BULLETIN OF THE POLISH
ACADEMY OF SCIENCES
MATHEMATICS
Vol. 64, No. 2-3, 2016

NUMBER THEORY

On the Equation $a^2 + bc = n$ with Restricted Unknowns

by

M. SKAŁBA

Presented by Andrzej SCHINZEL

To the memory of Professor Jerzy Browkin

Summary. We extend our previous results concerning the equation $a^2 + bc = n$ to all primes n and deal also with the general case of non-square n. Moreover, we provide partial results on patterns of '1' and '11' in the continued fractions of $\sqrt{n}$.

For a given positive integer n which is not a perfect square we are interested in the triples of positive integers (a, b, c) satisfying the title equation

$$a^2 + bc = n \tag{1}$$

and the restriction

$$b < c < \sqrt{n}. \tag{2}$$

The set of all such triples will be denoted by $T(n)$ and their number by $t(n)$. By trivial verification, $t(3) = t(5) = t(7) = t(13) = t(23) = t(47) = 0$ but

$$T(11) = \{(3, 1, 2)\}, \quad t(11) = 1.$$

Similarly

$$T(67) = \{(5, 6, 7), (7, 3, 6), (8, 1, 3)\}, \quad t(67) = 3.$$

The last two examples are emanations of a general phenomenon we have proved in [3]:

if n is a prime of the form $8k + 3$ and $n > 3$ then $t(n)$ is odd and positive a fortiori.

2010 *Mathematics Subject Classification*: 11E25, 11E16, 11A55.
Key words and phrases: reduction of indefinite forms, continued fractions.
Received 6 August 2016.
Published online 14 December 2016.

DOI: 10.4064/ba8079-11-2016

First we state explicitly a direct generalization.

THEOREM 1. *If $p > 3$ is a prime then $t(p)$ is odd for $p \equiv 1, 3 \pmod 8$ and even for $p \equiv 5, 7 \pmod 8$.*

The cases $p \equiv 3, 1 \pmod 8$ are proved in [3, Theorems 1 and 3]. The remaining cases $p \equiv 5, 7 \pmod 8$ can be proved in a completely analogous manner.

The cases with $t(p)$ even are less attractive because the case $t(p) = 0$ is not excluded. Therefore the next theorem may be of some interest.

THEOREM 2. *If a prime $p \neq 13$ satisfies $p \equiv 5, 7 \pmod 8$ and either (a) $p \equiv 1 \pmod{12}$ or (b) $p \equiv \pm 1 \pmod 5$ then $t(p)$ is even and $t(p) \geq 2$.*

For the proof we need a lemma.

LEMMA 1.

(a) *If p is a prime satisfying $p \equiv 1 \pmod{12}$ then there exist positive integers x, y such that*

$$x^2 + 4xy + y^2 = p.$$

(b) *If p is a prime and $p \equiv \pm 1 \pmod 5$ then there exist positive integers x, y such that*

$$x^2 + 3xy + y^2 = p.$$

Proof. Both assertions follow easily from Zagier's reduction procedure (see [5, Teil II, §13]).

Proof of Theorem 2. (a) By Lemma 1 we have the representation

$$p = (x + y)^2 + 2xy \quad \text{with } x < y.$$

It follows that $(x+y, 2x, y) \in T(p)$ or $(x+y, y, 2x) \in T(p)$ (because $p \neq 13$), hence $t(p) \geq 1$ and finally $t(p) \geq 2$ by Theorem 1.

(b) In this case

$$p = (x + y)^2 + xy \quad \text{with } x < y,$$

and $(x + y, x, y) \in T(p)$.

From now on we only assume that a given positive integer n is not a perfect square. We want to investigate the set $T(n)$ and its magnitude $t(n)$.

For each $(a, b, c) \in T(n)$ we consider the quadratic form

$$f(x, y) = bx^2 - 2axy - cy^2. \tag{3}$$

The discriminant Δ of f equals $\Delta = 4n$. We will first prove that the form f is reduced. By definition we should verify that the parameter $\eta = (a + \sqrt{n})/b$ of the form f satisfies the inequalities

$$\eta > 1, \quad -1 < \bar{\eta} < 0 \tag{4}$$

(for the general definition of the parameter of a form consult e.g. [4]). In fact

$$\eta = \frac{a+\sqrt{n}}{b} > \frac{\sqrt{n}}{b} > 1, \qquad \bar\eta = \frac{a-\sqrt{n}}{b} < 0,$$
$$\bar\eta = \frac{a-\sqrt{n}}{b} = \frac{-c}{a+\sqrt{n}} > \frac{-c}{\sqrt{n}} > -1.$$

The parameters η coming from triples $(a,b,c) \in T(n)$ are characterized by the system of inequalities

$$\eta > 1, \qquad -1 < \bar\eta < 0, \qquad \eta - \bar\eta > 2, \qquad 2\eta\bar\eta > \bar\eta - \eta, \tag{5}$$

and form a suitable "fundamental region" in the plane $(\bar\eta, \eta)$. So, we can call our form $f(x,y)$ *super-reduced.*

In the next theorem we show a connection of equation (1) under the restrictions (2) with continued fractions.

THEOREM 3. *Let n be a positive integer not a square. In order to list all triples (a,b,c) satisfying $a^2+bc=n$ and $b,c<\sqrt{n}$ we can proceed as follows. Fix a reduced form $g_j(x,y)$ in each $GL(2,\mathbb{Z})$-equivalence class of forms with discriminant $\Delta = 4n$ for $j=1,\dots,h$ where h is the number of these classes. Let η_j be the parameter of the form g_j. Let $p_u^{(j}/q_u^{(j)}, p_{u+1}^{(j)}/q_{u+1}^{(j)}$ be a pair of consecutive convergents to η_j, where $-1 \le u \le k_j - 2$, k_j being the period of η_j. If*

$$|g_j(p_u^{(j)}, q_u^{(j)})| < \sqrt{n} \quad \text{and} \quad |g_j(p_{u+1}^{(j)}, q_{u+1}^{(j)})| < \sqrt{n}$$

then $b := |g_j(p_u^{(j)}, q_u^{(j)})|$, $c := |g_j(p_{u+1}^{(j)}, q_{u+1}^{(j)})|$ and $a := \sqrt{n-bc}$ form a desired triple.

Moreover, all the relevant triples (a,b,c) can be obtained in the above way.

LEMMA 2. *If a rational fraction p/q has the property that*

$$\left|\xi - \frac{p}{q}\right| < \frac{1}{2q^2} \tag{6}$$

then p/q is a convergent of ξ.

This is Satz 2.11 from [2].

LEMMA 3. *Let $\xi = [b_0, b_1, \dots]$ be an infinite continued fraction with all b_j positive integers and let P_λ/Q_λ denote its λth convergent. Then for each $\lambda \ge 1$,*

$$\frac{P_\lambda}{Q_\lambda} - \frac{P_{\lambda-1}}{Q_{\lambda-1}} = (-1)^{\lambda-1}\frac{1}{Q_\lambda Q_{\lambda-1}},$$
$$\frac{P_{\lambda+1}}{Q_{\lambda+1}} - \frac{P_{\lambda-1}}{Q_{\lambda-1}} = (-1)^{\lambda-1}\frac{b_{\lambda+1}}{Q_{\lambda+1} Q_{\lambda-1}},$$
$$\frac{P_{\lambda+2}}{Q_{\lambda+2}} - \frac{P_{\lambda-1}}{Q_{\lambda-1}} = (-1)^{\lambda-1}\frac{b_{\lambda+1}b_{\lambda+2}+1}{Q_{\lambda+2} Q_{\lambda-1}},$$

and for $n \geq 3$ one has

$$\frac{P_{\lambda+n}}{Q_{\lambda+n}} - \frac{P_{\lambda-1}}{Q_{\lambda-1}} = (-1)^{\lambda-1}\frac{b}{Q_{\lambda+n}Q_{\lambda-1}} \quad \text{with } b \geq 3.$$

These are special cases of formula (4) on page 14 of [2].

LEMMA 4. *Let $g(x,y)$ be a reduced form with a non-square positive discriminant Δ. If coprime integers r,s satisfy the inequality*

$$|g(r,s)| < \sqrt{\Delta}/2$$

then r/s is a convergent of η or $\overline{\eta}$ where η is the parameter of the form $g(x,y)$.

For completeness we provide the proof of this lemma, because we have not found it in the literature. Write explicitly $g(x,y) = ax^2+bxy+cy^2$ where $\gcd(a,b,c) = 1$ and $b^2 - 4ac = \Delta$. We have $\eta = \frac{-b+\sqrt{\Delta}}{2a}$ (see e.g. [4]). So

$$g(x,y) = a(x-y\eta)(x-y\overline{\eta}),$$

where the bar denotes conjugation in the real quadratic field $\mathbb{Q}(\sqrt{\Delta})$. Let (t,u) be the smallest non-trivial solution of the equation

$$|t^2 - \Delta u^2| = 4$$

in positive integers t,u. Define the sequence (r_n,s_n) by the equation

$$2ar_n - (-b+\sqrt{\Delta})s_n = (2ar - (-b+\sqrt{\Delta})s)\left(\frac{t-u\sqrt{\Delta}}{2}\right)^n.$$

First we have

$$\lim_{n\to\infty}|r_n| = \lim_{n\to\infty}|s_n| = \infty \quad \text{and} \quad \lim_{n\to\infty}|r_n - s_n\eta| = 0.$$

Fix a number $\varepsilon > 0$ satisfying

$$\frac{\lfloor\sqrt{\Delta}/2\rfloor}{\sqrt{\Delta}-|a|\varepsilon} < \frac{1}{2},$$

and choose n such that

$$|r_n - s_n\eta| < \varepsilon < \varepsilon|s_n|.$$

Then

$$\left|\frac{r_n}{s_n} - \eta\right| < \varepsilon,$$

$$\left|\frac{r_n}{s_n} - \overline{\eta}\right| > |\eta-\overline{\eta}| - \left|\frac{r_n}{s_n} - \eta\right| > \frac{\sqrt{\Delta}}{|a|} - \varepsilon.$$

Hence

$$\left|\frac{r_n}{s_n} - \eta\right| = \frac{|g(r,s)|}{|a|s_n^2} \Big/ \left|\frac{r_n}{s_n} - \overline{\eta}\right| < \frac{\lfloor\sqrt{\Delta}/2\rfloor}{|a|s_n^2}\cdot\left(\frac{\sqrt{\Delta}}{|a|} - \varepsilon\right)^{-1} < \frac{1}{2s_n^2}.$$

By Lemma 2 the fraction r_n/s_n is a convergent to η.

Now it follows that the initial fraction r/s is a convergent to η or $\overline{\eta}$. In fact, let $\overline{a_0, a_1, \ldots, a_{k-1}}$ be the continued fraction expansion of η, with k being the period. Define $(a'_n)_{n\in\mathbb{Z}}$ for all integral indices n by "prolonging mod k":

$$a'_n := a_{n \bmod k} \quad \text{for } n \in \mathbb{Z}.$$

Moreover define recursively sequences p_n, q_n $(n \in \mathbb{Z})$ by

$$\begin{aligned} p_{-2} &= 0, \quad p_{-1} = 1, \quad p_n = a'_n p_{n-1} + p_{n-2}, \\ q_{-2} &= 1, \quad q_{-1} = 0, \quad q_n = a'_n q_{n-1} + q_{n-2} \quad (n \in \mathbb{Z}). \end{aligned}$$

It is easily verifiable (induction on n) that p_{-n}/q_{-n} is the $(n-1)$th convergent to $\overline{\eta}$ for $n \geq 2$.

Proof of Theorem 3. Let $f(x, y)$ be the form obtained from g_j by

$$f(x, y) = g_j(p_u^{(j)} x + p_{u+1}^{(j)} y, q_u^{(j)} x + q_{u+1}^{(j)} y).$$

The form f is equivalent to g_j and we get a desired triple by setting

$$b := |f(1, 0)|, \quad c := |f(0, 1)|, \quad a := \left| \frac{f(1, 0) + f(0, 1) - f(1, 1)}{2} \right|.$$

The point is that

$$f(1, 0)f(0, 1) = g_j(p_u^{(j)}, q_u^{(j)}) \cdot g_j(p_{u+1}^{(j)}, q_{u+1}^{(j)}) < 0$$

because $p_u^{(j}/q_u^{(j)}, p_{u+1}^{(j)}/q_{u+1}^{(j)}$ are consecutive convergents to η_j.

Now assume that (a, b, c) is a desired triple and consider the super-reduced form (3). There exists $j \in \{1, \ldots, h\}$ such that $f(x, y) = bx^2 - 2axy - cy^2$ is equivalent to $g_j(x, y)$. Let $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ satisfy

$$g_j(\alpha x + \beta y, \gamma x + \delta y) = f(x, y) \quad \text{and} \quad \alpha\delta - \gamma\beta = \pm 1.$$

Now

$$|g_j(\alpha, \gamma)| = |f(1, 0)| = b < \sqrt{n} \quad \text{and} \quad |g_j(\beta, \delta)| = |f(0, 1)| = c < \sqrt{n},$$

and we infer by Lemma 4 that each of the fractions α/γ and β/δ is a convergent to η or to $\overline{\eta}$. First we exclude the possibility that both η and $\overline{\eta}$ are involved: the numbers α/γ and β/δ would then be of distinct signs, hence so would be $\alpha\delta$ and $\beta\gamma$. This contradicts the equality $\alpha\delta - \beta\gamma = \pm 1$.

If both α/γ and β/δ are convergents to η then by Lemma 3 they are consecutive convergents, because

$$g_j(\alpha, \gamma) \cdot g_j(\beta, \delta) = b \cdot (-c) < 0.$$

Moreover we can assume that α/γ and β/δ lie in the first period, and we are done.

If both α/γ and β/δ are convergents to $\overline{\eta}$ then they are again consecutive convergents. We replace them by $\eta_j + \overline{\eta}_j - \alpha/\gamma$ and $\eta_j + \overline{\eta}_j - \beta/\delta$, which are consecutive convergents to η (we use the same trick of considering a two-sided infinite continued fraction as in the proof of Lemma 4).

We finish the paper by presenting some broader perspective connected with equations similar to (1). The solutions of these equations, suitably restricted, allow us to detect the patterns of '1' and '11' in the continued fractions of $\sqrt{p}$ for some primes p.

THEOREM 4. *Let p be a prime number of the form $12k+7$ and assume that $\mathbb{Z}[\sqrt{p}]$ is a unique factorization domain. Then*

(i) *the number 1 appears as a partial quotient in the continued fraction expansion of $\sqrt{p}$;*

(ii) *if additionally there exist positive integers x, y satisfying*

$$p = x^2 + xy + y^2, \quad y \text{ odd and } 3y < x, \tag{7}$$

then one can find two consecutive 1's in the continued fraction expansion of $\sqrt{p}$.

LEMMA 5. *Let p be a prime number of the form $3k+1$. Then*

(i) *there exist positive integers a, b, c satisfying*

$$p = a^2 - bc \quad \text{and} \quad b, c < \sqrt{p};$$

(ii) *if additionally there exist positive integers x, y satisfying (7) then there exist positive odd integers a, b, c satisfying*

$$4p = a^2 + bc \quad \text{and} \quad b, c < \sqrt{p}.$$

Proof. (i) It is very well known that there exist positive integers x, y such that

$$p = x^2 + xy + y^2 = (x+y)^2 - xy,$$

so for the proof of (i) it suffices to set $a = x+y$, $b = x$ and $c = y$.

(ii) Now we have

$$4p = 4x^2 + 4xy + 4y^2 = (2x+y)^2 + 3y \cdot y,$$

and by (7) we can set $a = 2x+y$, $b = 3y$, $c = y$.

LEMMA 6. *Let p, q be positive integers satisfying $|p^2 - \xi^2 q^2| < \xi$. Then p/q is a convergent of ξ.*

This is Satz 2.12 from [2].

Proof of Theorem 4. (i) By Lemma 5 there exist positive integers a, b, c satisfying

$$a^2 - p = bc \quad \text{and} \quad b, c < \sqrt{p}.$$

It follows that

$$a + \sqrt{p} = \gamma_1 \cdot \ldots \cdot \gamma_k \cdot \delta_1 \cdot \ldots \cdot \delta_l$$

where γ_i, δ_j are all irreducible in $\mathbb{Z}[\sqrt{p}]$ and with some $\varepsilon \in \{-1, 1\}$,

$$N(\gamma_1 \cdot \ldots \cdot \gamma_k) = \varepsilon b \quad \text{and} \quad N(\delta_1 \cdot \ldots \cdot \delta_l) = \varepsilon c.$$

Set

$$\gamma_1 \cdot \ldots \cdot \gamma_k = q + r\sqrt{p}, \qquad \delta_1 \cdot \ldots \cdot \delta_l = s + t\sqrt{p}.$$

First consider the case $kl = 0$. The equality $k = l = 0$ would imply $\varepsilon b = \varepsilon c = 1$ and $p = a^2 - 1$, a contradiction. Now consider the case $k > 0$ and $l = 0$. Then

$$0 < a^2 - p = b < \sqrt{p}, \quad \text{hence} \quad \sqrt{p} < a < \sqrt{p} + 1/2.$$

Let $\sqrt{p} = [b_0, b_1, \ldots]$. Then

$$b_0 = \lfloor \sqrt{p} \rfloor = a - 1 \quad \text{and} \quad \sqrt{p} - 1 < b_0 < \sqrt{p} - 1/2.$$

Finally,

$$b_1 = \left\lfloor \frac{1}{\sqrt{p} - b_0} \right\rfloor < 2, \quad \text{hence} \quad b_1 = 1.$$

Now assume that $k, l > 0$. We will work with the equality

$$a + \sqrt{p} = (q + r\sqrt{p})(s + t\sqrt{p}). \tag{8}$$

Without loss of generality we assume that $q, s > 0$. The equality $t = 0$ would imply $s = 1$, hence $l = 0$, which is not the case. Similarly, $r \neq 0$. Using

$$|q^2 - pr^2| = b < \sqrt{p}, \qquad |s^2 - pt^2| = c < \sqrt{p}$$

we infer by Lemma 6 that both $q/|r|$ and $s/|t|$ are convergents of $\sqrt{p}$. Comparing the coefficients of 1 and $\sqrt{p}$ on both sides of (8) we get

$$a = qs + prt, \qquad 1 = qt + rs.$$

It follows that (8) can be rewritten as

$$a + \sqrt{p} = (q - r\sqrt{p})(s + t\sqrt{p})$$

with all q, r, s, t positive and satisfying $qt - rs = 1$ and $(q, r) = (s, t) = 1$. Set

$$\frac{q}{r} = \frac{P_\mu}{Q_\mu} \quad \text{and} \quad \frac{s}{t} = \frac{P_\nu}{Q_\nu}.$$

We obviously have $\mu \neq \nu$. Moreover $\mu \equiv \nu \pmod 2$ because

$$(q^2 - pr^2)(s^2 - pt^2) = a^2 - p = bc > 0.$$

Concluding, by Lemma 3 we have $\{\mu, \nu\} = \{\lambda - 1, \lambda + 1\}$ and

$$b_{\max(\mu,\nu)} = 1.$$

(ii) Using Lemma 5 we now start with the equality

$$a^2 - 4p = -bc \quad \text{with } a, b, c \text{ odd positive and } b, c < \sqrt{p}.$$

In the same way as in case (i) we decompose $a + 2\sqrt{p}$ into irreducibles

$$a + 2\sqrt{p} = \gamma_1 \cdot \ldots \cdot \gamma_k \cdot \delta_1 \cdot \ldots \cdot \delta_l$$

in such a way that

$$N(\gamma_1\cdot\ldots\cdot\gamma_k)=\varepsilon b \quad\text{and}\quad N(\delta_1\cdot\ldots\cdot\delta_l)=-\varepsilon c$$

with $\varepsilon\in\{-1,1\}$ properly chosen. Set again

$$\gamma_1\cdot\ldots\cdot\gamma_k=q+r\sqrt{p},\qquad \delta_1\cdot\ldots\cdot\delta_l=s+t\sqrt{p}.$$

Start with the case $kl=0$. The subcase $k=l=0$ is not possible because then $a^2-4p=-1$, a contradiction. If $k>0$ and $l=0$ we have

$$(2f+1)^2-4p=-b>-\sqrt{p},\quad\text{and hence}\quad \sqrt{p}>f+\frac{1}{2}>\sqrt{p-\sqrt{p}/4}$$

where $a=2f+1$. We shall prove that $\sqrt{p}=[f,1,1,\ldots]$. Obviously $f<\sqrt{p}$; in order to prove $f>\sqrt{p}-1$ it suffices to show that

$$\sqrt{p-\sqrt{p}/4}-\frac{1}{2}>\sqrt{p}-\frac{2}{3}, \tag{9}$$

which is equivalent to $9p>1$, so it does hold. Concluding, $b_0=\lfloor\sqrt{p}\rfloor=f$. Further $f<\sqrt{p}-1/2$, and hence

$$\xi_1=\frac{1}{\sqrt{p}-f}<2\quad\text{and}\quad b_1=1.$$

From $\sqrt{p}=[f,1,\xi_2]$ we get $\xi_2=(\sqrt{p}-f)/(f+1-\sqrt{p})$, and the inequality $\xi_2<2$ follows from (9); hence $b_2=1$.

For $k,l>0$ we proceed in the same way as in case (i) and arrive at the equality

$$a+2\sqrt{p}=(P_\mu-Q_\mu\sqrt{p})(P_\nu+Q_\nu\sqrt{p}),$$

but now

$$(P_\mu^2-pQ_\mu^2)(P_\nu^2-pQ_\nu^2)=a^2-4p=-bc<0,$$

hence $\mu\not\equiv\nu \pmod 2$. Using $P_\mu Q_\nu-P_\nu Q_\mu=2$ we infer by Lemma 3 that $\{\mu,\nu\}=\{\lambda+2,\lambda-1\}$, and finally

$$b_{\max(\mu,\nu)}=b_{\max(\mu,\nu)-1}=1.$$

Remark. The natural question arises about the applicability of our results to concrete primes p. By Hecke's prime number theorem [1] the primes p satisfying condition (7) form a positive proportion of all primes. The issue of unique factorization in $\mathbb{Z}[\sqrt{p}]$ is even more elusive—following Gauss we strongly believe that it holds for infinitely many primes p but we cannot prove it.

References

[1] E. Hecke, *Eine neue Art von Zetafunktionen und ihre Beziehung zur Verteilung der Primzahlen, I, II*, Math. Z. 1 (1918), 357–376, and Math. Z. 6 (1920), 11–51.

[2] O. Perron, *Die Lehre von den Kettenbrüchen*, Band I, *Elementare Kettenbrüche*, Teubner, Stuttgart, 1954.
[3] M. Skałba, *Note on an analogue of Fermat's two squares theorem for primes* $p \equiv 3 \pmod 8$, Int. J. Number Theory 13 (2017), 129–132.
[4] M. Trifković, *Algebraic Theory of Quadratic Numbers*, Universitext, Springer, 2013.
[5] D. B. Zagier, *Zetafunktionen und quadratische Körper*, Springer, Berlin, 1981.

M. Skałba
Institute of Mathematics
University of Warsaw
Banacha 2
02-097 Warszawa, Poland
E-mail: skalba@mimuw.edu.pl