned}(2n + 1)^2 &= 4n^2 + 4n + 1\\ (2n + 1)^2 &= 4n\,(n + 1) + 1\\ (2n + 1)^2 &= 8m + 1\end{aligned}$$

da stets $n\,(n + 1) = 2m$ eine gerade Zahl ist, weil entweder n oder n+1 gerade ist.

Wenn man nun alle Zahlen $z = x^2 + 2y^2$ untersucht, so gibt es für ungerades z (also auch für Primzahlen > 2) wegen $x^2 \equiv 1 \bmod 8$ (bei ungeradem x) nur folgende 2 Fälle:

1. $x^2 = 8n + 1$ und $y^2 = 8m + 1$, $\Longrightarrow x^2 + 2y^2 = 8n + 16m + 3 \equiv 3 \bmod 8$
2. $x^2 = 8n + 1$ und $y^2 = 4m$, $\Longrightarrow x^2 + 2y^2 = 8n + 8m + 1 \equiv 1 \bmod 8$

Daher können weder die Primzahltypen $p \equiv 5$ mod 8 noch die Typen $r \equiv 7$ mod 8 die Darstellung $x^2 + 2y^2$ besitzen.

Die entsprechende Untersuchung der Zahlen $z = x^2 - 2y^2$ liefert

1. $x^2 = 8n + 1$ und $y^2 = 8m + 1$, $\Longrightarrow x^2 - 2y^2 = 8n - 16m - 1 \equiv 7 \bmod 8$

2. $x^2 = 8n + 1$ und $y^2 = 4m$, $\Longrightarrow x^2 - 2y^2 = 8n - 8m + 1 \equiv 1 \bmod 8$

Daher können weder die Primzahltypen $p \equiv 5$ mod 8 noch die Typen $q \equiv 3$ mod 8 die Darstellung $x^2 - 2y^2$ besitzen.

Die entsprechende Untersuchung von $2x^2 - 1$ liefert

1. $x^2 = 8n + 1 \Longrightarrow 2x^2 - 1 = 16n + 1 \equiv 1 \bmod 8$
2. $x^2 = 4n \Longrightarrow 2x^2 - 1 = 8n - 1 \equiv 7 \bmod 8$

Daher können weder die Primzahltypen $q \equiv 3$ mod 8 noch die Typen $p \equiv 5$ mod 8 die Darstellung $2x^2 - 1$ besitzen.

Damit ist aber noch nicht gezeigt, dass

- jede Primzahl $q \equiv 3 \bmod 8$ tatsächlich eine Darstellung $q = x^2 + 2y^2$ besitzt,
- jede Primzahl $r \equiv 7 \bmod 8$ tatsächlich eine Darstellung $r = x^2 - 2y^2$ besitzt,
- jede Primzahl $u \equiv 1 \bmod 8$ tatsächlich sowohl eine Darstellung $u = x^2 + 2y^2$ als auch eine Darstellung $u = x^2 - 2y^2$ besitzt.

Dies folgt aber – nach einer Darstellung von Gerhard Kowol – folgendermaßen:

Es sei $ax^2 + bxy + cy^2 = (a, b, c)$ und $D = b^2 - 4ac$. Die Darstellbarkeit einer Primzahl p durch $x^2 + ny^2$, kurz $(1, 0, n) = p$, wird durch folgenden Satz vollständig geklärt.

Satz 1. *Sei $n \in \mathbb{Z}$ und p Primzahl mit $(D, p) = 1$, $D = -4n$. Ist p durch $(1, 0, n)$ darstellbar, so folgt D ist QR (quadratischer Rest) mod p. Ist umgekehrt D QR mod p und die Klassenzahl h(D) gleich 1, dann ist p so darstellbar.*

Beweis. ($\Rightarrow$): Aus $x^2 + ny^2 = p$ folgt $x^2 \equiv -ny^2\,(p)$. Da ersichtlich $(y, p) = 1$ gilt, gibt es ein ganzzahliges z mit $yz \equiv 1\,(p)$. Multipliziert man die erste Kongruenz mit $4z^2$, so erhält man das Gewünschte: $(2xz)^2 \equiv -4n = D\,(p)$.

($\Leftarrow$): Sei D QR mod p. Dann existiert ein ganzzahliges q mit $D \equiv q^2\,(p)$. Man kann q als gerade annehmen, andernfalls man q durch q + p ersetzt. Es ist also $D \equiv q^2 \equiv 0\,(4)$. Zusammen mit der vorigen Kongruenz liefert das $D \equiv q^2\,(4p)$. Daher existiert ein ganzzahliges r mit $D = q^2 - 4pr$. Die quadratische Form (p, q, r) hat somit Diskriminante D und stellt p dar, indem man $x = 1$, $y = 0$ einsetzt. Auch ist sie primitiv, andernfalls würde $p \mid q$, r gelten und damit $(D, p) \neq 1$, Wspr. Da nach Voraussetzung die Klassenzahl gleich 1 ist, sind alle primitiven Formen mit Diskriminante D zueinander äquivalent, stellen somit die selben Zahlen dar; insbesondere also p. □

Bemerkung 1. Da $\left(\frac{-4n}{p}\right) = \left(\frac{-n}{p}\right)$ (Legendresymbol) gilt, ist für die bei Georg Glöcklers Untersuchungen auftretenden Fälle nur zu klären, wann $\left(\frac{-1}{p}\right)$, $\left(\frac{-2}{p}\right)$, $\left(\frac{2}{p}\right)$ gleich 1 ist. Der erste und dritte Fall folgt aus dem 1. bzw. 2.

Ergänzungssatz. Der zweite durch Kombination wegen $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{2}{p}\right)$. Die beiden Faktoren müssen somit beide entweder $+1$ oder beide -1 sein. Ersteres erfüllen genau die Primzahlen der Gestalt p = 8n + 1, zweiteres die der Gestalt 8n + 3.

Bemerkung 2. Der Beweis ist konstruktiv, dh. man findet damit auch wirklich eine Lösung. In vielen Fällen, insbesondere stets wenn |n| Primzahl ist, kann man das auf den Seiten 10 und 11 für $x^2 + y^2$ bzw. $x^2 + 2y^2$ angegebene Verfahren, angepasst an das entsprechende n, anwenden. In den anderen Fällen kann man das Verfahren anwenden, um allgemein von einer beliebigen Form zur reduzierten überzugehen.

Bemerkung 3. Ist $x^2 + ny^2$ positiv definit, also n > 0, so ist $h(D) = 1$ genau für n = 1, 2, 3, 4, 7. Dabei entspricht der Fall n = 4 dem Fall n = 1 wegen $x^2 + 4y^2 = x^2 + (2y)^2$. In all diesen Fällen ist die Darstellung eindeutig; bei $n = 1$ kann man zusätzlich x und y vertauschen. Ist $x^2 + ny^2$ indefinit, also n < 0, so fängt die Liste der entsprechenden n an mit n = -2, -5, -13, -17, -29, -41, ... Es ist unbekannt, ob es nur endlich viele derartige n gibt. In all diesen Fällen existieren stets unendlich viele Lösungen. Wie man aus einer alle findet, ist bekannt.

Im Nachlass von Georg Glöckler (Nr. 8 der Liste) befinden sich zwei Tabellen (Tabelle 2 auf der nächsten Seite). Offenbar hat Glöckler erkannt, dass die Form $x^2 + 2y^2$ nur dann Primzahlen vom Typ $p = 8n + 1$ liefert, wenn x ungerade und y gerade ist, und Primzahlen vom Typ $p = 8n + 3$ nur dann, wenn x und y ungerade sind. Die Tabellen liefern zugleich die Lösungen x und y der Gleichung $p = x^2 + 2y^2$.

Eine Verallgemeinerung des Satzes von Fermat lautet:

Satz 2. *Eine positiv definite binäre quadratische Form mit der Determinante 1 stellt genau dann die ungerade Primzahl p dar, wenn* $p \equiv 1\,(4)$ *ist.*[2]

[2]Harald Scheid: Zahlentheorie, Mannheim1994, S.243

$1 + 8n = (2p+1)^2 + 2(2q)^2$

p \ q	0	1	2	3	4	5	6	7	8	9	10	11	12
0	(1)	–	–	73	–	–	–	401	521	–	457	577	–
1	–	17	41	–	137	–	–	401	–	673	–	–	–
2	–	–	–	97	–	–	313	–	–	–	–	–	1201
3	–	–	–	–	–	–	337	–	–	–	–	–	–
4	[illegible]	[illegible]	[illegible]	–	–	281	–	–	593	–	881	1049	–
5	–	–	–	193	–	–	409	–	–	769	–	–	–
6	–	–	–	241	–	–	457	–	–	–	–	–	1321
7	–	233	257	–	353	–	–	617	–	–	–	1193	–
8	–	–	–	–	–	–	577	–	–	937	–	–	–
9	–	–	–	433	–	–	–	–	–	1009	–	–	–
10	–	449	–	–	569	641	–	–	953	–	–	1409	–
11	–	–	–	601	–	–	–	–	–	–	–	–	1777
12	–	–	–	–	–	–	–	–	–	–	–	–	–
13			761										

$3 + 8n = (2p+1)^2 + 2(2q+1)^2$

p \ q	0	1	2	3	4	5	6	7	8	9	10	11	12
0	3	19	–	–	163	–	–	–	–	–	883	–	[illegible]
1	11	–	59	107	–	251	347	–	587	–	[illegible]	–	1259
2	–	43	–	–	–	–	–	–	–	–	907	–	–
3	–	67	–	–	211	–	–	499	–	–	–	–	–
4	83	–	131	179	–	–	419	–	659	–	–	–	–
5	–	139	–	–	283	–	–	571	–	–	–	–	–
6	–	–	–	–	331	–	–	619	–	–	–	–	–
7	227	–	–	–	–	467	563	–	–	947	–	1283	–
8	–	307	–	–	–	–	–	739	–	–	1171	–	–
9	–	379	–	–	523	–	–	811	–	–	–	–	–
10	443	–	491	–	–	683	–	–	1019	1163	–	1499	–
11	–	547	–	–	691	–	–	–	–	–	–	–	–
12	–	643	–	–	789	–	–	–	–	–	–	–	–

Tabelle 2: $x^2 + 2y^2$

Für kleine Primzahlen $p \equiv 1\,(4)$ kann man die Darstellungen $p = x^2+y^2$ und $p = x^2+2y^2$ durch Ausprobieren schnell finden. Man prüft einfach durch Einsetzen der natürlichen Zahlen $n \leq \frac{1}{2}(p-1)$ für x, ob die Differenz $p - x^2$ eine Quadratzahl oder ihr Doppel

ist. Das geht heutzutage insbesondere mit Hilfe der Tabellenkalkkation sehr schnell. Ein anderes Verfahren liefert die Theorie der binären quadratischen Formen und der quadratischen Reste modulo p.

3 Binäre quadratische Formen

Carl Friedrich Gauß hat in seinen „Disquisitiones Arithmeticae“ eine binäre quadratische Form folgendermaßen definiert:

$$F(x,y) = ax^2 + 2bxy + cy^2 = (a,b,c)$$

Gibt es zu einer Zahl p zwei Zahlen x,y, so dass

$$p = ax^2 + 2bxy + cy^2$$

so sagt man, die Zahl p wird durch die Form (a,b,c) dargestellt. Ist zudem $ggT(x,y) = 1$, so wird p *eigentlich* dargestellt.
In moderner Schreibweise mit Vektoren und Matritzen ist

$$ax^2 + 2bxy + cy^2 = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & b \\ b & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

mit $\begin{pmatrix} a & b \\ b & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax+by \\ bx+cy \end{pmatrix}$ und dem Skalarprodukt

$$\begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} ax+by \\ bx+cy \end{pmatrix} = ax^2 + bxy + bxy + cy^2$$

Hier ist $\triangle = det \begin{pmatrix} a & b \\ b & c \end{pmatrix} = ac - b^2$. In dieser Schreibweise wird also eine binäre quadratische Form durch die symmetrische Matrix $\mathbf{A} = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$ definiert.
Um nun die Zahlen p zu bestimmen, die durch eine solche Form dargestellt werden, ist zu fragen, ob es verschiedene Formen $\mathbf{A}$ und $\mathbf{A'}$ gibt, welche die gleichen Zahlen darstellen. Dies ist in der Tat der Fall. Denn für jede Zahl p hat die Form $A' = (p,m,n) = \begin{pmatrix} p & m \\ m & n \end{pmatrix}$, also $p = pu^2 + 2muv + nv^2$ die triviale Lösung $u = 1$, $v = 0$.

Solche Formen $\mathbf{A} = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$ und $\mathbf{A'} = \begin{pmatrix} a' & b' \\ b' & c' \end{pmatrix}$, die so beschaffen sind, dass es zu jeder Darstellung $p = ax_0^2 + 2bx_0y_0 + cy_0^2$ auch eine Darstellung $p = a'u_0^2 + 2b'u_0v_0 + c'v_0^2$ gibt, nennt man äqivalent. Wie hängen sie miteinander zusammen?
Es ist die Form $\mathbf{A'} = \begin{pmatrix} a' & b' \\ b' & c' \end{pmatrix}$ mit $p = \begin{pmatrix} u & v \end{pmatrix} A' \begin{pmatrix} u \\ v \end{pmatrix}$ eine zu $\mathbf{A} = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$ mit $p = \begin{pmatrix} x & y \end{pmatrix} \mathbf{A} \begin{pmatrix} x \\ y \end{pmatrix}$ äqivalente Form, falls eine Matrix $\mathbf{M} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ mit

$\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ und $det\,\mathbf{M} = \alpha \cdot \delta - \beta \cdot \gamma = 1$ existiert, so dass $\begin{pmatrix} u \\ v \end{pmatrix} = \mathbf{M} \begin{pmatrix} x \\ y \end{pmatrix}$ und

$$\mathbf{A} = \mathbf{M}^T \cdot \mathbf{A}' \cdot \mathbf{M}$$

ist, mit $\mathbf{M}^T = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}$. Es ist dann

$$\mathbf{A}' \cdot \mathbf{M} = \begin{pmatrix} a' & b' \\ b' & c' \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

$$\mathbf{A}' \cdot \mathbf{M} = \begin{pmatrix} a'\alpha + b'\gamma & a'\beta + b'\delta \\ b'\alpha + c'\gamma & b'\beta + c'\delta \end{pmatrix}$$

und

$$\mathbf{M}^T \cdot \mathbf{A}' \cdot \mathbf{M} = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} \begin{pmatrix} a'\alpha + b'\gamma & a'\beta + b'\delta \\ b'\alpha + c'\gamma & b'\beta + c'\delta \end{pmatrix}$$

$$\mathbf{A} = \begin{pmatrix} a'\alpha^2 + 2b'\alpha\gamma + c'\gamma^2 & a'\alpha\beta + b'\alpha\delta + b'\gamma\beta + c'\gamma\delta \\ a'\beta\alpha + b'\beta\gamma + b'\delta\alpha + c'\delta\gamma & a'\beta^2 + 2b'\beta\delta + c'\delta^2 \end{pmatrix}$$

und daher ist

$$a = a'\alpha^2 + 2b'\alpha\gamma + c'\gamma^2 \quad b = a'\alpha\beta + b'\left(\alpha\delta + \gamma\beta\right) + c'\gamma\delta \quad c = a'\beta^2 + 2b'\beta\delta + c'\delta^2 \quad (2)$$

Zwei äqivalente Formen haben dieselbe Determinante. Denn es ist wegen $det\,\mathbf{M}^T = det\,\mathbf{M} = 1$

$$\begin{aligned} det\,\mathbf{A}' &= det\,\left(\mathbf{M}^T\mathbf{A}\mathbf{M}\right) \\ &= det\,\mathbf{M}^T \cdot det\,\mathbf{A} \cdot det\,\mathbf{M} \\ &= det\,\mathbf{A} \end{aligned}$$

Wird nun eine Zahl von einer Form $\mathbf{A}$ dargestellt, so wird sie auch von jeder zu $\mathbf{A}$ äquivalenten Form $\mathbf{A}'$ dargestellt. Denn wegen der Rechenregeln $(\mathbf{A} \cdot \mathbf{B})^T = \mathbf{B}^T\mathbf{A}^T$und $\left(\mathbf{A}^{-1}\right)^T = \left(\mathbf{A}^T\right)^{-1}$ folgt aus $p = \begin{pmatrix} x & y \end{pmatrix} \mathbf{A} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}^T \mathbf{A} \begin{pmatrix} x \\ y \end{pmatrix}$

$$p = \begin{pmatrix} x \\ y \end{pmatrix}^T \mathbf{M}^T\mathbf{A}' \cdot \mathbf{M} \begin{pmatrix} x \\ y \end{pmatrix}$$

$$p = \left(\mathbf{M} \begin{pmatrix} x \\ y \end{pmatrix}\right)^T \cdot \mathbf{A}' \cdot \mathbf{M} \begin{pmatrix} x \\ y \end{pmatrix}$$

$$p = \begin{pmatrix} u & v \end{pmatrix} \mathbf{A}' \begin{pmatrix} u \\ v \end{pmatrix}$$

Eine Form (a, b, c) heißt positiv definit, wenn $\triangle > 0$ ist. Sie heißt reduziert, wenn $a < c$ und $-a < b \leq a$ oder $a = c$ und $0 \leq 2b \leq a$ ist.

Man kann nun zeigen:

Satz 3. *Jede positiv definite Form ist äqivalent zu genau einer reduzierten Form.*[3]

[3] H. Scheid: Zahlentheorie, Mannheim 1994, S.241

Alle zueinander äquivalente Formen bilden somit eine Klasse, die durch genau eine reduzierte Form repräsentiert wird. Die folgende Tabelle enthält alle reduzierten Formen für $0 < \triangle \leq 8$:

$\triangle$	1	2	3	4	5	6	7	8
(a,b,c)	$(1,0,1)$	$(1,0,2)$	$(1,0,3)$	$(1,0,4)$	$(1,0,5)$	$(1,0,6)$	$(1,0,7)$	$(1,0,8)$
			$(2,1,2)$	$(2,0,2)$	$(2,1,3)$	$(2,0,3)$	$(2,1,4)$	$(2,0,4)$
								$(3,1,3)$

Daher gibt es für $\triangle = 1$ und $\triangle = 2$ jeweils nur eine Äquivalenzklasse von binären quadratischen Formen.

Wie findet man nun zu einer Primzahl $p = 4n + 1$ die Darstellung $p = x^2 + y^2$?

Für jede Primzahl $p \equiv 1 \bmod 4$ ist -1 quadratischer Rest mod p, d.h. die Kongruenz $x^2 \equiv -1 \bmod p$ hat Lösungen.
Wenn man eine Lösung m gefunden hat, gibt es eine ganze Zahl n, so dass $m^2 = -1 + np$ ist. Die Form $p = pu^2 + 2muv + nv^2$ hat dann die Lösung $u = 1$, $v = 0$ und die Determinante $\triangle = np - m^2 = 1$.
Der nächste Schritt besteht darin, eine Matrix $\mathbf{M} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ mit $\alpha\delta - \beta\gamma = 1$ zu finden, so dass $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbf{M^T} \cdot \begin{pmatrix} p & m \\ m & n \end{pmatrix} \cdot \mathbf{M}$. Denn dann erhält man die Lösung (x, y) der Form $p = x^2 + y^2$ durch $\begin{pmatrix} x \\ y \end{pmatrix} = \mathbf{M^{-1}} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \delta \\ -\gamma \end{pmatrix}$, also $x = \delta$ und $y = -\gamma$.
Aus (2) folgt dann mit $A' = \begin{pmatrix} p & m \\ m & n \end{pmatrix}$ und $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$$1 = p\alpha^2 + 2m\alpha\gamma + n\gamma^2 \quad 0 = p\alpha\beta + m\,(\alpha\delta + \gamma\beta) + n\gamma\delta \quad 1 = p\beta^2 + 2m\beta\delta + n\delta^2 \quad (3)$$

Auflösen nach γ und δ liefert unter Berücksichtigung von $np - m^2 = 1$

$$\gamma = -\frac{m}{n}\alpha \pm \frac{1}{n}\sqrt{n - \alpha^2}$$
$$\delta = -\frac{m}{n}\beta \mp \frac{1}{n}\sqrt{n - \beta^2}$$

Da γ und δ ganze Zahlen sind, stehen unter der Wurzel Quadratzahlen, d.h. es ist

$$n - \alpha^2 = x^2 \qquad\qquad n - \beta^2 = y^2$$

und diese Bedingung ist erfüllt durch

$$y^2 = \alpha^2 \qquad\qquad x^2 = \beta^2$$

mit $\alpha^2 + \beta^2 = n$.
Somit folgt

$$\gamma = \frac{1}{n}(-m\alpha - \beta)$$
$$\delta = \frac{1}{n}(-m\beta + \alpha)$$

mit geeigneten Vorzeichen, damit in der Tat die Bedingung $\alpha\delta - \beta\gamma = 1$ erfüllt wird. Durch Einsetzen dieser Ergebnisse überzeugt man sich davon, dass auch die Gleichung $0 = p\alpha\beta + m(\alpha\delta - \beta\gamma) + n\gamma\delta$ in (3) erfüllt ist.

Als Beispiel wollen wir die Darstellung der Primzahl $541 = 10^2 + 21^2$ auf diese Weise berechnen. Man findet $52^2 = 541 \cdot 5 - 1$ und damit die binäre quadratische Form

$$A' = \begin{pmatrix} 541 & 52 \\ 52 & 5 \end{pmatrix}$$

Wegen $5 = 1^2 + 2^2$ führt der Ansatz $\alpha = 1$ und $\beta = -2$ zu

$$\gamma = \frac{1}{5}(-52 + 2) \qquad \delta = \frac{1}{5}(52 \cdot 2 + 1)$$
$$\gamma = -10 \qquad \delta = 21$$

und es ist in der Tat $541 = 10^2 + 21^2$.

Es gibt genau $\frac{p-1}{2}$ quadratische Reste und Nichtreste modulo einer Primzahl p. Daher muss eine der Zahlen a mit $1 \leq a \leq \frac{p-1}{2}$ die Bedingung $a^2 \equiv -1\,(p)$ erfüllen, falls $p \equiv 1\,(4)$ ist.

Für die Form $A = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ erhält man aus (2) entsprechend

$$1 = p\alpha^2 + 2m\alpha\gamma + n\gamma^2 \qquad 0 = p\alpha\beta + m(\alpha\delta + \gamma\beta) + n\gamma\delta \qquad 2 = p\beta^2 + 2m\beta\delta + n\delta^2$$

und da $det\mathbf{A} = 2$ ist, muss auch $det\mathbf{A'} = np - m^2 = 2$ sein, d.h. es ist $m^2 \equiv -2\,(p)$.
Es folgt

$$\gamma = -\frac{m}{n}\alpha \pm \frac{1}{n}\sqrt{n - 2\alpha^2} \qquad \delta = -\frac{m}{n}\beta \pm \frac{1}{n}\sqrt{2(n - \beta^2)}$$

Da γ und δ ganze Zahlen sind, ist

$$n - 2\alpha^2 = x^2 \qquad n - \beta^2 = 2y^2, \text{ also} \qquad 2\alpha^2 - \beta^2 = 2y^2 - x^2$$

und daher ergibt der Ansatz $x^2 = \beta^2$ und $y^2 = \alpha^2$ die Bedingung $2\alpha^2 + \beta^2 = n$ und wir erhalten

$$\gamma = -\frac{m}{n}\alpha - \frac{1}{n}\beta \qquad \delta = -\frac{m}{n}\beta + \frac{1}{n}2\alpha \tag{4}$$

mit geeigneten Vorzeichen, damit $n\,(\alpha\delta - \beta\gamma) = n$ erfüllt ist.
Die Darstellung $p = x^2 + 2y^2$ ist wegen $m^2 \equiv -2\,(p)$ nur für Primzahlen p mit dem quadratischen Rest -2 modulo p möglich, für die also $\left(\frac{-2}{p}\right) = 1$ ist.[4] Dies ist der Fall für $p \equiv 1\,(8)$ oder $p \equiv 3\,(8)$. Denn wegen $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$ ist $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$ und nach den Ergänzungssätzen zun quadratischen Reziprozitätsgesetz ist

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \qquad\qquad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Für $p \equiv 1\,(8)$ und $p \equiv 3\,(8)$ ist

$$\begin{aligned} p &= 8n+1 & \qquad p &= 8n+3 \\ \frac{p-1}{2} &= 4n & \qquad \frac{p-1}{2} &= 4n+1 \\ \frac{p^2-1}{8} &= 8n^2{+}2\mathrm{n} & \qquad \frac{p^2-1}{8} &= 8n^2+6n+1 \end{aligned}$$

Für $p = 8n+1$ folgt also $\left(\frac{-1}{p}\right) = 1$ und $\left(\frac{2}{p}\right) = 1$, daher auch $\left(\frac{-2}{p}\right) = 1$.
Für $p = 8n+3$ folgt also $\left(\frac{-1}{p}\right) = -1$ und $\left(\frac{2}{p}\right) = -1$, daher ebenfalls $\left(\frac{-2}{p}\right) = 1$.

Wir berechnen als Beispiel die Darstellung $p = x^2 + 2y^2$ für p =193. Man findet $34^2 = 6 \cdot 193 - 2$, also $m = 34$ und $n = 6$.
Aus (4) folgt

$$\gamma = -\frac{34}{6}\alpha - \frac{1}{6}\beta \qquad\qquad \delta = -\frac{34}{6}\beta + \frac{1}{6}2\alpha$$

und aus $2\alpha^2 + \beta^2 = 6$ ergibt sich der Ansatz $\alpha = -1$ und $\beta = -2$ und es folgt

$$\begin{aligned} \gamma &= \frac{34}{6} + \frac{1}{6}2 & \qquad \delta &= \frac{34}{6}2 - \frac{1}{6}2 \\ \gamma &= 6 & \qquad \delta &= 11 \end{aligned}$$

mit $\alpha\delta - \beta\gamma = -11 + 12 = 1$.
In der Tat ist $193 = 11^2 + 2 \cdot 6^2$.

Ich habe im Nachlass von Georg Glöckler allerdings keinen Hinweis gefunden, der nahe legt, dass Glöckler Lösungen einer quadratischen Form auf diesem Wege berechnet hat. Alles deutet darauf hin, dass er eine Lösung durch probieren und alle weiteren durch Rekursionsformeln gefunden hat.[5]

[4] Legendre-Symbol
[5] vgl. Gloeckler_136_Kompl_Qadrupel_200421.pdf