POLYNOMIALS ASSUMING SQUARE VALUES

M. Ram Murty[1]

in honour of R.P. Bambah on his 80th birthday

Abstract. If $f(x_1, ..., x_n) \in \mathbb{Z}[x_1, ..., x_n]$ has the property that every integer specialization gives an integral square value, then f is itself the square of a polynomial. We also give an effective version of this result by using an effective version of a classical theorem of E. Noether along with a theorem of Lang and Weil.

1. Introduction

Given a polynomial $f(x_1, ..., x_n) \in \mathbb{Z}[x_1, ..., x_n]$ with the property that every integer specialization of the x_i's results in a square value, does it follow that f is itself the square of a polynomial? Below, we will show that the answer is yes. In fact, it is not necessary to assume that an infinite number of specializations give rise to a square value. A finite number, depending on the size of the coefficients and the degree of the polynomial suffice and this is our main theorem. The question raises other questions that belong to number theory and algebraic geometry. We will discuss these questions at the end.

The case $n = 1$ of this problem is classical. For example, it appears as a problem in the book by Pólya and Szegö (see p. 132 of [7]). Of course, an analogous result is true for k-th powers also. As the referee points out, the multi-variable version of this problem was first investigated by Kojima [4] in 1915. A modern treatment of it can be found in Theorem 52 of [9].

After giving an expository treatment of the single and several variable cases of the problem, we will prove the following effective theorem:

Theorem 1. *Let $f(x_1, ..., x_n) \in \mathbb{Z}[x_1, ..., x_n]$. Then, there is an effectively computable constant $C = C(f)$, depending only on f such that if every integer specialization of $x_1, ..., x_n$ with $|x_i| \leq C$ makes $f(x_1, ..., x_n)$ a perfect integral square, then $f(x_1, ..., x_n)$ is itself the square of a polynomial.*

The effectively computable constant $C(f)$ seems to be humongous and depends on the size of the coefficients of f, the degree d and n. It may be possible by using the work of Deligne, to improve this estimate for $C(f)$, but at present, there are some technical difficulties in this approach. How one may circumvent these difficulties will be addressed in a later paper. However, a refinement of the argument used to prove Theorem 1 will enable us to show:

[1]Research partially supported by a Natural Sciences and Engineering Research Council (NSERC) grant.

Mathematics Subject Classification(2000): Primary 11R09, Secondary 11C08.

Key words and phrases: polynomials, absolute irreducibility, squares, Lang-Weil theorem, resultants.

Theorem 2. *Let $f(x_1, ..., x_n) \in \mathbb{Z}[x_1, ..., x_n]$ have total degree d and let*

$$k = \binom{n+d-1}{n}.$$

Let $||f||$ denote the sum of the absolute values of all the coefficients of f. Put $\psi = 2dt^{2^t}$ where $t = (d+1)(d+2)/2$. If for all integer specializations with $0 \leq a_i \leq H$ where

$$H = 2\max(6d\psi, 9(d-1)^2(d-2)^2, 1319007) + k^{2^k}\log 4||f||,$$

we have that $f(a_1, ..., a_n)$ is a perfect square, then $f(x_1, ..., x_n)$ is itself the square of a polynomial.

2. Preliminaries

We begin by recalling several results we will need in the later discussion. These are of interest in their own right. The first concerns an old result due to Schur [10]. Given a polynomial $f(x) \in \mathbb{Z}[x]$, we say a prime p is a *prime divisor* of f if $p|f(n)$ for some natural number n. An excellent introduction to the topic of prime divisors of polynomials can be found in [2].

Lemma 3. (Schur) *Let $f(x)$ be a non-constant polynomial with integer coefficients. Then f has infinitely many prime divisors.*

Proof. The proof follows Euclid. We induct on the degree of f. For polynomials of degree one, this is clear. Let

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

If $a_0 = 0$, we are done by induction, so we may suppose $a_0 \neq 0$. Since $f(x)$ can assume the values ± 1 only a finite number of times, we deduce that f has at least one prime divisor. Suppose there are only finitely many such prime divisors, $p_1, ..., p_r$ (say). For each natural number m, let $N_m = (p_1 \cdots p_r)^m a_0$ and consider

$$f(N_m) = a_0(a_n a_0^{n-1}(p_1 \cdots p_r)^{nm} + \cdots + a_1 a_0(p_1 \cdots p_r) + 1).$$

For m sufficiently large, the term in the parentheses above is in absolute value greater than 1 and coprime to $p_1 \cdots p_r$. This is a contradiction. ▫

We also need to recall some basic facts about resultants (see p. 200ff of [5]). Let R be a commutative ring. Given two polynomials

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

and

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$$

in $R[x]$, we define the resultant $R(f,g)$ to be the determinant of the $(m+n)\times(m+n)$ matrix

$$\begin{pmatrix} a_n & a_{n-1} & \cdots & a_0 & 0 & \cdots & 0 \\ & a_n & a_{n-1} & \cdots & a_0 & \cdots & 0 \\ & & \cdots & \cdots & & & \\ & & & & a_n & \cdots & a_0 \\ b_m & b_{m-1} & \cdots & b_0 & 0 & \cdots & 0 \\ & b_m & b_{m-1} & \cdots & b_0 & \cdots & 0 \\ & & \cdots & \cdots & & & \\ & & & & b_m & \cdots & b_0 \end{pmatrix}$$

It is not hard to see that there are polynomials $A(x), B(x) \in R[x]$ so that

$$A(x)f(x) + B(x)g(x) = R(f,g).$$

It is well-known that if the coefficients of f and g lie in a field K such that $a_n b_m \neq 0$ and f, g split into factors of degree 1 in $K[x]$, then $R(f,g) = 0$ if and only if f and g have a common root (see p. 203 of [5]). In particular, if $f(x) \in \mathbb{Z}[x]$ has n distinct roots in $\mathbb{C}$, the natural number $R(f,f')$ is non-zero. Thus, if $f(x)$ is squarefree, that is, a product of distinct irreducible polynomials, then $R(f,f')$ is non-zero.

3. The case $n = 1$

We can now prove:

Theorem 4. *Suppose that $f(x) \in \mathbb{Z}[x]$ is a polynomial such that $f(n)$ is a perfect square for every integer n. Then $f(x) = g(x)^2$ for some $g(x) \in \mathbb{Z}[x]$.*

Proof. Since $\mathbb{Z}[x]$ is a UFD, we may factor $f(x)$ as a product of irreducible polynomials. By grouping the even powers of the irreducibles occurring in the factorization, we may write $f(x) = g(x)^2 h(x)$ where $h(x)$ is squarefree, that is, a product of distinct irreducible polynomials. Let us suppose that the degree of h is ≥ 1. By Lemma 3, h has infinitely many prime divisors and so we choose one p which is coprime to $R(h,h')$. Thus, there is a natural number n so that $p|h(n)$. Hence $p|f(n)$. As $f(n)$ is a perfect square, we see that the power of p dividing $f(n)$ is an even power. The same must be true for $h(n)$. Thus, $p^2|h(n)$. Now, $h(n+tp) \equiv h(n) (\mathrm{mod}\ p)$ so that by the same reasoning, we deduce $p^2|h(n+tp)$. However, $h(n+tp) = h(n)+pth'(n) (\mathrm{mod}\ p^2)$ so that $p|h'(n)$ if we choose t coprime to p (such as $t = 1$ say). In particular, $p|R(h,h')$ contrary to our choice of p. Thus, the degree of h is zero so that h must be a constant. This constant must be a square. □

4. The higher dimensional case

Before we begin the discussion of the multi-variable case, it is useful to recall the classical theorem that if R is a UFD then so is $R[x]$. In particular, $\mathbb{Z}[x_1, ..., x_n] = \mathbb{Z}[x_1, ..., x_{n-1}][x_n]$ is a UFD. Given two polynomials $f, g \in \mathbb{Z}[x_1, ..., x_n]$ we may consider them as polynomials in x_n with coefficients in $\mathbb{Z}[x_1, ..., x_{n-1}]$. Thus, we may consider the resultant $R_{x_n}(f, g)$ as a polynomial in $x_1, ..., x_{n-1}$. By taking an algebraic closure of $\mathbb{Q}(x_1, ..., x_{n-1})$, we see that any polynomial factors as a product of linear factors, and we may deduce, as before that $R_{x_n}(f, g) = 0$ if and only if f and g have a common root. In particular, if $f_{x_n} = \partial f/\partial x_n$, then $R(f, f_{x_n}) = 0$ if and only if f and $\partial f/\partial x_n$ have a common root. Thus, if f is squarefree, then the resultant $R(f, f_{x_n}) \neq 0$.

Theorem 5. (Kojima, 1915) *Now suppose that we have $f(x_1, ..., x_n) \in \mathbb{Z}[x_1, ..., x_n]$ having the property that every integer specialization of $x_1, ..., x_n$ makes $f(x_1, ..., x_n)$ a square. Then, $f(x_1, ..., x_n)$ is the square of a polynomial.*

Proof. We proceed by induction on the number of variables. As before, we may factor $f = g^2 h$, with h a squarefree polynomial. If h has fewer than n variables, we are done by induction. Suppose then that h is a polynomial of n variables. As h is squarefree, the resultant $R(h, h_{x_n})$ (which is a polynomial in $x_1, ..., x_{n-1}$) is not identically zero. Thus, we may choose $(x_1, ..., x_{n-1}) = (a_1, ..., a_{n-1})$ so that the resultant $R := R(h, h_{x_n})(a_1, ..., a_{n-1})$ is not zero. Thus, $h(a_1, ..., a_{n-1}, x_n)$ is a non-zero polynomial in the single variable x_n. For otherwise, its derivative would also be zero and consequently R would be zero which is not the case. By Lemma 3, this polynomial has infinitely many prime divisors. Choose a prime p not dividing R. As before, there is an a_n so that $p|h(a_1, ..., a_n)$. As $f(a_1, ..., a_n)$ is a square, we deduce $p^2|h(a_1, ..., a_n)$. The same is true for $h(a_1, ..., a_n + p)$. But then,

$$h(a_1, ..., a_{n-1}, a_n + p) \equiv h(a_1, ..., a_n) + p h_{x_n}(a_1, ..., a_n) \pmod{p^2}$$

from which we deduce that

$$p|h_{x_n}(a_1, ..., a_n)$$

so that $p|R$, a contradiction. □

5. Absolutely irreducible polynomials mod p

We now turn to the question of making Theorem 5 effective. The results we invoke form a chapter in classical elimination theory and we refer the reader to (pages 177-215) of [11]. We summarise these results below.

Recall that a polynomial f with coefficients in a field K is said to be absolutely irreducible if it is irreducible over the algebraic closure of K.

Let $f(x_1,..,x_n) \in \mathbb{Z}[x_1,..,x_n]$ be a polynomial of the form g^2h with h non-constant. Let us note that a polynomial of the form

$$y^2 - f(x_1,...,x_n) \tag{1}$$

with $f(x_1,..,x_n) \in \mathbb{Z}[x_1,...,x_n]$ is irreducible over $\overline{\mathbb{Q}}$. For if it is reducible, it must be a product of two factors which are linear in y and this can only happen only if the discriminant $4f(x_1,...,x_n)$ is a perfect square, which is not the case, by hypothesis. Thus, (1) is absolutely irreducible over $\mathbb{Q}$.

Given a polynomial $f(x_1,...,x_n)$, suppose we can find a prime p such that the number of solutions $(x_1,...,x_n,y)$ mod p of the congruence

$$y^2 \equiv f(x_1,...,x_n)(\text{mod } p)$$

is strictly less than p^n. Then, there is an n-tuple $(a_1,...,a_n)$ so that

$$f(a_1,...,a_n)$$

is not a square mod p. Under which conditions can we do this? If the polynomial (1) is absolutely irreducible, that is irreducible over $\overline{\mathbb{F}}_p$, then a famous theorem of Lang and Weil[6] allows us to do this. The question that arises now is if we can find a prime p for which (1) is absolutely irreducible mod p.

Given a polynomial f with integer coefficients, we denote by $||f||$ the sum of the absolute values of its coefficients. Clearly, $||fg|| \leq ||f||||g||$. However, a more natural height function for polynomials is given by taking the maximum of the absolute values of the coefficients of f and denoting this by $H(f)$. It is evident that $H(f) \leq ||f|| \leq C(d,n)H(f)$, where $C(d,n)$ is a constant depending on the number of variables and the total degree d. In fact, we may take

$$C(d,n) = \binom{d+n}{n},$$

by a simple calculation. Thus, the two heights are comparable.

Proposition 6. (Gelfond's inequality)

$$H(f_1)\cdots H(f_r) \leq e^{d_1+\cdots+d_n} H(f_1\cdots f_r),$$

where d_i is the degree in x_i of the product $f_1\cdots f_r$.

Proof. See page 229 of [3]. ▫

Corollary 7. *If $f|g$, then $||f|| \leq c_1(d,n)||g||$ for some effectively computable constant $c_1(d,n)$ depending only on n and the total degree d of g.*

How is all this relevant to our situation? As before, let us write $f = g^2h$, with h a squarefree polynomial. Then, by Corollary 7, we have that $||h|| \leq c_1(d,n)||f||$. We will need to use this inequality in applying the following theorem due to E. Noether, in our context.

Proposition 8. (E. Noether, 1922) *Let K be a field. Given a polynomial*

$$f(x_1,...,x_n) = \sum_{i_1+\cdots+i_n\leq d} a_{i_1,...,i_n} x_1^{i_1}\cdots x_n^{i_n} \in K[x_1,...,x_n],$$

there exist forms $g_1,...,g_s$ in variables $A_{i_1,\cdots,i_n}$ with $i_1+\cdots+i_n \leq d$, such that the polynomial $f(x_1,...,x_n)$ is reducible over $\overline{K}$ or of degree $< d$ if and only if all the s polynomials g_j vanish when we specialize $A_{i_1,...,i_n}$ with $a_{i_1,...,i_n}$. Moreover, if

$$k = \binom{n+d-1}{n},$$

then the degree of g_j is bounded by k^{2^k}. These forms depend only on n and d and are independent of the field K in the sense that if the characteristic of K is zero, they are fixed forms with rational integer coefficients, while if the characteristic of K is a prime p, they are obtained by reducing the integral coefficients modulo p. In the case characteristic of K is zero, then

$$||g_j|| \leq 4^{k^{2^k}}, \quad 1 \leq j \leq s.$$

Proof. See page 190 of [11]. ▫

Corollary 9. *Let k be as in the previous proposition. Given a polynomial $f(x_1,...,x_n) \in \mathbb{Z}[x_1,...,x_n]$, which is absolutely irreducible, there exists a natural number N_f such that*

$$N_f \leq (4||f||)^{k^{2^k}},$$

and f is absolutely irreducible mod p for every prime p coprime to N_f.

Proof. By Proposition 8, there is a polynomial g_j such that when we specialize to the coefficients of f, the value of g_j is a non-zero integer. We let N_f be the smallest of the absolute values of the non-zero values among the g_j's thus obtained. Since the coefficients of f are bounded by $H(f)$, and the degree of g_j is bounded by k^{2^k}, we get

$$0 < N_f \leq ||g_j||||f||^{k^{2^k}} \leq (4||f||)^{k^{2^k}}.$$

Moreover, for every prime p coprime to N_f, we deduce by Noether's theorem that f is absolutely irreducible mod p. This completes the proof. ▫

We will need the following effective version of the theorem of Lang and Weil, proved by Schmidt [11].

Proposition 10. *Let $F(x_1, ..., x_n)$ be a polynomial over $\mathbb{F}_p$ which is of total degree $d > 0$ and absolutely irreducible. Let N be the number of zeros of F in $\mathbb{F}_p^n$. Then,*

$$|N - p^{n-1}| \leq p^{n-2}(\omega(p, d) + 2d\psi),$$

where

$$\omega(p, d) = (d-1)(d-2)p^{1/2} + d^2,$$

and $\psi = 2dt^{2^t}$ with $t = (d+1)(d+2)/2$.

6. Proof of Theorem 1

We apply Corollary 9 to the polynomial

$$F(x_1, ..., x_n, y) := y^2 - f(x_1, ..., x_n).$$

Thus, if p is coprime to N_F, F is absolutely irreducible mod p. By Proposition 10, the number of zeros N mod p satisfies

$$|N - p^n| \leq p^{n-1}(\omega(p, d) + 2d\psi).$$

Of these zeros, the number with $y = 0$ can be at most dp^{n-1} since the number of solutions of

$$f(x_1, ..., x_n) \equiv 0 (\text{mod } p),$$

is bounded by this quantity. So if, we let N^* be the number of zeros of F with $y \neq 0$, we get

$$|N^* - p^n| \leq p^{n-1}(\omega(p, d) + 2d\psi + d).$$

In particular, the number of specializations mod p for which $f(x_1, ..., x_n)$ is a perfect square mod p is

$$\leq \frac{1}{2}p^n + \frac{1}{2}p^{n-1}(\omega(p, d) + 2d\psi + d)$$

and this is strictly less than p^n if

$$\omega(p, d) + 2d\psi + d < p.$$

If we choose

$$p > 6d\psi, \quad \text{and} \quad \sqrt{p} > 3(d-1)(d-2),$$

we see that

$$\omega(p, d) + 2d\psi + d < p.$$

So we need p coprime to N_F and $p > \max(6d\psi, 9(d-1)^2(d-2)^2)$. This completes the proof of Theorem 1.

7. Proof of Theorem 2

In the proof of Theorem 1, let us consider all specializations of $f(a_1, ..., a_n)$ with $0 \leq a_i \leq H$ with H given as in the statement of Theorem 2. We claim that there is a prime $p < H$ which is coprime to N_F and satisfying

$$p > C(d) := \max(6d\psi, 9(d-1)^2(d-2)^2).$$

Indeed, by [12]

$$\theta(H) := \sum_{p<H} \log p > .998684H$$

provided $H \geq 1,319,007$. Since $H = 2(C(d) + \log N_F)$, we see that

$$\sum_{p<H,(p,N_F)=1} \log p > \frac{9}{5}(C(d) + \log N_F) - \log N_F > 0$$

and so there is a prime of the desired type. This completes the proof.

8. Concluding remarks

It is clear that the bounds obtained in Theorems 1 and 2 are not optimal. However, Proposition 8 is optimal in the following sense. Ruppert [8] has shown that if $f \in \mathbb{Z}[x, y]$ is absolutely irreducible and has $\deg_x f = m$, $\deg_y f = n$ and height $H(f) = H$, then for any prime p with

$$p > [m(n+1)n^2 + (m+1)(n-1)m^2]^{mn+(n-1)/2} H^{2mn+n-1},$$

the reduction of f mod p is absolutely irreducible. Moreover, if we assume the Bouniakowsky conjecture [1] that predicts that for any irreducible polynomial $g(t) \in \mathbb{Z}[t]$, $g(n)/\delta$ is prime for infinitely many values of n (here, $\delta = \gcd\{g(r) : r \in \mathbb{Z}\}$), then there are infinitely many absolutely irreducible polynomials $f \in \mathbb{Z}[x, y]$ which are reducible mod p where p is a prime with $p > H^{2m}$. Thus, in the case $n = 2$, the power of H in Proposition 8 cannot be substantially improved, modulo the Buniakowsky conjecture, which is generally believed. A closer examination of the proof in [8] shows that what is actually proved is that given $f \in \mathbb{Z}[x, y]$, there is a non-zero natural number N_f satisfying

$$N_f < [m(n+1)n^2 + (m+1)(n-1)m^2]^{mn+(n-1)/2} H^{2mn+n-1},$$

such that f is absolutely irreducible mod p whenever p is coprime to N_f. Thus, refining Proposition 8 will not lead to any substantial improvement of our bounds. It may be possible to improve these bounds by other techniques, partly geometric and partly analytic in nature. This will be investigated in a future paper.

Concerning the case of higher powers, the methods extend, in principle. However, getting definitive bounds is not all that straightforward by the methods of this paper. Part of the

difficulty is first to establish the absolute irreducibility of the polynomial

$$y^k - f(x_1, ..., x_n),$$

when $f(x_1, .., x_n)$ is not a perfect k-th power. This is easily done if k is prime and then the argument of this paper easily extends. Thus, one can proceed inductively in this fashion. It is clear that this will again lead to humongous bounds. Consequently, it is thus desirable to think of alternate ways in which better bounds can be obtained.

Acknowledgements. This paper was first presented at the Chandigarh conference in honour of Professor R.P. Bambah organized by Professors Madhu Raka and R.J. Hans-Gill. I thank them both for their kind hospitality. I would also like to thank Michael Roth, Dinesh Thakur and the referee for their comments on an earlier version of this paper.

References

[1] V. Buniakowsky, Nouveaux théorèmes relatifs à la distinction des nombres premiers et à la décomposition des entiers en facteurs, *Mém. Acad. Sci. St. Pétersbourg Sci. Math. Phys.*, **6** (1857), 305-329.

[2] I. Gerst and J. Brillhart, Prime divisors of polynomials, *American Math. Monthly,* **78** (1971), 250-266.

[3] M. Hindry and J. Silverman, Diophantine geometry, an introduction, *Graduate Texts in Math.,* **201** Springer-Verlag, New York, 2000.

[4] T. Kojima, Note on number-theoretical properties of algebraic functions, *Tohoku Mathematical Journal,* **8** (1915), Series 1, 24-37.

[5] S. Lang, Algebra, Second edition, Addison-Wesley, 1984.

[6] S. Lang and A. Weil, Number of points on varieties in finite fields, *American Journal of Math.,* **76** (1954), 819-827.

[7] G. Pólya and G. Szegö, Problems and Theorems in Analysis II, translated from the German by C.E. Billigheimer, *Classics in Mathematics,* Springer-Verlag, 1998.

[8] W. M. Ruppert, Reducibility of polynomials $f(x, y)$ modulo p, *Journal of Number Theory,* **77** (1999), 62-70.

[9] A. Schinzel, Polynomials with special regard to reducibility, Cambridge University Press, 2000.

[10] I. Schur, Über die existenz unendlich vieler primzahlen in einiger speziellen arithmetischen progressionen, S-B Berlin Math. Ges., **11** (1912), 40-50.

[11] W. Schmidt, Equations over finite fields, An elementary approach, *Springer Lecture Notes,* **536**, 1976.

[12] J. B. Rosser and L. Schoenfeld, Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$, *Math. Comp.*, **29** (1975), 243-269.

Address of author:
Department of Mathematics,
Queen's University,
Kingston, Ontario,
K7L 3N6, Canada
e-mail: murty@mast.queensu.ca