ON A CLASS OF EXPONENTIAL EQUATIONS[1]

HOWARD RUMSEY, JR. AND EDWARD C. POSNER

We shall prove the following theorem.

THEOREM. *Let a be either 2 or an odd integer. Let $q_1, \cdots, q_j$; $r_1, \cdots, r_k$ be distinct primes, which are relatively prime to a. Then the exponential equation*

$$(1) \qquad a^x = q_1^{y_1} \cdots q_j^{y_j} + r_1^{z_1} \cdots r_k^{z_k}$$

has only a finite number of solutions in non-negative integers x; $y_1, \cdots, y_j$; $z_1, \cdots, z_k$. Furthermore, all such solutions may be found in a finite number of steps.

The fact that equation (1) has only a finite number of solutions is immediate from the following more general result which is proved in Gelfond's book [**3**, p. 37].

LEMMA 1. *Suppose the numbers $\xi_1, \cdots, \xi_m; \psi_1, \cdots, \psi_n; \eta_1, \cdots, \eta_p$ are integers in some algebraic number field K, none of which is an algebraic unit, and suppose A, B, C $(ABC \neq 0)$ are numbers in K, and that the numbers*

$$\xi_1 \cdots \xi_m; \psi_1 \cdots \psi_n; \eta_1 \cdots \eta_p$$

are mutually relatively prime. Then the equation

$$A\xi_1^{x_1} \cdots \xi_m^{x_m} + B\psi_1^{y_1} \cdots \psi_n^{y_n} + C\eta_1^{z_1} \cdots \eta_p^{z_p} = 0$$

has only a finite number of solutions in non-negative integers $x_1, \cdots, x_n$; $y_1, \cdots, y_m$; $z_1, \cdots, z_p$.

Thus the new result is that equation (1) can be solved *constructively* (in a finite number of steps). But our proof is based on an entirely new method. For earlier work on the constructive solvability of exponential equations similar to (1), we refer to the partial list at the end of this paper.

To simplify the notation of the proof we set

$$B = q_1^{y_1} \cdots q_j^{y_j}, \qquad C = r_1^{z_1} \cdots r_k^{z_k}.$$

Equation (1) implies

Received by the editors July 5, 1963.

[1] This paper presents the results of one phase of research carried out at the Jet Propulsion Laboratory, California Institute of Technology, under Contract No. NAS 7-100, sponsored by the National Aeronautics and Space Administration.

$$a^{2x} = (B + C)^2 = (B - C)^2 + 4BC.$$

Factoring the right-hand side in the field $R(\sqrt{(-BC)})$we have

$$a^{2x} = (B - C + 2\sqrt{(-BC)})(B - C - 2\sqrt{(-BC)}). \tag{2}$$

It should be noted that the field $R(\sqrt{(-BC)})$ depends only on the $(k+j)$-tuple of parities of $y_1, \cdots, y_j, z_1, \cdots, z_k$. Therefore we shall be considering only a finite number 2^{k+j} of fields. We also have to consider the two cases: $a=2$ and $a=p_1^{\alpha_1} \cdots p_i^{\alpha_i}$ where $p_1, \cdots, p_i$ are odd primes and $\alpha_1, \cdots, \alpha_i$ are positive integers. We consider the latter case first. By treating equation (2) as an equation in ideals over $R(\sqrt{(-BC)})$ and using unique ideal factorization it is easy to show that equation (2) implies

$$\mathcal{P}_1^{2\alpha_1 x} \cdots \mathcal{P}_i^{2\alpha_i x} = (B - C + 2\sqrt{(-BC)}), \tag{3}$$

where $\mathcal{P}_m$ $(m=1, \cdots, i)$ are prime ideals in $R(\sqrt{(-BC)})$ such that $\mathcal{P}_m\overline{\mathcal{P}}_m=(p_m)$ $(m=1, \cdots, i)$,[2] and $(B-C+2\sqrt{(-BC)})$ is the ideal generated by $B-C+2\sqrt{(-BC)}$.

Equation (3) can hold only if the left-hand side is a principal ideal. Thus the possible values of x are integer multiples of the order of the element $\mathcal{P}=\mathcal{P}_1^{2\alpha_1} \cdots \mathcal{P}_i^{2\alpha_i}$ in the class group of $R(\sqrt{(-BC)})$. If we set $h=$order $\mathcal{P}$, $x=hr$, and $\mathcal{P}^h=(H)$ where $H \in R(\sqrt{(-BC)})$, equation (3) implies

$$uH^r = B - C + 2\sqrt{(-BC)}, \tag{4}$$

where u is a unit in $R(\sqrt{(-BC)})$.

Thus when a is an odd integer we have shown that equation (1) implies an equation of the form

$$uH^r - \bar{u}\overline{H}^r = 4\sqrt{(-BC)}, \tag{5}$$

where H is one of a finite number of integers in $R(\sqrt{(-BC)})$, H is relatively prime to BC, H is not a unit, and u is a unit in $R(\sqrt{(-BC)})$.

In the case $a=2$ an analogous derivation shows that the *same* conditions must hold except that equation (5) is replaced by

$$uH^r - \bar{u}\overline{H}^r = \sqrt{(-BC)}. \tag{6}$$

To complete the proof of our theorem we need the following lemma.

LEMMA 2. *Let D be a positive integer. Let H be an algebraic integer in $R(\sqrt{(-D)})$ not a unit. Let $P=(p_1, \cdots, p_m)$ be a fixed set of rational primes all relatively prime to H. Let u be any unit in $R(\sqrt{(-D)})$. Then*

[2] $\overline{\mathcal{P}}_m$ is the ideal conjugate to $\mathcal{P}_m$ and (p_m) is the ideal generated by p_m.

there exist effectively computable constants $X_1, \cdots, X_m$ *such that* $x_i \geqq X_i$ $(i=1, 2, \cdots, m)$ *implies that the equation*

$$(7) \qquad u\bar{H}^r - \bar{u}\bar{H}^r = p_i^{x_i} \cdots p_m^{x_m}\sqrt{(-D)}$$

has no solutions in non-negative integers r; $x_1, \cdots, x_m$.

This lemma actually suffices to prove the theorem. We have only to apply it to equations (5) and (6) to obtain upper bounds on the exponents $y_1, \cdots, y_j; z_1, \cdots, z_k$ in equation (1).

We must consider three cases in the proof of the lemma. The first is when $u = \pm 1$. In this case equation (7) becomes

$$(8) \qquad H^r - \bar{H}^r = \pm\, p_1^{x_1} \cdots p_m^{x_m}\sqrt{(-D)}.$$

Let p be a prime in P and let x be the corresponding exponent. Equation (8) implies

$$(9) \qquad H^r \equiv \bar{H}^r \pmod{p^x}.$$

Denote by $r(x)$ the smallest positive exponent r such that congruence (9) holds. Since H and p are relatively prime, $r(x)$ is well defined and the values of r which satisfy congruence (9) are integer multiples of $r(x)$. To obtain the upper bound for x which is called for in the lemma we choose X so large that there exists a prime $q \notin P$ and relatively prime to D such that

$$(10) \qquad H^{r(X)} \equiv \bar{H}^{r(X)} \pmod{q}.$$

The *existence* of such a q is guaranteed by Lemma 1 (we assume H and $\bar{H}$ are relatively prime, otherwise the lemma is trivial). Such an X and q may be *found constructively* by considering the *linear recurring sequence*

$$A_r = (H^r - \bar{H}^r)/(H - \bar{H}),$$

and finding the first $r(X)$ such that $A_{r(X)}$ is divisible by some such q.[3] If $x \geqq X$ and

$$H^r \equiv \bar{H}^r \pmod{p^x},$$

then, as we remarked above, r is divisible by $r(x)$. Therefore, from (10), we also have

$$H^r \equiv \bar{H}^r \pmod{q}.$$

[3] In practice, this search can be further simplified, but since this simplification is not necessary for the validity of the theorem, we shall not discuss it here.

In other words if $x \geqq X$, p^x divides $H^r - \bar{H}^r$ *only if* q divides $H^r - \bar{H}^r$. Thus there are *no* solutions to equation (8) for $x \geqq X$; since p was an arbitrary prime in P, the lemma is proved if $u = \pm 1$.

The second case we consider is $D = 1$ and $u = \pm\sqrt{(-1)}$. In this case equation (7) becomes

$$H^r + \bar{H}^r = \pm p_1^{x_1} \cdots p_m^{x_m}.$$

As before, we let p be a prime in P, let $x \geqq 2$ be an integer, and define $r(x)$ to be the smallest positive integer r such that

$$H^r \equiv -\bar{H}^r \pmod{p^x}. \tag{11}$$

In this case it is easy to show that the only integers r which satisfy congruence (11) are *odd* multiples of $r(x)$. By Lemma 1 we may select X so large that

$$H^{r(X)} \equiv -\bar{H}^{r(X)} \pmod{q}$$

for some $q \notin P$. Now the proof of the lemma proceeds exactly as before.

The last case we must consider is $D = 3$ and $u = \pm w$ or $\pm w^2$ where $w = (1 + \sqrt{(-3)})/2$. Let u be fixed, let p be a prime in P and let x be the corresponding exponent in equation (7). First we shall determine those integers s for which

$$uH^s \equiv \bar{u}\bar{H}^s \pmod{p^x}. \tag{12}$$

Denote by $h(x)$ the smallest positive integer h such that

$$H^h \equiv \bar{H}^h \pmod{p^x},$$

and by $r(x)$ the smallest positive integer s such that congruence (12) holds. Let $r = r(x)$ and let s be any integer for which (12) holds. Then, since p is relatively prime to H, we have

$$H^{s-r} \equiv \bar{H}^{s-r} \pmod{p^x}.$$

It follows that $h(x)$ divides $s - r(x)$. Thus p^x divides $uH^s - \bar{u}\bar{H}^s$ only if

$$s = r(x) + nh(x) \tag{13}$$

for some integer n. Now we observe that $h = h(x)$ divides $3r = 3r(x)$. This follows from the congruence

$$H^{3r} \equiv \pm (uH^r)^3 \equiv \pm (\bar{u}\bar{H}^r)^3 \equiv \bar{H}^{3r} \pmod{p^x}.$$

On the other hand, by the definition of $h(x)$ we clearly have $r(x) < h(x)$. It follows that either $h = 3r$ or $h = 3r/2$. We may replace equation (13) by

$$s = \begin{cases} r(x)(3n+1), & r(x) \text{ odd,} \\ (r(x)/2)(3n+2), & r(x) \text{ even.} \end{cases} \tag{14}$$

That is, p^x divides $uH^s - \bar{u}\overline{H}^s$ only if equation (14) holds for some integer n.

We can constructively select an integer X and a prime $q \neq 3$; $p_1, \cdots, p_m$ such that one of the two following cases is true:

$$r = r(x) \text{ is odd and } uH^r \equiv \bar{u}\overline{H}^r \pmod{q} \text{ or}$$

$$r = r(x) \text{ is even and } u^2H^{r/2} \equiv \bar{u}^2\overline{H}^{r/2} \pmod{q}.$$

If there were no such x and q, equation (7) (or one like it) would hold for arbitrarily large values of the exponent x of p. But this contradicts Lemma 1.

We complete the proof by observing that if $r = r(x)$, $x \geqq X$, and $uH^s \equiv \bar{u}\overline{H}^s \pmod{p^x}$, then either

$$uH^s \equiv \pm (uH^r)^{3n+1} \equiv \pm (\bar{u}\overline{H}^r)^{3n+1} \equiv \bar{u}\overline{H}^s \pmod{q}$$

or

$$uH^s \equiv \pm (u^2H^{r/2})^{3n+2} \equiv \pm (\bar{u}^2\overline{H}^{r/2})^{3n+2} \equiv \bar{u}\overline{H}^s \pmod{q}$$

as required.

Bibliography

1. J. W. S. Cassels, *On a class of exponential equations*, Ark. Mat. (4) **17** (1960), 97–103.

2. A. O. Gelfond, *Transcendental and algebraic numbers*, Dover, New York, 1960.

3. ———, *Sur la divisibilité de la différence des puissances de deux nombres entiers par une puissance d'un ideal premier*, Mat. Sb. (N.S.) **7** (49) (1940), 7–25.

4. A. Makowski, *On the diophantine equation* $2^x + 11^y = 5^z$, Nordisk Mat. Tidskr. **81** (1959), 81–96.

5. T. Nagell, *Sur une classe d'équations exponentielles*, Ark. Mat. (3) **54** (1958), 569–582.

California Institute of Technology