DIOPHANTINE PROBLEMS INVOLVING POWERS MODULO ONE[1]

BY
EDWARD C. POSNER

1. Introduction

In [1] the following two results were proved: If θ is a real number and the fractional parts of three different positive integral powers of θ are equal, then θ to some positive integral power is a rational integer; if the fractional parts of two different powers of θ are equal for infinitely many pairs of powers, then the same conclusion follows. Here we give different proofs of these results, but the main purpose of this paper is to generalize the second result to complex numbers, and to apply this generalization to problems in diophantine equations.

2. The real case

We begin with a new proof for the real case. If the fractional part of θ^m equals the fractional part of θ^n, then $\theta^m - \theta^n - a = 0$ for some rational integer a, and conversely. We hereafter assume $m > n$, $\theta > 1$, so that $a > 0$. The case $\theta < -1$ is similar. Observe that an equation $x^m - x^n - a = 0$ with $m > n$, $a > 0$, has exactly one positive root, and this root θ is greater than 1. Also, the set of roots of this equation of largest absolute value is readily seen to be $\{\varepsilon_r \theta\}$, $r = (m, n)$, $\{\varepsilon_r\}$ the set of r r^{th} roots of unity. We now prove Theorems 1 and 2 together.

THEOREM 1. *The fractional parts of three different positive integral powers of a real number θ are equal only when θ is the q^{th} root of a rational integer for some positive integer q.*

THEOREM 2. *The fractional parts of two different positive integral powers of a real number θ are equal for only a finite number of pairs of powers unless θ is the q^{th} root of an integer for some positive integer q.*

Proofs. We assume that we have such a θ not the q^{th} root of a rational integer and arrive at a contradiction. Let θ (> 1) satisfy $f(\theta) = 0$, where $f(x) = x^p + a_{p-1} x^{p-1} + \cdots + a_0$, a_i rational integers, $0 \leqq i \leqq p - 1$, is the monic irreducible equation satisfied by θ over the rationals. (We have integer coefficients because θ is an algebraic integer, satisfying as it does at least one equation $\theta^m - \theta^n - a = 0$, a a rational integer.) Since θ itself is not rational, $p > 1$. Now since f divides the polynomial $x^m - x^n - a$, a a rational integer (because $\theta^m - \theta^n - a = 0$), we conclude by the remarks

Received June 30, 1960; received in revised form April 27, 1961.

[1] A portion of the work reported herein was conducted for the Jet Propulsion Laboratory of the California Institute of Technology under a program sponsored by the National Aeronautics and Space Administration.

preparatory to these two theorems that the set of roots of f of largest absolute value is contained in the set $\{\varepsilon_r \theta\}$. Thus, by replacing θ by a power of θ, we may assume that θ is the unique root of f of largest absolute value. Also, f has no root of absolute value $\leqq 1$. For in Theorem 1, we have

$$\theta^m - \theta^n - a = 0, \qquad \theta^m - \theta^l - b = 0,$$

$m > n > l$; a, b rational integers. Then if $f(\zeta) = 0$, $|\zeta| \leqq 1$, we have $\zeta^m - \zeta^n - a = 0$, $\zeta^m - \zeta^l - b = 0$. That is, we would have three points inside or on the unit circle on the same horizontal line an integral distance apart. Since $\zeta \neq 0$ because f is irreducible, two of the three powers of ζ coincide, and the same must therefore hold for θ. Thus θ would be a root of unity. In the case of Theorem 2, let $g_i(\theta) = \theta^{m_i} - \theta^{n_i} - c_i = 0$, c_i rational integers, $m_i > n_i$, $m_{i+1} > m_i$, $i = 1, 2, \cdots$. Since f is irreducible, $f(x)$ divides $g_i(x)$ for every i. If $f(\zeta) = 0$ and $|\zeta| < 1$, then $c_i = 0$ since n_i can be assumed to get arbitrarily large (by Theorem 1; or, if $n_i = n_j$, $i > j$, then $\theta^{m_i} - \theta^{m_j} = c_i - c_j$, and m_j gets arbitrarily large). Thus $\zeta^{m_i} = \zeta^{n_i}$; ζ and so θ would be a root of unity. If, finally, $f(\zeta) = 0$ and $|\zeta| = 1$, then $f(x)$ would be a reciprocal polynomial, θ^{-1} would be a root of f, and we would be again in the previous case. We have proved that all the algebraic conjugates of θ exceed 1 in absolute value.

Consider the p-dimensional real algebra B with basis $\tilde{1}, \psi, \psi^2, \cdots, \psi^{p-1}$ with $f(\psi) = 0$ defining multiplication. Let M denote the real linear transformation from B onto B given by $Mu = \psi \cdot u$ for u in B. The characteristic polynomial of M is $(-1)^p f(\lambda)$, all of whose roots are distinct since f is irreducible. Let

$$\theta_1\,(=\theta), \theta_2, \cdots, \theta_g; \quad \theta_{g+1}, \cdots, \theta_e; \quad \bar{\theta}_{g+1}, \cdots, \bar{\theta}_e$$

denote these p roots of f, where θ_i is real, $1 \leqq i \leqq g$, and $2e - g = p$. Write the vector space direct sum $B = W_1 \dotplus W_2 \dotplus \cdots \dotplus W_e$, where W_i is the invariant subspace of B corresponding to the characteristic root θ_i. Thus W_i is 1-dimensional, $1 \leqq i \leqq g$, and 2-dimensional, $g + 1 \leqq i \leqq e$.

Put an orthogonal structure on B so that the W_i are orthogonal, and choose an orthonormal basis of B consisting of g vectors in the W_i, $1 \leqq i \leqq g$, and of $2(e - g)$ vectors in the W_i, $g + 1 \leqq i \leqq e$, so chosen that on W_i, $g + 1 \leqq i \leqq 2e$, M acts as the 2×2 matrix

$$\begin{pmatrix} \mathrm{Re}\ (\theta_i) & -\mathrm{Im}\ (\theta_i) \\ \mathrm{Im}\ (\theta_i) & \mathrm{Re}\ (\theta_i) \end{pmatrix}.$$

Let $\tau_i(u)$ for u in B denote the length of the projection of u on W_i, $1 \leqq i \leqq e$. Then $\| u \|^2 = \sum_{i=1}^{e} (\tau_i(u))^2$, $\tau_i(Mu) = |\theta_i|\, \tau_i(u)$, $1 \leqq i \leqq e$,

$$\| Mu \|^2 = \sum_{i=1}^{e} |\theta_i|^2 (\tau_i(u))^2.$$

Let $\phi(u)$ denote the direction cosine of u in the W_1 direction, so that

$$(\phi(u))^2 = (\tau_1(u))^2 \cdot \left(\sum_{i=1}^{e} (\tau_i(u))^2\right)^{-1},$$

$$(\phi(Mu))^2 = (\tau_1(u))^2 \left(\sum_{i=1}^{e} |\theta_i/\theta|^2 (\tau_i(u))^2\right)^{-1}.$$

Since $|\theta_i/\theta| < 1$ if $i \neq 1$, $|\phi(Mu)| > |\phi(u)|$ unless $\tau_1(u) = 0$, i.e., unless u is in $V = W_2 \dotplus \cdots \dotplus W_e$, or unless $\tau_i(u) = 0$ whenever $i \neq 1$, i.e., unless u is in W_1. Continuing, for k a positive integer,

$$(\phi(M^k u))^2 = (\tau_1(u))^2 \cdot \left(\textstyle\sum_{i=1}^{e} |\theta_1/\theta|^{2k} (\tau_i(u))^2\right)^{-1},$$

so that $|\phi(M^k u)|$ approaches 1 monotonically as k approaches infinity, unless u is in V or W_1. The vector $\tilde{1}$ however is neither in V nor in W_1, since $\{\tilde{1}, \psi, \psi^2, \cdots, \psi^{p-1}\} = \{\tilde{1}, M\tilde{1}, \cdots, M^{p-1}\tilde{1}\}$ spans B and $p \neq 1$. We may choose the basis for B so that $\tau_1(\tilde{1}) > 0$; then $\tau_1(\psi^k) > 0$, $k \geqq 0$, and so $\phi(\psi^k)$ increases monotonically to 1 as k approaches infinity. Thus the angle between ψ^k and W_1 approaches zero monotonically with k.

If, as we are assuming in Theorem 1, $\theta^m - \theta^n - a = 0$, $\theta^m - \theta^l - b = 0$, then $\psi^m - \psi^n - a = 0$ in B, $\psi^m - \psi^l - b = 0$ in B. Let L be the 1-dimensional subspace spanned by $\tilde{1}$ in B. Then $\psi^m - \psi^n$, $\psi^m - \psi^l$ are both in L. But for $1 \leqq i \leqq e$, $\tau_i(\psi^k) = |\theta_i|^k \tau_i(\tilde{1})$, for all nonnegative integers k; furthermore, no $\tau_i(\tilde{1})$ is zero since $\{1, \psi, \psi^2, \cdots, \psi^{p-1}\}$ spans B. So

$$\tau_i(\psi^l) < \tau_i(\psi^n) < \tau_i(\psi^m), \qquad 1 \leqq i \leqq e.$$

Now $\tilde{1}$, ψ^l, ψ^n, ψ^m are in the same plane. Since $p > 1$, we can project this plane onto the two- or three-dimensional subspace $W_1 \dotplus W_2$, with projections v, α, β, γ say. None of these four projected vectors are in W_1 or W_2, since $\tau_i(\tilde{1}) \neq 0$, $1 \leqq i \leqq e$, and thus $\tau_i(\psi^k) \neq 0$, $1 \leqq i \leqq e$, $k = 0, 1, 2, \cdots$. First assume W_2 is one-dimensional. We shall prove that v and α are on opposite sides of W_1, and also α and β. For α makes a smaller angle with W_1 than v does, whereas β makes a smaller angle with W_1 than α does. Yet $\tau_2(\psi^n) > \tau_2(\psi^l) > \tau_2(\tilde{1})$, so that the W_2-component of β exceeds that of α, which in turn exceeds the W_2-component of v. In Figure 1, if α and v were on the same side of W_1, then the endpoint of β would be on the line Λ parallel to v, and β would have a smaller W_2-component than v has. To prove that α and β are on opposite sides of W_1, consider Figure 2. If β

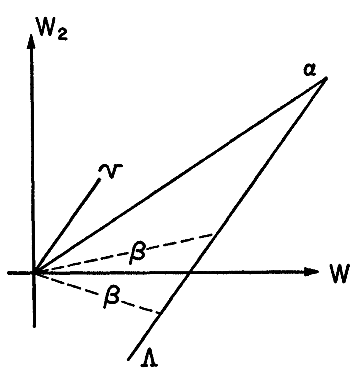

Figure 1

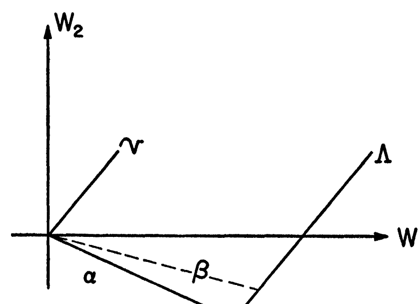

Figure 2

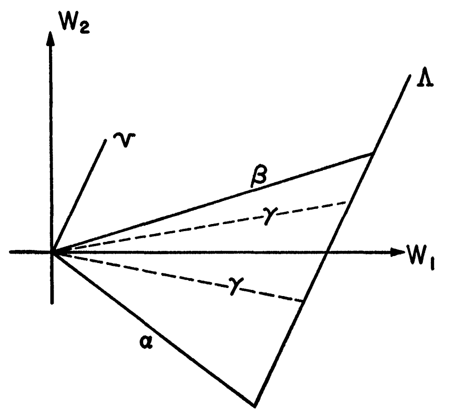

Figure 3

were on the same side of W_1 as α, then again β would have a smaller W_2-component than α. This proves that the relative positions of v, α, β are as in Figure 3. Then γ, which makes a still smaller angle with W_1 than β makes, lies between α and β. We reach a similar component contradiction. The proof is essentially the same in case W_2 is two-dimensional, and is omitted. Theorem 1 is proved.

To prove Theorem 2, we must prove that $\psi^{m_i} - \psi^{n_i}$ cannot be in L for infinitely many pairs (m_i, n_i). Now $m_i - n_i \neq m_j - n_j$, $i \neq j$. For if $m_i - n_i = m_j - n_j = \nu$ say, then $\theta^{n_i}(\theta^\nu - 1) = c_i$, $\theta^{n_j}(\theta^\nu - 1) = c_j$, so that $\theta^{n_i - n_j} = c_i c_j^{-1}$ is rational, with $n_i \neq n_j$, contrary to assumption. Since $m_i - n_i$ never takes the same value twice, $m_i - n_i$ approaches infinity with i. Since $\| M^{-1} \| < 1$ (because all the characteristic roots of M are greater than 1 in absolute value), we have

$$\| \psi^{m_i} \| \cdot \| \psi^{n_i} \|^{-1} = \| \psi^{m_i} \| \cdot \| M^{-(m_i - n_i)} \psi^{m_i} \|^{-1}$$
$$\geqq 1/\| M^{-(m_i - n_i)} \| = (1/\| M^{-1} \|)^{m_i - n_i};$$

this approaches infinity with i. But since the endpoints of ψ^{m_i} and ψ^{n_i} lie on a line parallel to L, and make an arbitrarily small angle with W_1, $\| \psi^{m_i} \| \cdot \| \psi^{n_i} \|^{-1}$ approaches 1. Thus Theorem 2 is proved.

3. The complex case

The rest of this paper is devoted principally to the case when θ is not real. We first note that Theorem 1 can be false for θ complex. In fact, $\theta = (1 + \sqrt{-11})/2$ satisfies $\theta^2 - \theta = -3$, $\theta^5 - \theta = 15$, but is not the q^{th} root of a rational integer for any q. But it does follow from known results, without using Theorem 4, for θ not a q^{th} root of a rational integer, that $\theta^m - \theta^l$ is a rational integer for only finitely many m, given l. For by the next theorem, if $\theta^m - \theta^l$ is a rational integer infinitely often, then θ^r is imaginary quadratic for some r dividing every such m and l. We thus may assume

θ itself to be an algebraic integer in an imaginary quadratic field. Write $\theta^j = A_j + B_j\sqrt{-D}$, D positive and square-free, A_j, B_j rational integers (both integers or both halves of odd integers if $D \equiv 3\ (4)$), $j = 0, 1, 2, \cdots$. Let $Q = |\theta|^2$ so that $|\theta^j|^2 = A_j^2 + DB_j^2 = Q^j$. If now $\theta^m - \theta^l$ is a rational integer, then $\operatorname{Im}(\theta^m - \theta^l) = 0$, so that $B_m = B_l$. Let $DB_l^2 = C$ say; C is not zero, for then B_l would be zero, $\theta^l = A_l$ would be rational. We have $A_m^2 + C = Q^m$; by [2, Satz 698, p. 65], the largest prime divisor of the polynomial $x^2 + C$, $C \neq 0$, tends to infinity with x, so that $A_m^2 + C = Q^m$ is satisfied for only finitely many A_m, and hence only finitely many m. If $D \equiv 3\ (4)$ and B_l is half an odd integer, we obtain the same conclusion from $(2A_m)^2 + 4C = 4Q^m$. This proves the assertion. (This result will not be used in the sequel.)

The following theorem generalizes Theorem 2 and is used in the proof of Theorem 4, which is the main result of this paper.

THEOREM 3. *Let θ be a complex number satisfying equations $I\theta^m - J\theta^n = A$, $m > n$ nonnegative integers, I, J, A rational integers depending on m and n, for infinitely many pairs m, n. Let*

$$\overline{|\theta|} \neq 1 \quad \textit{and} \quad 0 \neq J = \lambda I, \ |\log|\lambda|| = o(m - n).$$

(Here $\overline{|\theta|}$ denotes the maximum of the absolute values of the algebraic conjugates of θ.) Then for some positive integer r dividing all such m and n, θ^r is rational or imaginary quadratic. Conversely, if θ is imaginary quadratic, and not the q^{th} root of a rational number for any positive integer q, and the positive integer k is given, as well as the positive number ε, then θ satisfies infinitely many equations $I\theta^{n+k} - J\theta^n = A$, I, J, A rational integers, $0 \neq J = \lambda I$, $1 - \varepsilon < |\lambda| < 1$.

Proof. Since θ satisfies an equation $I\theta^m - J\theta^n = A$, θ is algebraic. We may assume in fact that $|\theta| = \overline{|\theta|}$, since any algebraic conjugate of θ satisfies the same equations with rational coefficients that θ does. We prove in fact that all the conjugates of θ have the same absolute value that θ has. For if ζ is a conjugate of θ with $|\zeta| \neq |\theta|$, write $\zeta = \mu\theta$; $|\mu| < 1$ since $|\theta| = \overline{|\theta|}$. Then $I\theta^m - J\theta^n = I\zeta^m - J\zeta^n$, or $\theta^m - \lambda\theta^n = \zeta^m - \lambda\zeta^n$, $\theta^m - \zeta^m = \lambda(\theta^n - \zeta^n)$, $\lambda = (\theta^m - \zeta^m)(\theta^n - \zeta^n)^{-1}$ since $\theta^n - \zeta^n \neq 0$ because $|\zeta| < |\theta|$, $n \neq 0$. Thus

$$\lambda = \theta^m(1 - \mu^m)(\theta^n(1 - \mu^n))^{-1} = \theta^{m-n}(1 - \mu^m)(1 - \mu^n)^{-1}.$$

Now $|\mu| < 1$ and $|\theta| \neq 1$, so $|\log|\lambda||$ is $O(m - n)$ but not $o(m - n)$. Thus $|\zeta| = |\theta|$ for every algebraic conjugate ζ of θ.

From now on, we assume only that θ satisfies one equation $I\theta^m - J\theta^n = A$, and that all the algebraic conjugates of θ have the same absolute value that θ has. If ζ is such a conjugate, and $I\theta^m - J\theta^n = A$, then $I\zeta^m - J\zeta^n = A$. We conclude that $I\zeta^m = I\theta^m$, $J\zeta^n = J\theta^n$, or else $I\zeta^m = I\bar{\theta}^m$, $J\zeta^n = J\bar{\theta}^n$. For there are only two horizontal line segments in the complex plane (only one if θ^m is real) going between the circles of radius $|I\theta^m|$ and $|J\theta^n|$ such that the difference of the endpoint on the former circle and the endpoint on the latter circle is A. Thus ζ differs from θ or $\bar{\theta}$ by multiplication by a root of unity. Let r be the least common multiple of all the orders of the roots of unity which occur, so that r divides m and n. We shall prove that θ^r is rational or imaginary quadratic.

Let $p(x)$ be the irreducible polynomial for θ over the rationals, and let $q(x)$ be the polynomial whose roots are the r^{th} powers of the roots of $p(x)$. Then $q(x)$ has rational coefficients; furthermore, q has one or two distinct roots, namely θ^r, and $\bar{\theta}^r$ if θ^r is not real. Thus the irreducible polynomial $h(x)$ for θ^r over the rationals, which divides $q(x)$, has one or two different roots. Since $h(x)$ has distinct roots, $h(x)$ is of degree one or two. If $h(x)$ is of degree one, θ^r is rational; if $h(x)$ has two distinct roots, they are θ^r and $\bar{\theta}^r$, and so θ^r is imaginary quadratic. This proves the first part of the theorem.

To prove the converse, let $\eta = u + iv$, $v \neq 0$, be an arbitrary nonreal complex number, and consider $\{s = \sigma + it \mid t > 0 \text{ and } (1 - \varepsilon)t < \operatorname{Im}(\eta s) < t\}$. This is the region of the upper half plane where $(1 - \varepsilon)t < ut + v\sigma < t$, that is, where $(1 - \varepsilon) - u < v\sigma/t < 1 - u$. This region is a nontrivial cone $K(\eta; \varepsilon)$ in the upper half plane.

Now given the imaginary quadratic number θ not the q^{th} root of a rational number for any positive integer q, let $\eta = \theta^k$, a nonreal complex number. Since θ^q is never real, $\arg\theta$ is an irrational multiple of 2π. Then θ^n is in $K(\eta; \varepsilon)$ for infinitely many n. If we let $I_1 = \operatorname{Im}(\theta^n)$, $J_1 = \operatorname{Im}(\theta^{n+k})$, then $1 - \varepsilon < |J_1/I_1| < 1$, and $\operatorname{Im}(I_1\theta^{n+k} - J_1\theta^n) = 0$, so that $I_1\theta^{n+k} - J_1\theta^n$ is real, hence equal to a rational number A_1. Putting I_1, J_1, A_1 over a common denominator completes the proof of Theorem 3.

We remark that Theorem 3 is false if we replace $o(m - n)$ by either $o(m)$ or $O(m - n)$. For if θ is real quadratic but not the square root of a rational number, we can obtain for every m as above an equation $I\theta^m - J\theta^{m-1} = A$, I, J, A nonzero integers. By symmetry, assume θ has an algebraic conjugate ζ with $\zeta = \mu\theta$, $|\mu| < 1$. Then as before, $J = \lambda I$,

$$\lambda = \theta^m(1 - \mu^m)(\theta^{m-1}(1 - \mu^{m-1}))^{-1} = \theta(1 - \mu^m)(1 - \mu^{m-1})^{-1},$$

$$|\log|\lambda|| = O(1) = O(m - n) = o(m),$$

where $n = m - 1$. This is the required counterexample. We also remark that if θ is an algebraic integer, the condition $\overline{|\theta|} \neq 1$ may be dropped, for if all the conjugates of θ have absolute values 1, then θ is a root of unity [3, p. 137, Theorem 11.5]. The same comment applies in Theorem 4, which we are now ready to consider.

THEOREM 4. *Let ω be a complex number satisfying infinitely many equations of the form $I\omega^m - J\omega^n = A$, $m > n$, I, J, A rational integers not all zero depending on m and n.*

Furthermore, let $\overline{|\omega|} \neq 1$, $|\log|J/I|| = o(m-n)$, $\log|J| = o(m-n)$ (*or even* $\log|J| = o(m)$ *if* ω *is imaginary quadratic, in which case the conditions* $\overline{|\omega|} \neq 1$, $|\log|J/I|| = o(m-n)$ *may also be dropped*). *Then* ω *is a* q^{th} *root of a rational number for some positive integer* q.

Proof. We use Theorem 3 to conclude that ω may be assumed to be imaginary quadratic over the field of rational numbers. (This is the only use made of the additional conditions.) Let $\omega = \theta F^{-1}$, θ an algebraic integer, F a positive rational integer. Let $\theta^2 - P\theta + Q = 0$, P, Q rational integers with $P^2 - 4Q < 0$.

We shall prove that θ to some positive integral power is a positive integer by proving that $\arg\theta$ is a rational multiple of 2π. This shall be done by constructing rational approximations to $(\arg\theta)/\pi$ which are too good. To do this, we shall show that if $d = (m, n)$, then $\mathrm{Im}\,(\theta^m)$ is not much bigger than $\mathrm{Im}\,(\theta^d)$, by proving that $\mathrm{Im}\,(\theta^m)D^{-1/2}$ practically divides $\mathrm{Im}\,(\theta^d)D^{-1/2}$. Then $|\sin\arg\theta^m|$ is not much bigger than $\mathrm{Im}\,(\theta^d)D^{-1/2}Q^{-m/2}$, and therefore not much bigger than $Q^{-(m-d)/2}$, which implies that $m\arg\theta$ is too small mod 2π.

We may assume that θ is an element of $\mathfrak{O}$, the ring of algebraic integers in the field obtained from the field of rational numbers by adjoining $\sqrt{P^2 - 4Q}$, of smallest absolute value satisfying infinitely many equations

$$I\theta^m - JF^{m-n}\theta^n = AF^m,$$

I, J, A rational integers not all zero depending on m, n, and θ, F independent of m, n, but not of θ, $|J| = e^{o(m)}$, such that no positive integral power of θ is a rational integer. Then if the rational prime p divides P and Q, P^2 does not divide Q. For then θp^{-1} would be in $\mathfrak{O}$, satisfying as it does

$$(\theta p^{-1})^2 - (Pp^{-1})(\theta p^{-1}) = Qp^{-2},$$

and would also satisfy the equations

$$(p^m I)(\theta p^{-1})^m - JF^{m-n}p^n(\theta p^{-1})^n = AF^m.$$

Then p^n divides AF^m in $\mathfrak{O}$, hence in the ring of rational integers. First let $(p, F) = 1$. Then p^n divides A, and

$$(p^{m-n}I)(\theta p^{-1})^m - JF^{m-n}(\theta p^{-1})^n = (Ap^{-n})F^m,$$

Ap^{-n} a rational integer, contradicting the minimality of $|\theta|$. If however p divides F, let $F = pG$, G an integer. Then

$$(p^m I)(\theta p^{-1})^m - JG^{m-n}p^{m-n}p^n(\theta p^{-1})^n = Ap^mG^m,$$

$$I(\theta p^{-1})^m - JG^{m-n}(\theta p^{-1})^n = AG^m,$$

again contradicting the minimality of $|\theta|$. This proves the assertion about the common prime divisors of P and Q.

Write $F = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_l^{\alpha_l}$, $p_1, p_2, \cdots, p_l$ distinct primes, $\alpha_1, \alpha_2, \cdots, \alpha_l$ positive integers. By cancelling these p_i as much as possible from the I, J, A

in $I\theta^m - JF^{m-n}\theta^n = AF^m$, we conclude that θ satisfies infinitely many equations

$$H\theta^m - Jp_1^{\beta_1}p_2^{\beta_2}\cdots p_l^{\beta_l}\theta^n = AF^n p_1^{\beta_1}p_2^{\beta_2}\cdots p_l^{\beta_l},$$

$0 \leqq \beta_i \leqq \alpha_i(m-n)$, H a rational integer prime to p_i if $\beta_i > 0$. Then $p_i \mid H\theta^m$ in $\mathfrak{O}$, $p_i \mid (H\theta^m)(\overline{H\theta^m})$, $p_i \mid H^2Q^m$, $p_i \mid Q$ if $\beta_i > 0$.

For any (positive, negative, or zero) integer j, write $\theta^j = A_j + B_j\sqrt{-D}$, D positive and square free, $D \not\equiv 3$ (4), A_j, B_j rational integers (the case $D \not\equiv 3$ (4) is similar and will not be discussed further). Then

$$A_{j+k} = A_jA_k - DB_jB_k\,, \qquad B_{j+k} = A_jB_k + A_kB_j\,,$$

since $\theta^j\theta^k = \theta^{j+k}$. Also,

$$A_{-j} = A_j\,\theta^{-j}, \qquad B_j = -B_jQ^{-j},$$

since $\theta^{-j} = (\theta^j)^{-1}$ and $A_j^2 + DB_j^2 = |\,\theta^j\,|^2 = (|\,\theta\,|^2)^j = Q^j$.

We know that $HB_m = Jp_1^{\beta_1}\cdots p_l^{\beta_l}$, since $\operatorname{Im}(H\theta^m) = \operatorname{Im}(Jp_1^{\beta_1}\cdots p_l^{\beta_l}\theta^n)$. Let $d = (m, n)$, $d = rm - sn$. We treat the case $r, s > 0$; the case $r, s < 0$ is similar. We have

$$B_d = B_{rm-sn} = A_{rm}B_{-sn} + B_{rm}A_{-sn} = (-A_{rm}B_{sn} + B_{rm}A_{sn})Q^{-sn}.$$

Let $Q = Q'Q''$, $(Q', P) = (Q', Q'') = 1$, $Q'' = (Q, P)$ a product of distinct primes. We shall show that B_{rm} is a multiple of $(Q'')^{[m(r-1)/2]}B_m$, B_{sn} of $(Q'')^{[n(s-1)/2]}B_n$. We first prove that A_l and B_l are multiples of $(Q'')^{[l/2]}$, $l = 0, 1, 2, \cdots$. The equation $\theta^2 = P\theta - Q$ shows that $Q'' \mid \theta^2$ in $\mathfrak{O}$. Then $(Q'')^{[l/2]} \mid \theta^l$ in $\mathfrak{O}$, and so $(Q'')^{[l/2]}$ divides A_l and B_l, since $D \not\equiv 3$ (4). Let p be a prime dividing Q'' (it can be proved that $p^{[(l+1)/2]}$ divides A_l if p is odd, but we shall not use this fact). We know that $p^{[m/2]}$ divides A_m, but suppose first that $p^{[(m+1)/2]}$ divides A_m. Observe that B_{tm} is a multiple of $p^{[m(t-1)/2]}B_m$ if $t = 1$; assuming the result for B_{tm}, we prove it for $B_{(t+1)m}$. Now $B_{(t+1)m}B_m^{-1} = A_{tm} + A_m(B_{tm}B_m^{-1})$. Here $p^{[tm/2]}$ divides A_{tm}, whereas $A_m(B_{tm}B_m^{-1})$ is an integer divisible by $p^{[(m+1)/2]}p^{[m(t-1)/2]}$ by the induction hypothesis and the assumption that $p^{[(m+1)/2]}$ divides A_m. Since $[(m+1)/2] + [m(t-1)/2] \geqq [tm/2]$, we have proved that B_{tm} is a multiple of $p^{[m(t-1)/2]}B_m$, $t = 1, 2, \cdots$, in case $p^{[(m+1)/2]}$ divides A_m. Now consider the case in which $p^{[(m+1)/2]}$ does not divide A_m. Such an m is odd, since $p^{[m/2]}$ always divides A_m. Since $A_m^2 + DB_m^2 = Q^m$, $A_m^2 + DB_m^2$ is divisible by p^m. Now B_m is divisible by $p^{[m-1)/2}$, but if B_m were divisible by $p^{(m+1)/2}$, then B_m^2 would be divisible by p^{m+1}, so that A_m^2 would be divisible by p^m, and A_m by $p^{(m+1)/2}$. This contradiction shows that B_m is not divisible by $p^{(m+1)/2}$. The proof that B_{tm} is a multiple of $p^{[m(t-1)/2]}B_m$ when $p^{[(m+1)/2]}$ divides A_m shows that B_{tm} is a multiple of B_m in any case. But since B_{tm} is a multiple of $p^{[tm/2]}$, and B_m is not a multiple of $p^{(m+1)/2}$, $B_{tm}B_m^{-1}$ is a multiple of $p^{[tm/2]-(m-1)/2}$, and so of $p^{[m(t-1)/2]}$. Thus $B_{tm}B_m^{-1}$ is a multiple of $p^{[m(t-1)/2]}$ for every prime p dividing Q'', and so of $(Q'')^{[m(t-1)/2]}$, since Q''

is a product of distinct primes. This proves the assertion about B_{rm}, and similarly about B_{sn}.

Consider $B_d = (-A_{rm} B_{sn} + B_{rm} A_{sn})(Q')^{-sn}(Q'')^{-sn}$. Here $A_{rm} B_{sn}$ is a multiple of $(Q'')^{[rm/2]+[n(s-1)/2]}B_n$, $B_{rm} A_{sn}$ of $(Q'')^{[sn/2]+[m(r-1)/2]}B_m$. From the equation $HB_m = Jp_1^{\beta_1} \cdots p_l^{\beta_l} B_n$, we conclude $(Q')^{sn}(Q'')^{sn}Jp_1^{\beta_1} \cdots p_l^{\beta_l} B_d$ is a multiple of $(Q'')^{[(rm+sn-m-1)/2]}B_m$, $(Q')^{sn}(Q'')^{[(m-(rm-sn)+1)/2]}Jp_1^{\beta_1} \cdots p_l^{\beta_l} B_d$ is a multiple of B_m, $(Q')^{sn}(Q'')^{[(m-d+1)/2]}Jp_1^{\beta_1} \cdots p_l^{\beta_l} B_d$ is a multiple of B_m.

We shall need to know that $(Q', B_m) = 1$. Let the prime p divide Q' and B_m; then $p \mid Q^m = A_m^2 + DB_m^2$, so that $p \mid A_m$, $p \mid \theta^m$ in $\mathfrak{O}$. Let

$$\theta^j = R_j \theta + S_j, \qquad j = 1, 2, \cdots,$$

so that $R_1 = 1$, $S_1 = 0$; $R_2 = P$, $S_2 = -Q$. We have

$$R_{j+1} = R_j P - S_j, \qquad S_{j+1} = -R_j Q.$$

Thus $p \mid S_m$, hence $p \mid R_m \theta$ in $\mathfrak{O}$. Thus $p \mid R_m A_1$, $p \mid R_m B_1$. If p does not divide R_m, then $p \mid A_1$, $p \mid B_1$, $p \mid \theta$ in $\mathfrak{O}$. Let k be the least integer such that $p \mid R_{k+1}$, so that $k \geqq 1$. Now $p \mid S_k$, $p \mid R_{k+1} = R_k P - S_k$, $p \mid R_k P$, $p \mid R_k$ or $p \mid P$. Since p does not divide R_k by the minimality of k, we conclude $p \mid P$. But $P \mid Q$ so $p \mid Q''$ and not Q'. Thus the assumption that $p \mid R_m$ must be retracted, and we have instead $p \mid \theta$. But then

$$(\theta p^{-1})^2 = \bar{P}(\theta p^{-1}) - \bar{Q},$$

$\bar{P}$, $\bar{Q}$ rational integers, so that $\theta^2 = (\bar{P}p)\theta - \bar{Q}p^2$, $\bar{P}p = P$, $\bar{Q}p^2 = Q$ by the uniqueness of P and Q. This however contradicts the fact that Q'' is the product of distinct primes. This contradiction proves that

$$(Q', B_m) = 1.$$

Then $(Q'')^{[(m-d+1)/2]}Jp_1^{\beta_1'} \cdots p_l^{\beta_l'} B_d$ is a multiple of B_m, where $\beta_i' = \beta_i$ unless $p_i \mid Q'$, in which case $\beta_i' = 0$. Let $m = ed$, e an integer >1, so that in turn B_m is a multiple of $(Q'')^{[d(e-1)/2]}B_d$. These two facts taken together imply $B_m = I(Q'')^{\varepsilon} J_1 p_1^{\gamma_1} \cdots p_l^{\gamma_l} B_d$, $\varepsilon = 0$ or 1, $J_1 \mid J$, $\gamma_i \leqq \beta_i$, $1 \leqq i \leqq l$, $\gamma_i = 0$ if $p_i \mid Q'$. If $\gamma_i > 0$, then $\beta_i > 0$ and $p_i \mid Q$, but not Q', so $p_i \mid Q''$.

We will obtain an upper bound for $p_1^{\gamma_1} \cdots p_l^{\gamma_l}$. We have

$$H\theta^m = Jp_1^{\beta_1} \cdots p_l^{\beta_l} + AF^n p_1^{\beta_1} \cdots p_l^{\beta_l}.$$

Let $\gamma_i > 0$ so that p_i divides Q''. Observe that the right-hand side of this equation is divisible in $\mathfrak{O}$ by $p_i^{[\beta_i + n/2]}$, since θ^n is divisible by $p_i^{[n/2]}$, F^n by p_i^n. Thus $p_i^{[\beta + n/2]} \mid H\theta^m$ in $\mathfrak{O}$, $p_i^{2[\beta_i + n/2]} \mid H^2 Q^m$. Recalling $(p_i, H) = 1$, we conclude that $p_i^{2[\beta_i + n/2]} \mid Q^m$. Since $p_i \mid Q''$, and Q'' is the product of distinct primes, p_i^m divides Q^m, but no higher power of p_i divides Q^m. This means

$$2[\beta_i + n/2] \leqq m, \qquad \beta_i \leqq [(m - n + 1)/2] \leqq [(m - d + 1)/2],$$

$$\gamma_i \leqq [(m - d + 1)/2]$$

unless $\gamma_i = 0$. Since $p_i \mid Q''$ if $\gamma_i > 0$, we conclude

$$p_1^{\gamma_1} \cdots p_l^{\gamma_l} \leqq (Q'')^{[(m-d+1)/2]},$$

which is the required upper bound.

Thus our previous relation between B_m and B_d yields

$$| B_m | \leqq Q'' | J | (Q'')^{(m-d+1)/2} | B_d |.$$

To prove $\phi = \arg \theta$ a rational multiple of 2π, consider the argument of θ^m mod 2π: For a suitable positive integer s, an even one if θ^m is in the first or fourth quadrant, odd if θ^m is in the second or third quadrant,

$$\begin{aligned} | \arg \theta^m - s\pi | &= | m\phi - s\pi | \leqq 2 \sin | m\phi - s\pi | \\ &= 2 | B_m | \sqrt{D} Q^{-m/2} \leqq 2(Q'')^{3/2} | J | (Q'')^{(m-d)/2} | B_d | \sqrt{D} Q^{-m/2} \\ &\leqq 2(Q'')^{3/2} | J | (Q'')^{(m-d)/2} Q^{d/2} Q^{-m/2} \end{aligned}$$

since $| B_d | \sqrt{D} \leqq Q^{d/2}$. So

$$\begin{aligned} | m\phi - s\pi | &< 2(Q'')^{3/2} | J | (Q/Q'')^{-(m-d)/2} \\ &= 2(Q'')^{3/2} | J | (Q')^{-(m-d)/2} < 2(Q'')^{3/2} | J | (Q')^{-m/4} \end{aligned}$$

since $d \mid m$ and $d < m$.

First let $Q' > 1$. Then

$$2 | J | (Q'')^{3/2} (Q')^{-m/4} = \exp\left(-\frac{\log Q'}{4} m + o(m) + \log 2 + \frac{3}{2} \log Q''\right),$$

since $| J | = e^{o(m)}$. Thus, for large m, $| m\phi - s\pi | < e^{-Cm}$, C a positive constant, since $\log Q' > 0$. But by a theorem of A. O. Gel'fond [4, p. 34, Theorem IV], if $| m\phi - s\pi | < e^{-Cm}$ for an infinite number of integers m, s with C a positive constant and ϕ the argument of an algebraic number, then ϕ is a rational multiple of $(2)\pi$. The theorem is proved in the case $Q' > 1$.

There remains the case $Q' = 1$. That is, $Q \mid P$, so that $Q \leqq | P |$. But $P^2 < 4Q$, $Q^2 < 4Q$, $Q < 4$, $Q = 1, 2$, or 3. Since Q must divide P, and yet P^2 must be less than $4Q$, we find that θ must satisfy one of the following six equations:

$$\theta^2 \pm \theta + 1 = 0; \qquad \theta^2 \pm 2\theta + 2 = 0; \qquad \theta^2 \pm 3\theta + 3 = 0.$$

Thus $\theta^3 = \pm 1$, $\theta^4 = -4$, or $\theta^6 = -27$. This completes the proof of Theorem 4.

Remarks. We recall that if ω is imaginary quadratic and ω^q is rational for q a positive integer, then $q = 2, 3, 4$, or 6. Also, in Theorem 4, $o(m - n)$ may not be replaced by $O(m - n)$, nor may $o(m)$ be replaced by $O(m)$, as arguments similar to the one following Theorem 3 show. The special case of Theorem 4 wherein θ is an imaginary quadratic integer and $n = 1$ for all m says that $| B_m | > e^{-Cm}$ for all m, C a positive constant, unless of course θ is the q^{th} root of a rational integer.

4. Applications to diophantine equations

We apply Theorem 4 to prove the following two theorems.

THEOREM 5. *Let* $b_{l+2} = Pb_{l+1} - Qb_l$, P, Q *rational numbers*, $b_0 = 0$, *be a linear recurring sequence of order two with the property that there is no positive integer* q *such that* $b_{nq} = 0$, $n = 0, 1, 2, \cdots$. *Then if* L *is sufficiently large, those* b_l *with* $l > L$ *are all different.*

Proof. Consider the two-dimensional algebra B over the rationals spanned by 1, ψ with $\psi^2 = P\psi - Q$. In B, define $\psi^l = P_l\psi - Q_l$, P_l, Q_l rational numbers, $P_0 = 0$, $Q_0 = -1$; $P_1 = P$, $Q_1 = -Q$, $l = 0, 1, 2, \cdots$. Then

$$\psi^{l+1} = P_l\psi^2 - Q_l\psi = P_l(P\psi - Q) - Q_l\psi = (P_lP - Q_l)\psi - P_lQ,$$

so that

$$P_{l+1} = PP_l - Q_l, \qquad Q_{l+1} = P_lQ.$$

Thus

$$P_{l+2} = PP_{l+1} - Q_{l+1} = PP_{l+1} - QP_l,$$

and the P_l satisfy the same linear recurrence that the b_l satisfy. Furthermore, $P_0 = 0$. Since $b_1 \neq 0$ because the sequence $\{b_l\}$ does not consist of all zeros, the sequence $\{P_l\}$ differs from $\{b_l\}$ by multiplication by a constant, so that $P_l = P_n$ if $b_l = b_n$. If $P_l = P_n$ with $n > l$ say, then $\psi^n - \psi^l + Q_n - Q_l$ is zero in B, which is just another way of saying that the polynomial $x^n - x^l - a$ $(a = Q_l - Q_n)$ is divisible by $x^2 - Px + Q$.

First assume the equation $x^2 - Px + Q = 0$ has two real roots with distinct absolute values, the absolute value of the larger, say θ, not being 1. We find, by the same order of magnitude argument as used in Theorem 3, that $x^2 - Px + Q$ does not divide $x^n - x^l - a$, a rational, $n > l$, if l is large enough.

If the absolute values of the roots of $x^2 - Px + Q = 0$ are distinct but the absolute value of the larger root θ is 1, let ζ be the other root of

$$x^2 - Px + Q = 0,$$

so that $\zeta = \mu\theta$, $|\mu| < 1$. As in Theorem 3, we have this time

$$1 = \theta^{n-l}(1 - \mu^n)(1 - \mu^l)^{-1}.$$

If $\theta = +1$, we have $1 - \mu^l = 1 - \mu^n$, $\mu^l = \mu^n$, $n = l$ and not $n > l$. If $\theta = -1$ and $n - l$ is even, we reach the same contradiction; if $\theta = -1$ and $n - l$ is odd, $-1 = (1 - \mu^n)(1 - \mu^l)^{-1}$, $\mu^l - 1 = 1 - \mu^n$, $\mu^l + \mu^n = 2$, contradicting $|\mu| < 1$.

Next assume $x^2 - Px + Q = 0$ has distinct real roots opposite in sign; then $P = 0$, $x^2 + Q = 0$, $b_{l+2} = -Qb_l$, $b_{2l} = 0$, $l = 0, 1, 2, \cdots$, which case has been ruled out by the hypothesis of this theorem.

Now assume the equation $x^2 - Px + Q = 0$ has a double root r, which is of course rational. If $r = 0$, then $x^2 = 0$, $b_{2l} = 0$, $l = 0, 1, 2, \cdots$, which has been ruled out. Let $r \neq 0$. If $x^n - x^l - a$ is a multiple of

$$x^2 - Px + Q,$$

then the equation $x^n - x^l - a = 0$ has r as a double root. So the equation

$$\left(\frac{d}{dx}(x^n - x^l - a)\right) = 0$$

has r as a root, whereupon $nr^{n-1} - lr^{l-1} = 0$, or $r^{n-l} = l/n$. Since $n > l$, $|r| < 1$; let $s = 1/|r|$, $s > 1$. Then $s^{n-l} = n/l$; since $n > l$, $n - l \geqq 1$ and $s^{n-l} \geqq s$, $n/l \geqq s$, $l \leqq n/s$, $n - l \geqq n - n/s = \delta n$ say, $\delta > 0$. So again $n/l = s^{n-l} \geqq s^{\delta n}$. Now $s^{\delta n} > n$ if n is sufficiently large, since $\delta > 0$. Thus $n/l > n$ if n, and so l, is sufficiently large, which leads to the contradiction $l < 1$, l a positive integer.

Finally, let θ be a nonreal number such that $\theta^2 = P\theta - Q$. Define

$$\theta^l = P_l\,\theta - Q_l, \qquad l = 0, 1, 2, \cdots,$$

so that $P_0 = 0$, $Q_0 = -1$; $P_1 = P$, $Q_1 = Q$. As above, if $b_l = b_n$ with $n > l$, then $P_l = P_n$, $\theta^n - \theta^l - a = 0$, a rational. By Theorem 4, if this happens for arbitrarily large l, then $\theta^q = b$, b rational, for some positive integer q. Then $b_{l+q} = bb_l$, $l = 0, 1, 2, \cdots$, so that $b_{nq} = 0$, $n = 0, 1, 2, \cdots$, which has been ruled out by the hypotheses. (Recall $q = 1, 3, 4$, or 6 here.) This proves Theorem 5.

THEOREM 6. *If the positive integer y is sufficiently large, the equation*

$$2^{m+2} - 7y^2 = x^2$$

has at most one solution in positive integers x, m.

Proof. By [5, p. 663], $2^{m+2} - 7y^2 = x^2$ if and only if

$$\theta^m = \pm(x \pm y\sqrt{-7})/2,$$

where $\theta = (1 + \sqrt{-7})/2$. If also $2^{n+2} - 7y^2 = x_1^2$, $m > n$, then

$$\theta^n = \pm(x_1 \pm y\sqrt{-7})/2,$$

$\theta^m \pm \theta^n$ is a rational integer. By Theorem 4, however, $\theta^m \pm \theta^n$ is not a rational integer if m is sufficiently large, since θ is not the q^{th} root of a rational integer for any positive integer q. This proves the theorem.

REFERENCES

1. FRED SUPNICK, H. J. COHEN, AND J. F. KESTON, *On the powers of a real number reduced modulo one*, Trans. Amer. Math. Soc., vol. 94 (1960), pp. 244–257.
2. E. LANDAU, *Vorlesungen über Zahlentheorie*, vol. 3, Leipzig, Hirzel, 1927.
3. HARRY S. POLLARD, *The theory of algebraic numbers*, Carus Mathematical Monographs, no. 9, Mathematical Association of America, 1950.
4. A. O. GEL'FOND, *Transcendental and algebraic numbers*, translated from the 1st Russian ed., New York, Dover Publications, 1960.

5. TH. SKOLEM, S. CHOWLA, AND D. J. LEWIS, *The diophantine equation* $2^{n+2} - 7 = x^2$ *and related problems*, Proc. Amer. Math. Soc., vol. 10 (1959), pp. 663–669.

HARVEY MUDD COLLEGE
CLAREMONT, CALIFORNIA
CALIFORNIA INSTITUTE OF TECHNOLOGY
PASADENA, CALIFORNIA