



# On the power-free values assumed by polynomials

C Hooley

## ► To cite this version:

C Hooley. On the power-free values assumed by polynomials. Hardy-Ramanujan Journal, 2003, pp.30-55.  
⟨hal-01109884⟩

**HAL Id: hal-01109884**

**<https://hal.science/hal-01109884v1>**

Submitted on 27 Jan 2015

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



HAL Authorization

## On the power-free values assumed by polynomials<sup>1</sup>

BY C. HOOLEY

In honorem Nicholas Katz annos LX nati

### 1. Introduction.

It has long been conjectured that a polynomial  $f(n)$  of degree  $r > 1$  with integer coefficients infinitely often assumes square-free values provided that it have no non-trivial fixed square divisors and, indeed, that there is an asymptotic formula

$$N^{(2)}(x) \sim A(f)x$$

for the number of such square-free values furnished by the integers  $n$  not exceeding  $x$ . There has therefore been a voluminous history of the study of problems of this type, of which the earlier part up to 1967 was described in moderate detail in our paper of that year on the square-free values of cubic polynomials [7]. Yet, since there has been substantial progress on this matter subsequently and since our summary was compiled nearly forty years ago, it seem appropriate before discussing our present theme to mention some background to these problems and the main milestones in their resolution.

At the outset we must remind the reader that, following Browkin, Filaseta, Greaves, and Schinzel [3], Granville [6] demonstrated in 1998 that the truth of the conjecture above would follow from that of the so-called *abc* Hypothesis, a supposition so powerful that it implies the validity of many ambitious speculations in the theory of numbers. Historically, however, the usual axis of attack has been to consider the *sth* power-free values taken by  $f(n)$  for values of  $s$  as small as possible in terms of  $r$  and, in particular, to obtain an asymptotic formula

$$N(x) = N^{(r)}(x) \sim A(f)x \tag{0}$$

for the number of these values provided by integers  $n$  up to  $x$ , it being supposed that  $f(n)$  has no non-trivial fixed *sth* power divisors. For  $s \geq r$  the primitivity and irreducibility of  $f(n)$  ensures that this necessary and always assumed condition is in place but is invariably best retained — as is done in our description — for simplicity and because the reducible case is always easier than the irreducible one. This having been said, the first result appears to be due to Nagell [16], who shewed in 1922 that  $f(n)$  is infinitely often *sth* power-free provided that  $s \geq r$ . This was followed by Ricci's asymptotic formula (0) obtained by a sieve method under the same condition [19], although in the meantime a more precise formula was provided by Estermann [5] for the special case where  $f(n) = n^2 + k$  and  $s = 2$ .

---

<sup>1</sup>A summary of this article was delivered at the conference in Princeton, New Jersey, that was held in December 2003 to honour Nicholas Katz on the occasion of his sixtieth birthday.

Much later Atkinson and Lord Cherwell secured an analogy of Estermann's formula for the more general binomial  $f(n) = n^r + k$  when  $s \geq r$  in a paper [1] that may well have been a source of inspiration to later writers because of its penetrating discussion of the general problem. But it was only in 1953 that the barrier  $s \geq r$  was crossed when Erdős [4] proved in a characteristically ingenious manner that Nagell's result holds when  $s = r - 1$ , although his procedure did not supply a proof of formula (0) in this case. This deficiency was then removed by the present author by different methods in two papers [7], [8], in the latter of which he got the asymptotic formula

$$N(x) = A(f)x + O\left(x \log^{-A_1/\log \log \log x} x\right)$$

containing a remainder term that was subsequently improved in his tract ([10], subsequently referred to as I for convenience) to

$$O\left(x \log^{-(r-1)/(r+1)} x\right).$$

Before continuing the description of progress on the main theme, we should detour by mentioning that this work sparked an interest in related problems in which the integer argument  $n$  is replaced by a prime argument  $p$ , it being appropriate here to denote the consequential counterpart of  $N(x)$  by  $P(x)$ . Though most of the earlier work in which  $s \geq r$  could be fairly easily adopted to meet the needs of the new situation, the methods of Erdős and ourselves failed to yield the requisite results in the more important case  $s = r - 1$ . We ([11], [12]) therefore initiated a complicated analysis that led to the sought after conclusions for some polynomials of larger degrees  $r$  and, amongst other, for *normal* polynomials with  $r \geq 55$ .

But the situation was transformed in 1976 by an important paper by Nair [17], who shewed that the subject was amenable to a substantial modification of the ideas used by Halberstam and Roth in their investigations of gaps between power-free numbers. As a result, previous restrictions on  $s$  were shattered for the larger values of  $r$  whether or not the argument in  $f(n)$  were limited to the primes. For instance, while not yielding even the earlier results for  $s = r - 1$  when  $r \leq 6$ , his method as refined in the two following papers (Nair [18] and Huxley and Nair [15]) gave the admissible values  $s = r - 1$  for  $r \geq 6$ ,  $s = r - 2$  for  $r \geq 15$ ,  $s = r - 3$  for  $r \geq 27$ , etc., for general arguments  $n$ , a slight adjustment in the first two ranges to  $r \geq 7$  and  $r \geq 16$  being needed for prime arguments. Thus there is no limit to the deficiency  $r - s$  so long as  $r$  be large enough.

There — save for the establishment of the connection with the *abc* Conjecture — the matter has rested until the present even though the state of knowledge represented by these discoveries is far from complete. For instance, we know no more about the special binomial  $n^4 + 2$  than Erdős did over fifty years ago when he commented that it was still undecided whether it were infinitely often square-free. Our objective here, therefore, is to advance further — in partial emulation of Atkinson and Lord Cherwell — by treating the binomials  $n^r + 2$  of even degree with the aid of hypotheses milder than the *abc* Conjecture that are of a type familiar in analytical number theory. The first hypothesis  $R^\dagger$  - similar to hypotheses adopted in our papers [9] and [13] - concerns the size of trigonometrical sums taken over short ranges

of summation, while the second hypotheses  $P$  and  $P_1$ , which were developed in our paper [14] (designated by  $I_1$  for ease of reference), relate to the distribution of the solutions of the Pellian equation and are consistent with numerical evidence about small class numbers of binary quadratic forms with positive determinant. For these binomials, we then obtain significant improvements on previous work on the assumption of either one or two of these hypothesis; in particular, on the strength of Hypothesis  $R^\dagger$  alone or both this and Hypothesis  $P_1$  we derive the sufficient conditions, respectively,

$$s > \frac{3}{4}(r-1), \quad s > \frac{3}{4}(r-2) \quad \text{and } s \text{ even,}$$

for the validity of (0) and its analogue for prime arguments, thus conditionally settling Erdős's question about the biquadratic  $n^4+2$ . The effect of these deductions is demonstrated by means of a table that makes clear the measure of the conditional strengthening of the Nair-Huxley results.

Since our methods are fully explained in the coming exposition, it only remains for us to remark that in principle our findings can be extended to any primitive irreducible binomial of even degree.

## 2. Notation and conventions

In what follows  $f(n)$  denotes the binomial  $n^r+2$  of even degree  $r$  that usually exceeds 2, the sum  $N(x)$  related to this binomial being that which appears in equation (0) above. The letters  $q$  and  $p$  denote positive prime numbers; the former appertains to primes whose  $sth$  powers are involved in a sieving process leading to  $sth$  power-free numbers, while the latter appear in  $f(n)$  when its argument is restricted to be a prime.

The letter  $x$  denotes a number to be regarded as tending to infinity, all stated relations being valid for sufficiently large  $x$ ;  $\epsilon$  is an arbitrarily small positive number that is not necessarily the same on all occasions; the constants implied by the  $O$ -notation usually depend at most on  $\epsilon$  and  $r$ , except in the statement of Hypothesis  $R^\dagger$ . The functions  $d_r(m)$ ,  $\sigma_\alpha(m)$ , and  $\omega(m)$  are, respectively, the number of ways of expressing  $m$  as a product of  $r$  factors, the sum of the  $\alpha$ th powers of the divisors of  $m$ , and the number of distinct prime factors of  $m$ .

For any integer denoted by  $h$ , say, the symbol  $\bar{h}$  usually occurs in the numerator of a fraction and is then the multiplicative inverse of  $h$  modulo the denominator – coprime to  $h$  – of this fraction.

### 3. Decomposition of sum and the estimation of its easier components

In our exposition we limit attention to the case

$$s \leq r - 1, \quad (1)$$

which is the only one where we do not have satisfactory knowledge of at least one of  $N(x)$  and its analogue  $P(x)$  involving prime arguments, because the decompositions needed here are inappropriate for larger values of  $s$ . To treat  $N(x)$  by the simple asymptotic sieve (see chapter 1 of our tract I for a description of what we mean by this) we require a notation for various sums that count the number of positive integers  $n$  not exceeding  $x$  for which the irreducible polynomial  $f(n) = n^r + 2$  of even degree

$$r = 2r' \geq 4 \quad (2)$$

has certain ascribed properties. First  $N'(x)$  appertains to the property that  $f(n)$  be not divisible by the  $s$ th power  $q^s$  of any prime  $q$  not exceeding

$$\xi_1 = \frac{1}{6} \log x, \quad (3)$$

while  $M(x; \zeta_1, \zeta_2)$  appertains to the property that  $f(n)$  be divisible by some  $s$ th power  $q^s$  of a prime  $q$  satisfying  $\zeta_1 < q \leq \zeta_2$ , where for brevity we write  $M(x, \zeta) = M\left(x; \zeta, (x^r + 2)^{\frac{1}{s}}\right) = M(x; \zeta, \infty)$ . Also  $N_l(x)$  is to appertain to the property that  $f(n)$  be divisible by an integer  $l$  that is usually the  $s$ th power of a prime. Then obviously

$$N(x) \leq N'(x) \text{ and } N(x) \geq N'(x) - M(x, \xi_1),$$

whence, on setting

$$\xi_2 = x / \log x, \quad \xi_3 = x^{(r-1)/s} \log^{3/s} x, \quad (4)$$

we gain the equation

$$\begin{aligned} N(x) &= N'(x) + O\{M(x, \xi_1)\} \\ &= N'(x) + O\{M(x; \xi_1, \xi_2)\} + O\{M(x; \xi_2, \xi_3)\} + O\{M(x, \xi_3)\} \end{aligned} \quad (5)$$

whose constituents we proceed to examine on the additional assumption that

$$s > \frac{3}{4}(r - 1) \quad (6)$$

so that

$$\xi_3 < x^{\frac{4}{3}-\eta} \quad (7)$$

for a suitably small positive value of  $\eta$ . But, before we go on, we should remark that the more natural value  $x$  for  $\xi_2$  has been shunned because we shall wish to consider at the end the applicability of the method to the case where  $n$  is replaced by a prime argument  $p$ .

Being handled as in previous work (see, for example, I), the sums  $N'(x)$  and  $M(x; \xi_1, \xi_2)$  are dismissed with the help of the equation

$$\begin{aligned} N_l(x) &= \sum_{\substack{n \leq x \\ n^r + 2 \equiv 0, \pmod l}} 1 = \sum_{\substack{0 < \nu \leq l \\ \nu^r + 2 \equiv 0, \pmod l}} \sum_{\substack{n \leq x \\ n \equiv \nu, \pmod l}} 1 = \sum_{\substack{0 < \nu \leq l \\ \nu^2 + 2 \equiv 0, \pmod l}} \left( \frac{x}{l} + O(1) \right), \\ &= \frac{x\rho(l)}{l} + O\{\rho(l)\}, \end{aligned} \quad (8)$$

in which

$$\rho(l) = O\left(r^{\omega(l)}\right) \quad (9)$$

is the number of incongruent roots of the binomial congruence  $\nu^r + 2 \equiv 0, \pmod l$ . Then, letting  $l'$  denote a square-free product (possibly empty) of primes  $q$  up to  $\xi_1$  that does not exceed

$$\prod_{q \leq \xi_1} q = e^{\theta(\xi_1)} = O(e^{2\xi_1}) = O\left(x^{\frac{1}{3}}\right)$$

by (3), we have

$$\begin{aligned} N'(x) &= x \sum_{l'} \frac{\mu(l')\rho(l'^s)}{l'^s} + O\left(\sum_{l' \leq x^{\frac{1}{3}}} r^{\omega(l')}\right) \\ &= x \prod_{q \leq \xi_1} \left(1 - \frac{\rho(q^s)}{q^s}\right) + O(x^{\frac{1}{3}} \log^{r-1} x) \\ &= x \left\{1 + O\left(\frac{1}{\xi_1^{s-1}}\right)\right\} \prod_q \left(1 - \frac{\rho(q^s)}{q}\right) + O(x^{\frac{1}{3}} \log^{r-1} x) \\ &= x \prod_q \left(1 - \frac{\rho(q^s)}{q^s}\right) + O\left(\frac{x}{\log x}\right). \end{aligned} \quad (10)$$

Secondly

$$\begin{aligned} M(x; \xi_1, \xi_2) &\leq \sum_{\xi_1 < q \leq \xi_2} N_{q^s}(x) = \sum_{\xi_1 < q \leq \xi_2} \left(\frac{x\rho(q^s)}{q^s} + O(1)\right) \\ &= O\left(x \sum_{q > \xi_1} \frac{1}{q^s}\right) + O\{\pi(\xi_2)\} \\ &= O\left(\frac{x}{\xi_1^{s-1} \log \xi_1}\right) + O\left(\frac{\xi_2}{\log \xi_2}\right) = O\left(\frac{x}{\log x (\log \log x)}\right) \end{aligned} \quad (11)$$

by (4). Actually, the remainder terms in the last two equations may be improved in the circumstances currently prevailing because (6) implies that  $s > 2$ ; such an improvement,

however, would not substantially better the asymptotic formulae we first derive, while we wish later to consider the case  $s = 2$  when (6) is relaxed.

The sum  $M(x, \xi_3)$  could also be summarily settled because it resembles the sum  $P_2(x)$  in I that was treated by a large sieve method in similar circumstances. But the special nature of the polynomials  $f(n)$  we have in mind means it is more appropriate to employ properties of Diophantine equations that can partially usher in some of our later developments. We therefore end the Section by merely changing  $M(x, \xi_3)$  into a form to which our present approach will be applicable.

The conditions of summation in the sum

$$\sum_{\substack{q^s m = n^r + 2 \\ n \leq x; q > \xi_3}} 1$$

that is not less than  $M(x, \xi_3)$  imply that

$$m < (x^r + 2)/\xi_3^s < 2x^r/(x^{r-1} \log^3 x) = 2x/\log^3 x = x_1, \quad \text{say}, \quad (12)$$

on account of (4). Hence

$$M(x, \xi_3) \leq \sum_{m \leq x_1} \sum_{\substack{q^s m = n^r + 2 \\ 2 \nmid q}} 1 = \sum_{m \leq x_1} \Upsilon(m), \quad \text{say}, \quad (13)$$

the inner sum in which will be the subject of the next Section.

#### 4. The sums $\Upsilon(m)$ and $M(x, \xi_3)$

All cases to be considered can be treated by a method involving simple properties of algebraic number fields and known properties of Diophantine equations. Yet an especially easy procedure involving the Pellian equation is available when  $s$  is an even integer  $2s'$  and we therefore begin by giving an account of this, especially as we need to enlarge on the analysis when we come to make our more daring speculations.

Temporarily replacing the symbol  $m$  by  $D$  to avail ourselves of notations traditionally used for equations of the Pellian type, we observe that for even  $s$  the number  $\Upsilon(D)$  defined in (13) is bounded by the number of solutions  $T_1, U_1$  in positive integers of the equation

$$T_1^2 - DU_1^2 = -2 \quad (14)$$

for which  $T_1 \leq x^{r'}$ , where  $r'$  is defined by (2). If we pass by the case where  $D$  is a perfect square and where therefore  $\Upsilon(D) = 0$ , we have

$$(T_1 + \sqrt{DU_1})^2 = T_1^2 + DU_1^2 + 2\sqrt{DT_1U_1} = 2\{(T_1^2 + 1) + \sqrt{DT_1U_1}\}$$

with the consequence that  $T' = T_1^2 + 1, U' = T_1U_1$  furnishes a solution  $\eta'_D = T' + \sqrt{DU'}$  of the Pellian equation

$$T'^2 - DU'^2 = 1 \quad (15)$$

that is subject to the inequality  $\eta'_D < 2T' \leq 2x^r + 2$ . But, if  $\eta_D$  be the fundamental solution of (15), then

$$\eta'_D = \eta_D^w$$

where  $w = O(\log x)$ . Thus  $\Upsilon(D) = O(\log x)$  with the implication that

$$M(x, \xi_3) = O\left(\log x \sum_{m \leq x_1} 1\right) = O(x_1 \log x_1) = O\left(\frac{x}{\log^2 x}\right) \quad (16)$$

by (12).

In the general case where no restriction is placed on the parity of  $s$ , the sum  $\Upsilon(m)$  does not exceed the number of solutions of

$$q^s m = N^2 + 2$$

in integers  $N$  and *odd* primes  $q$ , the totality of which we shall see to be finite. Factorizing  $N^2 + 2$  as  $(N + \sqrt{-2})(N - \sqrt{-2})$ , we interpret the equation through the field  $\mathbb{Q}(\sqrt{-2})$ , which has class number one and discriminant 8. First the odd rational prime  $q$  is not a prime in  $\mathbb{Q}(\sqrt{-2})$  because otherwise it would divide one of  $N \pm \sqrt{-2}$  and hence both and thus  $2\sqrt{-2}$ , which situation is impossible. Therefore, writing  $q$  as a product  $q_1 q_2 = (\rho + \sigma\sqrt{-2})(\rho - \sigma\sqrt{-2})$  of conjugate primes in  $\mathbb{Q}(\sqrt{-2})$ , we see that  $(\rho + \sigma\sqrt{-2})^s$  divides one of the factors  $N + \sqrt{-2}$ , say, of  $N^2 + 2$  because  $(N + \sqrt{-2}, N - \sqrt{-2})$  is a divisor of  $2\sqrt{-2}$ . Hence

$$N + \sqrt{-2} = (\rho + \sigma\sqrt{-2})^s (\lambda + \mu\sqrt{-2}), \quad (17)$$

whence

$$m = \lambda^2 + 2\mu^2 \quad \text{and} \quad (\lambda, \mu) = 1. \quad (18)$$

Equating coefficients of  $\sqrt{-2}$  in (17) and thereby revealing the binary form

$$\begin{aligned} \psi_{\lambda, \mu}(\rho, \sigma) &= \frac{\lambda}{2\sqrt{-2}} \{(\rho + \sigma\sqrt{-2})^s - (\rho - \sigma\sqrt{-2})^s\} + \frac{\mu}{2} \{(\rho + \sigma\sqrt{-2})^s + (\rho - \sigma\sqrt{-2})^s\} \\ &= \frac{1}{2} \left( \mu - \frac{\lambda}{\sqrt{-2}} \right) (\rho - \sigma\sqrt{-2})^s + \frac{1}{2} \left( \mu + \frac{\lambda}{\sqrt{-2}} \right) (\rho + \sigma\sqrt{-2})^s \end{aligned}$$

with indeterminates  $\rho, \sigma$ , we deduce that

$$\psi_{\lambda, \mu}(\rho, \sigma) = 1. \quad (19)$$

Then, abstaining from any reference to the irreducibility or reducibility of  $\psi_{\lambda, \mu}(\rho, \sigma)$  for convenience, we bound the number of solutions of (19) by first noting that the discriminant of  $\psi_{\lambda, \mu}(\rho, \sigma)$  can be shewn to be

$$\pm \frac{s^{2(s-1)} m^{s-1}}{(2\sqrt{-2})^{2(s-1)}} \neq 0$$

by means of the transformation  $u = \rho - \sqrt{-2}\sigma, v = \rho + \sqrt{-2}\sigma$ . Being now ready to appeal to a theorem of Bombieri and Schmidt on the Thue equation [2], we initiate the last part of the estimation by stating



LEMMA 1. *If  $F(u, v)$  be a binary form of degree  $s \geq 3$  with integral coefficients and non-zero discriminant, then the indeterminate equation*

$$F(u, v) = 1$$

*has  $O(1)$  solutions.*

Being the Bombieri-Schmidt theorem when  $F(u, v)$  is irreducible, the result is true in the opposite case because then there are two *distinct* irreducible factors  $F_1(u, v), F_2(u, v)$  of  $F(u, v)$  that satisfy

$$F_1(u, v) - 1 = 0, F_2(u, v) - 1 = 0,$$

the solutions of which belong to a zero dimensional locus of cardinality  $O(1)$  by Bezout's theorem.

In conclusion, as  $q = \rho^2 + \sigma^2$ , the contribution to  $\Upsilon(m)$  due to a given primitive representation of  $m$  in (18) as  $\lambda^2 + 2\mu^2$  is  $O(1)$  and we infer that

$$\Upsilon(m) = O(2^{\omega(m)}).$$

Thus

$$M(x, \xi_3) = O\left(\sum_{m \leq x_1} 2^{\omega(m)}\right) = O(x_1 \log x_1) = O\left(\frac{x}{\log^2 x}\right), \quad (20)$$

which estimate includes the result in (16) when  $s$  is even.

## 5. Estimation of $M(x; \xi_2, \xi_3)$ - initial transformations and other preparations.

The sum  $M(x; \xi_2, \xi_3)$  is the hardest obstacle confronting us and so awkward does it become that we shall need in due course to adopt a conjecture about exponential sums over short ranges of summation. For simplicity we shall only treat the case where  $s$  is an even number  $2s'$ , although what is done is applicable with minor modifications to the other case until further conjectures about the Pellian equation are brought in later.

First, as at the beginning of (11),

$$M(x; \xi_2, \xi_3) \leq \sum_{\xi_2 < q \leq \xi_3} N_{q^s}(x), \quad (21)$$

the summand in which is only positive when there are solutions to the congruence

$$\Omega^2 \equiv -2, \quad \text{mod } q^s, \quad (22)$$

implied by  $\nu^{2r'} \equiv -2, \quad \text{mod } q^s$ , or equivalently, when  $\omega^2 \equiv -2, \quad \text{mod } q$ , is soluble. Since the class number of binary quadratic forms of determinant  $-2$  is one, the meeting of this condition is tantamount to the (unique) primitive representation of the prime  $q$  by the form  $X^2 + 2Y^2$  with *positive* integers  $X = X_q, Y = Y_q$ , where necessarily  $X_q$  is odd. Through these representations of the eligible values of  $q$  we then express the right side of (21) as

$$\sum_{\substack{\xi_2 < q \leq \xi_3 \\ X_q \leq x^{\frac{1}{3}}}} N_{q^s}(x) + \sum_{\substack{\xi_2 < q \leq \xi_3 \\ X_q > x^{\frac{1}{3}}}} N_{q^s}(x) = M_1(x; \xi_2, \xi_3) + M_2(x; \xi_2, \xi_3), \quad \text{say,}$$

to obtain

$$M(x; \xi_2, \xi_3) \leq M_1(x; \xi_2, \xi_3) + M_2(x; \xi_2, \xi_3).$$

To estimate  $M_1(x; \xi_1, \xi_2)$  let us observe here that (7) and the condition  $q \leq \xi$  imply that  $Y_q \leq (\frac{1}{2}\xi_3)^{\frac{1}{2}} < x^{\frac{2}{3}-\frac{1}{2}\eta}$  with the inference that the number of  $q$  over which the sum is taken is

$$O\left(x^{\frac{1}{3}}x^{\frac{2}{3}-\frac{1}{2}\eta}\right) = O\left(x^{1-\frac{1}{2}\eta}\right).$$

Therefore, inserting (8) in an analogue of (11), we get

$$\begin{aligned} M_1(x; \xi_2, \xi_3) &= O\left(x \sum_{q>\xi_2} \frac{1}{q^s}\right) + O\left(x^{1-\frac{1}{2}\eta}\right) \\ &= O\left(x^{2-s} \log^{s-1} x\right) + O\left(x^{1-\frac{1}{2}\eta}\right) = O\left(\frac{x}{\log^2 x}\right) \end{aligned}$$

with the conclusion that

$$M(x; \xi_2, \xi_3) \leq M_2(x; \xi_2, \xi_3) + O\left(\frac{x}{\log^2 x}\right). \quad (23)$$

The method to be now introduced has been simplified by our having hived off the sum  $M_2(x; \xi_2, \xi_3)$  from  $M(x; \xi_2, \xi_3)$  because tiresome partial summations can then be eliminated from the calculations surrounding exponential sums. Its genesis becomes palpable through making more explicit than hitherto the replacement of the polynomial  $n^r + 2$  by  $N^2 + 2$  with the consequential definition of  $\mathcal{N}_{q^s}(x)$  as the number of positive integers  $N$  up to  $x^{r'}$  for which  $N^2 + 1$  is divisible by  $q^s$ . This then leads us to the inequalities

$$N_{q^s}(x) \leq \mathcal{N}_{q^s}(x) = \sum_{\substack{\Omega^2 \equiv -2, \pmod{q^s} \\ 0 < \Omega \leq x^{r'}}} 1 \quad (24)$$

and

$$M_2(x; \xi_2, \xi_3) \leq \sum_{\substack{\xi_2 < q \leq \xi_3 \\ X_q > x^{\frac{1}{3}}}} \mathcal{N}_{q^s}(x), \quad (25)$$

in the former of which no two distinct congruent values of  $\Omega, \pmod{q^s}$ , can occur in the summation since here

$$q^s > (x/\log x)^s > x^{\frac{3}{4}(r-1)} > 2x^{\frac{1}{2}r} \quad (26)$$

when  $r \geq 4$ . Yet, if  $\Omega$  be the least positive root of (22) for a given prime  $q = X_q^2 + 2Y_q^2$ , then either  $\Omega$  or  $-\Omega$  will be the least absolute root  $\Omega_1, \pmod{q^s}$ , appertaining to a given primitive representation of  $q^s = (X_q^2 + 2Y_q^2)^s$  as  $X^2 + 2Y^2$ . Thus (24) may be rephrased as

$$\mathcal{N}_{q^s}(x) = \sum_{|\Omega_1| \leq x^{r'}} 1, \quad (27)$$

where  $\Omega_1$  will shortly be explicitly defined in terms of the representation of  $q^s$  by  $X^2 + 2Y^2$  to be unfolded. From this we must proceed to yet more majorizations before the method of exponential sums is brought into play.

In the next majorization we must lean a little more heavily on the theory of binary quadratic forms than before. If in fact any *odd* positive integer  $l$  have the primitive representation  $X_l^2 + 2Y_l^2$ , then not only is the pair of numbers

$$X'_l = G_1(X_l, Y_l) = \frac{1}{2}\{(X_l + \sqrt{-2}Y_l)^s + (X_l - \sqrt{-2}Y_l)^s\}, \quad (28)$$

$$Y'_l = G_2(X_l, Y_l) = \frac{1}{2\sqrt{-2}}\{(X_l + \sqrt{-2}Y_l)^s - (X_l - \sqrt{-2}Y_l)^s\} \quad (29)$$

an obvious solution of  $l^s = X^2 + 2Y^2$  but it is also a primitive one. Avoiding any appeal to even elementary algebraic number theory, we most easily demonstrate the latter point by noting first that the resultant of  $G_1(X, Y)$  and  $G_2(X, Y)$  is  $(-2\sqrt{-2})^{s^2}$  times the resultant of  $\frac{1}{2}(u^s + v^s)$  and  $\frac{1}{2\sqrt{-2}}(u^s - v^s)$ , which, being a combinant, is  $(-2\sqrt{-2})^{-s}$  times the resultant 1 of  $u^s$  and  $v^s$ . This means there are integral binary forms  $h_1(X, Y), k_1(X, Y), h_2(X, Y), k_2(X, Y)$  with the properties that

$$h_1(X_l, Y_l)X'_l + k_1(X_l, Y_l)Y'_l = (-1)^{\frac{1}{2}(s^2-s)}2^{\frac{1}{2}(s^2-s)}X_l^{2s-1} \quad (30)$$

and

$$h_2(X_l, Y_l)X'_l + k_2(X_l, Y_l)Y'_l = (-1)^{\frac{1}{2}(s^2-s)}2^{\frac{1}{2}(s^2-s)}Y_l^{2s-1},$$

which confirm the assertion because  $(X_l, Y_l) = 1$  and  $X'_l$  is odd. Then, taking  $q$  and the accompanying positive numbers  $X_q, Y_q$  as before, the root  $\Omega_1$  presented in (27) is to be the one (of least absolute value) appertaining to the primitive representation of  $q^s$  provided by  $X'_q, Y'_q$  in (28) and (29).

Next, we spread the definition of  $\Omega_1$  to cover the case of general *odd* numbers  $l$  that are primitively expressible as  $X_l^2 + 2Y_l^2$  with positive  $X_l, Y_l$ . For each such representation, the equations (28) and (29) provide a primitive representation of  $l^s$  to which will appertain a root  $\Omega = \Omega_1(X_l, Y_l)$  — reduced to its least absolute value,  $\pmod{l^s}$ , — of  $\Omega^2 \equiv -2, \pmod{l^s}$ , moreover, different representation of  $l$  give rise to different ones of  $l^s$ , although for composite  $l$  this is a fact we may ignore and therefore need not substantiate. Thus, effecting the next majorization by not limiting the summand in (25) to prime values  $q$ , we obtain

$$M_2(x; \xi_2, \xi_3) \leq \sum_{\substack{\xi_2 < l \leq \xi_3 \\ 2 \nmid l}} \sum_{\substack{X_l^2 + 2Y_l^2 = l \\ X_l > x^{\frac{1}{3}}; Y_l > 0 \\ (X_l, Y_l) = 1}} \chi(X_l, Y_l), \quad (31)$$

where  $\chi(X_l, Y_l)$  is 1 or 0 according as the least absolute value of the above root  $\Omega_1(X_l, Y_l)$  is not greater than or greater than  $x^{r'}$ .

We proceed to the final majorization through the action of

LEMMA 2. For any positive integer  $Q$ , the sum

$$t_Q(\theta) = \frac{1}{Q} \sum_{0 \leq |j| \leq Q} \left(1 - \frac{|j|}{Q}\right) e^{2\pi i j \theta}$$

is equal to

$$\frac{\sin^2 \pi Q \theta}{Q^2 \sin^2 \pi \theta}$$

with an obvious interpretation when  $\theta$  is an integer.

Since, for  $Q|\theta| \leq \frac{1}{2}$ ,

$$t_Q(\theta) \geq \frac{4}{\pi^2} \frac{\pi^2 Q^2 \theta^2}{Q^2 \pi^2 \theta^2} = \frac{4}{\pi^2}$$

and since the non-vanishing of  $\chi(X_l, Y_l)$  in (31) is to imply that

$$\frac{|\Omega_1(X_l, Y_l)|}{l^s} \leq \frac{x^{r'}}{(x/\log x)^s} < x^{\frac{1}{2}r - [\frac{3}{4}(r-1)] - 1 + \epsilon} < \frac{1}{2} \frac{x}{\xi_3 \log^2 x} \quad (32)$$

by (6) and (7), the choice

$$Q = [\xi_3 \log^2 x/x] \quad (33)$$

yields the inequality

$$\chi(X_l, Y_l) \leq \frac{\pi^2}{4} t_Q \left( \frac{\Omega_1}{l^s} \right),$$

in which no longer need we assume that  $\Omega_1$  is the least absolute residue in the congruence class it represents. Then, if we place this in (31) and *only then* weaken the conditions of summation, we deduce that

$$M_2(x; \xi_2, \xi_3) \leq \frac{\pi^2}{4} \sum_{\substack{x^{\frac{1}{3}} < X \leq \xi_3^{\frac{1}{2}} \\ 0 < Y \leq \xi_3^{\frac{1}{2}}; (X, 2Y)=1}} t_Q \left( \frac{\Omega_1(X, Y)}{(X^2 + 2Y^2)^s} \right),$$

whence, having drawn out the central term  $1/Q$  from  $t_Q(\theta)$  to leave

$$t_Q^*(\theta) = \frac{1}{Q} \sum_{0 < |j| \leq Q} \left(1 - \frac{|j|}{Q}\right) e^{2\pi i j \theta}, \quad (34)$$

we arrive at the inequality

$$\begin{aligned} M_2(x; \xi_2, \xi_3) &\leq \frac{\pi^2}{4Q} \sum_{\substack{x^{\frac{1}{3}} < X \leq \xi_3^{\frac{1}{2}} \\ 0 < Y \leq \xi_3^{\frac{1}{2}}; (X, 2Y)=1}} t_Q^* \left( \frac{\Omega_1(x, Y)}{(X^2 + 2Y^2)^s} \right) + \frac{\pi^2}{4Q} \sum_{0 < X, Y \leq \xi_3^{\frac{1}{2}}} 1 \\ &\leq \frac{\pi^2}{4Q} \sum_{\substack{x^{\frac{1}{3}} < X \leq \xi_3^{\frac{1}{2}} \\ 0 < Y \leq \xi_3^{\frac{1}{2}}; (X, 2Y)=1}} t_Q^* \left( \frac{\Omega_1(X, Y)}{(X^2 + 2Y^2)^s} \right) + O \left( \frac{\xi_3}{Q} \right) \end{aligned}$$

$$= R(x, \xi_3) + O\left(\frac{x}{\log^2 x}\right), \text{ say,} \quad (35)$$

because of (33). With (23), this implies that

$$M(x; \xi_2, \xi_3) \leq R(x, \xi_3) + O\left(\frac{x}{\log^2 x}\right). \quad (36)$$

Finally, by (34)

$$R(x, \xi_3) = \frac{\pi^2}{4Q} \sum_{0 < |j| \leq Q} \left(1 - \frac{|j|}{Q}\right) S(x, j),$$

where  $S(x, j)$  is the exponential sum

$$\sum_{\substack{x^{\frac{1}{3}} < X \leq \xi_3^{\frac{1}{3}} \\ 0 < Y \leq \xi_3^{\frac{1}{2}}; (X, 2Y)=1}} e^{2\pi i j \Omega_1(X, Y)/(X^2 + 2Y^2)^s}, \quad (37)$$

and therefore

$$R(x, \xi_3) = O\left(\frac{1}{Q} \sum_{0 < j \leq Q} |S(x, j)|\right). \quad (38)$$

This ends the first stage of the treatment of  $M(x; \xi_2, \xi_3)$ . Yet, before we go on to estimate  $S(x, j)$ , we should comment on the ideas behind what has just been done. First, so small is the expected size of  $M_2(x; \xi_2, \xi_3)$  that the substitution of  $\mathcal{N}_{q^s}(x)$  for  $N_{q^s}(x)$  is not foreseen to vitiate the calculations, while still being probably small the resulting sum can be safely augmented by using the bound (32) for  $\Omega_1/l^s$ . This means we can use the selected value of  $Q$ , which is optimum in regard to the number of terms in  $t_Q(\theta)$  but which does not compromise the estimations stemming from the formal middle ‘main term’ within it. Moreover, being only in need of upper bounds, we find it suffices to use the easy Lemma 2 in place of more complicated formulae about trigonometrical approximations to the function  $\frac{1}{2} + [t] - t$ .

## 6. The exponential sums $S(x, j)$ and the completion of the estimation of $M(x; \xi_2, \xi_3)$

To lead into the estimation of the sums  $S(x, j)$  we state two lemmata. The first, which is familiar and elementary, is

**LEMMA 3.** *Let  $u, v$  be coprime non-zero integers and let  $\bar{u}, \bar{v}$  be, respectively, the multiplicative inverses, modulus  $v, u$ , of  $u, v$ . Then*

$$u\bar{u} + v\bar{v} \equiv 1, \quad \text{mod } uv.$$

The second enunciates an identity associated with partial sums of the binomial expansion of  $(1 - x)^{-s}$ ; somewhat surprisingly, no reference to it could be found in classical treatises on algebra. Although, strictly speaking, we could dispense with it, this result serves to make explicit the former equation (30) in an illuminating and helpful way.

LEMMA 4. *Let*

$$\psi(x) = 1 + C_1x + \dots + C_{s-1}x^{s-1}$$

*be the sth partial sum of the development of  $(1-x)^{-s}$  as a (formal) infinite series. Then there is the identity*

$$(1-x)^s\psi(x) + x^s\psi(1-x) = 1.$$

Since

$$(1-x)^s \sum_{i=0}^{\infty} C_i x^i = 1,$$

it is obvious that a polynomial  $\phi_1(x)$  of degree  $s-1$  has the property that  $(1-x)^s\phi_1(x)$  is of the form  $\phi_2(x) = 1 - x^s(b_0 + \dots + b_{s-1}x^{s-1}) = 1 - x^s\phi_3(x)$  if and only if it be  $\psi(x)$ . Then, setting  $x = 1 - u$  and applying the principle again, we have also that

$$(1-u)^s\phi_3(1-u) = 1 - u^r\psi(1-u),$$

whence  $\phi_3(1-u) = \psi(u)$  and  $\phi_3(x) = \psi(1-x)$  in substantiation of the lemma.

We use the lemma to approach the roots  $\Omega_1$  appertaining to the representations given earlier of *odd* numbers of the type  $l^s$ . First, having been reminded of the definitions of  $G_1(X, Y)$  and  $G_2(X, Y)$  in (28) and (29), we express the identity as

$$\frac{1}{2}\{x^s + (1-x)^s\}\{\psi(1-x) + \psi(x)\} + \frac{1}{2}\{x^s - (1-x)^s\}\{\psi(1-x) - \psi(x)\} = 1$$

and obtain

$$\begin{aligned} & \frac{1}{2^s X^s} G_1(X, Y) \left\{ \psi\left(\frac{1}{2} - \sqrt{-2}\frac{Y}{2X}\right) + \psi\left(\frac{1}{2} + \sqrt{-2}\frac{Y}{2X}\right) \right\} \\ & + \frac{\sqrt{-2}}{2^s X^s} G_2(X, Y) \left\{ \psi\left(\frac{1}{2} - \sqrt{-2}\frac{Y}{2X}\right) - \psi\left(\frac{1}{2} + \sqrt{-2}\frac{Y}{2X}\right) \right\} = 1 \end{aligned}$$

on setting  $x = \frac{1}{2} + \frac{1}{2}\sqrt{-2}(Y/X)$  so that  $1-x = \frac{1}{2} - \frac{1}{2}\sqrt{-2}(Y/X)$ . Since here

$$\begin{aligned} & \psi\left(\frac{1}{2} - \sqrt{-2}\frac{Y}{2X}\right) + \psi\left(\frac{1}{2} + \sqrt{-2}\frac{Y}{2X}\right) \\ & = \frac{1}{2^{s-2}X^{s-1}} \sum_{0 \leq i \leq s-1} 2^{s-1-i} C_i X^{s-1-i} \frac{1}{2} \left\{ (X + \sqrt{-2}Y)^i + (X - \sqrt{-2}Y)^i \right\} \\ & = \frac{1}{2^{s-2}X^{s-1}} \Psi_1(X, Y), \quad \text{say,} \end{aligned}$$

and

$$\begin{aligned} & \psi\left(\frac{1}{2} - \sqrt{-2}\frac{Y}{2X}\right) - \psi\left(\frac{1}{2} + \sqrt{-2}\frac{Y}{2X}\right) \\ & = -\frac{\sqrt{-2}}{2^{s-2}X^{s-1}} \sum_{0 < i \leq s-1} 2^{s-1-i} C_i X^{s-1-i} \frac{1}{2\sqrt{-2}} \left\{ (X + \sqrt{-2}Y)^i - (X - \sqrt{-2}Y)^i \right\} \end{aligned}$$

$$= -\frac{\sqrt{-2}}{2^{s-2}X^{s-1}}\Psi_2(X, Y), \text{ say,} \quad (39)$$

there then emerges the identity

$$G_1(X, Y)\Psi_1(X, Y) + 2G_2(X, Y)\Psi_2(X, Y) = 2^{2s-2}X^{2s-1} \quad (40)$$

that contains binary forms  $\Psi_1, \Psi_2$  of degree  $s - 1$  with integral coefficients. We remark in passing that these forms are divisible by 2 because so is

$$C_{s-1} = \binom{2(s-1)}{s-1};$$

however, to take out this multiplier is unhelpful, since there are cases where a higher power of 2 could be removed.

To this point, the exposition has not been affected by the parity of  $s$ . But now, in accordance with the initial comment in §5, we assume that  $s$  is even until the enunciation of the first theorem.

We are now empowered to calculate the root  $\Omega_1(X, Y)$  appertaining to the primitive representation

$$G_1^2(X, Y) + 2G_2^2(X, Y)$$

of  $(X^2 + 2Y^2)^s$ , where the obviously odd numbers  $X$  and  $G_1(X, Y)$  are co-prime because the coefficient of  $Y^s$  in  $G_1(X, Y)$  in (28) is non-zero when  $s$  is even. We recall that the root  $\Omega$ , mod  $t$ , related to the representation of a positive number  $t$  as  $u^2 + 2v^2$  is determined, mod  $t$ , to be  $uu' + 2vv'$  if  $u', v'$  be chosen so that  $uv' - u'v = 1$  (See H.J.S.Smith, Report on the Theory of Numbers[20], Part III, Art 86). Thus

$$\begin{aligned} u\Omega = u^2u' + 2uvv' &= u^2u' + 2v(1 + u'v) \\ &\equiv u'(u^2 + 2v^2) + 2v, \quad \text{mod } (u^2 + 2v^2) \end{aligned}$$

and

$$\frac{\Omega}{u^2 + 2v^2} \equiv \frac{u'}{u} + \frac{2v}{u(u^2 + 2v^2)} \equiv \frac{\bar{v}}{u} + \frac{2v}{u(u^2 + 2v^2)}, \quad \text{mod } 1,$$

in the notation of Lemma 3. In the current situation this implies that the quotient  $\Omega_1(X, Y)/(X^2 + 2Y^2)^s$  appearing in the trigonometrical sum  $S(x, j)$  in (37) is

$$\frac{\overline{G_2(X, Y)}}{\overline{G_1(X, Y)}} + \frac{2G_2(X, Y)}{G_1(X, Y) \{G_1^2(X, Y) + 2G_2^2(X, Y)\}}, \quad \text{mod } 1. \quad (41)$$

Next, since we deduce from (40) that

$$\overline{G_2(X, Y)} \equiv \overline{2^{2s-3}X^{2s-1}}\Psi_2(X, Y), \quad \text{mod } G_1(X, Y),$$

the first term in (41) is

$$\frac{\overline{2^{2s-3}} \overline{X^{2s-1}} \Psi_2(X, Y)}{G_1(X, Y)}, \pmod{1},$$

and therefore

$$-\frac{\overline{G_1(X, Y)} \Psi_2(X, Y)}{2^{2s-3} X^{2s-1}} + \frac{\Psi_2(X, Y)}{2^{2s-3} X^{2s-1} G_1(X, Y)}, \pmod{1},$$

by Lemma 3, from which, moreover, flows the further determination of this term as

$$\begin{aligned} \frac{-\overline{2^{2s-3}} \overline{G_1(X, Y)} \Psi_2(X, Y)}{X^{2s-1}} &= -\frac{\overline{X^{2s-1}} \overline{G_1(X, Y)} \Psi_2(X, Y)}{2^{2s-3}} \\ &+ \frac{\Psi_2(X, Y)}{2^{2s-3} X^{2s-1} G_1(X, Y)}, \pmod{1}. \end{aligned}$$

Hence

$$\begin{aligned} \frac{\Omega_1(X, Y)}{(X^2 + 2Y^2)^s} &\equiv \left\{ -\frac{\overline{2^{2s-3}} \overline{G_1(X, Y)} \Psi_2(X, Y)}{X^{2s-1}} - \frac{\overline{X^{2s-1}} \overline{G_1(X, Y)} \Psi_2(X, Y)}{2^{2s-3}} \right\} \\ &+ \left\{ \frac{2G_2(X, Y)}{G_1(X, Y) \{G_1^2(X, Y) + 2G_2^2(X, Y)\}} + \frac{\Psi_2(X, Y)}{2^{2s-3} X^{2s-1} G_1(X, Y)} \right\}, \pmod{1}, \\ &\equiv \omega_1(X, Y) + \omega_2(X, Y), \pmod{1}, \text{ say,} \end{aligned} \quad (42)$$

in which  $\omega_2(X, Y)$  may be regarded as the correcting term in the approximation  $\omega_1(X, Y)$  to the argument in the sum  $S(x, j)$  defined by (37).

To shew that the substitution of  $\omega_1(X, Y)$  for this argument does not perturb the required estimations, we take the equation

$$e^{2\pi i j \Omega_1(X, Y) / (X^2 + 2Y^2)^s} = e^{2\pi i j \omega_1(X, Y)} + O(|j| \omega_2(X, Y))$$

with the consequential equation

$$\begin{aligned} S(x, j) &= \sum_{\substack{x^{\frac{1}{3}} < X \leq \xi_3^{\frac{1}{2}} \\ 0 < Y \leq \xi_3^{\frac{1}{2}}; (X, 2Y)=1}} e^{2\pi i j \omega_1(X, Y)} + O \left( |j| \sum_{\substack{x^{\frac{1}{3}} < X \leq \xi_3^{\frac{1}{2}} \\ 0 < Y \leq \xi_3^{\frac{1}{2}}}} |\omega_2(X, Y)| \right). \\ &= S^*(x, j) + O\{|j|T(x)\}, \text{ say.} \end{aligned} \quad (43)$$



Since the first element in  $\omega_2(X, Y)$  has magnitude less than

$$\frac{2}{\{G_1^2(X, Y) + 2G_2^2(X, Y)\}^{\frac{1}{2}}} = \frac{2}{(X^2 + 2Y^2)^{\frac{1}{2}s}},$$

its influence on  $T(x)$  is circumscribed by

$$2 \sum_{X^2 + 2Y^2 > x^{\frac{2}{3}}} \frac{1}{(X^2 + 2Y^2)^{\frac{1}{2}s}} = O\left(x^{\frac{2}{3}(1-\frac{1}{2}s)}\right)$$

because of familiar reasoning. Somewhat similarly, the second element in  $\omega_2(x)$  affects  $T(x)$  to the extent of a term that is

$$\begin{aligned} & O\left(\xi^{\frac{1}{2}(s-1)} \sum_{Y \leq \xi_3^{\frac{1}{2}}} \sum_{X > x^{\frac{1}{3}}} \frac{1}{X^{2s-1}}\right) \\ &= O\left(\xi_3^{\frac{1}{2}s} x^{-\frac{2}{3}(s-1)}\right) = O\left(x^{\frac{2}{3}-\frac{1}{2}s\eta}\right) \end{aligned}$$

by (7). Then, adding these estimates, multiplying by  $j$ , and summing over  $j$ , we find that the effect on  $\omega_2(X, Y)$  on  $R(x, \xi_3)$  in (38) extends to a term

$$O\left(Qx^{\frac{2}{3}-\frac{1}{2}s\eta}\right) = O\left(x^{1-\eta-\frac{1}{2}s\eta} \log^2 x\right) = O\left(\frac{x}{\log^2 x}\right) \quad (44)$$

by (33). However, before proceeding to the next estimations, we should repeat what we previously said about how the imposition of the bound  $X > x^{\frac{1}{3}}$  has permitted us to deal with the influence of the factor  $e^{2\pi i j \omega_1(X, Y)}$  without a resort to awkward partial summations.

Consulting (43) and then (42), we have

$$\begin{aligned} |S^*(x, j)| &\leq \sum_{\substack{x^{\frac{1}{3}} < X \leq \xi_3^{\frac{1}{2}} \\ 2 \nmid X}} \left| \sum_{\substack{0 < Y \leq \xi_3^{\frac{1}{2}} \\ (Y, X)=1}} e^{2\pi i j \omega_1(X, Y)} \right| \\ &\leq \sum_{\substack{x^{\frac{1}{3}} < X \leq \xi_3^{\frac{1}{2}} \\ 2 \nmid X}} \sum_{0 < a \leq 2^{2s-3}} \left| \sum_{\substack{0 < Y \leq \xi_3^{\frac{1}{2}}; (Y, X)=1 \\ Y \equiv a, \pmod{2^{2s-3}}} e^{2\pi i j 2^{2s-3} \overline{G_1(X, Y)} \Psi_2(X, Y)} / X^{2s-1} \right| \\ &= \sum_{\substack{x^{\frac{1}{3}} < X \leq \xi_3^{\frac{1}{2}} \\ 2 \nmid X}} \sum_{0 < a \leq 2^{2s-3}} \left| Z_j(a, \xi_3) \right|, \text{ say,} \end{aligned} \quad (45)$$

and then investigate the summand by considering the numerator in the quotient defining  $\omega_1(X, Y), \pmod{X^{2s-1}}$ .

Let the symbol  $b_i$  with or without attached superscript primes denote an integer when  $i$  is even. Then, since  $G_1(X, Y)$  is of the form

$$(-1)^{s'} 2^{s'} Y^s \left\{ 1 + \frac{b_2}{2} \left( \frac{X}{Y} \right)^2 + \dots + \frac{b_s}{2^{s'}} \left( \frac{X}{Y} \right)^s \right\}$$

by (28), its formal reciprocal by the multinomial theorem is of the form

$$\frac{(-1)^{s'}}{2^{s'} Y^s} \left\{ 1 + \sum_{h=1}^{\infty} \frac{b'_{2h}}{2^h} \left( \frac{X}{Y} \right)^{2h} \right\},$$

whence, reducing relations to the modulus  $X^{2s-1}$ , we infer that

$$\overline{G_1(X, Y)} \equiv (-1)^{s'} \overline{2}^{s'} \overline{Y}^s \left( 1 + b'_2 \overline{2}^2 X^2 \overline{Y}^2 + \dots + b'_{2s-2} \overline{2}^{2s-2} X^{2s-2} \overline{Y}^{2s-2} \right), \quad \text{mod } X^{2s-1}.$$

Also, from (39),  $\Psi_2(X, Y)$  is of the form

$$\begin{aligned} & (-1)^{s'-1} 2^{s'} \left( \frac{1}{2} C_{s-1} \right) Y^{s-1} + b''_2 X^2 Y^{s-3} + \dots + b''_{s-2} X^{s-2} Y \\ & \equiv Y^{s-1} \left\{ (-1)^{s'-1} 2^{s'} \left( \frac{1}{2} C_{s-1} \right) + b''_2 X^2 \overline{Y}^2 + \dots + b''_{s-2} X^{s-2} \overline{Y}^{s-2} \right\}, \quad \text{mod } X^{2s-1}, \end{aligned}$$

wherefore the numerator in  $\omega_1(X, Y)$  is of the type

$$-\overline{2}^{2s-3} \left( \frac{1}{2} C_{s-1} \right) \overline{Y} + b'''_2 X^2 \overline{Y}^3 + \dots + b'''_{s-2} X^{s-2} \overline{Y}^{s-1} = g_Y(X), \quad \text{say},$$

when taken, mod  $X^{2s-1}$ .

We are ready to apply the first conjecture, which we state as  
HYPOTHESIS  $R^\dagger$ . *Let*

$$g(u) = a_0 u + \dots + a_t u^t$$

*be a polynomial with integer coefficients of given degree  $t$ ; let also  $\eta_1$  be any given (small) positive constant and let  $K$  be a given positive integer. Then, for  $y^{\eta_1} < k < y$  and  $(k, K) = 1$ , we have*

$$\sum_{\substack{0 < h \leq y \\ (h, k) = 1 \\ h \equiv a, \quad \text{mod } K}} e^{2\pi i g(\overline{h})/k} = O\{(a_0, k)^{\frac{1}{2}} y^{\frac{1}{2} + \epsilon}\},$$

*where the constant implied by the  $O$ -notation depends at most on  $\epsilon, t, \eta_1$ , and  $K$ .*

The upper limit  $\xi_3^{\frac{1}{2}}$  for  $Y$  in the conditions of summation for  $Z_j(a, \xi_3)$  is subject to the inequalities

$$(X^{2s-1})^{\frac{1}{2s-1}} \leq \xi_3^{\frac{1}{2}} \leq (X^{2s-1})^{\frac{4-3\eta_1}{2(2s-1)}} < (X^{2s-1})^{\frac{2}{3}}$$

by (7). Hence, if we adopt Hypothesis  $R^\dagger$ , we have

$$Z_j(a, \xi_3) = O \left\{ (j, X^{2s-1})^{\frac{1}{2}} \xi_3^{\frac{1}{4}+\epsilon} \right\},$$

and the contribution of  $S^*(x, j)$  to  $R(x, \xi_3)$  via (45) and (38) is

$$\begin{aligned} & O \left( \frac{\xi_3^{\frac{1}{4}+\epsilon}}{Q} \sum_{0 < X \leq \xi_3^{\frac{1}{2}}} \sum_{0 < j \leq Q} (X^{2s-1}, j)^{\frac{1}{2}} \right) \\ &= O \left( \xi_3^{\frac{1}{4}+\epsilon} \sum_{0 < X \leq \xi_3^{\frac{1}{2}}} \sigma_{-\frac{1}{2}}(X^{2s-1}) \right) \\ &= O \left( \xi_3^{\frac{1}{4}+\epsilon} \sum_{0 < X \leq \xi_3^{\frac{1}{2}}} \sigma_{-\frac{1}{4}}(X) \right) = O \left( \xi_3^{\frac{3}{4}+\epsilon} \right) \end{aligned} \quad (46)$$

by a well-known estimate for the inner sum in the first line above. Therefore, by (7) and (44),

$$R(x, \xi_3) = O \left( \frac{x}{\log^2 x} \right)$$

and then, by (36),

$$M(x; \xi_2, \xi_3) = O \left( \frac{x}{\log^2 x} \right). \quad (47)$$

This estimate has been obtained on the assumption that  $s$  is even but a modification in the method leads to a like conclusion when  $s$  is odd.

## 7. The first conditional theorems.

Our first result follows immediately from (5), (10), (11), (20), and (47), which after the relaxation of the unnecessary condition (1) yields

**THEOREM 1.** *Suppose that Hypothesis  $R^\dagger$  is true. Then, for  $s > \frac{3}{4}(r-1)$ , the number  $N(x)$  of positive integers up to a large number  $x$  for which the polynomial  $n^r + 2$  of even degree  $r \geq 4$  is sth power-free is equal to*

$$x \prod_q \left( 1 - \frac{\rho(q^s)}{q^s} \right) + O \left( \frac{x}{\log x} \right),$$

where  $\rho(q^s)$  is the number of incongruent solutions of the binomial congruence  $\nu^r + 2 \equiv 0 \pmod{q^s}$ ; in these circumstances, the polynomial  $n^r + 2$  is infinitely often sth power-free.

*The conclusions of the theorem are unconditional when  $s \geq r - 1$ .*

The second conclusion follows from the asymptotic formula because  $\rho(q^s) \leq 2$  for all primes  $q$ . We should then remind the reader that the truth of the theorem for  $r \geq 2$  and  $s \geq 2$  is an old result.

To facilitate comparison with previous work, it is instructive to display for smaller even integers  $r$  the least value of  $s$  for which our result provides a valid asymptotic formula for  $N(x)$ . These are tabulated in the following array:

$r$	4	6	8	10	12	14	16	18	20
$s$	3	4	6	7	9	10	12	13	15
$r - s$	1	2	2	3	3	4	4	5	5

Thus, even for the special form of the polynomial considered, we do not advance from our previous work until  $r$  is 6 or more. But for larger  $r$  our result provides substantially smaller possible values of  $s$  than do the theorems of Nair and Huxley, although it must be remembered that the latter are unconditional. For example, for  $r = 18$  we can assume that the deficiency in  $s$  is compared with  $r$  is 5 whereas in the Nair-Huxley work it is only 2.

The calculations leading to the table reveal that in all cases the hypothetical estimate for the exponential sums is unnecessarily sharp because the values of  $s$  that appear are always tangibly larger than  $\frac{3}{4}(r - 1)$  and because therefore the implied exponent in  $\xi_3 = x^{\frac{(2-1)}{s}} \log^{\frac{3}{s}} x$  in (4) could be safely taken to exceed  $\frac{4}{3} + \epsilon$ . This is a not unimportant point in view of the likelihood that initial progress in the direction of substantiating the conjecture might well be restricted to the production of a bound of the type  $O(y^{1-\delta})$  for the exponential sums taken over short intervals of length  $y$ .

We have already indicated that we have laid out the treatment of  $N(x)$  in such a way that we could proceed with a minimum of fuss to the cognate and harder sum  $P(x)$  in which the argument in  $n^r + 2$  takes prime values  $p$  only. Indeed, following the philosophy of previous authors and ourselves but involving our extra techniques, we let  $P'(x)$  and  $P_l(x)$  be defined as were  $N(x)$  and  $N_l(x)$  except that we now refer to the relevant properties of  $f(n)$  when  $n$  is a prime  $p$ . Then evidently, as a companion of (5), we have

$$P(x) = P'(x) + O\{M(x; \xi_1, \xi_2)\} + O\{M(x; \xi_2, \xi_3)\} + O\{M(x; \xi_3)\}$$

with the same values of  $\xi_1, \xi_2, \xi_3$  as before, whence

$$P(x) = P'(x) + O\left(\frac{x}{\log x(\log \log x)}\right) \quad (48)$$

in virtue of (11), (47), and (20) (note comment after (7)). Also, not only do we have the relatively trivial estimate

$$P_l(x) = O\{N_l(x)\} = O\left(\frac{x\rho(l)}{l}\right) \quad (l \leq x)$$

supplied by (8) but also the estimate

$$\begin{aligned}
 P_l(x) &= \sum_{\substack{p \leq x \\ p^r + 2 \equiv 0, \pmod{l}}} 1 = \sum_{\substack{0 < \nu \leq l \\ \nu^r + 2 \equiv 0, \pmod{l}}} \sum_{\substack{p \leq x \\ p \equiv \nu, \pmod{l}}} 1 \\
 &= \sum_{\substack{0 < \nu \leq l \\ \nu^r + 2 \equiv 0, \pmod{l}}} \left\{ \frac{\text{li } x}{\phi(l)} + O\left(\frac{x}{\log^6 x}\right) \right\} \\
 &= \frac{\text{li } x \rho(l)}{\phi(l)} + O\left(\frac{x \rho(l)}{\log^6 x}\right)
 \end{aligned}$$

that is valid when  $l$  is odd or evenly even. Rewriting the former as

$$P_l(x) = \frac{\text{li } x \rho(l)}{\phi(l)} + O\left(\frac{x \rho(l)}{l}\right) \quad (l \leq x),$$

we have

$$\begin{aligned}
 P'(x) &= \sum_{l'} \mu(l') P_{l'^s}(x) = \text{li } x \sum_{l'} \frac{\mu(l'^s) \rho(l'^s)}{\phi(l'^s)} + O\left(\frac{x}{\log^6 x} \sum_{l \leq \log^3 x} r^{\omega(l)}\right) \\
 &\quad + O\left(x \sum_{\log^3 x < l \leq x^{\frac{1}{3}}} \frac{r^{\omega(l)}}{l^s}\right) \\
 &= \text{li } x \prod_{q \leq \xi_1} \left(1 - \frac{\rho(q^s)}{\phi(q^s)}\right) + O\left(\frac{x(\log \log x)^{r-1}}{\log^3 x}\right) + O\left(\frac{x(\log \log x)^{r-1}}{\log^3 x}\right) \\
 &= \text{li } x \prod_q \left(1 - \frac{\rho(q^s)}{\phi(q^s)}\right) + O\left(\frac{x}{\log^2 x}\right)
 \end{aligned}$$

by the argument in the last line of (11). Coalesced with (48), this yields the conditional

**THEOREM 2.** *In the first situation described in the statement of Theorem 1, the number  $P(x)$  of primes up to a large number  $x$  for which  $p^r + 2$  is  $s$ th power-free is equal to*

$$\text{li } x \prod_q \left(1 - \frac{\rho(q^s)}{\phi(q^s)}\right) + O\left(\frac{x}{\log x (\log \log x)}\right),$$

*there being therefore infinitely many primes  $p$  with the property that  $p^r + 2$  is  $s$ th power-free. These statements are unconditional when  $s \geq r$ .*

The tabulated values of  $r$  and  $s$  above being still relevant, we see, in particular, that there are irreducible polynomials  $f(n)$  of degree  $r$  for which  $f(p)$  is infinitely  $(r-1)$ -free whenever  $r$  is an even number no smaller than 4. Although conditional, this is a statement that advances one aspect of Nair's work, in which a like conclusion is only available for  $r \geq 8$ . Also, since previously we only narrowly failed to proceed from our successfully accomplished treatment of

this case for general arguments  $n$  for all  $r > 2$  to the restricted arguments  $p$  save when  $r$  was large, we should mention that only a very weak form of Hypothesis  $R^\dagger$  is needed to establish Theorem 2 when  $r \geq 4$  and  $s = r - 1$ .

This ends our analysis of the effect on our problem of taking Hypothesis  $R^\dagger$  – or a weaker form thereof – as the sole conjecture to be assumed. Wanting yet stronger results, we devote the first part of the next Section to what can be achieved when we augment our assumption by adding one about the distribution of the solutions of the Pellian equation before we consider in the second part the implications of only a conjecture of the latter type.

## 8. The Pellian equation and other conditional theorems.

Taken together, Theorem 1 in  $I_1$  and Conjecture in  $I_1$  imply the truth of the following hypothesis that we will now assume.

**HYPOTHESIS  $P$ .** *Let  $\gamma(x, \alpha)$  be the number of non-square positive determinants  $D$  up to  $x$  for which the fundamental solution of the Pellian equation does not exceed  $D^\alpha$ . Then, for any positive  $\alpha$  not less than  $\frac{1}{2}$ ,*

$$\gamma(x, \alpha) = O\left(x^{\frac{1}{2}} \log^2 x\right),$$

where the constant implied by the  $O$ -notation depends on  $\alpha$ .

Although the statement is unconditional for  $\alpha < 1$ , it is only conjectural for the longer range of  $\alpha$  upon which we shall lean. From it, we then have the

**COROLLARY 1.** *Let  $g(x, \alpha)$  be defined like  $\gamma(x, \alpha)$  except that the solutions to be counted are not restricted to be fundamental. Then*

$$g(x, \alpha) = O\left(x^{\frac{1}{2}} \log^2 x\right).$$

In the notation of the second paragraph of §4, each solution to be now counted is of the form  $\eta_D^u \leq D^\alpha$ , where  $\eta > \sqrt{D}$ . Hence  $u = O(1)$  and the result follows.

To avail ourselves of this hypothesis, we must assume that both  $r$  and  $s$  are even and then, having weakened (6) to merely

$$s > \frac{3}{4}(r - 2),$$

we lessen the value of  $\xi_3$  in (4) to

$$x^{\frac{r-2}{s}} \log^{\frac{8}{s}} x$$

with the implication that (7) is still valid. Hence, if we replace  $x_1$  in (12) by

$$x_2 = 2x^r / \xi_3^s = 2x^2 \log^{-8} x, \tag{49}$$

the analogue of (13) is

$$\begin{aligned} M(x, \xi_3) = \sum_{m \leq x_2} \Upsilon(m) &= \sum_{m \leq 2x^{\frac{1}{2}}} \Upsilon(m) + \sum_{2x^{\frac{1}{2}} < m \leq x_2} \Upsilon(m) \\ &= M_I(x) + M_{II}(x), \text{ say.} \end{aligned}$$

Going back to the beginning of §4, we first see that

$$M_I(x) = O \left( \log x \sum_{m \leq 2x^{\frac{1}{2}}} 1 \right) = O \left( x^{\frac{1}{2}} \log x \right).$$

Also, the sum  $M_{II}(x)$  does not exceed the number of non-square determinants  $D$  between  $2x^{\frac{1}{2}}$  and  $x_2$  for which  $\eta'_D \leq 2x^r + 2$  and for which therefore  $\eta'_D \leq D^{2r}$ . Hence, by Corollary 1 and then by (49),

$$M_{II}(x) = O \left( x_2^{\frac{1}{2}} \log^2 x_2 \right) = O \left( \frac{x}{\log^2 x} \right)$$

and thus

$$M(x, \xi_3) = O \left( \frac{x}{\log^2 x} \right).$$

The new circumstances do not affect the previous estimations of the other elements in (5) that make up  $N(x)$ . Consequently, we have the following conditional

**THEOREM 3.** *Let us assume Hypotheses  $R^\dagger$  and  $P$ . Then the assertions of Theorem 1 are true for even integers  $r$  and  $s$  satisfying  $r \geq 4$  and  $s > \frac{3}{4}(r - 2)$ .*

Likewise we have

**THEOREM 4.** *In the situation described in the statement of Theorem 3 the conclusion in Theorem 2 is valid.*

The improvement wrought by the extra hypothesis may seem disproportionally small in comparison with what is assumed, since it is only when  $r \equiv 4, \pmod{8}$ , that the value of  $s$  in the table is reduced and this only by 1. Nevertheless, we have produced a treatment of the infinitude of square-free numbers represented by  $n^4 + 2$ , thus creating a conditional demonstration of a proposition whose absence from the literature was a subject of comment by Erdős.

Having exhausted our intended applications of Hypothesis  $R^\dagger$ , we shall briefly explain what happens when the only conjecture assumed concerns Pell's equation. Although we could obtain some good results by continuing to adopt the previous Hypothesis  $P$ , it is more striking to assume the following analogue of what Conjecture 4 in  $I_1$  says about the equation  $T^2 - DU^2 = -1$ .

HYPOTHESIS  $P_1$ . Let  $\xi(x, \alpha)$  be the number of non-square determinants  $D$  up to  $x$  for which the fundamental solution  $T + U\sqrt{D}$  of the equation

$$T^2 - DU^2 = -2 \quad (50)$$

does not exceed  $D^\alpha$ . Then for any number  $\alpha$  not less than  $\frac{1}{2}$ ,

$$\xi(x, \alpha) = O\left(x^{\frac{1}{2}} \log x\right).$$

One property of (51), which we must remember during the enunciation but to which we did not need to advert at the beginning of §4, is that for non-square determinants it possesses a least positive solution  $\theta = T + u\sqrt{D}$  with  $T, U > 0$  – deemed fundamental – with the property that all solutions are provided by  $\theta^{2m+1}/2^m$  for integral  $m$ . The thinking upon which the conjecture is based being similar to that employed in §5 of  $I_1$ , we can therefore proceed as earlier to the relevant deduction, which we state as

COROLLARY 2. Let  $z(x, \alpha)$  be defined as  $\xi(x, \alpha)$  except that the solutions with  $T, U > 0$  to be counted are not restricted to be fundamental. Then

$$z(x, \alpha) = O\left(x^{\frac{1}{2}} \log x\right).$$

Let now  $r \geq 4$  and  $s = r - 2$  be even integers. Then take

$$\xi_2 = \xi_3 = x \log^{\frac{4}{r}} x$$

so that the term  $M(x; \xi_2, \xi_3)$  becomes absent from (5) and  $x_1$  in (12) is replaced by

$$x_3 = 2x^r / x^{r-2} \log^{\frac{4(r-2)}{r}} x = 2x^2 \log^{\frac{8}{r}-4} x.$$

In this scene we have

$$M(x; \xi_1, \xi_2) = O\left(\frac{x}{\log x (\log \log x)}\right) + O\{\pi(\xi_2)\} = O\left(x \log^{\frac{4}{r}-1} x\right),$$

whereas, by Corollary 2 and the reasoning behind (50),

$$M(x, \xi_3) = O\left(x^{\frac{1}{2}} \log x\right) + O\left(x_3^{\frac{1}{2}} \log x_3\right) = O\left(x \log^{\frac{4}{r}-1} x\right).$$

We therefore infer

THEOREM 5. Let us assume Hypothesis  $P_1$ . Then

$$N(x) \sim x \prod_q \left(1 - \frac{\rho(q^s)}{q^s}\right)$$

when  $s = r - 2$  and  $r$  is an even integer exceeding 4.



We observe that the method just fails to secure the above formula when  $r = 4$  and is seemingly wholly unable to deliver its analogue for  $P(x)$  for any value of  $r$ ; on the other hand, the substitution of the weaker Conjecture  $P$  secures the formula whenever  $r > 6$ . And, as a parting comment on  $N(x)$ , we should emphasize that it has only been by assuming both Hypothesis  $R^\dagger$  and Hypothesis  $P$  that we were able to deal with the most interesting case regarding the square-free values taken by quartic polynomials.

### 9. Connection between Hypotheses $R^\dagger$ and $P_2$ .

Hypotheses  $R^\dagger$  and  $P_1$  share the feature of applicability to the subject of the power-free values of polynomials. But their affinity is deeper than that because the former hypothesis for exponential sums with cubic polynomial arguments implies an improvement in the unconditional asymptotic formula for  $\xi(x, \alpha)$  that the method in  $I_1$  provides. In fact, if we work instead with the cognate equation  $T^2 - DU^2 = -1$  to illustrate the point by reference to Theorem 2 of  $I_1$ , there is for  $0 < \alpha \leq \frac{1}{2}$  the formula

$$Y(x, \alpha) \sim \frac{\alpha}{2\pi} x^{\frac{1}{2}} \log x. \quad (51)$$

for the number  $Y(x, \alpha)$  of (non-square) determinants  $D$  up to  $x$  for which the fundamental selection of this equation does not exceed  $2D^{\frac{1}{2}+\alpha}$ . However, on examining in detail the proof of this formula that is indicated by the dialogue in  $I_1$ , one sees that the techniques required are similar to those that have been directed in the past to the easier divisor type problems without a penetrating examination of the remainder terms. If, however, one attempt to introduce exponential sums into the framework to refine the calculations, one then arrives at the subject of Hypothesis  $R^\dagger$  for cubic sums after an analysis that enlarges on that of §5. The use of some conjecture such as this hypothesis seeming unavoidable at this point, we can then conditionally deduce that formula (5) holds in an extended range of the type  $0 < \alpha \leq b$  for some  $b > \frac{1}{2}$ . Yet, even on the strength of this powerful hypothesis, the scope of the method is severely circumscribed to values of  $b$  less than 1 because, for reasons given in  $I_1$  it surely cannot account for non-fundamental solutions that must appear beyond this point. Thus Hypothesis  $R^\dagger$  is not likely to help us to establish the status of the bolder conjectures in  $I_1$  even though it extends the validity of a formula upon which some of these speculations are based.

## References

- 1 *F. V. Atkinson and Lord Cherwell*, The mean values of arithmetical functions, Quart. J. Math., Oxford (1) 20 (1949), 65-79
- 2 *E Bombieri and W.M.Schmidt*, On Thue's equation, Invent. Math., 88(1987), no 1, 69-81.
- 3 *J. Browkin, M. Filaseta, G. Greaves, and A. Schinzel*, Square-free values of polynomials and the abc-conjecture, Sieve methods, exponential sums, and their applications in Number Theory, Greaves, G.R.H., Harman, G., Huxley, M.N., Eds., Cambridge University Press, 1996.
- 4 *P. Erdős*, Arithmetical properties of polynomials, J. London Math. Soc., 28 (1953), 416-425.
- 5 *T. Estermann*, Einige Sätze über quadratfreie Zahlen Math. Annalen, 105 (1931), 653-662.
- 6 *A. Granville*, ABC means we can count square-frees, Internat. Math. Res. Notices 19 (1998), 991-1009.
- 7 *C. Hooley*, On the square-free values of cubic polynomials, J reine angew. Math., 229 (1968), 147-154.
- 8 *C. Hooley*, On the power-free values of polynomials, Mathematika, 14 (1967), 21-6.
- 9 *C. Hooley*, On the Brun-Titchmarsh theorem, J. reine angew. Math., 255 (1972), 60-79.
- 10 *C Hooley*, Applications of sieve methods to the theory of numbers, Cambridge University Press, 1976.
- 11 *C. Hooley*, On power-free numbers and polynomials : I, J. reine angew Math., 293/294 (1977), 67-85.
- 12 *C. Hooley*, On power-free numbers and polynomials: II, J. reine angew. Math, 295 (1977), 1-21 (corrigendum, same journal, vol 299/300)
- 13 *C. Hooley*, On the greatest prime factor of a cubic polynomial, J. reine angew. Math., 303/304 (1978), 21-50.
- 14 *C. Hooley*, On the Pellian equation and the class number of indefinite binary quadratic forms, J. reine angew. Math., 353 (1984), 98-131.
- 15 *M. N. Huxley and M. Nair*, Power-free values of polynomials III, Proc. London Math. Soc. (3), 41 (1980), 66-82.
- 16 *T. Nagell*, Zur Arithmetik dei Polnome, Abhandl. Math. Sem. Hamburg, 1(1992), 179-194.

- 17 *M. Nair*, Power-free values of polynomials, *Mathematika*, 23(1976), 159-83.
- 18 *M. Nair*, Power-free values of polynomials II, *Proc. London Math. Soc.* (3), 38 (1979), 353-368.
- 19 *G. Ricci*, Ricerche aritmetiche sui polinomi, *Rend. Circ. Mat. Palermo*, 57 (1933), 433-475.
- 20 *H. J. S. Smith*, Report on the theory of numbers, reprinted in the *Collected Works*, Oxford University Press, 1894.

### Address

School of Mathematics,  
University of Wales, Cardiff,  
P.O. Box 926,  
Cardiff,  
CF24 4YH.  
(Received on 25-02-2004)