POLYNOMIALS THAT DIVIDE INFINITELY MANY TRINOMIALS

Edward C. Posner and Howard Rumsey, Jr.

Summary. This paper extends some recent results on divisibility of trinomials with rational coefficients. It proves the theorem that a polynomial dividing infinitely many trinomials divides at most a cubic in some power of the variable. Furthermore, it rules out a large class of cubics, so that certain polynomials dividing infinitely many trinomials divide a linear or quadratic in a power of the variable; the converse, that every polynomial over the rationals dividing at most a quadratic in a power of the variable divides infinitely many trinomials, is trivial. The methods used are from elementary number theory, algebraic number theory, and diophantine approximation.

1. INTRODUCTION

Cônsider a quadratic or linear polynomial p(x) with rational coefficients. Since the space of polynomials modulo p(x) is at most two-dimensional with basis 1, x, any three powers of x are linearly dependent modulo p(x). In other words, for every pair of distinct positive integers m, n, there exist rational integers a, b, c, not all zero, such that p(x) divides $ax^m - bx^n - c$. Such three-termed polynomials are called *trinomials* (we stipulate that two trinomials differing by a constant multiple are not considered different). Thus we have proved that every quadratic polynomial p(x) divides infinitely many trinomials. Similarly, a quadratic in x^r $(r \geq 1)$ divides infinitely many trinomials in x^r. Thus every divisor of a quadratic in x^r divides infinitely many trinomials (division shall be taken to mean over the polynomials with rational coefficients). The theorem we should have liked to prove is the converse of this: if p(x) is a polynomial with rational coefficients that divides infinitely many trinomials, then p(x) is a divisor of a linear or quadratic polynomial in x^r, for some integer $r \geq 1$.

We have been unable to prove this conjecture. But we have proved that if p(x) divides infinitely many trinomials, then p(x) divides at most a cubic polynomial in x^r, and this cubic divides infinitely many trinomials in x^r. This reduces the conjecture to the consideration of cubics that divide infinitely many trinomials. Furthermore, we have been able to show that a large class of cubics can be ruled out.

2. PRELIMINARY LEMMAS

The lemmas in this section extend several results in [1]. The first lemma considers trinomials with two roots of equal absolute value.

LEMMA 1. *Consider a trinomial* $f(x) = ax^m - bx^n - c$ *with real coefficients and* $a, c \neq 0$, $m > n > 0$ (conventions we shall aaopt throughout this paper). *Let* θ_1 *and*

Received January 20, 1965.

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.

θ_2 be two distinct roots of f(x), *of the same absolute value. Let* r *be the greatest common divisor of* m *and* n, *but if* b = 0, *let* r *equal* m. *Then either* $\theta_1^r = \theta_2^r$ *or* $\theta_1^r = \bar{\theta}_2^r$.

Proof. We assume $b \neq 0$, since otherwise the proof is trivial. Consider the two circles in the complex plane centered at the origin and with radii $a\,|\theta_1|^m$ and $b\,|\theta_1|^n$, respectively (see Figure 1). It is clear from the figure that either

$$a\theta_1^m = a\theta_2^m \text{ and } b\theta_1^n = b\theta_2^n \qquad \text{or} \qquad a\theta_1^m = a\bar{\theta}_2^m \text{ and } b\theta_1^n = b\bar{\theta}_2^n.$$

In the first case, $\theta_1^m = \theta_2^m$ and $\theta_1^n = \theta_2^n$, so that $\theta_1^r = \theta_2^r$. Similarly, the second case yields $\theta_1^r = \bar{\theta}_2^r$.

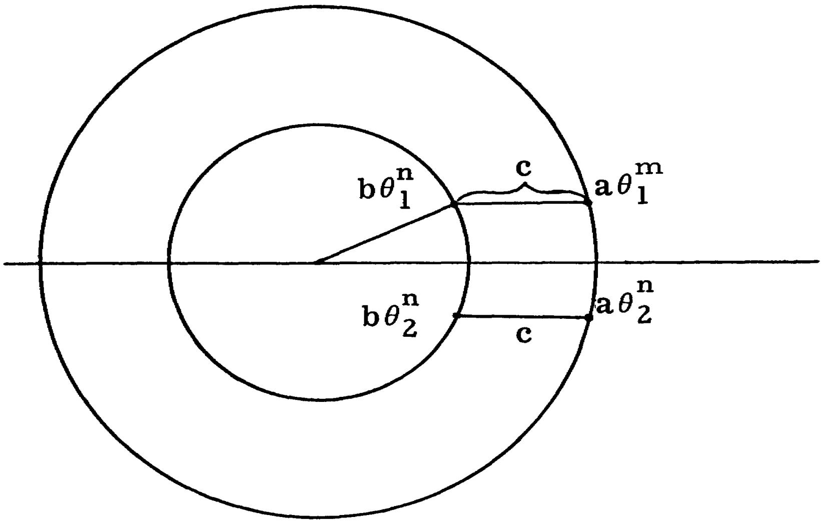

Figure 1.

The next lemma does not rely on Lemma 1.

LEMMA 2. *If the polynomial* p(x) *divides infinitely many trinomials with rational coefficients, then all the roots of* p(x) *lie on at most two concentric circles with centers at the origin.*

Proof. Assume to the contrary that $\theta_1, \theta_2, \theta_3$ are roots of p(x) such that $|\theta_1| > |\theta_2| > |\theta_3|$. We may assume, without loss of generality, that p(x) divides infinitely many trinomials $ax^m - bx^n - c$ such that $m - n$ increases without bound (if p(x) does not meet this requirement, consider $x^n p\left(\frac{1}{x}\right)$, where n is the degree of p). It is obvious that p divides a trinomial with exponents m, n if and only if

$$D = \begin{vmatrix} \theta_1^m & \theta_1^n & 1 \\ \theta_2^m & \theta_2^n & 1 \\ \theta_3^m & \theta_3^n & 1 \end{vmatrix} = 0.$$

But a simple computation shows that

$$D \sim \theta_1^m \theta_2^n \left(1 - \left(\frac{\theta_3}{\theta_2}\right)^n\right)$$

as $m - n \to \infty$. Hence $D = 0$ does not occur infinitely often, contrary to our original assumption.

LEMMA 3. *Let* θ_1, θ_2 *be roots of infinitely many trinomials* $ax^m - bx^n - c$, *and let* $|\theta_1| \neq |\theta_2|$. *Then either* θ_1^m *and* θ_1^n *are real infinitely often, or* θ_2^m *and* θ_2^n *are real infinitely often.*

Proof. We may assume that $m - n < n$ for infinitely many of the trinomials $ax^m - bx^n - c$ of which θ_1 and θ_2 are roots (otherwise, consider θ_1^{-1}, θ_2^{-1}, and the corresponding trinomials). We also assume that $|\theta_1| > |\theta_2|$. Then a simple computation shows that

$$\frac{b}{a} = \frac{\theta_1^m - \theta_2^m}{\theta_1^n - \theta_2^n}.$$

This implies that

$$\left|\frac{b}{a} - \theta_1^{m-n}\right| \leq A\,|\theta_1|^{m-n}\lambda^n,$$

where A is an absolute constant and $\lambda = \left|\frac{\theta_2}{\theta_1}\right| < 1$. Thus

$$|\sin((m - n)\arg\theta_1)| \leq A\lambda^n; \tag{1}$$

in other words,

$$|(m - n)\log\theta_1 - (m - n)\log|\theta_1|| \leq e^{-n\varepsilon}$$

for some $\varepsilon > 0$. Now, by [2 , Theorem IV, p. 34], we conclude that θ_1 and $|\theta_1|$ are not multiplicatively independent. Thus θ_1^d is real for some integer power d. Inequality (1) thus shows that θ_1^{m-n} must be real for infinitely many trinomials $ax^m - bx^n - c$. But since

$$\theta_1^n = \frac{c}{a\theta_1^{m-n} - b} \quad \text{and} \quad \theta_1^m = \theta_1^n\,\theta_1^{m-n},$$

both θ_1^m and θ_1^n are real for infinitely many trinomials. Similarly, if we assume $|\theta_2| > |\theta_1|$, then we see that θ_2^m and θ_2^n are real infinitely often.

3. REDUCTION TO THE CUBIC CASE

THEOREM 1. *Let* $p(x)$ *be a polynomial that divides infinitely many trinomials with rational coefficients. Then there exists a polynomial* q *over the rationals, of degree at most* 3, *dividing infinitely many trinomials over the rationals, and such that* $p(x)$ *divides* $q(x^e)$ *for some integer* e.

Proof. We shall give the proof in two parts, depending on whether p has any multiple roots. First assume that p has a multiple root ϕ, and let θ be any other root of p. Let $T(x) = ax^m - bx^n - c$ be any of the trinomials divisible by $p(x)$; then $T(\theta) = T(\phi) = T'(\phi) = 0$. But these equations imply that

$$\begin{vmatrix} \theta^m & \theta^n & 1 \\ \phi^m & \phi^n & 1 \\ m\phi^{m-1} & n\phi^{n-1} & 0 \end{vmatrix} = 0 .$$

Thus

$$\frac{y^m - 1}{m} = \frac{y^n - 1}{n},$$

where $y = \theta/\phi$. But a simple argument shows that this equation can hold for infinitely m, n only if $|y| = 1$. We conclude that $|\theta| = |\phi|$. Since θ was arbitrary, all the roots of p must have the same modulus. On the other hand, $T'(\phi) = 0$ implies that $\phi^{m-n} = R$ for some rational number R. But this implies that ϕ^m and ϕ^n are rational, and hence ϕ^d is rational if d is the greatest common divisor of m and n. Now let θ be any other root of p(x); then, by Lemma 1, $\theta^d = \phi^d$. Thus if e is the greatest common divisor of all the exponents m and n that appear in trinomials divisible by p, then all the roots of p are also roots of some polynomial $x^e - h$, where h is a rational number.

Observe that trinomials can have double roots at most; since p has a multiple root and divides some trinomials, p(x) must divide $(x^e - h)^2$. Moreover, $(x - h)^2$ clearly divides infinitely many trinomials. Therefore the proof is complete if p has a multiple root.

Now assume that p has only the simple roots $\theta_1, \theta_2, \cdots, \theta_u$, and that p has rational coefficients. There are two cases to consider, depending on whether these roots lie on one or two circles (Lemma 2). The proof in the one-circle case is essentially a simplified version of the proof in the two-circle case, and we omit it.

Thus we assume that $|\theta_1| \neq |\theta_u|$, and we appeal to Lemma 3 to conclude that p(x) divides an infinite number of trinomials $ax^m - bx^n - c$ such that θ_1^m and θ_1^n, say, are real. Let e be the greatest common divisor of the exponents appearing in these trinomials. Let $\theta_1, \theta_2, \cdots, \theta_v$ have the same modulus, and let $\theta_{v+1}, \cdots, \theta_u$ have the same modulus. The argument used to show that all the roots of p satisfy the equation $x^e - h = 0$ when p has a multiple root can be applied to this case to show that $\theta_1, \cdots, \theta_v$ satisfy an equation of the form $x^e - h = 0$, where h is some fixed real number.

Now we must see what happens to the numbers $\theta_{v+1}, \cdots, \theta_u$ when we raise them to the power e. Let $ax^m - bx^n - c$ be a trinomial divisible by p(x), and let d be the greatest common divisor of m and n. Then, by Lemma 1, $\theta_{v+1}^d, \cdots, \theta_u^d$ are all equal or assume one or the other of two mutually conjugate values. If there exists a trinomial such that the greatest common divisor of its exponents m and n is e, then the numbers $\theta_{v+1}, \cdots, \theta_u$ are all roots of a polynomial $x^e - k$ with k a fixed real number, or else they are roots of a polynomial $(x^e - k)(x^e - \bar{k})$ for some complex number k. Even if e is not the greatest common divisor of the exponents of some trinomial, one can easily show that either one of the above alternatives holds, or else there is some power d such that $\theta_{v+1}^d, \cdots, \theta_u^d$ are all real and have the same value.

Thus essentially only two cases remain: p(x) divides a polynomial $q(x^e)$, where either

$$q(x^e) = (x^e - h)(x^e - k) \quad \text{or} \quad q(x^e) = (x^e - h)(x^e - k)(x^e - \bar{k}).$$

It is clear from our derivation that in either case q(x) divides infinitely many trinomials; hence, to complete the proof of the theorem, we need only show that q(x) has rational coefficients.

To this end, define

$$Q(x) = \prod_i (x - \theta_i^d).$$

Then Q(x) has rational coefficients, since $p(x) = \prod_i (x - \theta_i)$ does. But it is apparent that

$$q(x) = \frac{Q(x)}{\gcd(Q(x), Q'(x))}.$$

Therefore q(x) has rational coefficients and the proof is complete.

4. THE CUBIC CASE

The significance of the preceding theorem is that it reduces the problem of finding polynomials that divide infinitely many trinomials to finding cubic polynomials that divide infinitely many trinomials. Furthermore, by using the transformations $x \to 1/x$, $x \to cx$ (c rational), we may restrict our search to cubics q(x) satisfying the following conditions:

(i) $q(x) = x^3 + Ax^2 + Bx + C$ (A, B, C rational integers);

(ii) q has three distinct roots θ, s, t such that $s = \bar{t}$ and $\theta > |s|$;

(iii) There is no rational integer that divides θ, s, and t.

The following theorem summarizes the results we have obtained regarding cubics that divide infinitely many trinomials.

THEOREM 2. *Let* q(x) *be a cubic polynomial, satisfying conditions* (1), (2), (3) *above and such that* $s^d \neq t^d$ *for all integers* d. *The following are necessary conditions that* q(x) *divide infinitely many trinomials:*

(1) *There exist mutually relatively-prime ideals* P, P_θ, P_s, P_t *in the splitting field of* q(x) *such that*

$$(\theta) = PP_sP_t, \quad (s) = PP_tP_\theta, \quad (t) = PP_\theta P_s,$$

where (β) *denotes the principal ideal generated by* β.

(2) $P^3 = (c)$, *where* c *is a positive rational integer such that* $c^{1/3} < |s| < \theta$.

Remarks. The first condition and the condition that P^3 be a rational ideal can be expressed directly in terms of the coefficients of q(x). However, the resulting conditions are somewhat uninformative and throw no new light on the problem. As a second remark, we point out that these results can be slightly refined in case q(x) is reducible (in other words, if θ is a rational integer). These refinements do not make the problem significantly easier, and we shall omit all of them except to remark that in the reducible case c = 1. Finally, we observe that, by the inequality on c, cubic Salem numbers cannot be roots of infinitely many trinomials. (The *Salem* (or PV) numbers are real algebraic integers greater than 1 all of whose algebraic conjugates are less than 1 in absolute value. Thus, since cubic units are Salem numbers, condition (2) proves the conjecture for algebraic units.)

The proof of Theorem 2 depends on a number of lemmas. In all the lemmas, θ, s, t refer to the three roots of a cubic q(x) satisfying conditions (i), (ii), (iii).

LEMMA 4. *Either* $s^d = t^d$ *for some rational integer* d, *or*

$$\lim_{m \to \infty} |s^m - t^m|^{1/m} = |s|.$$

Proof. This is merely a special case of the theorem in Gelfond [2, Theorem IV, p. 34].

LEMMA 5. *Assume that* $s^d \neq t^d$ *for all positive* d, *and let* m *and* n *be the exponents in some trinomial divisible by* q(x). *Then* m - n = o(m).

Proof. Observe that if m and n are exponents in a trinomial $ax^m - bx^n - c$, then

$$\frac{\theta^m - s^m}{\theta^n - s^n} = \frac{s^m - t^m}{s^n - t^n} = \frac{b}{a}.$$

But

$$\left|\frac{\theta^m - s^m}{\theta^n - s^n}\right|^{\frac{1}{m}} \sim \theta^{\frac{m-n}{m}},$$

while

$$\left|\frac{s^m - t^m}{s^n - t^n}\right|^{\frac{1}{m}} \sim |s|^{\frac{m-n}{m}} \quad \text{by Lemma 1}.$$

Hence

$$\theta^{\frac{m-n}{m}} \sim |s|^{\frac{m-n}{m}}.$$

Since $\theta \neq |s|$, we conclude that m - n = o(m).

LEMMA 6. θ *divides* st; s *divides* $t\theta$; t *divides* θs.

Proof. If m and n are exponents in a trinomial divisible by θ, s, t, then

$$\begin{vmatrix} 1 & 1 & 1 \\ \theta^n & s^n & t^n \\ \theta^m & s^m & t^m \end{vmatrix} = 0.$$

In particular, θ^n must divide $s^n t^n (t^{m-n} - s^{m-n})$. But since $\frac{m-n}{m}$ approaches 0 as n approaches infinity, θ divides st for n sufficiently large. The other results follow by symmetry.

LEMMA 7. *Let* Q *be a prime ideal in the splitting field of* q(x), *and let* $s^d \neq t^d$. *Let* $Q^\alpha \| \theta$; *that is, let* $Q^\alpha | \theta$ *but* $Q^{\alpha+1} \nmid \theta$. *Similarly, let* $Q^\beta \| s$ *and* $Q^\gamma \| t$. *Then one of the following possibilities must occur:*

$$\alpha = \beta \geq \gamma, \qquad \beta = \gamma \geq \alpha, \qquad \gamma = \alpha \geq \beta.$$

Proof. If all three of the inequalities are false, we may without loss of generality assume that $\alpha > \beta \geq \gamma$. Then the fact that $D = 0$ in the last lemma implies that if $k = m - n$, then $Q^{\alpha n + \gamma n} \mid s^n t^n (t^k - s^k)$; hence

$$\text{(F)} \qquad Q^{(\alpha-\beta)n} \mid t^k - s^k.$$

But $k = o(n)$ by Lemma 5. Therefore, condition (F) implies that s and t are *multiplicatively dependent* [2, Theorem V, p. 35]. But s and t are conjugates of each other; therefore $s^d = t^d$ for some positive integer d.

We are now able to prove Theorem 2. Before giving the proof we point out that if $s^d = t^d$ for some integer d, then q(x) divides infinitely many trinomials automatically. This is true because $s^d = t^d$ implies that q(x) divides some quadratic in x^d with rational coefficients (namely, $(x^d - \theta^d)(x^d - s^d)$).

Proof of Theorem 2. Lemma 7 implies that if Q is some prime ideal that divides one of the three roots of the cubic, then Q divides at least two of the roots. Therefore, if p is some rational prime that divides θst, then p divides the discriminant $\Delta = (\theta - s)^2 (s - t)^2 (t - \theta)^2$, since each ideal in p divides at least one of the factors in Δ. It follows that each rational prime that divides θst must ramify (see [3, Satz 115]).

Now there are only four distinct ways in which a prime p can ramify and still satisfy the conditions imposed by Lemma 7. These ways are listed below (we use Q, Q_θ, etc. as prime ideals in the splitting field of q(x)):

$$\text{(1)} \qquad (p) = Q^6,$$

$$\text{(2)} \qquad (p) = Q^3,$$

$$\text{(3)} \qquad (p) = Q^3 Q_\theta Q_s Q_t,$$

$$\text{(4)} \qquad (p) = Q_\theta^2 Q_s^2 Q_t^2.$$

The third way of ramifying can not occur under the conditions of Theorem 2. To see this, let $p^h \| \theta$st. Then, by symmetry, $Q^h \| \theta$, $Q^h \| s$, and $Q^h \| t$. But this implies that Q divides the rational integer $\theta + s + t$. Therefore p divides $\theta + s + t$. It follows that Q_θ divides $\theta + s + t$; hence, by Lemma 7, Q_θ divides θ, s, and t. Thus $h \geq 3$ (since Q_θ^3 divides θst). All of these results together imply that $(p) = Q^3 Q_\theta Q_s Q_t$ divides θ, s, and t. But this contradicts the assumption that θ, s, and t are not all divisible by a rational prime. Therefore the third way (3) of ramifying does not occur.

By symmetry and arguments similar to the one just given, the three other types of ramification lead to the ideal factorizations listed below, where $p^h \| \theta$st; (- - - means other ideal factors).

$$\text{(1)} \qquad (\theta) = Q^{2h} - - -, \qquad (s) = Q^{2h} - - -, \qquad (t) = Q^{2h} - - -,$$

$$\text{(2)} \qquad (\theta) = Q^{h} - - -, \qquad (s) = Q^{h} - - -, \qquad (t) = Q^{h} - - -,$$

$$\text{(3)} \qquad (\theta) = Q_s^h Q_t^h - - -, \qquad (s) = Q_t^h Q_\theta^h - - -, \qquad (t) = Q_\theta^h Q_s^h - - -.$$

If we now combine these factorizations for all the primes p that divide θst, we obtain the ideal decomposition given in Theorem 2, namely

$$\text{(G)} \qquad (\theta) = PP_sP_t, \qquad (s) = PP_tP_\theta, \qquad (t) = PP_\theta P_s,$$

and $P^3 = (c)$, where P, P_s, P_t, P_θ are relatively prime, and where c is the largest divisor of θst that consists solely of powers of primes p such that $(p) = Q^3$ or Q^6. This completes the proof of the first part of the theorem.

The proof of the second part relies heavily on the factorization (G). We begin the proof by defining the *linear recurring sequences* $\{\alpha_n\}$, $\{\beta_n\}$, $\{\gamma_n\}$ ($n = 0, 1, 2, \cdots$) by means of the equations

$$\left.\begin{aligned} \theta^n &= \alpha_n \theta^2 + \beta_n \theta + \gamma_n, \\ s^n &= \alpha_n s^2 + \beta_n s + \gamma_n, \\ t^n &= \alpha_n t^2 + \beta_n t + \gamma_n \end{aligned}\right\} \qquad (n = 0, \pm 1, \pm 2, \cdots).$$

The following facts are elementary consequences of this definition:

(1) α_n, β_n, and γ_n ($n = 0, 1, \cdots$) are rational integers;

(2) $\alpha_{n+1} - \theta\alpha_n = \dfrac{s^n - t^n}{s - t}$;

(3) $\lim\limits_{n \to +\infty} \alpha_n/\theta^n = B$ for some nonzero constant B;

(4) q(x) divides a trinomial with positive exponents m and n if and only if

$$\begin{vmatrix} \alpha_n & \alpha_{n+1} \\ \alpha_m & \alpha_{m+1} \end{vmatrix} = 0;$$

(5) P_θ, P_s, P_t are relatively prime to all α_n ($n > 0$).

(6) Let $P^{(n)}$ be defined for $n = 0, 1, \cdots$ as the part of the prime factorization of α_n that contains exactly those primes p that divide c. Then

$$\lim_{n \to \infty} [P^{(n)}]^{1/n} = c^{1/3} = |P|.$$

(Actually this result (6) is not quite elementary, since it depends on [2, Theorem VI, p. 35].)

Define Q as the greatest common divisor of $\alpha_n/P^{(n)}$ and $\alpha_{n+1}/P^{(n+1)}$ ($n \geq 0$). We should like to show that Q satisfies an inequality of the form

$$\text{(E)} \qquad Q \leq A\theta^{n/2}|P|^{-n/2}$$

for some constant A. To prove this, we observe that since Q divides α_n and α_{n+1}, it also divides the three numbers

$(s^n - t^n)/(s - t)$ $(= \alpha_{n+1} - \theta\alpha_n)$, $(\theta^n - t^n)/(\theta - t)$, and $(\theta^n - s^n)/(\theta - s)$.

It also follows from (5) above that

$$QP^n P_\theta^n \mid s^n - t^n, \qquad QP^n P_s^n \mid t^n - \theta^n, \qquad QP^n P_t^n \mid \theta^n - s^n.$$

Therefore

$$Q^3 |P|^{3n/2}(P^3 P_\theta^2 P_s^2 P_t^2)^{n/2} \mid (s^n - t^n)(t^n - \theta^n)(\theta^n - s^n),$$

which is to say that

$$Q^3 |P|^{3n/2}(\theta st)^{n/2} \mid (s^n - t^n)(t^n - \theta^n)(\theta^n - s^n).$$

The rational integer $[(s^n - t^n)(t^n - \theta^n)(\theta^n - s^n)]^2$ is less than some constant times $|s|^{2n}\,\theta^{4n}$. Thus

$$Q^3 |P|^{3n/2}(\theta st)^{n/2} \le A\,|s|^n\,\theta^{2n} = A(\theta st)^{n/2}\,\theta^{3n/2}$$

for some constant A; inequality (E) follows.

It is also possible to prove the similar result

$$\text{(E')} \qquad R \le A'\,\theta^{n/2}\,|P|^{-n/2}$$

for some constant A, where R is the greatest common divisor of $\alpha_n/P^{(n)}$ and $\alpha_m/P^{(m)}$. We omit this proof, since it is similar to the one just given.

We are now in a position to complete the proof of Theorem 2. We observe that if m and n are exponents in a trinomial divisible by q(x) then, since

$$\begin{vmatrix} \alpha_n & \alpha_{n+1} \\ \alpha_m & \alpha_{m+1} \end{vmatrix} = 0,$$

any integer that divides α_n must divide $\alpha_m\alpha_{n+1}$. Hence, for n sufficiently large and for $B' = \lim |\alpha_n/2\theta^n|$,

$$B'\,\theta^n\,|\alpha_n| \le P^{(n)}QR.$$

By combining this inequality with inequalities (E) and (E') and property (6) above, we conclude that as n tends to infinity,

$$Q^{1/n} \sim \theta^{1/2}\,|P|^{-1/2}.$$

Now we apply Roth's theorem to $\alpha_{n+1} - \theta\alpha_n = \dfrac{s^n - t^n}{s - t}$ to obtain the inequalities

$$C\,|s|^n > \left|\frac{s^n - t^n}{s - t}\right| = |\alpha_{n+1} - \theta\alpha_n| \ge \alpha_n \frac{1}{(\alpha_n/P^{(n)}Q)^{2+\varepsilon(n)}} \qquad \text{(C constant)},$$

where $\varepsilon(n) = o(n)$. Therefore, by extracting nth roots, we deduce that

$$|s| \geq \lim_{n\to\infty} \frac{[P^{(n)}]^{\frac{2+\varepsilon(n)}{n}} [Q]^{\frac{2+\varepsilon(n)}{n}}}{\alpha_n^{1/n}} = |P|.$$

Thus, the proof would be complete if we could only show that the absolute values of s and P are distinct. But were the two absolute values equal, it would follow easily that $s^6 = t^6$. Thus, p would divide a quadratic in x^6. Therefore, $|s| > |P|$, and the proof of Theorem 2 is complete.

5. CONCLUDING REMARKS

We conjectured at the beginning of this paper that polynomials over the rationals dividing infinitely many trinomials divide a quadratic in x^r with rational coefficients, for some $r \geq 1$. We then should like to know what the divisors of quadratics in x^r can look like. In the linear case, we know these divisors quite well, from Capelli's Theorem; see Nagell's book ([4, Chapter VIII]) for this and related results otherwise hard to find in one place. A similar class of results should exist for quadratics in x^r, but we have not pursued this matter.

Finally, we mention a generalization of our conjecture, which we state as a conjecture even though the present conjecture has not been settled: If a polynomial with rational coefficients divides infinitely many i-*nomials* (i or fewer nonzero coefficients), it divides a polynomial of degree less than i in x^r for some $r \geq 1$. (The converse of this is true here as in the trinomial case.)

REFERENCES

1. E. C. Posner, *Diophantine problems involving powers modulo one*, Illinois J. Math. 6 (1962), 251-263.

2. A. O. Gelfond, *Transcendental and algebraic numbers* (translated from the first Russian edition), Dover, New York, 1960.

3. E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, Chelsea, New York, 1948.

4. T. Nagell, *Larobök i Algebra*, Almquist, Stockholm, 1952.

Jet Propulsion Laboratory,
California Institute of Technology