ACTA ARITHMETICA
XXII (1973)

Hasse Principle in algebraic equations

by

MASAHIKO FUJIWARA (Tokyo)

§ 0. Introduction. In this paper we make some observations regarding Hasse Principles for algebraic equations of one variable (in § 1) and for homogeneous forms (in § 2).

First of all, we give the definition of Hasse Principle. Let k be an algebraic number field of finite degree and $k_\mathfrak{p}$ its completion with respect to $\mathfrak{p}$ where $\mathfrak{p}$ is a prime spot, discrete or not. Let $k[x_1, \ldots, x_n]$ be the polynomial ring in n variables with coefficients in k and $f(x_1, \ldots, x_n)$ belong to $k[x_1, \ldots, x_n]$.

We say Hasse Principle/k (resp. strong Hasse Principle/k) holds for $f(x_1, \ldots, x_n)$, when "$f(x_1, \ldots, x_n) = 0$ has a solution in k if and only if it has a solution in $k_\mathfrak{p}$ for all prime spots $\mathfrak{p}$ (resp. for all but a finite number of exceptions)." If $f(x_1, \ldots, x_n)$ is a form, a solution means a non-trivial one.

In § 1 we will obtain various results on the strong Hasse Principles for algebraic equations of one variable and for binary forms over algebraic number fields. As the strong Hasse Principle for irreducible polynomials of one variable is known to hold (Hasse [4]), we have only to deal with the reducible cases. The special case when $f(x) = x^m - a$ is considered in Artin–Tate (Chap. 9, 10 [1]) and in H. B. Mann (Chap. 16 [5]). Another special case is considered in Van der Waerden [10]. Our proofs are based mainly on algebraic number theory with some class field theory.

In § 2 our aim is to disprove Hasse Principles for forms of degree 5. As is well known, the Hasse–Minkowski theorem assures the validity of Hasse Principles for any quadratic forms. So far as forms of higher degree are concerned, things are not at all simple if the form is irreducible of odd degree. (See [2], p. 72.) For forms of degree 3, E. S. Selmer [7] first disproved Hasse Principles by his famous counterexample $3x^3 + 4y^3 + 5z^3 = 0$ and later others were found by Swinnerton-Dyer [8], Mordell [6] and Cassels–Guy [3]. These four papers seem to contain all counterexamples for irreducible forms of odd degree known up to now. In this section we assert and show that the irreducible form of degree 5, $(x^3 + 5y^3)(x^2 + xy + y^2) - 17z^5$ is a counterexample. The proof is based on algebraic number theory together with some results of § 1.

The author is very happy to have a chance to express his hearty gratitude to Dr. G. Fujisaki and Dr. M. Ishida for their warm and continual encouragement.

§ 1. Strong Hasse Principle. Throughout this section, we fix the following notations.

k: an algebraic number field of finite degree,

$\mathfrak{p}$: a prime ideal of k,

$k_\mathfrak{p}$: a completion of k with respect to $\mathfrak{p}$,

$f(x) \in k[x]$: the polynomial ring of one variable over k,

$k(f)$: the composite field of k and the roots of f,

a.a.p.: almost all prime ideals, i.e., all prime ideals but a finite number of exceptions,

S.H.P./k: Strong Hasse Principle over k.

First of all we make two obvious remarks which will be used frequently.

Remarks. (1) If $f(x)$ has no roots in k, S.H.P. holds for $f(x)$ if and only if there exist an infinite number of primes $\mathfrak{p}$ such that $f(x)$ has no roots in $k_\mathfrak{p}$.

(2) If $K \supset k$ and $f(x)$ has no roots in K, then the validity of S.H.P./K for $f(x)$ implies that of S.H.P./k for $f(x)$.

The next lemma is well known.

Lemma 1. *Let $f(x)$ be irreducible over k and α any one of its roots. Then for a.a.p., the following statements are equivalent.*

(1) *$f(x)$ has some roots in $k_\mathfrak{p}$.*

(2) *$\mathfrak{p}$ has a prime factor of relative degree 1 in $k(\alpha)$.*

Proposition 1. *If $f(x)$ is a Galois equation (i. e. $k(f)$ can be obtained from k by an adjunction of any one root of $f(x)$) then S.H.P. holds for $f(x)$.*

Proof. As $k_\mathfrak{p}(f) = k_\mathfrak{p}(\alpha)$ for any root α of f, we can assume that $k_\mathfrak{p}(f) = k_\mathfrak{p}$ for a.a.p. On the other hand if $k(f) \neq k$, by the density theorem of Tschebotareff, there exist an infinite number of prime ideals in k which do not factor completely in $k(f)$. This implies $k_\mathfrak{p}(f) \neq k_\mathfrak{p}$ for an infinite number of $\mathfrak{p}$ and contradicts the assumption, hence $k(f) = k$ and f can be solved in k, q.e.d.

Proposition 2. *If $f(x)$ is a polynomial of fourth degree then S.H.P. holds for $f(x)$.*

Proof. (f: irreducible). The Galois group G of f is either symmetric group S_4, alternating group A_4, a group B_4' of order 8 or a group B_4 of order 4. If G is B_4, $f(x)$ is a Galois equation so that S.H.P. holds by Proposition 1. It is easily seen that if G is A_4 or B_4' then S.H.P. holds over the subfield K of $k(f)$ corresponding to B_4 and if G is S_4 then it holds over the subfield K of $k(f)$ corresponding to A_4.

By the Remark (2) it holds over k.

(f: reducible.) So far as S.H.P. is concerned, we can assume without any loss of generality that $f(x)$ is written in the form $(x^2-\Delta)(x^2-\Delta')$. If $k(f) = k(\sqrt{\Delta}, \sqrt{\Delta'})$ is of degree 2 over k then $f(x)$ is a Galois equation and Proposition 1 applies. If $k(f)$ is of degree 4 over k then $k(\sqrt{\Delta\Delta'})$ contains no root of f and $f(x)$ is a Galois equation over $k(\sqrt{\Delta\Delta'})$ and Proposition 1 applies, q.e.d.

Corollary. *Let m, n be integers which are not squares. Then there exist an infinite number of primes p such that*

$$\left(\frac{m}{p}\right) = \left(\frac{n}{p}\right) = -1.$$

This Corollary will be generalized after Proposition 4.

Proposition 3. *Let $f(x)$ be a reducible polynomial of degree 5 which is written as $f = gh$ where g is irreducible of degree 3 and h is irreducible of degree 2. Let D_g, D_h be the respective discriminants. Then S.H.P./k holds for $f(x)$ if and only if D_g is not multiplicatively congruent to D_h modulo k^2.*

Proof. ($k(g)/k$: degree 3.) In this case the density of prime ideals of k which do not split completely in $k(g)$ (resp. $k(h)$) is $\frac{2}{3}$ (resp. $\frac{1}{2}$) and $\frac{2}{3}+\frac{1}{2} > 1$. Hence there are an infinite number of prime ideals in k which do not split in either $k(g)$ or $k(h)$. This shows the validity of S.H.P. for $f(x)$ by Lemma 1. In this case D_g is in k^2 and hence D_g is not congruent to D_h modulo k^2.

($k(g)/k$: degree 6.)

Case 1. $k(g) \supset k(h)$. Let α be a root of $g(x)$. As $k(g)/k$ is not cyclic, a prime ideal $\mathfrak{p}$ of k which remains prime in $k(\alpha)$ must split completely in $k(g)/k(\alpha)$. It follows, by the translation theorem of class field theory, except for a finite number of $\mathfrak{p}$, $N_{k(\alpha)/k}\mathfrak{p} = \mathfrak{p}^3$ splits completely in $k(h)$. Hence $\mathfrak{p}$ itself splits completely in $k(h)$. Summing up, except for a finite number of $\mathfrak{p}$, if g has no root in $k_\mathfrak{p}$ then h has a root in $k_\mathfrak{p}$. This implies that S.H.P. fails.

In this case, as $k(g)$ has only one subfield of degree 2, $k(\sqrt{D_g}) = k(\sqrt{D_h})$ and D_g is congruent to D_k modulo k^2.

Case 2. $k(g) \cap k(h) = k$. Let K be a subfield of $k(g)$ corresponding to A_3. As K contains no roots of g or h, it is easily seen that S.H.P. holds for $f(x)$ over K by the arguments of the first case. In this case, D_g is not congruent to D_h modulo k^2, q.e.d.

Using this proposition it is quite easy to construct examples for which the S.H.P. fails. For example $f(x) = (x^3+5)(x^2+3)$ has no S.H.P./$\boldsymbol{Q}$.

More precisely, by the above proof, $f(x)$ can be solved at all primes except $\mathfrak{Q}_2, \mathfrak{Q}_3$ and $\mathfrak{Q}_5$. This fact will be used in § 2.

THEOREM 1. *For $f(x) = g(x)h(x)$ where $g(x)$ and $h(x)$ are irreducible over k, S.H.P. holds except the following case* (*):

(*) $\quad k(g) \supsetneqq k(h)$ *and* $k(\alpha) \not\supset k(\beta)$ *for any root α of g and β of h*

(or the case where g and h are exchanged).

Proof. If $k(g) = k(h)$, S.H.P. holds for f since we know that it holds for any irreducible polynomials. When $k(g) \not\supset k(h)$ or $k(g) \not\subset k(h)$, put $K = k(g) \cap k(h)$. As K/k is a Galois extension, K contains no root of g or h. Therefore we have only to prove S.H.P. over K. We distinguish two cases.

Case 1 (g and h are irreducible over K). First we show that $G\big(K(g)/k\big)$ (resp. $G\big(K(h)/K\big)$) contains an element σ_g (resp. σ_h) that fixes no root of g (resp. h) in the following; assume each element of $G = G\big(K(g)/K\big)$ fixes some root of g. Let $\alpha_1, \ldots, \alpha_n$ be the roots of g. Since G is transitive, for each i, there is an element a_i in G which sends α_1 to α_i. Then, letting H_1 be the stability subgroup of α_1 in G, we have

$$G = H_1 \cup a_2 H_1 \cup \ldots \cup a_n H_1 \quad \text{(disjoint union)}.$$

Therefore $\#G = mn$ where $\#H_1 = m$. Put $H_i = a_i H_1 a_i^{-1}$. Then $\#H_i = m$ and $G = H_1 \cup \ldots \cup H_n$ by the assumption. But this union is no longer disjoint since each H_i contains 1. Hence $\#G < mn$ and we have a contradiction. Thus we have proved our assertion. Now,

$$K(f) = K(g) \cdot K(h) \quad \text{and} \quad G\big(K(f)/K\big) = G\big(K(g)/K\big) \times G\big(K(h)/K\big).$$

Regarding (σ_g, σ_h) as an element of $G\big(K(f)/K\big)$, there exists a prime ideal, hence an infinite number of prime ideals, in K whose Frobenius automorphism in $K(f)$ is (σ_g, σ_h). These prime ideals are easily seen, from their construction, to have no prime factors of relative degree 1 in either $K(\alpha)$ or $K(\beta)$ where α (resp. β) is any root of g (resp. h). Hence S.H.P. holds for $f = gh$ over K.

Case 2 (g or h is reducible over K). As K/k is a Galois extension, irreducible factors of g are conjugate over k. Therefore the solvability of g in $K_\mathfrak{p}$ is equivalent to that of any one irreducible factor of g in $K_\mathfrak{p}$. The same goes with h and hence we can reduce this case to case 1. Hence S.H.P. holds for f over K.

Now, the case left to prove is the one when $k(g) \supsetneqq k(h)$ and $k(\alpha) \supset k(\beta)$ for some root α of g and β of h. In this case, take an element of $G\big(k(h)/k\big)$ that fixes no root of h and denote by σ_g its prolongation to the automorphism of $k(g)$ over k. As σ_g fixes no root of g by the assumption, the prime ideal in k whose Frobenius automorphism in $k(g)$ is σ_g has

no prime factor of relative degree 1 in either $k(\alpha)$ or $k(\beta)$. Hence S.H.P. holds for $f = gh$ over k and this completes the proof of Theorem 1, q.e.d.

Remark. In the case (*), whether S.H.P. holds or not appears a little complicated. An example for which S.H.P. holds is $(x^4-2)(x^2+1)$ and the one for which S.H.P. fails is $(x^3+5)(x^2+3)$. The latter example is already referred to and the former can be verified by a direct computation of the Galois group of x^4-2. Van der Waerden [10] has got a necessary (but not sufficient) condition for the validity of S.H.P. for $f = gh$ where g quadratic and h of odd prime degree.

PROPOSITION 4. *Let $f(x) = (x^2-\Delta_1)(x^2-\Delta_2)\ldots(x^2-\Delta_m)$ where $\Delta_1, \Delta_2, \ldots, \Delta_m$ are numbers of k which are not squares in k. Then the following assertions are equivalent:*

(1) *S.H.P./k does not hold for $f(x)$;*

(2) *Some Δ_i is multiplicatively congruent to a product of an even number of others modulo k^2.*

Proof. First we note that if $\Delta_1, \ldots, \Delta_m$ are multiplicatively independent modulo k^2 then S.H.P. holds. For, in this case, $k(f) = k(\sqrt{\Delta_1}, \ldots, \sqrt{\Delta_m})$ is of degree 2^m over k and, putting $K = k(\sqrt{\Delta_1\Delta_2}, \sqrt{\Delta_2\Delta_3}, \ldots, \sqrt{\Delta_{m-1}\Delta_m})$ K contains no root of $f(x)$. It is clear that $k(f)$ is of degree 2 over K and f is a Galois equation over K. Hence Proposition 1 applies and S.H.P. holds over k.

(2) $\Rightarrow$ (1). Let $\Delta_1 \equiv \Delta_{i_1} \ldots \Delta_{i_{2l}} \pmod{k^2}$. Apply the quadratic residue symbol on both sides. Then

$$\left(\frac{\Delta_1}{\mathfrak{p}}\right) = \left(\frac{\Delta_{i_1}}{\mathfrak{p}}\right) \ldots \left(\frac{\Delta_{i_{2l}}}{\mathfrak{p}}\right)$$

and it follows that there exists no prime ideal $\mathfrak{p}$ making all these factors -1 at the same time. In another words

$$(x^2-\Delta_1)(x^2-\Delta_{i_1})\ldots(x^2-\Delta_{i_{2l}})$$

can be solved in $k_\mathfrak{p}$ for a.a.p. and hence S.H.P. does not hold for this product. Consequently, S.H.P. does not hold for $f(x)$.

(1) $\Rightarrow$ (2). If S.H.P. does not hold for $f(x)$ then there exist Δ_i with the following property: S.H.P. holds for $(x^2-\Delta_1)\ldots(x^2-\Delta_i)$ but not for $(x^2-\Delta_1)\ldots(x^2-\Delta_i)(x^2-\Delta_{i+1})$. Then owing to the above-mentioned remarks, $\Delta_1, \ldots, \Delta_{i+1}$ are multiplicatively dependent modulo k^2 and therefore Δ_{i+1} can be written as a product of some of $\Delta_1, \ldots, \Delta_i \bmod k^2$. If this product consists of an odd number of Δ_k's, it is easily shown, by considering again quadratic residue symbols, that S.H.P. holds for $f(x)$ and this is a contradiction. Therefore the product should consist of an even number of Δ_k's, q.e.d.

COROLLARY. *Let $m_1, \dots, m_l$ be integers which are not squares. Then there exist infinitely many primes p such that $\left(\frac{m_1}{p}\right) = \dots = \left(\frac{m_l}{p}\right) = -1$ if and only if each m_i is not multiplicatively congruent modulo $\boldsymbol{Q}^2$ to a product of an even number of others.*

By the way, it is clear that there always exist infinitely many primes p such that $\left(\frac{m_1}{p}\right) = \dots = \left(\frac{m_l}{p}\right) = 1$ for any set of integers $m_1, \dots, m_l$.

PROPOSITION 5. *Let $F(x, y)$ be an irreducible binary form over k. Then S.H.P./k holds for $F(x, y)$.*

Proof. $F(x, y)$ is irreducible if and only if $F(x, 1)$ is irreducible. Put $F(x, 1) = f(x)$. Then it is clear that $F(x, y) = 0$ has a non-trivial solution in k (resp. $k_\mathfrak{p}$) if and only if $f(x) = 0$ has a solution in k (resp. $k_\mathfrak{p}$). Therefore the validity of S.H.P. for $F(x, y)$ is equivalent to that for $f(x)$ and the latter is known to be true in Hasse [4].

Remark. As a counterexample, put $F(x, y) = (x^3 + 5y^3)(x^2 + 3y^2)$. By the remark after Proposition 3, this form has a non-trivial zero in $\boldsymbol{Q}_p$ for all primes p except $p = 2, 3, 5$. This fact will be used in § 2.

§ 2. Hasse Principle for forms of degree 5. We prove the next theorem step by step.

THEOREM 2. *Hasse Principle over $\boldsymbol{Q}$ does not hold for the following irreducible form of degree 5*

$$(x^3 + 5y^3)(x^2 + xy + y^2) - 17z^5.$$

We have only to prove that the following equation

$$(*) \qquad (x^3 + 5y^3)(x^2 + xy + y^2) = 17z^5$$

has a non-trivial solution in every local field and has no such solution in $\boldsymbol{Q}$.

PROPOSITION 6. *The equation (*) has a non-trivial solution in $\boldsymbol{Q}_p$ for all primes p and in $\boldsymbol{R}$.*

Proof. Solvability in $\boldsymbol{R}$ is obvious. Solvability in $\boldsymbol{Q}_p$ where $p \neq 2, 3, 5$ is easily seen by the remark at the end of § 1, for $x^2 + xy + y^2$ can play the role of $x^2 + 3y^2$ there. Now let

$$F(x, y, z) = (x^3 + 5y^3)(x^2 + xy + y^2) - 17z^5.$$

If $p = 2$ we put $(x, y, z) = (1, 0, 1)$, then $F(1, 0, 1) \equiv 0 \pmod 2$ and $\frac{\partial F}{\partial z}(1, 0, 1) \not\equiv 0 \pmod 2$. This assures the 2-adic solution of (*) by Hensel's lemma ([2], Chap. I, Th. 3).

If $p = 3$ we put $(x, y, z) = (-1, 0, 1)$, then $F(-1, 0, 1) \equiv 0 \pmod 3$ and $\frac{\partial F}{\partial z}(-1, 0, 1) \not\equiv 0 \pmod 3$.

If $p = 5$ we put $(x, y, z) = (2, 0, 1)$, then $F(2, 0, 1) \equiv 0 \pmod 5$ and $\frac{\partial F}{\partial y}(2, 0, 1) \not\equiv 0 \pmod 5$.

These assure the 2 (resp. 3, 5) adic solutions of (*) by the same lemma, q.e.d.

Now, we proceed to the proof of the non-existence of the non-trivial integral solutions of the equation (*). First we make some reductions of the equation to simpler simultaneous equations. Let p be a prime number and (x, y, z) be an integral solution of (*). We can assume x and y are coprime. Assume p^n divides both

$$(1) \qquad x^3 + 5y^3$$

and

$$(2) \qquad x^2 + xy + y^2.$$

Then p^n divides

$$(1) - (2) \cdot x = 5y^3 - x^2y - xy^2 = y(5y^2 - x^2 - xy).$$

Here we can assume p divides neither x nor y, for if p divides one of x, y then it divides the other. Hence p^n divides

$$(3) \qquad 5y^2 - x^2 - xy.$$

Thus p^n divides $(2) + (3) = 6y^2$. Therefore p^n divides 6. Let d denote the largest common divisor of (1) and (2). If 2 divides d then both x and y must be even by (1) and (2). Therefore $d = 1$ or 3.

In the following we show $d = 3$ is impossible. In this case looking at the right hand side of (*), we can see that 3^5 divides $(x^3 + 5y^3)(x^2 + xy + y^2)$. Therefore 3^4 divides $x^3 + 5y^3$ or $x^2 + xy + y^2$.

First, if 3^4 divides $x^3 + 5y^3 = N(x + y\theta)$, where $\theta = \sqrt[3]{5}$ and N stands for the norm from $\boldsymbol{Q}(\theta)$ to $\boldsymbol{Q}$, then, considering $3 = (2 - \theta)^3$ in $\boldsymbol{Q}(\theta)$, $(2 - \theta)^4 = 3(2 - \theta)$ divides $x + y\theta$. It follows that 3 divides both x and y, since $1, \theta, \theta^2$ is the basis of the integers in $\boldsymbol{Q}(\theta)$. This contradicts our assumption $(x, y) = 1$.

Secondly, if 3^4 divides

$$x^2 + xy + y^2 = N\left(x + \frac{1 + \sqrt{-3}}{2} y\right),$$

where N stands for the norm from $\boldsymbol{Q}(\sqrt{-3})$ to $\boldsymbol{Q}$, then considering $3 = -(\sqrt{-3})^2$, 3 divides both x and y and contradicts the assumption $(x, y) = 1$. Therefore, we have proved $d = 1$.

Since 17 remains prime in $Q(\sqrt{-3})$, if 17 divides

$$x^2+xy+y^2 = N\left(x+\frac{1+\sqrt{-3}}{2}y\right),$$

where N is the norm from $Q(\sqrt{-3})$ to Q, then 17 divides both x and y.

Thus we can assume 17 divides x^3+5y^3 but not x^2+xy+y^2. Taking all these facts into account, we have proved that if there exist non-trivial integral solutions of (*) then the following system (**) of equations in x, y, z, w must be satisfied by some non-zero integers.

$$(**)\qquad \begin{cases} x^3+5y^3 = 17z^5, \\ x^2+xy+y^2 = w^5, \\ (x, y) = 1. \end{cases}$$

LEMMA 2. *Let k be a cubic field over Q and ζ be an integer of k such that $\mathrm{Sp}(\zeta) = 0$. Assume a prime p factors in k as a product of three distinct prime divisors; say $p = \mathfrak{p}\mathfrak{p}'\mathfrak{p}''$. Then, if $\mathfrak{p}\mathfrak{p}'$ divides ζ then p divides ζ.*

This lemma is found in exercise 21 of Sec. 7, Chap. 3 of [2] and can be proved easily.

PROPOSITION 7. *(**) has no non-trivial integral solutions.*

Proof. Let x, y, z, w be an integral solution of (**). Denoting $\sqrt[3]{5}$ by θ, the field $Q(\theta)$ has 1, θ, θ^2 as an integral basis, has class number 1 and has $1-4\theta+2\theta^2$ as its fundamental unit [9].

We notice that $x^3+5y^3 = N(x+y\theta)$, where N is the norm from $Q(\theta)$ to Q. Assume a prime p divides z, then p factors in prime ideals in $Q(\theta)$ in one of the following ways:

$$(1)\ p = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3, \quad (2)\ p = \mathfrak{p}, \quad (3)\ p = \mathfrak{p}_1\mathfrak{p}_2,$$
$$(4)\ p = \mathfrak{p}^3, \quad (5)\ p = \mathfrak{p}_1\mathfrak{p}_2^2.$$

As the primes which ramify in $Q(\theta)$ are 3 and 5 and these ramify completely, (5) is impossible.

Letting $\alpha = x+y\theta$, we write down the conditions for p^5 to divide $N(\alpha)$.

Case (1). $\mathrm{Sp}(\alpha\theta) = \mathrm{Sp}(x\theta+y\theta^2) = 0$. So by Lemma 6, $\mathfrak{p}_1^5$, $\mathfrak{p}_2^5$, $\mathfrak{p}_3^5$ or p divides $\alpha\theta$. Since neither p nor $\mathfrak{p}_i$ divides θ, $\mathfrak{p}_1^5$, $\mathfrak{p}_2^5$, $\mathfrak{p}_3^5$ or p divides α.

Case (2). p divides α.

Case (3). $\mathfrak{p}_1^5$ or $\mathfrak{p}_2^5$ or p divides α.

Case (4). $\mathfrak{p}^5$ divides α and therefore p divides α.

In all these cases if p divides α then p divides both x and y and this contradicts the assumption $(x, y) = 1$.

We notice here that in $Q(\theta)$, $17 = (-2+\theta^2)(4+5\theta+2\theta^2)$ and it is easily checked by a direct computation that if $4+5\theta+2\theta^2$ divides $x+y\theta$ then 17 divides both x and y. Taking all these into account, $\alpha = x+y\theta$ must take the form of one of the following types: $(-2+\theta^2)\zeta^5$, $(-2+\theta^2)\varepsilon\zeta^5$, $(-2+\theta^2)\varepsilon^2\zeta^5$, $(-2+\theta^2)\varepsilon^3\zeta^5$, $(-2+\theta^2)\varepsilon^4\zeta^5$ where ζ is an integer of $Q(\theta)$ and ε is the fundamental unit $1-4\theta+2\theta^2$ in $Q(\theta)$.

We are going to show in the following that $x+y\theta$ can never take any one of these five forms.

Put $\zeta = u+v\theta+w\theta^2$ where $u, v, w \in \boldsymbol{Z}$. Then

$$\zeta^5 = \left(u+\theta(v+w\theta)\right)^5 = u^5+5A,$$

where A is an integer of $Q(\theta)$.

As $\varepsilon = 1-4\theta+2\theta^2$, $\varepsilon^2 = -79+12\theta+20\theta^2$, $\varepsilon^3 = -359+528\theta-186\theta^2$ and $\varepsilon^4 = 8641+104\theta-3016\theta^2$, putting $(-2+\theta^2)\varepsilon^i = a_i+b_i\theta+c_i\theta^2$ $(i = 0, \ldots, 4)$, it is easily seen that 5 does not divide c_i $(i = 0, \ldots, 4)$. If $x+y\theta$ takes one of the above-mentioned forms then, for some i,

$$x+y\theta = (a_i+b_i\theta+c_i\theta^2)\zeta^5 = (a_i+b_i\theta+c_i\theta^2)(u^5+5A)$$
$$= a_iu^5+5B+(b_iu^5+5C)\theta+(c_iu^5+5D)\theta^2$$

where B, C, D are rational integers. Since 5 does not divide c_i, this equality shows that 5 divides u. Consequently 5 divides both x and y. This contradicts our assumption $(x, y) = 1$. Thus we have proved $x^3+5y^3 = 17z^5$ has no non-trivial integral solution with $(x, y) = 1$ and finished the proof of Proposition 7.

Proposition 7 together with Proposition 6 completely proves Theorem 2.

References

[1] E. Artin and J. Tate, *Class Field Theory*, Benjamin 1968.

[2] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press 1966.

[3] J. W. S. Cassels and M. J. T. Guy, *On the Hasse Principle for cubic surfaces*, Mathematika 13 (1966), pp. 111–120.

[4] H. Hasse, *Zwei Bemerkungen zu der Arbeit „Zur Arithmetik der Polynome" von U. Wegner in den Math. Ann. 105, S. 628–631*, Math. Ann. 106 (1932), pp. 455–456.

[5] H. B. Mann, *Introduction to Algebraic Number Theory*, Columbus 1955.

[6] L. J. Mordell, *On the conjecture for the rational points on a cubic surface*, Journal London Math. Soc. 40 (1965), pp. 149–158.

[7] E. S. Selmer, *The diophantine equation $ax^3+by^3+cz^3 = 0$*, Acta Math. 85 (1951), pp. 203–362.

[8] H. P. F. Swinnerton-Dyer, *Two special cubic surfaces*, Mathematika 9 (1962), pp. 54–56.

[9] H. Wada, *A table of fundamental units of purely cubic field*, Proc. Japan Acad. 46 (10) (1970), pp. 1135–1140.

[10] B. L. van der Waerden, *Noch eine Bemerkung zu der Arbeit „Zur Arithmetik der Polynome" von U. Wegner in Math. Ann. 105, S. 628–631*, Math. Ann. 109 (1934), pp. 679–680.

DEPARTMENT OF MATHEMATICS
TOKYO METROPOLITAN UNIVERSITY

Received on 5. 10. 1971 (229)

ACTA ARITHMETICA
XXII (1973)

On absolute (j, ε)-normality in the rational fractions with applications to normal numbers

by

R. G. Stoneham (New York, N.Y.)

1. Introduction. In [1, Th. 6, p. 233], we established the (j, ε)-normality [1, Def., p. 222] of a broad class of rational fractions $Z/m < 1$ in lowest terms of type A [1, Th. 4, p. 227, and Def., Type A, p. 229] when represented in bases g such that $(g, m) = 1$.

We shall now present results based on a relaxation of the requirement $(g, m) = 1$ and consider the consequences for the (j, ε)-normal properties of the representations of Z/m in bases g such that $(g, m) > 1$ where g contains some but not all prime factors of m.

Essentially, the above implies that we shall now permit the representations to have non-periodic parts for such g and, of course, the definition of (j, ε)-normality [1, Lemma, and Def., p. 222) does not preclude this occurrence.

Let $m = 2^b \prod_{i=1}^{r} p_i^{b_i}$ and assume in contrast to the basic requirement for Type A, i.e. $b_i > z_i + s_i$ for *at least one* odd prime p_i that one or more of the p_i are such that $b_i > z_i + s_i$, hence, Z/m is surely of Type A and (j, ε)-normal on all g such that $2 \leqslant g < m/D$ where $(g, m) = 1$. Since we obtain non-periodic parts for those g which contain some but not all prime factors of m, we may write

$$Z/m = ZI(u)/g^u M = Q/g^u + R/g^u M \tag{1.0}$$

where $ZI(u)/M = Q + R/M$ with $I(u)$ some positive integer, and $Q \geqslant 0$ is the set of u digits in the non-periodic part. We shall call $R/M < 1$ in lowest terms the "associated" fraction when Z/m is represented in a base such that $(g, M) = 1$ since M contains all the residual prime factors of m not contained in g.

Now if the associated fraction R/M is still of Type A, then Z/m is (j, ε)-normal in all such additional bases g, i.e. those that contain some but not all prime factors of m. The essential point is to select those prime factors in the choice of g which leaves behind in the associated fraction