MINIMAL SOLUTIONS OF DIOPHANTINE EQUATIONS

L. HOLZER

OUR aim is to prove: *If a, b, c are positive integers, if $ab > 1$, if a, b, c are relatively prime in pairs, and all are free of squares, if $-ab$ is a quadratic residue of c, bc of a, ca of b, and if $F(x, y, z) = ax^2 + by^2 - cz^2$, we have non-trivial solutions of*

$$F(x,y,z) = 0 \tag{1}$$

with the inequalities $|x| < \sqrt{bc}$, $|y| < \sqrt{ca}$, $|z| < \sqrt{ab}$.

It is clear that among the three inequalities we need only prove the third, since the two others necessarily follow.

If $ab = 1$ there is always a solution with $z = 1$. This case is known and will not be considered. The inequalities for x and y still hold, except that if $c = 1$ one sign $<$ must be replaced by $=$.

I

LEMMA 1: *If a_1,a_2,a_3 are any integers, $f(x,y,z) = a_1x + a_2y + a_3z$, there are integers u,v,w not all zero with $|u| < \sqrt{bc}$, $|v| < \sqrt{ca}$, $|w| < \sqrt{ab}$, $f(u,v,w) \equiv 0$ mod abc.*

Proof: Putting $x = 0, 1, \ldots, [\sqrt{bc}]$ (the bracket signifies the greatest integer), $y = 0, 1, \ldots, [\sqrt{ca}]$, $z = 0, 1, \ldots, [\sqrt{ab}]$, we have more than abc numbers $f(x,y,z)$. Therefore we must have a pair of triples (x_1,y_1,z_1) (x_2,y_2,z_2) with $f(x_1,y_1,z_1) \equiv f(x_2,y_2,z_2)$ mod abc. Putting $u = x_2 - x_1$ etc., we have $f(u,v,w) \equiv 0$ mod abc.

LEMMA 2: *There are numbers u,v,w satisfying the inequalities $|u| < \sqrt{bc}$, etc. and $F(u,v,w) \equiv 0$ mod abc.*

Proof: If $A^2 \equiv c/b$ mod a, $B^2 \equiv a/c$ mod b, $C^2 \equiv -b/a$ mod c we put $f = ab(x - Cy) + bc(y - Az) + ca\,(z - Bx)$ and have $u \equiv Cv$ mod c, $v \equiv Aw$ mod a, $w \equiv Bu$ mod b, $F(u,v,w) \equiv 0$ mod abc.

We use the abbreviation $F(u,v,w) = F_1$. If there is any other triple (u',v',w') essentially different, i.e. not $(-u, -v, -w)$, we write $F_3 = F(u',v',w')$, $F_2 = auu' + bvv' - cww'$.

LEMMA 3: *We have only the cases $F_1 = 0$ or abc, likewise F_3, whereas F_2 can be $= 0, \pm abc, \pm 2\,abc$.*

Proof: The proof for F_1 (and F_3) results immediately from the inequalities and $F_1 \equiv 0$ mod abc. The congruences $u \equiv Cv$ mod c, $u' \equiv Cv'$ mod c, etc. imply $auu' + bvv' \equiv 0$ mod c, etc., $F_2 \equiv 0$ mod abc. The inequalities show that F_2 has one of the five values.

Received February 9, 1949.

The theorem is proved if F_1 or $F_3 = 0$. Therefore we suppose $F_1 = F_3 = abc$.

For the rest of the demonstration it is significant that the cases $w = 0$ and $w = w'$ need not be taken into consideration in the sense that they either result in an equation (1) with $|z| < \sqrt{ab}$ or are impossible.

LEMMA 4: *The case $w = 0$ need not be taken into consideration.*

Proof: We have $au^2 + bv^2 = abc$, i.e. $au^2 \equiv 0 \bmod b$, and as a and b are prime to each other $u^2 \equiv 0 \bmod b$, $u \equiv 0 \bmod b$, for b is free of squares. Writing $u = bu_1$, $v = av_1$, so that u_1, v_1 are integers, we have $av_1^2 + bu_1^2 = c$, an equation (1) which satisfies $|z| = 1 < \sqrt{ab}$.

LEMMA 5: *The case $w = w'$ need not be taken into consideration.*

Proof: We have in their turn:

(i) $F_2 = abc$. At once $a(u - u')^2 + b(v - v')^2 = 0$, i.e., $u = u'$, $v = v'$. The two triples would not be different from each other.

(ii) $F_2 = -abc$. We have $a(u - u')^2 + b(v - v')^2 = 4\,abc$, and analogously as in the proof of Lemma 4 we get $u - u' = bu_1$, $v - v' = av_1$, $av_1^2 + bu_1^2 = 4c$, a solution of (1) with $z = 2 < \sqrt{ab}$ except for the cases $a = b = 1$; $a = 1$, $b = 2$ or 3 and vice versa. In all these cases there exists a solution with $z = 1$.

(iii) $F_2 = 0$. We get $a(u - u')^2 + b(v - v')^2 = 2abc$. As above there is

$$av_1^2 + bu_1^2 = 2c. \tag{2}$$

Expressing u', v' by u, v, u_1, v_1 and substituting in $F_2 = 0$ we get

$$uu_1 + vv_1 = c. \tag{3}$$

Eliminating u_1 from (2) and (3) we obtain the quadratic equation for v_1

$$(au^2 + bv^2)v_1^2 - 2bcvv_1 + (bc^2 - 2cu^2) = 0, \tag{4}$$

whose discriminant must be a square. This gives easily

$$2(au^2 + bv^2) - abc = ct^2 \quad (t \text{ an integer}). \tag{5}$$

Taking in account $F_1 = abc$, we obtain from (5)

$$ab + 2w^2 = t^2.$$

We can consider w and t as positive. We have $w < \sqrt{ab}, \sqrt{ab} < t < \sqrt{3ab}$. We put

$$(t + w\sqrt{2})(-1 + \sqrt{2}) = T + U\sqrt{2}, \text{ i.e., } T = -t + 2w,\ U = t - w.$$

We have $U > 0$. The boundary values $t = \sqrt{3ab}$ and $w = \sqrt{ab}$, $t = \sqrt{ab}$ and $w = 0$ give $U = \sqrt{ab}(\sqrt{3} - 1)$, $U = \sqrt{ab}$, respectively, whereas the relative minimum calculated by differentiating

$$t - w - \frac{\lambda}{2}(t^2 - 2w^2 - ab)$$

partially with respect to t and w gives

$$1 - \lambda t = 0,\ -1 + 2\lambda w = 0,\ t = 2w = \sqrt{2ab},\ U = \sqrt{\frac{ab}{2}}.$$

In any case we have $U < \sqrt{ab}$. We have also

$$T^2 + ab = 2U^2. \tag{6}$$

With n = norm with respect to the field $R(\sqrt{-ab})$ (R is the rational field) (2) and (6) can be written

$$\frac{1}{a}\,\mathrm{n}(av_1 + \sqrt{-ab}\,u_1) = 2c, \tag{7}$$

$$\mathrm{n}(T + \sqrt{-ab}) = 2U^2. \tag{8}$$

With the abbreviations

$$2X = v_1T - bu_1, \quad 2Y = av_1 + u_1T, \tag{9}$$

we get by multiplying (7) and (8),

$$aX^2 + bY^2 = cU^2. \tag{10}$$

If a and b are odd or a is even the numbers X and Y are integers. For a,b odd gives T odd and $u_1 \equiv v_1 \bmod 2$ (see equation (2)), and an even a gives T and u_1 even (equations (2) and (6) taking into account b odd).

If b is even we get a similar conclusion by interchanging a and b.

(iv) $F_2 = 2abc$. We should have $a(u - u')^2 + b(v - v')^2 = -2abc$ which is impossible as a,b,c are positive.

(v) $F_2 = -2abc$. We get in a similar manner as in (iii),

$$av_1^2 + bu_1^2 = 6c, \tag{11}$$

$$uu_1 + vv_1 = 3c, \tag{12}$$

the equations (2) and (3) with $3c$ instead of c. The number $2(au^2 + bv^2) - 3abc$ must be $3c$ times a square. We get

$$3t^2 - 2w^2 = -ab \quad (t \text{ an integer}). \tag{13}$$

Now let n be the norm with respect to the field $R(\sqrt{6})$. We have

$$2(w^2 - 3t^2/2) = ab, \quad \mathrm{n}\{(2 - \sqrt{6})(w + t\sqrt{6}/2)\} = -ab.$$

We consider t and w as positive. If $t < \sqrt{ab}$, $w < \sqrt{ab}$, $U = |t - w| < \sqrt{ab}$, with $T = 2w - 3t$ we have the equation analogously as before

$$T^2 + ab = 6U^2. \tag{14}$$

Combining (11) and (14) as before, we have with the abbreviations

$$v_1T - bu_1 = 6X, \quad av_1 + u_1T = 6Y, \tag{15}$$

the equation $aX^2 + bY^2 = cU^2$.

Now all depends on the fact that the left sides of the equations (15) are divisible by 6. The demonstration as above that $6X$ and $6Y$ are even, holds. With $6X = X'$, $6Y = Y'$ we have three cases:

(i) $a \equiv 0 \bmod 3$. Then $T \equiv 0 \bmod 3$, $bu_1^2 \equiv 0 \bmod 3$, $u_1 \equiv 0 \bmod 3$ as a and b are prime to each other, $X' \equiv Y' \equiv 0 \bmod 3$.

(ii) $b \equiv 0 \bmod 3$, $T \equiv 0 \bmod 3$, $X' \equiv 0 \bmod 3$, $v_1 \equiv 0 \bmod 3$, therefore $Y' \equiv 0 \bmod 3$.

(iii) If a,b both are not divisible by 3 we conclude: As $(-ab)$ is quadratic

residue mod 3 the rational prime number 3 is the product of two different conjugated prime ideals j,j' in $R(\sqrt{-ab})$. It is only necessary to change perhaps the sign of T and u_1 so that we have

$$v_1 + \sqrt{-ab}\,\frac{u_1}{a} \equiv 0 \bmod j,$$
$$T + \sqrt{-ab} \equiv 0 \bmod j'.$$

Then $X' + \sqrt{-ab}\,\frac{Y'}{a} \equiv 0 \bmod 3, \quad X' \equiv Y' \equiv 0 \bmod 3.$

II

Suppose $F_1 = abc$. We divide the set of triples (u,v,w) in categories.

(i) abc odd. We have four categories: (1) u,v,w odd; (2) u odd, v,w even; (3) and (4) analogously as (2) with v,w instead of u.

(ii) If abc is even we alter the letters for the moment as the sign of the coefficients is now of no importance. Let an equation $LX^2 + MY^2 + NZ^2 = 0$ be given with L even, therefore M, N odd. We have nine categories: u even, therefore v,w must be odd. For if v,w were even abc would result $\equiv 0 \bmod 4$. The categories are (1) $v \equiv w \equiv 1 \bmod 4$. (2) $v \equiv -w \equiv 1 \bmod 4$. (3) $-v \equiv w \equiv 1 \bmod 4$. (4) $v \equiv w \equiv -1 \bmod 4$. If u is odd we have the same four categories. A ninth will be v,w even.

Let us return to our original designation. In any case if two triples are of the same category we have $u \equiv u'$, $v \equiv v'$, $w \equiv w' \bmod 2$. In the case (ii) we have $F_2 \equiv F_1 \bmod 4$. In any case we have $F_2 = \pm abc$. With the integers

$$U = \frac{u \mp u'}{2}, \text{ etc.}$$

we have $|W| < \sqrt{ab}$ and $F(U,V,W) = 0$.

III

We exclude the case $ac = 1$, $b > 1$, for the solution (1,0,1) satisfies our main theorem. In the same way $bc = 1$, $a > 1$ is excluded. Therefore bc,ca,ab are not squares. All depends on the question: Are there different triples of the same category? We put all the pairs of triples (x_1,y_1,z_1) (x_2,y_2,z_2) (Lemma 1) with $z_2 > z_1$ in the drawer z_2. We have $(1 + [\sqrt{ab}])$ drawers, but on account of Lemma 4 we can consider the drawer $z_2 = 0$ void. How many pairs of triples do we find in the drawer with the greatest number of pairs?

We first prove two further lemmas.

LEMMA 6: *We consider H elements $A, \ldots$ by which a certain number of pairs of different elements is formed and arranged in classes according to the following rules*:

(1) *Each element occurs in at least one pair.*

https://doi.org/10.4153/CJM-1950-021-0 Published online by Cambridge University Press

(2) *The pairs in which any element occurs are all in the same class. We write class* (A).

(3) *If there are any pairs* (A,A') *and* (A,A'') *the pair* (A',A'') *exists and belongs to the class* (A).

(4) *The arrangement* (A,A') *or* (A',A) *in a pair is of no importance.*

Then there are at least $H/2$ *pairs.*

Proof: At first we form all pairs of the class (A) where A is any element. The $g \geqq 2$ elements which occur in pairs of the class (A) form $g(g-1)/2$ pairs, all existing and belonging to (A), therefore at least $g/2$ pairs.

If these are not all the pairs, then we have an element B not occurring in the pairs of (A). If g' elements occur in the pairs of (B) we have at least $g'/2$ pairs in the class (B).

Finally we see that, since

$$H = g + g' + g'' + \ldots + g^{(r)},$$

the number H' of the pairs satisfies

$$H' \geqq g/2 + g'/2 + \ldots + g^{(r)}/2 = H/2.$$

LEMMA 7: *If* S *is any of the numbers* bc, ca, ab *and* $S + t$ *is the first square surpassing the integer* S, *we have*

$$\sqrt{S+t} > \sqrt{S} + \frac{2t}{5\sqrt{S}}.$$

Proof: We have $S \geqq t$ ($S = t$ only in the case $S = 2$), therefore $25\,S > 20\,S + 4t$. Multiplying by $t/(25S)$ we get $t > \frac{4t}{5} + \frac{4t^2}{25S}$, $S + t > \left(\sqrt{S} + \frac{2t}{5\sqrt{S}}\right)^2$; hence the theorem.

We have at least

$$H = ([\sqrt{bc}] + 1)\,([\sqrt{ca}] + 1)\,([\sqrt{ab}] + 1) - abc$$

triples (x_1,y_1,z_1) which occur in any pair. According to the Lemma 8, $(H/2)$ is a lower bound for the number of pairs of triples.

According to Lemma 5 we can suppose that in a drawer all pairs have different values z_1. For, the case $w = w'$ need not be taken into consideration.

Now we use Lemma 7. If $(bc + P)$, $(ca + Q)$, $(ab + R)$ are the first squares surpassing the numbers bc, ca, ab, we have the following important inequality:

$$H > \left(\sqrt{bc} + \frac{2P}{5\sqrt{bc}}\right)\left(\sqrt{ca} + \frac{2Q}{5\sqrt{ca}}\right)\left(\sqrt{ab} + \frac{2R}{5\sqrt{ab}}\right) - abc$$

$$> \frac{2}{5}(Pa + Qb + Rc) > 2\,c/5.$$

We have less than $\sqrt{ab}$ drawers; the drawer with the most pairs contains more than $c/5\sqrt{ab}$ pairs. Supposing this number to exceed 5, so that $c > 25\sqrt{ab}$, we are sure to have at least 5 pairs in a drawer.

We have at least 5 different pairs of triples $(u^{(1)},v^{(1)},w^{(1)})$, $(u^{(2)},v^{(2)},w^{(2)})$, etc. All these pairs can be normed, e.g. by $w^{(j)} > 0$. These we can arrange into

pairs (u,v,w) (u',v',w'). As there are at most nine categories, at least one pair consists of two triples of the same category.

If $c > 25\sqrt{ab}$ we have solutions of (1) with $|z| < \sqrt{ab}$.

IV

The disagreeable restriction $c > 25\sqrt{ab}$ can be removed easily. We require the following theorem from the theory of numbers:

THEOREM: *In a field let j be any integer ideal, $\mathfrak{a}$ a number prime to j. There are infinitely many prime ideals (π) of the first degree with $\pi \equiv \mathfrak{a} \bmod j$.*

This theorem, the generalized prime number theorem, was found by E. Hecke and published in the *Mathematische Zeitschrift*, vol. 1 (1918), p. 375 (special case) and vol. 6 (1920), p. 38. A simple proof founded on Takagi's class field theory was given by H. Hasse in the *Jahresbericht der Deutschen Mathematikervereinigung*, vol. 35 (1926), p. 32.

According to this theorem there are an infinity of principal prime ideals (π) of the first degree, with $\pi \equiv 1 \bmod 8ab$, in the field $R(\sqrt{-ab})$ prime to c. The conjugated prime ideal π' and the norm $\mathrm{n}(\pi) = p$ (a rational prime number) satisfy the same congruence. If $p > 25\sqrt{ab}$, then $cp > 25\sqrt{ab}$. Suppose $-ab = 2^g t$, $g = 0$ or $g = 1$, t a negative integer. As p is a quadratic residue of t and $p \equiv 1 \bmod 8$, so also t, -1 and 2 are quadratic residues of p. The number $-ab$ is a quadratic residue of p, therefore of cp. As the numbers bc and p are quadratic residues of a, so also is the number bcp. In the same manner we find cap to be a quadratic residue of b.

Therefore there will be solutions of

$$ax^2 + by^2 = cpz^2$$

with $|z| < \sqrt{ab}$. We have

$$a\,\mathrm{n}\left(x + \frac{b}{\sqrt{-ab}}\,y\right) = pcz^2,$$

and as $ax^2 + by^2 \equiv 0 \bmod p$, we can get (by changing perhaps the sign of y) that the expression in the norm is $\equiv 0 \bmod \pi'$. We have

$$\mathrm{n}(\pi) = \mathrm{n}(r + s\sqrt{-ab}) = p,\ \pi = r + s\sqrt{-ab}$$

and multiplying,

$$a\,\mathrm{n}\{(rx + bsy) + \sqrt{-ab}(-ry/a + sx)\} = p^2cz^2.$$

Both terms $rx + bsy$ and $-ry/a + sx$ are divisible by p. With the abbreviations $rx + bsy = pX$, $-ry + asx = pY$ we have

$$aX^2 + bY^2 = cz^2, \quad \text{with } |z| < \sqrt{ab}.$$

V

REMARK 1: The bound for $|z|$ is exceedingly narrow, and apparently cannot be surpassed easily by any general one which is lower. We have, e.g.,

the equation $157\,x^2 + 3y^2 = z^2$ with the minimal solution $(1,9,20 = [\sqrt{471}]-1)$.

REMARK 2: If a has a quadratic factor, so that $a = a'r^2$ where a' is free of squares, we have a solution (x',y',z') of

$$a'x^2 + by^2 - cz^2 = 0 \qquad (a'bc > 1)$$

with $|x'| < \sqrt{bc}$, $|y'| < \sqrt{ca'}$, $|z'| < \sqrt{a'b}$. The solution (x',ry',rz') of (1) satisfies the inequalities of our main theorem.

We can proceed similarly if b and c have any quadratic factor.

REMARK 3: Writing $g(x,y) = ax^2 + 2bxy + cy^2$, we consider

$$g(x,y) = mz^2. \tag{16}$$

We suppose a,c,m positive integers, b an integer, $d = b^2 - ac$ negative, d' (positive) the greatest factor of d free of squares, m prime to d. Further we assume a,b,c to be co-prime (i.e., to have the greatest common divisor 1). We can replace the classical binary form $g(x,y)$ by any equivalent one. As g represents an infinity of prime numbers, and there are always equivalent forms whose first coefficient is any number represented by the form prime to the discriminant d, there is no restriction of generality in taking the first coefficient to be a prime number not dividing dm.

If (16) has solutions, so has the equation

$$u^2 - dv^2 = amz^2, \tag{17}$$

which we prove very easily by multiplying (16) by a, and putting $ax + by = u$, $y = v$. But also every solution of (17) gives a solution of (16), since we have $(u/v)^2 \equiv d \bmod a$, $b^2 \equiv d \bmod a$; and since a is a prime number, we have, after changing the sign of v if necessary, $u/v \equiv b \bmod a$, $u = ax + by$, $g(x,v) = mz^2$.

Thus the equation (16) has solutions with $|z| < |\sqrt{d}| = \sqrt{-d}$ if $d' > 1$ and these solutions are non-trivial. Of course, we assume the other conditions mentioned above too. If $d' = 1$, there are solutions with $|z| = |\sqrt{d}|$.

VI

Mr. Aubry gave, in *Sphinx-Oedipe*, vol. 8 (1913), p. 150, the following bounds: The equation $pX^2 = Y^2 + rZ^2$ has for $r > 0$ solutions with $|X| < \sqrt{2r/3}$. If r is negative he gives the bounds $|X| < \sqrt{-r}$, $|Z| < \sqrt{p}$, $|Y| < \sqrt{-2rp}$. Our bound for Y is better, namely $|Y| < \sqrt{-rp}$.

Graz, Austria