

Separatum

MATHEMATICA
SCANDINAVICA

55

ON THUE'S THEOREM

KURT MAHLER

Extract.

Let $F(x, y)$ be an irreducible binary form of degree $n \geq 3$ with integral coefficients. For large integers w an upper bound for the number of integral solutions of

$$F(u, v) = w, \quad (u, w) = (v, w) = 1$$

is established with a new method based on two different kinds of equivalence relations.

1.

Let

$$F(x, y) = f_0x^n + f_1x^{n-1}y + \dots + f_ny^n$$

be an irreducible binary form with integral coefficients, of degree $n \geq 3$ and of height

$$a = \max(|f_0|, |f_1|, \dots, |f_n|).$$

Further put

$$f(x) = F(x, 1), \quad F^*(x, y) = F(y, x), \quad f^*(x) = F^*(x, 1).$$

Denote by z_h ($h=1, 2, \dots, n$) the zeros of $f(z)$ where those with $1 \leq h \leq n_0$ are the real ones. Then $z_h^* = z_h^{-1}$ ($h=1, 2, \dots, n$) are the zeros of $f^*(x)$, and again those with $1 \leq h \leq n_0$ are real. $F(x, y)$ is exactly then a definite form when $n_0=0$.

Next let $v(w)$ for every integer $w \neq 0$ be the number of integers U satisfying

$$f(U) \equiv 0 \pmod{w}, \quad 0 \leq U \leq |w|-1, \quad (U, w) = 1,$$

and let $v^*(w)$ be the analogous number for $f^*(x)$; evidently

$$v^*(w) = v(w).$$

It is easily seen that

$$v(w) \leq n^t,$$

where t denotes the number of distinct prime factors of w . This upper bound depends thus only on the degree and not also on the height of $F(x, y)$.

A famous theorem by A. Thue, based on his classical theorem on the rational approximations of real algebraic numbers ([9], [10]) states that the Diophantine equation

$$F(u, v) = w$$

has for every integer $w \neq 0$ at most finitely many integral solutions u, v .

Two solutions u, v and u', v' of Thue's equation will be considered as distinct if and only if $u/v \neq u'/v'$. In this notation the following result will be proved.

THEOREM. *Denote by w an integer satisfying*

$$(A): \quad |w| \geq (450a^4n^4)^{n/(n-2)}.$$

Then the equations

$$(B): \quad F(u, v) = w, \quad (u, w) = (v, w) = 1$$

have fewer than

$$32nv(w) \leq 32n^{t+1}$$

distinct integral solutions u, v .

For definite forms the number of distinct integral solutions of (B) will be proved to be at most $2v(w)$ and in fact not to exceed $v(w)$.

Older upper estimates for the number of integral solutions of Thue's equation can be found in the papers [1], [2], and [4]. For some recent results see the remarks at the end of this paper.

2.

The measure of $f(x)$ is as usual defined by

$$M(f) = |f_0| \prod_{h=1}^n \max(1, |z_h|)$$

and the discriminant by

$$D(f) = f_0^{2n-2} \prod_{1 \leq h < k \leq n} (z_h - z_k)^2.$$

I proved in [5] that

$$2^{-n}a \leq M(f) \leq \sqrt{n+1}a,$$

in [6] that

$$1 \leq |D(f)| \leq n^n M(f)^{2n-2},$$

and that for $h=1, 2, \dots, n$,

$$|f'(z_h)| \geq (n-1)^{-(n-1)/2} |D(f)|^{\frac{1}{2}} M(f)^{-(n-2)}.$$

Denote now by c and C the two constants

$$c = (4(n-1))^{(n-1)/2} |D(f)|^{-\frac{1}{2}} M(f)^{n-2}$$

and

$$C = \sqrt{1/3} n^{(n+2)/2} |D(f)|^{-\frac{1}{2}} M(f)^{n-1}.$$

It is easily seen that if $f(x)$ is replaced by $f^*(x)$, the same constants are obtained.

A proof just as in the paper [2] leads to the following results in which $\varrho(x)$ and $\varrho^*(x)$ are defined by

$$\varrho(x) = \min_{h=1, 2, \dots, n} |x - z_h| \quad \text{and} \quad \varrho^*(x) = \min_{h=1, 2, \dots, n} |x - z_h^{-1}|.$$

LEMMA 1. For real x and y ,

$$|y|^n \varrho(x/y) \leq c |F(x, y)| \quad \text{if } y \neq 0$$

and

$$|x|^n \varrho^*(y/x) \leq c |F(x, y)| \quad \text{if } x \neq 0.$$

LEMMA 2. If for a real number x

$$\varrho(x) \leq 1/(2C),$$

then the minimum $\varrho(x)$ is attained at a real zero z_h of $f(x)$, and this zero is unique.

LEMMA 3. If $F(x, y)$ is a definite form, then

$$|F(x, y)| > (2cC)^{-1} \{\max(|x|, |y|)\}^n.$$

These lemmas are new and stronger than previous estimates.

3.

We next need a result which is implicit in Thue's proof of his theorem on the rational approximations of algebraic numbers. It is necessary to carry out his

considerations and estimates with some care for the occurring constants, and for this purpose Lemma 1 of my paper [3] may be used.

I omit the details since Thue's method is well known. The final result is as follows.

LEMMA 4. *Let the notation be as before; let $z = z_h$ be one of the zeros of $f(x)$, and let $k \geq 1$ be a constant. Denote by Σ the set of all rational numbers u/v , where u and $v \neq 0$ are integers, such that*

$$\left| \frac{u}{v} - z \right| \leq k|v|^{-n} \quad \text{and} \quad |v| \geq 2(4a)^{90(n+1)}k^{18/n},$$

and assume that Σ is not the null set. Let u_1/v_1 be an element of Σ with smallest $|v_1|$, and let u_l/v_l be any other element of Σ . Then the zero z is real, and v_l satisfies the inequality

$$|v_l| < |v_1|^{48(n+1)}.$$

4.

From now on denote by S the set and by N the number of all distinct pairs of integers u, v satisfying the conditions (B) where w is any integer with the property (A). The latter assumption evidently excludes any solutions of $F(u, v) = w$ for which

$$u = 0 \quad \text{or} \quad v = 0 \quad \text{or} \quad |u| = |v|.$$

Hence the elements of S are either of

$$\text{Type A, when } 0 < |u| < |v|,$$

or of

$$\text{Type B, when } 0 < |v| < |u|.$$

Denote by $S(A)$ and $S(B)$ the sets and by $N(A)$ and $N(B)$ the numbers of the distinct integral solutions of types A and B, respectively, so that

$$S = S(A) \cup S(B) \quad \text{and} \quad N = N(A) + N(B).$$

On replacing the form $F(x, y)$ by the form $F^*(x, y) = F(y, x)$, the solutions of Type A become solutions of Type B, and vice versa, and here both forms belong to the same constants c and C . The following considerations will therefore give the same upper estimates for $N(A)$ and $N(B)$, so that twice this number is an upper bound for N .

5.

To obtain such estimates, we require two different subdivisions of the solutions u, v in $S(A)$ into equivalence classes.

A solution u, v in $S(A)$ for which

$$|v| \geq (2cC|w|)^{1/n}$$

and therefore

$$c|v|^{-n}|w| \leq (2C)^{-1}$$

is called a *major solution*. Since $F(u, v) = w$ and $|u| < |v|$, Lemma 1 implies that for such major solutions

$$\varrho(u/v) \leq c|v|^{-n}|w| \leq (2C)^{-1}.$$

Hence, by Lemma 2, the minimum $\varrho(u/v)$ is attained at one and only one zero z_h of $f(x)$, and this zero is real and therefore $1 \leq h \leq n_0$.

This suggests the following definition.

DEFINITION. Two major solutions u/v and u'/v' of type A are said to be ϕ -equivalent, in symbols $\{u, v\} \phi \{u', v'\}$, if both belong to the same zero z_h of $f(x)$.

It is obvious that ϕ -equivalence is an equivalence relation and that there are exactly n_0 distinct ϕ -equivalence classes, one corresponding to each of the real zeros z_h , $1 \leq h \leq n_0$, of $f(x)$.

For the present assume that

$$n_0 \geq 1.$$

This hypothesis excludes the case when $F(x, y)$ is a definite form ($n_0 = 0$), when a slightly different method will be applied.

6.

A second class division will first be defined for the wider set of distinct pairs of integers u, v satisfying

$$(u, w) = (v, w) = 1,$$

but not necessarily also $F(u, v) = w$.

The definition is as follows.

DEFINITION. Two pairs of integers u, v and u', v' satisfying $(u, w) = (v, w) = 1$ are said to be $\$$ -equivalent, in symbols $\{u, v\} \$ \{u', v'\}$, if

$$uv' - u'v \equiv 0 \pmod{w}.$$

It is easily proved that also $\$$ -equivalence is an equivalence relation, and that the following two further properties hold.

If $u \equiv u' \pmod{w}$, $v \equiv v' \pmod{w}$, $(u, w) = (v, w) = 1$, then also $(u', w) = (v', w) = 1$ and $\{u, v\} \$ \{u', v'\}$.

If $(t, w) = (u, w) = (v, w) = 1$, then also $(tu, w) = (tv, w) = 1$ and $\{u, v\} \$ \{tu, tv\}$.

Choose in particular t such that

$$tv \equiv 1 \pmod{w}.$$

There now exists one and only one integer U satisfying

$$U \equiv tu \pmod{w}, \quad 0 \leq U \leq |w| - 1, \quad (U, w) = 1,$$

and since $\{u, v\} \$ \{tu, tv\} \$ \{U, 1\}$, the pair $U, 1$ can serve as the representative of the $\$$ -equivalence class of u, v . Moreover, this representative is unique.

7.

Consider now any pair u, v in $S(A)$ so that in particular $(u, w) = (v, w) = 1$. If $U, 1$ is the representative of the $\$$ -equivalence class of u, v , then $\{u, v\} \$ \{U, 1\}$ and therefore

$$u \equiv vU \pmod{w}.$$

By hypothesis $F(x, y)$ is a homogeneous polynomial in x and y of degree n and has integral coefficients. It follows that

$$F(u, v) \equiv F(vU, v) = v^n F(U, 1) \equiv 0 \pmod{w},$$

and since $(v, w) = 1$,

$$F(U, 1) \equiv 0 \pmod{w}.$$

This congruence is thus a *necessary*, but in general not also a sufficient, condition for the $\$$ -equivalence class of $U, 1$ to contain a solution of (B). The property

$$(U, w) = 1$$

is a consequence of the equations (B).

Hence, from the definition of $\nu(w)$ in section 1, there are at most $\nu(w)$ distinct $\$$ -equivalence classes of representatives $U, 1$ containing solutions u, v of (B) of type A. Let this be the equivalence classes $\$, \$_2, \dots, \$_{Y(w)}$. Here the number $Y(w)$ satisfies the inequality

$$0 \leq Y(w) \leq \nu(w).$$

8.

We next subdivide the elements u, v of $S(A)$ into three disjoint subsets $S^{(1)}$, $S^{(2)}$, and $S^{(3)}$ according as to whether

$$S^{(1)}: \quad |v| < 15a^2n^2|w|^{1/n},$$

or

$$S^{(2)}: \quad 15a^2n^2|w|^{1/n} \leq |v| < 2(4a)^{90(n+1)}k^{18/n},$$

or

$$S^{(3)}: \quad |v| \geq 2(4a)^{90(n+1)}k^{18/n},$$

respectively. Here k denotes the number

$$k = c|w|.$$

It is clear from the hypothesis (A) that

$$k > 1.$$

If $N^{(1)}$, $N^{(2)}$, and $N^{(3)}$ are the numbers of elements of $S^{(1)}$, $S^{(2)}$, and $S^{(3)}$, respectively, evidently

$$N(A) = N^{(1)} + N^{(2)} + N^{(3)}.$$

9.

The elements of $S^{(1)}$ are not necessarily major solutions of the equations (B); hence we cannot subdivide these solutions into ϕ -equivalence classes. They may, however, be distributed among the \mathcal{S} -equivalence classes \mathcal{S}_j where $j = 1, 2, \dots, Y(w)$, unless $Y(w) = 0$. Denote by $S_j^{(1)}$ the subset of all those pairs u, v of $S^{(1)}$ which lie in \mathcal{S}_j .

Suppose that any set $S_j^{(1)}$ contains two distinct pairs u, v and u', v' . Then, firstly,

$$0 \neq uv' - u'v \equiv 0 \pmod{w}.$$

Hence there is an integer $g \neq 0$ such that

$$uv' - u'v = gw.$$

Since u, v and u', v' both lie in $S^{(1)}$,

$$|u| < |v| < 15a^2n^2|w|^{1/n} \quad \text{and} \quad |u'| < |v'| < 15a^2n^2|w|^{1/n},$$

so that

$$|w| \leq |gw| = |uv' - u'v| < 2(15a^2n^2|w|^{1/n})^2 = 450a^4n^4|w|^{2/n},$$

whence

$$|w| < (450a^4n^4)^{n/(n-2)},$$

contrary to the hypothesis (A).

This proves that each set $S_j^{(1)}$ contains at most one element and that therefore

$$(1): \quad N^{(1)} \leq Y(w) \leq v(w).$$

10.

One shows easily that the two constants c and C of section 2 satisfy the inequalities

$$(2cC)^{1/n} < 2a^2n^2 < 15a^2n^2 \quad \text{and} \quad 2a^2n^2 < 2(4a)^{90(n+1)}k^{18/n}.$$

Hence all solutions u, v in $S^{(2)}$ and in $S^{(3)}$ are major. These solutions can thus simultaneously be distributed among the \mathfrak{f} -equivalence classes \mathfrak{f}_h and the \mathfrak{S} -equivalence classes \mathfrak{S}_j .

Denote then by $S_{hj}^{(2)}$ and $S_{hj}^{(3)}$ the subsets of elements of $S^{(2)}$ and of $S^{(3)}$ which lie in both \mathfrak{f}_h and \mathfrak{S}_j , and let $N_{hj}^{(2)}$ and $N_{hj}^{(3)}$ be the numbers of elements of these subsets, respectively.

Before determining upper estimates for $N_{hj}^{(2)}$ and $N_{hj}^{(3)}$, let us consider more generally two distinct major solutions u, v and u', v' of (B) of type A which both lie in \mathfrak{f}_h and in \mathfrak{S}_j . Here, say

$$|v| \leq |v'|.$$

By the definition of \mathfrak{f}_h , both solutions belong to the same zero z of $f(x)$. Since they are major,

$$|(u/v) - z| \leq c|v|^{-n}|w| \quad \text{and} \quad |(u'/v') - z| \leq c|v'|^{-n}|w|,$$

and since they are distinct.

$$0 < |(u/v) - (u'/v')| = |\{(u/v) - z\} - \{(u'/v') - z\}| \leq c|v|^{-n}|w| + c|v'|^{-n}|w|,$$

or equivalently,

$$0 < |uv' - u'v| \leq c|w|\{|v||v'|^{-(n-1)} + |v|^{-(n-1)}|v'|\}.$$

By hypothesis both u, v and u', v' lie in the same class \mathfrak{S}_j . Hence $uv' - u'v$ is a non-vanishing integral multiple gw of w and therefore has at least the absolute value $|w|$. It follows then from the last inequality that

$$|w| \leq 2c|w||v|^{-(n-1)}|v'|$$

since $|v| \leq |v'|$. Thus

$$|v'| \geq (2c)^{-1}|v|^{n-1},$$

an inequality which can be written as

$$(2c)^{-1/(n-2)}|v'| \geq ((2c)^{-1/(n-2)}|v|)^{n-1}.$$

We note that the letter w has disappeared from this formula.

It can immediately be generalised. For this purpose let

$$(P): \quad u_1, v_1; u_2, v_2; \dots, u_I, v_I \quad \text{where } |v_1| \leq |v_2| \leq \dots \leq |v_I|,$$

be finitely many distinct major solutions of (B) of type A which all belong to the same class ϕ_h and the same class S_j . By the last inequality,

$$(2c)^{-1/(n-2)}|v_{i+1}| \geq ((2c)^{-1/(n-2)}|v_i|)^{n-1} \quad (i = 1, 2, \dots, I-1)$$

and therefore

$$(2c)^{-1/(n-2)}|v_I| \geq ((2c)^{-1/(n-2)}|v_1|)^{(n-1)^{I-1}}.$$

Here, as is easily proved,

$$(2c)^{+1/(n-2)} < 11an,$$

and so we obtain the inequality

$$(Q): \quad |v_I| > ((11an)^{-1}|v_1|)^{(n-1)^{I-1}}$$

on which the next estimates will be based.

11.

As a first application, assume that the set $S_{hj}^{(2)}$ consists of exactly the I pairs (P). By the definition of $S^{(2)}$,

$$|v_1| \geq 15a^2n^2|w|^{1/n} \quad \text{and} \quad |v_I| < 2(4a)^{90(n+1)}k^{18/n}$$

where, as already noted,

$$k = c|w| > 1.$$

One shows easily that

$$c^{1/n} < 2an$$

whence

$$|v_I| < 2(4a)^{90(n+1)}(2an)^{18}|w|^{18/n}.$$

The inequality (Q) therefore implies that

$$((11an)^{-1} \cdot 15a^2n^2|w|^{1/n})^{(n-1)^{I-1}} < 2(4a)^{90(n+1)}(2an)^{18}|w|^{18/n}.$$

Here by $n \geq 3$,

$$n^{18} < (4a)^{5(n+1)}, \quad 2(4a)^{18} < (4a)^{5(n+1)},$$

and

$$(11an)^{-1} \cdot 15a^2 n^2 > 4a, \quad 2(4a)^{90(n+1)} (2an)^{18} < (4a)^{100(n+1)},$$

and

$$(4a|w|^{1/n})^{(n-1)^{l-1}} < (4a)^{100(n+1)} |w|^{18/n}.$$

It follows then that

$$(4a)^{(n-1)^{l-1} - 100(n+1)} < |w|^{\{18 - (n-1)^{l-1}\}/n}.$$

If here $(n-1)^{l-1} \leq 18$, then

$$I \leq 6$$

by $n \geq 3$. Let therefore $(n-1)^{l-1} > 18$ so that the exponent of $|w|$ is negative. By the hypothesis (A),

$$|w|^{1/n} \geq (450 \cdot a^4 n^4)^{1/(n-2)} > (4a)^{4/(n-2)},$$

hence by the last inequality,

$$(4a)^{(n-1)^{l-1} - 100(n+1)} < (4a)^{4\{18 - (n-1)^{l-1}\}/(n-2)}$$

and therefore

$$(n+2)(n-1)^{l-1} < 100(n-2)(n+1) + 72.$$

Again by $n \geq 3$ this inequality requires that

$$I \leq 7.$$

On combining the two cases it follows that each of the numbers $N_{hj}^{(2)}$ is at most 7. Hence on summing over all the classes \mathfrak{f}_h and \mathfrak{S}_j we find that

$$(2): \quad N^{(2)} \leq 7 \cdot n_0 \cdot Y(w) \leq 7nv(w).$$

For definite forms $n_0 = 0$ and therefore also $N^{(2)} = 0$.

12.

Let us similarly assume that the set $S_{hj}^{(3)}$ consists exactly of the I pairs (P). By the definition of $S^{(3)}$,

$$|v_1| \geq 2(4a)^{90(n+1)} k^{18/n} > (4a)^{90(n+1)},$$

while by the Lemma 4 of Thue,

$$|v_I| < |v_1|^{48(n+1)}$$

and by the formula (Q),

$$|v_I| > ((11an)^{-1}|v_1|)^{(n-1)^{I-1}}.$$

Since

$$11an < (4a)^{n+1},$$

by the lower estimate for $|v_1|$,

$$(11an)^{-1}|v_1| > |v_1|^{89/90}.$$

Hence

$$|v_1|^{(89/90)(n-1)^{I-1}} < |v_I| < |v_1|^{48(n+1)}$$

and therefore

$$(n-1)^{I-1} < (4320/89)(n+1) < 50(n+1).$$

By $n \geq 3$ it follows that

$$I \leq 8.$$

On summing again over all the equivalence classes ϕ_h and S_j , we obtain the estimate

$$(3): \quad N^{(3)} \leq 8 \cdot n_0 \cdot Y(w) \leq 8nv(w).$$

If $F(x, y)$ is definite, again $n_0 = 0$ and therefore $N^{(3)} = 0$.

13.

On combining the formulae (1), (2), and (3), it follows that

$$N(A) = N^{(1)} + N^{(2)} + N^{(3)} \leq v(w) + 7nv(w) + 8nv(w) < 16nv(w),$$

and $N(A) \leq v(w)$ when $F(x, y)$ is a definite form.

It is clear that exactly the same upper estimate is obtained for $N(B)$; simply apply the proof just given to the equation $F^*(u, v) = w$. Hence

$$N = N(A) + N(B) < 32nv(w),$$

as was to be proved. In the same way, for definite forms,

$$N \leq 2v(w).$$

This latter result can be improved to

$$N \leq v(w),$$

as shall finally be proved.

By Lemma 3, now

$$|F(x, y)| > (2cC)^{-1}(\max(|x|, |y|))^n.$$

Impose on w the condition that

$$(C): \quad |w| \geq 2^{n/(n-2)}(2cC)^{2/(n-2)};$$

by

$$(2cC)^{2/(n-2)} \leq (4a^4n^4)^{n/(n-2)},$$

this is weaker than the former hypothesis (A).

We do not now distinguish between solutions u, v of (B) of the two types A and B, nor do we need the ϕ -equivalence classes, but we still must distribute the distinct solutions of (B) among the $\$$ -equivalence classes $\$j$. It evidently suffices to prove that each such class contains at most one solution u, v .

If this is false, let u, v and u', v' be two distinct solutions in the class $\$j$ so that $uv' - u'v$ is a non-vanishing integral multiple gw of w and has at least the absolute value $|w|$. Since from $F(u, v) = F(u', v') = w$

$$2cC|w| > (\max(|u|, |v|))^n \quad \text{and} \quad 2cC|w| > (\max(|u'|, |v'|))^n,$$

it follows that

$$|w| \leq |gw| = |uv' - u'v| < 2 \cdot (2cC|w|)^{2/n}.$$

This implies that

$$|w| < 2^{n/(n-2)}(2cC)^{2/(n-2)},$$

contrary to the assumption (C). This concludes the proof.

14.

The first version of this paper was concluded on 16 August, 1982. Shortly afterwards I saw the paper by J. H. Silverman, "Integer points and the rank of Thue elliptic curves", Invest. Math 66 (1982), 395–404. Here the author proved for the case $n=3$ that Thue's equation $F(u, v) = w$ has for sufficiently large $|w|$ fewer than

$$\varkappa^{R_F(w)+1}$$

integral solutions where $\varkappa > 1$ is an effective absolute constant and $R_F(w)$ denotes the rank of the Mordell-Weil group of rational points on the curve

$$F(x, y) = wz^n.$$

I was later informed by the author that he could extend this result to all degrees $n \geq 3$.

Also, in a letter of 23 May, 1983, he announced the result that for all $w \neq 0$ Thue's equation has at most

$$c^{r(wD)+1}$$

integral solutions where $c > 1$ is a constant which depends only on the degree n , $D = D(f)$ is again the discriminant, and $r(nD)$ denotes the number of distinct prime factors of nD .

Next, in a letter of 16 February, 1983, J. H. Evertse of Leiden, Netherlands, told me that in his Ph.D. thesis, not yet published, he had proved that for all $w \neq 0$ Thue's equation has at most

$$2(7^{(15v+1)^2} + 6 \times 7^{2v(t+1)})$$

integral solutions satisfying $(u, v) = 1$. Here $v = \binom{n}{3}$, and t is again the number of distinct prime factors of w . This result (which for large $|w|$ is less good than mine) has the great advantage that it depends only on n and w , but is independent of the coefficients of $F(x, y)$. It thus solves an old problem by C. L. Siegel.

REFERENCES

1. H. Davenport and K. F. Roth, *Rational approximations of algebraic numbers*, *Mathematika* 2 (1955), 160–167.
2. D. J. Lewis and K. Mahler, *On the representation of integers by binary forms*, *Acta Arith.* 6 (1961), 333–363.
3. K. Mahler, *Zur Approximation algebraischer Zahlen*, I, *Math. Ann.* 107 (1933), 691–730.
4. K. Mahler, *Zur Approximation algebraischer Zahlen*, II, *Math. Ann.* 108 (1933), 37–55.
5. K. Mahler, *On some inequalities for polynomials in several variables*, *J. London Math. Soc.* 37 (1962), 341–344.
6. K. Mahler, *An inequality for the discriminant of a polynomial*, *Michigan Math. J.* 11 (1964), 257–262.
7. A. Thue, *Om en general i store hele tal ulösbar ligning*, *Norske Vid. Selsk. Skr.* 7 (1908); Selected mathematical papers, pp. 219–231.
8. A. Thue, *Über Annäherungswerte algebraischer Zahlen*, *J. Reine Angew. Math.* 135 (1909), 284–305; Selected mathematical papers, pp. 232–253.