ACTA ARITHMETICA
145.1 (2010)

On polynomials that are sums of two perfect qth powers

by

C. Hooley (Cardiff)

1. Introduction. Following two recent publications, we advert again to the long held expectation that, if $F(x_0, \dots, x_r)$ be a polynomial with rational integral coefficients that assumes values of a certain shape for all integral $x_0, \dots, x_r$ (or at least for all sufficiently large values thereof), then it is actually identically of this shape in appropriate circumstances. In the first of these ([4]—designated by I in the sequel for convenience), to which we refer the reader for some history of the matter and our mention of Schinzel's work [7], we proved that this expectation was fulfilled when $F(x_0, \dots, x_r)$ is a cubic that is always equal to a sum of two perfect cubes for integral values of $x_0, \dots, x_r$. Knowing that we could reduce the proposition by an algebraical process to the most interesting cases where $r = 0$, we began with a polynomial $F(x)$ and successfully treated the two situations where it was assumed that $F(n)$ for all large integers n was either (i) a sum of two positive cubes or (ii) merely a sum of two (non-zero) cubes of either sign. Indeed, in each case we ultimately gained an identity for $F(x)$ that yielded a representation of $F(n)$ of the type postulated; moreover, that in the second case was the basis of the identity for $F(x_0, \dots, x_r)$ that was sought for the general proposition. We then went on in the second paper [5] to consider cubic polynomials $F(x)$ that have the property that $F(n)$ is always equal for large n to a value assumed through integers u, v by an irreducible binary cubic form

$$au^3 + bu^2v + cuv^2 + dv^3,$$

using a different method to reach similar but slightly weaker conclusions.

The purpose of the present communication is to extend the findings of I to polynomials $F(x_0, \dots, x_r)$ of *odd prime* degree q that are equal to the sum of two perfect qth powers when $x_0, \dots, x_r$ are integers. Although our procedure has features in common with I and, in particular, still begins with

2010 *Mathematics Subject Classification*: 11D41, 11P99.
Key words and phrases: polynomials, higher powers.

DOI: 10.4064/aa145-1-1

the case $r = 0$, there are substantial departures from the previous method because, amongst other things, there are more possibilities regarding $F(x)$ to eliminate and because there is a greater reliance on algebraical number theory than before. It is only in the later stages that our exposition falls into line with the earlier paper, at which point we rely heavily on I to avoid needless repetition.

We have thus raised to an unconditional status an increased portion of Schinzel's theorem [7] about polynomials equal to the sum of two nth powers that was obtained on his Conjecture C. And in making this statement, we should add in accordance with later comment that our conclusions are still valid if it be merely assumed that the degree of F do not exceed q. But to remove this restriction to allow high degrees for given q would be to elevate the problem to a level of difficulty we are currently unable to overcome.

2. Notation. Although the meaning of the notation should usually be clear from the context in which it arises, the following guide may be helpful.

The letters $x, x_0, \dots, x_r, \xi, \eta$ denote variables or indeterminates in polynomials; a, b are stated rationals in §4 but otherwise integers; A, B, C, r, s are integers, save when the last is a complex variable; d, d, e, g, j, h, k, l, m, n, ν are integers that are usually positive; p is a positive prime number; for any integer denoted by δ, say, $\bar{\delta}$ is a solution of $\delta\bar{\delta} \equiv 1, \bmod k$, to a modulus k whose definition is evident from the context.

The letter X is a positive variable to be regarded as tending to infinity, all stated inequalities being true for sufficiently large values of X; $c, c_1, \dots$ are positive constants depending at most on the polynomial $F(x)$ of *odd prime* degree q under consideration, as are constants implied by the O-notation. The function $\sigma_{-\alpha}(m)$ is the function $\sum_{d|m} d^{-\alpha}$.

3. Preparations. The form $\xi^q + \eta^q$ underlying our investigations is equivalent through the substitution

$$\xi = r - s, \qquad \eta = s$$

to the form

$$rg(r, s) = r(r^{q-1} - qr^{q-2}s + \cdots + qs^{q-1}), \tag{0}$$

in which $r > 0$ if $\xi^q + \eta^q > 0$; also, $0 < s < r$ when ξ, η are both positive but either $s < 0$ or $s > r$ when one of ξ, η is positive and the other negative. Being equivalent to the cyclotomic form derived from the primitive qth roots of unity, the form $g(r, s)$ only primitively admits prime divisors that apart from q are congruent to 1, mod q. Therefore the divisibility of $rg(r, s)$ by a prime $p \not\equiv 1, \bmod q$, implies that $p \,|\, r$ even when $p = q$, since all terms in

$g(r,s)$ save the first are multiples of q. Also, as

$$g(r,s) = \frac{1}{r}\{(r-s)^q + s^q\},$$

it should be noted that for positive integers N and r the equation $g(r,s) = N$ has at most one solution in an integer (indeed, any real number) s of any sign for which $s \le \frac{1}{2}r$, the other being $r - s$.

In the case where both ξ and η are positive we have

$$\frac{r^q}{2^{q-1}} \le (r-s)^q + s^q < r^q, \tag{1}$$

the first inequality remaining true when $s = \eta$ is negative (or equivalently greater than r). Hence in considering the equation $rg(r,s) = F(n)$ under investigation when $0 < s < r$ and $X_0 < n \le X$ for large X, we find that

$$r^q/2^{q-1} \le c_1 X^q \quad \text{and} \quad c_2 n^q \le r^q$$

so that

$$r \le c_3 X \tag{2}$$

and

$$n \le c_4 r. \tag{3}$$

Also, even if s be negative, (2) is still valid, although then (3) must be replaced by a suitable variant when we consider qth powers of opposite signs.

To simplify some of the more analytical parts of the demonstrations we shall use Selberg's remarkable upper and lower bounds for the characteristic function of an interval. Consulting Theorem A.4 in Vaaler's work [8] and first taking $\beta = 1, \alpha = 0$ therein, we discover an upper bounding function $\mathit{\Gamma}(u)$ for the characteristic function of the interval $[0,1]$ with the property that the transform

$$\hat{\mathit{\Gamma}}(t) = \int_{-\infty}^{\infty} \mathit{\Gamma}(u) e^{2\pi i u t}\, du$$

enjoys the features

$$\hat{\mathit{\Gamma}}(t) = \begin{cases} 2 & \text{if } t = 0, \\ 0 & \text{if } |t| > 1, \end{cases} \tag{4}$$

and therefore

$$|\hat{\mathit{\Gamma}}(t)| \le 2 \tag{5}$$

always. Similarly, by taking $\beta = 4$, $\alpha = 2$, we obtain a lower bound $\gamma(u)$ for the characteristic function of $[2,4]$, where

$$\hat{\gamma}(t) = \int_{-\infty}^{\infty} \gamma(u) e^{2\pi i u t}\, du = \begin{cases} 1 & \text{if } t = 0, \\ 0 & \text{if } |t| > 1, \end{cases} \tag{6}$$

so that

$$|\hat{\gamma}(t)| \leq 1 \tag{7}$$

always.

Lemmata used in the first stage of work and also possibly afterwards will be stated at once, while those only needed later will be appended at the appropriate places. First, for any polynomial $\phi(x)$ with rational integral coefficients whether irreducible or reducible, we let $\rho^*(k)$ denote the number of incongruent zeros, mod k, of $\phi(x)$ and then let

$$S^*(h,k) = \sum_{\substack{0<\nu\leq k \\ \phi(\nu)\equiv 0,\,\mathrm{mod}\,k}} e^{2\pi i h\nu/k}, \tag{8}$$

where obviously

$$|S^*(h,k)| \leq \rho^*(k); \tag{9}$$

furthermore we shall agree to suppress the asterisks from the notation when $\phi(x)$ is the polynomial $F(x)$ under consideration.

In regard to the first arithmetical function we shall require results in the elementary theory of congruences and also some known estimates that flow from the prime ideal theorem and a classical principle due to Dedekind (for the former, see Nagell [6, Chapter 3], and for the latter see Erdős [2]). These are enunciated in

LEMMA 1. *The function $\rho^*(k)$ is multiplicative. Also, if the polynomial $\phi(x)$ defining $\rho^*(k)$ be irreducible, then*

(i) $p(k_1k_2) = O\{\rho^*(k_1)\rho^*(k_2)\}$;

(ii) $\displaystyle\sum_{k\leq y} \rho^*(k) = O(y)$;

(iii) $\displaystyle\sum_{p\leq y} \rho^*(p) \sim y/\log y$;

(iv) $\displaystyle\prod_{p\leq y} \left(1 + \frac{\rho^*(p)}{p}\right) \sim c(f)\log y$ *(with $c(f) > 0$).*

We also require the generalized version of part (ii) above that is stated in

LEMMA 2. *Let Δ be a square-free product of primes exceeding the discriminant of an irreducible polynomial $\phi(x)$. Then, for some small positive constant δ, we have*

$$\sum_{\substack{d\leq y \\ d\equiv 0,\,\mathrm{mod}\,\Delta}} \rho^*(d) = \frac{A\rho^*(\Delta)\psi(\Delta)y}{\Delta} + O\{\rho^*(\Delta)y^{1-\delta}\},$$

where

$$\psi(\Delta) = \prod_{p|\Delta} \left(1 + \frac{\rho^*(p) - 1}{p}\right)^{-1}$$

and A is a positive constant.

Also, without any conditions on Δ, we have

$$\sum_{\substack{d \le y \\ d \equiv 0, \bmod \Delta}} \rho^*(d) = O\left(\frac{\rho^*(\Delta) y}{\Delta}\right).$$

If

$$\Phi_1(s) = \sum_d \frac{\rho^*(d)}{d^s}$$

for $\sigma > 1$ in the first place and if $\zeta_\alpha(s)$ be the zeta function of the corpus $\mathbb{Q}(\alpha)$ defined by a zero α of $\phi(x)$, then it is familiar by the principle of Dedekind's already mentioned that

$$\Phi_1(s) = \zeta_\alpha(s) H(s),$$

where $H(s)$ is regular and bounded for $\sigma > 1 - 2\delta$ and $H(1) \neq 0$. Also, as $\rho(p^\alpha) = \rho(p)$ for $\alpha > 1$ when $p \nmid \Delta$, the function $\Phi_\Delta(s)$ defined as

$$\sum_{d \equiv 0, \bmod \Delta} \frac{\rho^*(d)}{d^s} \qquad (\sigma > 1)$$

equals

$$\frac{\rho(\Delta)}{\Delta^s} \prod_{p|\Delta} \left(1 - \frac{1}{p^s}\right)^{-1} \sum_{(d,\Delta)=1} \frac{\rho^*(d)}{d^s}$$

by multiplicativity and Euler's theorem, while

$$\Phi_1(s) = \prod_{p|\Delta} \left\{1 + \frac{\rho^*(p)}{p^s}\left(1 - \frac{1}{p^s}\right)^{-1}\right\} \sum_{(d,\Delta)=1} \frac{\rho^*(d)}{d^s}$$

by a parallel argument. Since therefore

$$\begin{aligned} \Phi_\Delta(s) &= \frac{\rho(\Delta)}{\Delta^s} \prod_{p|\Delta} \left(1 + \frac{\rho^*(p) - 1}{p^s}\right) \Phi_1(s) \\ &= \frac{\rho(\Delta)}{\Delta^s} \prod_{p|\Delta} \left(1 + \frac{\rho^*(p) - 1}{p^s}\right) H(s) \zeta_\alpha(s) \end{aligned}$$

for $\sigma > 1 - 2\delta$, we infer the first part of the lemma by contour integration and the properties of $\zeta_\alpha(s)$.

The second part is more elementary. Indeed, by parts (i) and (ii) of Lemma 1, we have at once that

$$\sum_{\substack{d\le y\\ d\equiv 0,\,\mathrm{mod}\,\Delta}}\rho^*(d)=\sum_{\Delta d'\le y}\rho^*(\Delta d')=O\Big(\rho^*(\Delta)\sum_{d'\le y/\Delta}\rho(d')\Big)=O\Big(\frac{\rho^*(\Delta)y}{\Delta}\Big).$$

As in I, we shall use properties of the sum $S^*(h,k)$ that are extensions of some of those of $\rho^*(k)$ expressed in Lemma 1. Being similar to those stated in I and in particular Lemma 2 therein ([1]), these are stated without proof in

LEMMA 3. *The sum $S^*(h,k)$ is multiplicative in the sense that, if $(k_1,k_2)=1$ and $k_1\overline{k}_1\equiv 1,\mathrm{mod}\,k_2, k_2\overline{k}_2\equiv 1,\mathrm{mod}\,k_1$, then*

$$S^*(h,k_1k_2)=S^*(h\overline{k}_2,k_1)S^*(h\overline{k}_1,k_2).$$

If $\phi(x)$ be irreducible and of degree q, then for any positive integers d and h,

$$\sum_{\substack{k\le y\\ (k,d)=1}}|S^*(h\overline{d},k)|=O\Big(\frac{y\sigma_{-1/4}(h)}{\log^{\delta_1}y}\Big),$$

where δ_1 is a small positive number that depends on q.

Later on we shall introduce a variant of the second half of this lemma in which $\phi(x)$ need not be irreducible and in which the numbers k in the summation are of a special type.

4. Adoption of Hypothesis P—the reducibility of $F(x)$. Examining first the case where both qth powers are positive, we are ready to consider the implications of

HYPOTHESIS P. *$F(x)$ is a polynomial of degree q having the property that $F(n)$ is equal to a sum of two positive perfect qth powers for all sufficiently large integers n and thus for all n exceeding some number X_0.*

We shall shew under the hypothesis that $F(x)$ is reducible and then that it contains a linear factor. Although it might seem at first sight that the method used to deduce the latter fact would establish the former one as well, the nature of the algebraic fields underlying our situation invalidates such a programme. It is therefore necessary to bring in another method to secure the first property before going on to demonstrate the existence of a linear factor.

([1]) We take the opportunity to point out that a factor $(\log\log x)^{c_5}$ was inadvertently excluded from the estimate (3) in I. This, however, did not vitiate the application of the estimate.

To shew that $F(x)$ is not irreducible we assume the opposite and deduce a contradiction. Here we shun the method of I, which indeed is still applicable, in favour of a slightly simpler one that does not depend on the arithmetical properties of $g(r,s)$. In the new procedure, for reasons that will become apparent, we do not apply the hypothesis for all n exceeding X_0 but only to a suitable subset of them that we now define within the following framework.

Introducing a sufficiently small positive constant δ_2 to determine the parameter

$$\zeta = \zeta(X) = \frac{1}{2}\,\delta_2 \log\log X \tag{10}$$

by means of which is defined the set of primes p satisfying

$$c_6 < p \le \zeta \tag{11}$$

for a suitably large positive constant c_6, we let d_1 denote, generally, a square-free product (possibly 1) of such primes so that

$$d_1 \le \prod_{c_6<p\le\zeta} p \le \exp\Big(\sum_{p\le\zeta} \log p\Big) = e^{\theta(\zeta)} < e^{2\zeta} = \log^{\delta_2} X. \tag{12}$$

Next define $\omega^*(M) = \omega^*_\zeta(M)$ to be the number of distinct prime factors p of a non-zero integer M that are of type (11). Then we shall only apply Hypothesis P to the set $\mathscr{S}_1 = \mathscr{S}_1(X)$ of numbers n between X_0 and X for which

$$\omega^*\{F(n)\} \le \frac{3}{2}\log\log\zeta, \tag{13}$$

the cardinality $C(X)$ of the excluded numbers n up to X being not more than

$$\frac{1}{2^{\frac{3}{2}\log\log\zeta}} \sum_{n\le X} 2^{\omega^*\{F(n)\}} = \frac{1}{2^{\frac{3}{2}\log\log\zeta}} \sum_{n\le X} \sum_{d_1\mid F(n)} 1.$$

Hence, since (12) certainly means that $d_1 \le X$,

$$\begin{aligned} C(X) &\le \frac{1}{2^{\frac{3}{2}\log\log\zeta}} \sum_{d_1} \sum_{\substack{n\le X \\ F(n)\equiv 0,\bmod d_1}} 1 \le \frac{2X}{2^{\frac{3}{2}\log\log\zeta}} \sum_{d_1} \frac{\rho(d_1)}{d_1} \\ &\le \frac{2X}{2^{\frac{3}{2}\log\log\zeta}} \prod_{p\le\zeta} \left(1 + \frac{\rho(p)}{p}\right) = O(X\log^{1-\frac{3}{2}\log 2}\zeta) < \frac{1}{4}X - X_0 \end{aligned}$$

in view of Lemma 1, the assumed irreducibility of $F(x)$, and the inequality $1 - \frac{3}{2}\log 2 < 0$. Thus the cardinality of $\mathscr{S}_1$ exceeds $\frac{3}{4}X$.

On the other hand, by Hypothesis P, this cardinality does not exceed the number $\Upsilon(X)$ of solutions in r, s and n of the equation

$$rg(r,s) = F(n) \tag{14}$$

that are subject to the conditions (13), $0 < s \leq \frac{1}{2}r$, $X_0 < n \leq X$, and therefore also to the constraints on s, r and n contained in (2) and (3). Also, writing (14) as

$$rm = F(n) \tag{15}$$

and noting from the initial comment in §3 that no value of m is presented more than once when r and n are given, we see that $\Upsilon(X)$ does not exceed the number $\Upsilon_1(X)$ of solutions of (15) conforming to (2) and (3) for which

$$\omega^*(rm) \leq \frac{3}{2}\log\log\zeta$$

and for which therefore either

$$\omega^*(r) \leq \frac{3}{4}\log\log\zeta \tag{16}$$

or

$$\omega^{**}(m) = \sum_{\substack{c_6 < p \leq \zeta \\ p \mid m;\, p \nmid r}} 1 \leq \frac{3}{4}\log\log\zeta. \tag{17}$$

Consequently, splitting $\Upsilon(X)$ into sums $\Upsilon_2(X), \Upsilon_3(X)$ that represent the contributions due to r, m, n for which (16), (17) hold, respectively, we have

$$\Upsilon(X) \leq \Upsilon_1(X) \leq \Upsilon_2(X) + \Upsilon_3(X), \tag{18}$$

to utilize which we agree that the symbol d_2 shall represent a square-free product of primes p satisfying the conditions $c_6 < p \leq \zeta$, $p \nmid r$ so that

$$(d_2, r) = 1. \tag{19}$$

Since

$$\sum_{\substack{n \leq c_4 r \\ F(n) \equiv 0, \bmod r}} 1 = O\{\rho(r)\},$$

we have

$$\Upsilon_2(X) = O\Big(a^{\frac{3}{4}\log\log\zeta} \sum_{r \leq c_3 X} a^{-\omega^*(r)}\rho(r)\Big) = O\Big(a^{\frac{3}{4}\log\log\zeta} \sum\nolimits_1\Big), \quad \text{say,} \tag{20}$$

on choosing a suitable constant $a > 1$. Next, having set

$$b = 1 - \frac{1}{a} < 1 \tag{21}$$

and having noted that

$$a^{-\omega^*(r)} = \prod_{\substack{c_6\le p\le\zeta\\ p\mid r}} (1-b) = \sum_{d_1\mid r}\mu(d_1)b^{\omega(d_1)}, \tag{22}$$

we infer from Lemmata 1 and 2 that

$$\begin{aligned}\sum\nolimits_1 &= \sum_{r\le c_3X}\rho(r)\sum_{d_1\mid r}\mu(d_1)b^{\omega(d_1)} = \sum_{d_1}\mu(d_1)b^{\omega(d_1}\sum_{\substack{r\le c_3X\\ r\equiv 0,\bmod d_1}}\rho(r)\\ &= c_3AX\sum_{d_1}\frac{\mu(d_1)b^{\omega(d_1)}\rho(d_1)\psi(d_1)}{d_1} + O\Big(X^{1-\delta}\sum_{d_1}\rho(d_1)\Big)\\ &= c_7X\prod_{c_6<p\le\zeta}\left\{1-\frac{b\rho(p)}{p}\left(1+\frac{\rho(p)-1}{p}\right)^{-1}\right\} + O(X^{1-\delta}\log^{\delta_2}X)\end{aligned}$$

in virtue of (12). Here the product is

$$\begin{aligned}\prod_{c_6<p\le\zeta}\left\{1-\frac{b\rho(p)}{p}+O\Big(\frac{1}{p^2}\Big)\right\} &= O\Big\{\prod_{c_6<p\le\zeta}\Big(1-\frac{b\rho(p)}{p}\Big)\Big\}\\ &= O\Big\{\prod_{c_6<p\le\zeta}\Big(1+\frac{\rho(p)}{p}\Big)^{-b}\Big\} = O\{\log^{-b}\zeta\}\end{aligned}$$

by Lemma 1, whence (20) leads to

$$\Upsilon_2(X) = O(X\log^{\frac{3}{4}\log a+a^{-1}-1}\zeta),$$

in which $\log\zeta$ appears with exponent

$$\frac{3}{4}\log\frac{4}{3}-\frac{1}{4}<0 \tag{23}$$

if $a = 4/3$. Consequently

$$\Upsilon_2(X) = o(X). \tag{24}$$

To treat $\Upsilon_3(X)$ is harder because for the first time here we have to consider congruential conditions on numbers in a range of length X where the moduli of the congruences are considerably larger than X. We must therefore take account of the uniform distribution of the roots of congruences through the use of Lemma 2, which is most expeditiously introduced into the method by means of the functions $\Gamma(u)$ discussed in §3.

First, from the definition of $\Upsilon_3(X)$ and the analogue

$$a^{-\omega^{**}(m)} = \sum_{d_2}\mu(d_2)b^{\omega(d_2)} \qquad (a = 4/3)$$

of (22),

$$\Upsilon_3(X) = \sum_{r\le c_3X} \sum_{\substack{rm=F(n)\\ n\le c_4r\\ \omega^{**}(m)\le \frac34\log\log\zeta}} 1$$

$$\le a^{\frac34\log\log\zeta} \sum_{r\le c_3X} \sum_{rm=F(n)} \Gamma\Big(\frac{n}{c_4r}\Big) \sum_{d_2\mid m} \mu(d_2) b^{\omega(d_2)}$$

$$= a^{\frac34\log\log\zeta} \sum_{r\le c_3X} \sum_{d_2} \mu(d_2) b^{\omega(d_2)} \sum_{F(n)\equiv 0,\bmod rd_2} \Gamma\Big(\frac{n}{c_4r}\Big)$$

$$= a^{\frac34\log\log\zeta} \sum_{r\le c_3X} \mu(d_2) b^{\omega(d_2)} \sum\nolimits_{r,d_2}, \quad \text{say.}$$

Next

$$\sum\nolimits_{r,d_2} = \sum_{\substack{F(\nu)\equiv 0,\bmod rd_2\\ 0<\nu\le rd_2}} \sum_{n\equiv\nu,\bmod rd_2} \Gamma\Big(\frac{n}{c_4r}\Big),$$

the inner sum in which equals

$$\sum_l \Gamma\Big(\frac{\nu+lrd_2}{c_4r}\Big) = \int_{-\infty}^{\infty} \Gamma\Big(\frac{\nu+rd_2u}{c_4r}\Big)\,du + \sum_h{}' \int_{-\infty}^{\infty} \Gamma\Big(\frac{\nu+rd_2u}{c_4r}\Big) e^{2\pi i h u}\,du$$

$$= \frac{c_4\hat\Gamma(0)}{d_2} + \frac{c_4}{d_2}\sum_h{}' \hat\Gamma\Big(\frac{c_4h}{d_2}\Big) e^{-2\pi i h\nu/rd_2}$$

by the Poisson summation formula and the substitution

$$w = \frac{\nu}{c_4r} + \frac{d_2u}{c_4}.$$

Hence, by the definition of $S(h,k)$ in (8) and then by (4) and (5),

$$\sum\nolimits_{r,d_2} = \frac{c_4\hat\Gamma(0)\rho(rd_2)}{d_2} + \frac{c_4}{d_2}\sum_h{}' \hat\Gamma\Big(\frac{c_4h}{d_2}\Big) S(-h,rd_2)$$

$$= \frac{2c_4\rho(rd_2)}{d_2} + O\Big(\frac{1}{d_2}\sum_{0<h\le d_2/c_4} |S(h,rd_2)|\Big),$$

which equation when inserted in (25) yields

$$\Upsilon_3(X) \le a^{\frac{3}{4}\log\log\zeta}\Big\{2c_4\sum_{r\le c_3X}\rho(r)\sum_{d_2}\frac{\mu(d_2)\rho(d_2)b^{\omega(d_2)}}{d_2} + O\Big(\sum_{d_2}\frac{1}{d_2}\sum_{0<h\le d_2/c_4}\sum_{r\le c_3X}|S(h,rd_2)|\Big)\Big\} = a^{\frac{3}{4}\log\log\zeta}\Big\{2c_4\sum\nolimits_2 + O\Big(\sum\nolimits_3\Big)\Big\}, \quad \text{say.} \tag{26}$$

To attend to $\sum_2$ we observe that the inner sum within it equals

$$\prod_{\substack{p\nmid r\\ c_6<p\le\zeta}}\Big(1-\frac{b\rho(p)}{p}\Big) = \prod_{c_6<p\le\zeta}\Big(1-\frac{b\rho(p)}{p}\Big)\prod_{\substack{p\mid r\\ c_6<p\le\zeta}}\Big(1-\frac{b\rho(p)}{p}\Big)^{-1} = O\Big\{\prod_{c_6<p\le\zeta}\Big(1+\frac{\rho(p)}{p}\Big)^{-b}\prod_{p\mid r}\Big(1+\frac{bq}{p}\Big)\Big\} = O\{\sigma_{-1/2}(r)\log^{-b}\zeta\}$$

because of Lemma 1. Therefore, using the second part of Lemma 2, we conclude that

$$\sum\nolimits_2 = O\Big(\frac{1}{\log^b\zeta}\sum_{r\le c_3X}\rho(r)\sum_{d\mid r}\frac{1}{d^{1/2}}\Big) = O\Big(\frac{1}{\log^b\zeta}\sum_{d\le c_3X}\frac{1}{d^{1/2}}\sum_{\substack{r\le c_3X\\ r\equiv 0,\bmod d}}\rho(r)\Big) = O\Big(\frac{X}{\log^b\zeta}\sum_{d\le c_3X}\frac{\rho(d)}{d^{3/2}}\Big) = O(X\log^{-b}\zeta). \tag{27}$$

Also, since the summand in the inner sum of $\sum_3$ is

$$|S(h\overline{r},d_2)|\,|S(h\overline{d}_2,r)| \le \rho(d_2)|S(h\overline{d}_2,r)|$$

by (9), (19), and the first part of Lemma 3, an application of the second part of that lemma shews that

$$\sum\nolimits_3 \le \sum_{d_1}\frac{\rho(d_1)}{d_1}\sum_{0<h\le d_1/c_4}\sum_{\substack{r\le c_3X\\ (r,d_1)=1}}|S(h\overline{d}_1,r)| = O\Big(\frac{X}{\log^{\delta_1}X}\sum_{d_1}\frac{\rho(d_1)}{d_1}\sum_{0<h\le d_1/c_4}\sigma_{-1/4}(h)\Big),$$

whence, by (12) and Lemma 1, we get

$$\sum\nolimits_3 = O\Big(\frac{X}{\log^{\delta_1} X}\sum_{d_1}\rho(d_1)\Big) = O\Big(\frac{X}{\log^{\delta_1} X}\sum_{d\le\log^{\delta_2} X}\rho(d)\Big) \tag{28}$$
$$= O(X\log^{\delta_2-\delta_1} X) = O(X\log^{-b}\zeta)$$

because $\delta_2 < \delta_1$ when δ_2 in (12) is small enough.

Finally, from (26), (27), (28), (21), and (23) we deduce that

$$\Upsilon_3(X) = O(X\log^{\frac{3}{4}\log a + a^{-1} - 1}\zeta) = o(X)$$

and then from (18) and (24) that

$$\Upsilon(X) = o(X).$$

Being contradictory to our earlier assertion that $\Upsilon(X) > \frac{3}{4}X$, this statement demonstrates that $F(X)$ cannot be irreducible when Hypothesis P is in place.

5. $F(x)$ has a linear factor—first part. We still assume that the polynomial $F(x)$ adheres to Hypothesis P. Having shewn on this that $F(X)$ cannot be irreducible, we now shall demonstrate that $F(x)$ cannot lack a linear factor by once more assuming the opposite and deducing it is impossible. The method is very different from the former one, and despite initial appearances, could not have been applied to establish the reducibility of $F(x)$.

Our assumption and the fact that q is a prime number mean that the reducible polynomial $F(x)$ has a factorization

$$aF_1^{a_1}(x)\dots F_j^{a_j}(x) \tag{29}$$

containing a positive integer a and at least two distinct irreducible polynomials $F_1(x),\dots,F_j(x)$ with integral coefficients and degrees greater than 1 and less than $q-1$. From this factorization, according to a procedure to be described later, we shall select a polynomial designated by the symbol $f(x)$ that is one of the factors $F_i(x)$ or a product of two such factors when every choice of the former type is unsatisfactory. But, having agreed to let P denote, generally, a square-free product of primes that are not congruent to 1, mod q, and that exceed c_6, we let $M(X,P)$ be the number of integers n between $\frac{1}{2}X$ and X for which $f(n)$ is divisible by P and consider the sum

$$\Psi(X) = \sum_{A_1X<P\le 2A_1X} M(X,P)$$

for a sufficiently large positive constant A_1. This is then subjected to an initial development by way of the Poisson summation formula in order to reveal its dependence on entities whose treatment demands an appropriate

choice of the polynomial $f(x)$ above. These are in fact examples of $\rho^*(k)$ and the sum $S^*(h,k)$ when k is taken to be type of P and the polynomial $\phi(x)$ defining them is $f(x)$.

Following closely the treatment of the sum $\sum_{r,d}$ in (25) but with the lower bound $\gamma(4n/X)$ in place of $\Gamma(n/c_4 r)$, we see that

$$M(X,P) \geq \sum_{f(n)\equiv 0,\,\mathrm{mod}\,P} \gamma\Big(\frac{4n}{X}\Big) = \sum_{\substack{f(\nu)\equiv 0,\,\mathrm{mod}\,P\\ 0<\nu\leq P}} \sum_{n\equiv\nu,\,\mathrm{mod}\,P} \gamma\Big(\frac{4n}{X}\Big),$$

where the inner sum equals

$$\int_{-\infty}^{\infty} \gamma\Big(\frac{4\nu+4Pu}{X}\Big)\,du + \sum_h{}' \int_{-\infty}^{\infty} \gamma\Big(\frac{4\nu+4Pu}{X}\Big)e^{2\pi i h u}\,du$$
$$= \frac{X}{4P}\hat{\gamma}(0) + \frac{X}{4P}\sum_h{}'\hat{\gamma}\Big(\frac{hX}{4P}\Big)e^{-2\pi i h\nu/P}.$$

Hence, by (6) and (7),

$$M(X,P) \geq \frac{X\hat{\gamma}(0)\rho^*(P)}{4P} + \frac{X}{4P}\sum_h{}'\hat{\gamma}\Big(\frac{hX}{4P}\Big)S^*(-h,P)$$
$$= \frac{X\rho^*(P)}{4P} + O\Big(\frac{X}{P}\sum_{0<h\leq 4P/X}|S^*(h,P)|\Big)$$

and thus

$$\Psi(X) \geq \frac{1}{8A_1}\sum_{A_1X<P\leq 2A_1X}\rho^*(P) + O\Big(\sum_{0<h\leq 8A_1}\sum_{P\leq 2A_1X}|S^*(h,P)|\Big) \tag{30}$$
$$= \frac{1}{8A_1}\Psi_1(X) + O\Big(\sum_{0<h\leq 8A_1}\Psi_2(X,h)\Big), \quad \text{say.}$$

The restricted nature of the numbers P inhibits the development of this equation because of consequential algebraic difficulties that will be addressed in the next section.

6. $F(x)$ has a linear factor—the algebraical background and the estimation of $\Psi_1(X)$. In considering $\rho^*(P)$ we first concentrate on the case where the polynomial $f(x)$ chosen is irreducible and of degree d ([2]), then deducing from what we find the results needed in the contrary instance where $f(x)$ is a product of two distinct factors. This study begins with the investigation of $\rho^*(p)$ for $p \not\equiv 1$, mod q, or, equally well, of $\rho^*(p)$ for $p \equiv 1$, mod q,

([2]) This and other symbols below are placed in Roman font to avoid confusion with earlier ones expressed in italics.

since the behaviour of $\rho^*(p)$ over all primes p is known from classical theorems (see, for example, our Lemma 1). Therefore it is not surprising that we begin by introducing a field $\mathbb{G} = \mathbb{Q}(\beta)$ generated by a zero β of $f(x)$, and the cyclotomic field $\mathbb{Z} = \mathbb{Q}(\sqrt[q]{1})$ of degree $q-1$, since the condition $p \equiv 1$, mod q, is tantamount to there being exactly $q-1$ zeros, mod p, of the corresponding cyclotomic polynomial. But difficulties arise because $\mathbb{G}$ and $\mathbb{Z}$ are not necessarily linearly disjoint, that is, the degree of the combination $\mathbb{W} = \mathbb{W}_\beta$ of $\mathbb{G}$ and $\mathbb{Z}$ is not necessarily $\mathrm{d}(q-1)$. However, in the present instance where $\mathbb{Z}$ is Galoisian, such difficulties are abated because the degree $[\mathbb{W} : \mathbb{G}]$ is independent of the zero β chosen and is equal to $\mathrm{e}(q-1)$ for some divisor e of d, where for convenience we write

$$\mathrm{d} = \mathrm{eg}. \tag{31}$$

To build on this situation, letting $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_{q-1}$ be the conjugates over $\mathbb{Q}$ of a primitive qth root of unity and $\beta_1 = \beta, \beta_2, \dots, \beta_{\mathrm{d}}$ the conjugates over $\mathbb{Q}$ of β, we choose a rational integer c with the properties

- $\mathrm{c}\beta$ is an algebraic integer,
- $\alpha_{i_1} + \mathrm{c}\beta_{j_1} \neq \alpha_{i_2} + \mathrm{c}\beta_{j_2}$ if $(\alpha_{i_1}, \beta_{j_1}) \neq (\alpha_{i_2}, \beta_{j_2})$

and, as in the usual proof of the simplicity of algebraic extensions, form the algebraic integer

$$\theta = \alpha + \mathrm{c}\beta$$

that has the property that $\mathbb{W}_\beta = \mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\theta)$. Then, the degree of θ over $\mathbb{Q}$ being $\mathrm{e}(q-1)$, the conjugates of θ over $\mathbb{Q}$ are of the form $\alpha_i + \mathrm{c}\beta_j$ for $\mathrm{e}(q-1)$ distinct pairs (i, j). Next, if possible, choose a pair α_k, β_l that does not appear in the above representation of the conjugates of θ and form the number $\theta^{(2)} = \alpha_k + \mathrm{c}\beta_l$, whose conjugates over $\mathbb{Q}$ are unequal to those of θ and are in number $\mathrm{e}(q-1)$ as $\mathbb{Q}(\theta^{(2)}) = \mathbb{W}_{\beta_l}$. Finally, forming $\theta^{(3)}$ in like manner if necessary and continuing the process until the pairs (α_i, β_j) are exhausted, we deduce that the polynomial

$$\Phi(x) = \prod_{\substack{1 \le i \le q-1 \\ 1 \le j \le \mathrm{d}}} (x - \alpha_i - \mathrm{c}\beta_j)$$

is equal to

$$\prod_{1 \le \iota \le \mathrm{g}} m_\iota(x),$$

where $m_\iota(x)$ is the monic polynomial with rational integral coefficients that is the product

$$\prod_{1 \le u \le \mathrm{e}(q-1)} (x - \theta_u^{(\iota)})$$

taken over all the conjugates $\theta_u^{(\iota)}$. Here we note that the polynomials $m_\iota(x)$ are relatively prime to each other and have no repeated factors.

To apply this information to meet our current wants, we consider the reduction, mod p,

$$\overline{\Phi}(x) = \prod_{1\le \iota \le \mathrm{g}} \bar{m}_\iota(x)$$

of the identity for $\Phi(x)$ when $p > c_6$. First, if $u_1, \dots, u_{q-1}$ and $v_1, \dots, v_{\mathrm{d}}$ be the zeros, in $\mathbb{F}_p$ or an extension $\mathbb{F}_{p^\gamma}$ thereof, of the polynomials $(x^q-1)/(x-1)$ and $f(x)$, respectively, the reduction $\overline{\Phi}(x)$ is seen to equal

$$\prod_{\substack{1\le i\le q-1\\ 1\le j\le \mathrm{d}}} (x - u_i - \mathrm{c}v_j)$$

by consideration of symmetric functions and the integrity of $\mathrm{c}\beta$. Also, by use of resultants and discriminants, the polynomials $\bar{m}_\iota(x)$ have no common zeros and have no repeated factors. Moreover, a zero $u_i + \mathrm{c}v_j$ belongs to $\mathbb{F}_p$ if and only if u_i and v_j do, since otherwise it would be a multiple zero, as is seen by taking conjugates of u_i, v_j appropriately.

Let now $\rho_\iota^\dagger(p)$ be the number of incongruent solutions of

$$m_\iota(x) \equiv 0, \bmod p$$

and $\rho^{\dagger\dagger}(p)$ the number of incongruent solutions of

$$(x^q - 1)/(x - 1) \equiv 0, \bmod p.$$

Then, for $p > c_6$,

$$\rho^{\dagger\dagger}(p)\rho^*(p) = \rho_1^\dagger(p) + \cdots + \rho_{\mathrm{g}}^\dagger(p),$$

or in other words,

$$\frac{1}{q-1}(\rho_1^\dagger(p) + \cdots + \rho_{\mathrm{g}}^\dagger(p)) = \begin{cases} \rho^*(p) & \text{if } p \equiv 1, \bmod q,\\ 0 & \text{if } p \not\equiv 1, \bmod q, \end{cases} \tag{32}$$

which relation provides the formula for $\rho^*(p)$ we sought under the restriction $p \equiv 1$, mod q.

In associating this information with the Dedekind zeta functions it is helpful to let the symbol $H_i(s)$ denote a function of s that for $\sigma > 1 - 2\delta$ is both regular and bounded above and below in magnitude by a positive constant and is real when s is real. To estimate the sum $\Psi_1(X)$ in the first case where $f(x)$ is irreducible, we form the function

$$\begin{aligned} \mathrm{Z}(s) = \sum_P \frac{\rho^*(P)}{P^s} &= \prod_{\substack{p\not\equiv 1, \bmod q\\ p>c_6}} \left(1 + \frac{\rho^*(p)}{p^s}\right) \\ &= \prod_{p>c_6}\left(1+\frac{\rho^*(p)}{p^s}\right) \Big/ \prod_{\substack{\rho\equiv 1, \bmod q\\ p>c_6}} \left(1+\frac{\rho^*(p)}{p^s}\right) = \mathrm{Z_I}(s)/\mathrm{Z_{II}}(s), \quad \text{say,} \end{aligned} \tag{33}$$

for $\sigma > 1$ in the first place. Here, by the methods underlying the proof of Lemma 2 and the connection between $\rho^*(p)$ and the number of linear prime ideals over $\mathbb{Q}(\beta)$ dividing p, we easily find that

$$\mathrm{Z_I}(s) = \zeta_\beta(s) H_1(s) \quad (s > 1 - 2\delta), \tag{34}$$

where $\zeta_\beta(s)$ is the zeta function of the corpus $\mathbb{Q}(\beta)$. Next, by (32),

$$\begin{aligned}\mathrm{Z_{II}}(s) &= \prod_{p>c_6} \left\{ 1 + \frac{1}{q-1} \left(\frac{\rho_1^\dagger(p) + \cdots + \rho_{\mathrm{g}}^\dagger(p)}{p^s} \right) \right\} \\ &= \prod_{1\le\iota\le \mathrm{g}} \prod_{p>c_6} \left(1 + \frac{1}{q-1} \frac{\rho_\iota^\dagger(p)}{p^s} \right) H_2(s) \\ &= \prod_{1\le\iota\le \mathrm{g}} \prod_{p>c_6} \left(1 + \frac{\rho_\iota^\dagger(p)}{p^s} \right)^{1/(q-1)} H_3(s).\end{aligned}$$

Then compare

$$1 + \frac{\rho_\iota^\dagger(p)}{p^s}$$

with the corresponding part of the Euler product for the zeta function $\zeta_{\theta^{(\iota)}}(s)$ that consists of the factors related to the linear prime ideal divisors of p over $\mathbb{Q}(\theta^{(\iota)})$, concluding that

$$\mathrm{Z_{II}}(s) = \Big(\prod_{1\le\iota\le \mathrm{g}} \zeta_{\theta^{(\iota)}}(s) \Big)^{1/(q-1)} H_4(s) \tag{35}$$

provided that the analytic continuation of the fractional power into the (cut) domain $\sigma \le 1$ be appropriately defined.

We deduce from (33)–(35) that the principal part of $\mathrm{Z}(s)$ in the neighbourhood of $s = 1$ is

$$\frac{A_2}{(s-1)^{1-\mathrm{g}/(q-1)}} \tag{36}$$

and find by a contour integral method (see, for example, Wilson [9]) that

$$\sum_{P\le y} \rho^*(P) \sim \frac{A_3 y}{\log^{\mathrm{g}/(q-1)} y},$$

since $\mathrm{g}/(q-1) < 1$ by (31) because $\mathrm{g} \le \mathrm{d} < q - 1$. Thus in the first case

$$\Psi_1(x) > \frac{A_4 A_1 X}{\log^{\mathrm{g}/(q-1)} X}. \tag{37}$$

In the other case the polynomial $f(x)$ is a product of two polynomials $f_1(x), f_2(x)$ each of which, being of the type considered under the primary heading, we associate through its subscript i with the notation $\mathrm{d}_i, \mathrm{e}_i, \mathrm{g}_i, \rho_i^*(p)$

for the entities previously described by $\mathrm{d}, \mathrm{e}, \mathrm{g}, \rho^*(p)$. Now, with the present meaning of $\rho(p)$, we have

$$\rho^*(p) = \rho_1^*(p) + \rho_2^*(p) \tag{38}$$

because the non-zero resultant of $f_1(x)$ and $f_2(x)$ is indivisible by p for $p > c_6$, where the function $\mathrm{Z}(s)$ defined in the first line of (33) becomes

$$\prod_{\substack{p \not\equiv 1, \bmod q \\ p > c_6}} \left(1 + \frac{\rho_1^*(p) + \rho_2^*(p)}{p^s}\right) = \prod_{\substack{p \not\equiv 1, \bmod q \\ p > c_6}} \left(1 + \frac{\rho_1^*(p)}{p^s}\right)\left(1 + \frac{\rho_2^*(p)}{p^s}\right) H_5(s)$$
$$= \mathrm{Z}_1(s)\mathrm{Z}_2(s)H_6(s), \quad \text{say.}$$

Hence, if we apply (36) to the two functions $\mathrm{Z}_1(s), \mathrm{Z}_2(s)$, we infer that the principal part of $\mathrm{Z}(s)$ in the neighbourhood of $s = 1$ is

$$\frac{A_5}{(s-1)^{2-(\mathrm{g}_1+\mathrm{g}_2)/(q-1)}}$$

and get

$$\Psi_1(X) > A_6 A_1 X \log^{1-(\mathrm{g}_1+\mathrm{g}_2)/(q-1)} X \tag{39}$$

in the second instance.

Finally, combining (37) and (39) for convenience by setting

$$E = \begin{cases} -\mathrm{g}/(q-1) & \text{when } f(x) \text{ chosen irreducible,} \\ 1 - (\mathrm{g}_1 + \mathrm{g}_2)/(q-1) & \text{when } f(x) \text{ a product of two factors,} \end{cases} \tag{40}$$

we summarize our findings through the inequality

$$\Psi_1(X) > A_7 X \log^E X. \tag{41}$$

7. $F(x)$ has a linear factor—the sum $\Psi_2(x, h)$. We go on to the second element $\Psi_2(X, h)$ of (30), in which we remember that h is bounded. Although there are difficulties in its treatment that necessitate our choosing the polynomial $f(x)$ very carefully, by way of compensation the fact that we now seek upper instead of lower bounds means we no longer have need of functions of type $\mathrm{Z}(s)$ and their analytic properties. Since, as in most of §6, the prime p will always be subject to an inequality $p > c_6$ to ensure the truth of all assertions made, this condition will be assumed to hold throughout this section without its being explicitly stated. In particular, this ruling applies to prime variables of summation and multiplication, it also being clear that the densities of sets of primes are not affected by the inclusion or exclusion of a finite number of their elements.

First, we need an upper bound for a certain product over primes p incongruent to 1, mod q, that parallels the bound (41). In the first case where

$f(x)$ is irreducible, we restate (32), as

$$\rho^*(p) - \frac{1}{q-1}(\rho_1^\dagger(p) + \cdots + \rho_{\mathrm{g}}^\dagger(p)) = \begin{cases} \rho^*(p) & \text{if } p \not\equiv 1, \bmod q, \\ 0 & \text{if } p \equiv 1, \bmod q, \end{cases}$$

in order to shew that

$$\prod_{\substack{p\le y\\ p\not\equiv 1,\bmod q}} \left(1+\frac{\rho^*(p)}{p}\right) = \prod_{p\le y}\left\{1+\frac{\rho^*(p)}{p} - \frac{1}{q-1}\left(\frac{\rho_1^\dagger(p)+\cdots+\rho_{\mathrm{g}}^\dagger(p)}{p}\right)\right\}$$

$$= O\left\{\prod_{p\le y}\left(1+\frac{\rho^*(p)}{p}\right)\prod_{1\le \iota\le \mathrm{g}}\prod_{p\le y}\left(1+\frac{\rho_\iota^\dagger(p)}{p}\right)^{-1/(q-1)}\right\}.$$

Hence, if we use Lemma 1(iii) and the notation (40), we deduce in the first case that

$$\prod_{\substack{p\le y\\ p\not\equiv 1,\bmod q}} \left(1+\frac{\rho^*(p)}{p}\right) = O(\log^{1-\mathrm{g}/(q-1)} y) = O(\log^{1+E} y), \tag{42}$$

which equation remains true in the second case because (38) shews that its left side then equals

$$O\left\{\prod_{\substack{p\le y\\ p\not\equiv 1,\bmod q}} \left(1+\frac{\rho_1(p)}{p}\right)\prod_{\substack{p\le y\\ p\not\equiv 1,\bmod q}} \left(1+\frac{\rho_2^*(p)}{p}\right)\right\} = O(\log^{2-(\mathrm{g}_1+\mathrm{g}_2)/(q-1)} y).$$

Soon we shall encounter certain sets $\mathscr{S}$ of primes p that are said to have positive lower density B. These conform to the asymptotic relation

$$\varliminf_{y\to\infty} \frac{\log y}{y}\sum_{\substack{p\le y\\ p\in\mathscr{S}}} 1 = B \qquad (B>0), \tag{43}$$

from which, by way of the sum

$$\sum_{\substack{p\le y\\ p\in\mathscr{S}}} \frac{1}{p}$$

and partial summation, it follows that

$$\prod_{\substack{p\le y\\ p\in\mathscr{S}}} \left(1+\frac{1}{p}\right) > \log^{B_0} y \tag{44}$$

for any positive number $B_0 < B$ and $y > y_0(B_0)$. This inequality is of course still valid if $\mathscr{S}$ have a density B corresponding to the replacement of the lower limit in (43) by a limit.

To apply the method behind the second part of Lemma 3 to the sums $S^*(h,P)$ in $\Psi_2(X,h)$ we need to shew that $\rho^*(p)$ is greater than 1 for an

adequate lower density of primes p for which $p \not\equiv 1, \bmod q$. This presents some difficulty and is the reason for the complicated way in which the polynomial has to be chosen.

We first suppose that at least one of the irreducible factors $g(x)$ in (29)—namely, one of the $F_i(x)$—has splitting field $\mathbb{S}$ of degree Δ between 2 and d! such that

$$\mathbb{Z} \not\subset \mathbb{S}. \tag{45}$$

Then the number $\rho^*(p)$ of zeros of $g(x), \bmod p$, takes its maximal value d if and only if p split into a product of Δ linear prime ideals over $\mathbb{S}$, the density of such p being $1/\Delta$ by the prime ideal theorem applied to $\mathbb{S}$ ([3]) (see, for example, the comments in the proof of Lemma 6 in [3]). If, in addition, such a prime be congruent to 1, mod q, then p splits totally in $\mathbb{Z}$ and therefore in the normal field $\mathbb{V}$ that is the least field containing $\mathbb{S}$ and $\mathbb{Z}$. Since the degree ∇ of $\mathbb{V}$ exceeds Δ in virtue of (45) and since the density of the last category of primes is $1/\nabla$, we deduce that the density of primes p for which $\rho^*(p) = \mathrm{d}$ and $p \not\equiv 1, \bmod q$, is

$$\frac{1}{\Delta} - \frac{1}{\nabla} > 0,$$

and we succeed in our quest in this instance by taking $f(x)$ to be $g(x)$.

We may therefore suppose that

$$\mathbb{Z} \subset \mathbb{S} \tag{46}$$

for each choice of an irreducible $g(x)$. By Chebotarev's theorem the primes p for which $\rho^*(p) > 1$ have a density whatever polynomial $g(x)$ be chosen. If for some $g(x)$ this density be not less than a number q_1 slightly greater than $1/(q-1)$, then the primes p for which $\rho^*(p) > 1$ and $p \not\equiv 1, \bmod q$, have a lower density not less than

$$q_1 - \frac{1}{q-1} > 0,$$

and again we get what we desire.

On the other hand, if the last assumption fail, then for each $g(x)$, the number of whose zeros, mod p, is denoted temporarily by $\rho'(p)$, we have

$$\sum_{p \le y} \rho'(p) \sim \frac{y}{\log y}$$

by Lemma 1(iii) and therefore

$$\sum_{\substack{p \le y \\ \rho'(p) \ge 1}} 1 + \sum_{\substack{p \le y \\ \rho'(p) \ge 2}} \{\rho'(p) - 1\} \sim \frac{y}{\log y}. \tag{47}$$

([3]) Or by Chebotarev's theorem.

Next, the case $\mathbb{Z} = \mathbb{S}$ in (46) being excluded because $\deg g(x) \le q-2$, the degree of $\mathbb{S}$ over $\mathbb{Q}$ is not less than $2(q-1)$ and the density of p for which $\rho'(p) = \mathrm{d}$ is at most $1/\{2(q-1)\}$. Hence the second sum in (47) is at most

$$(\mathrm{d}-2)\sum_{\substack{p\le y\\ \rho'(p)\ge 2}} 1 + \sum_{\substack{p\le y\\ \rho'(p)=\mathrm{d}}} 1 < \left\{(\mathrm{d}-2)q_1 + \frac{1}{2(q-1)} + o(1)\right\}\frac{y}{\log y}$$

as $y \to \infty$, wherefore the lower density of primes p for which $\rho'(p) \ge 1$ is not less than

$$1 - \left(\mathrm{d} - \frac{3}{2}\right)\frac{1}{q-1} - \delta_3$$

for a small positive number δ_3. This applies to two choices of $g(x)$ that we designate $f_1(x), f_2(x)$ in accordance with earlier notation, the polynomial $f(x)$ being $f_1(x)f_2(x)$. Thus the lower density of primes p for which $\rho_1^*(p) \ge 1$, $\rho_2^*(p) \ge 1$, and $p \not\equiv 1$, mod q, is at least

$$\begin{aligned} 1 - \left(\mathrm{d}_1 - \frac{3}{2}\right)\frac{1}{q-1} - \left(\mathrm{d}_2 - \frac{3}{2}\right)\frac{1}{q-1} - \frac{1}{q-1} - 2\delta_3 \\ = 1 - \frac{(\mathrm{d}_1 + \mathrm{d}_2 - 2)}{q-1} - 2\delta_3 \ge 1 - \frac{q-2}{q-1} - 2\delta_3 > 0 \end{aligned}$$

if q_1 be close enough to $1/(q-1)$. Consequently, since $\rho^*(p) = \rho_1^*(p) + \rho_2^*(p)$, there is a positive lower density of primes p incongruent to 1, mod q, for which $\rho^*(p) > 1$, the proof of our assertion being complete.

From this discussion we gain the result that brings to fruition the estimation of $\Psi(X, h)$ through the ideas behind the proof of Lemma 6 in [3].

Choose $f(x)$ according to the above procedures so that the primes p for which $p \not\equiv 1$, mod q, and $\rho^*(p) > 1$ form a set $\mathscr{S}$ of a positive lower density B. Then

$$\begin{aligned} &\prod_{\substack{p\le y\\ p\not\equiv 1,\,\mathrm{mod}\,q}} \left(1 + \frac{\rho^{*1/2}(p)}{p}\right) \\ &\qquad \le \prod_{\substack{p\le y\\ p\not\equiv 1,\,\mathrm{mod}\,q}} \left(1 + \frac{\rho^*(p)}{p}\right) \prod_{\substack{p\le y\\ p\in\mathscr{S}}} \left(1 + \frac{\rho^*(p)}{\sqrt{2}\,p}\right)\left(1 + \frac{\rho^*(p)}{p}\right)^{-1}, \end{aligned}$$

the multiplicand in the third product being not more than

$$1 - \left(1 - \frac{1}{\sqrt{2}}\right)\frac{\rho^*(p)}{p} + O\left(\frac{1}{p^2}\right) \le 1 - \frac{2-\sqrt{2}}{p} + O\left(\frac{1}{p^2}\right).$$

Hence, by (44) with $B_0 = \frac{1}{2}B$, the third product is seen to be

$$O\Big\{\prod_{\substack{p\le y\\ p\in\mathscr{S}}}\Big(1+\frac{1}{p}\Big)^{\sqrt{2}-2}\Big\} = O(\log^{B(1/\sqrt{2}-1)}y),$$

which in combination with (42) shews that

$$\prod_{\substack{p\le y\\ p\not\equiv 1,\bmod q}}\Big(1+\frac{\rho^{*1/2}(p)}{p}\Big) = O(\log^{1+E-\delta_4}y) \tag{48}$$

for some small positive number δ_4.

The estimation of $\Psi_2(X,h)$ follows sufficiently closely to that of $R(x,h)$ in [3] that we need only indicate the main points of divergence. Hence, adopting the notation of [3] and therefore temporarily abandoning the conventions hitherto used in the present paper, we restrict the numbers k in [3] to be of type P and allow the polynomial $f(x)$ therein to be the $f(x)$ of the present paper so that it is no longer necessarily irreducible, $\rho(p)$ being the present $\rho^*(p)$.

First, defining k_1 and k_2 more or less as before but noting they can be written as P_1 and P_2 because they are of type P (square-free), we note that Lemmata 7 and 8 in [3] are yet valid. Secondly, the bound corresponding to $\sum_2$ is also true, especially as the case related to $\sum_4$ is absent. Thirdly, estimate (8) holds, while (9) stands with the factor (h,k) absent because $0 < h \le 8A_1$ in (30). Then through our equation in (48) above, the sum $\sum_7$ in (11) of [3] becomes

$$O(\log^{1+E-\delta_4}x)$$

and therefore

$$\sum\nolimits_1 = O\{x(\log\log x)^{c_8}\log^{E-\delta_4}x\}$$

with the consequence that

$$R(h,x) = O(x\log^{E-\frac{1}{2}\delta_4}x).$$

Hence, reverting to our current notation, we have

$$\Psi_2(X,h) = O(X\log^{E-\frac{1}{2}\delta_4}X). \tag{49}$$

8. $F(x)$ has a linear factor—final phase. At last we can return to (30), deducing from (49) that

$$\Psi(X) > \frac{1}{8}A_7X\log^E X + O(X\log^{E-\frac{1}{2}\delta_4}X) > \frac{1}{16}A_7X\log^E X > 0$$

for $X > X_0$. Hence there is at least one value of n between $\frac{1}{2}X$ and X for which $F(n)$ is divisible by a number P greater than A_1X, where A_1 can be chosen as large as we wish. Consequently, by the preamble in §3, the

number r in the assumed representation of $F(n)$ by $rg(r,s)$ is divisible by P and thus exceeds A_1X. But this does not agree with inequality $r \le c_3X$ in (2), and we therefore deduce as required that $F(x)$ must have a rational linear factor.

9. Establishment of the first theorem. In proceeding to the first theorem we shall still need the numbers P but with the slight difference that they are now permitted to have small prime divisors. With this understanding, an estimate regarding them is stated as

LEMMA 4. *Let $\tau(y;h,k)$ be the number of integers P not exceeding y that are congruent to $h, \bmod k$, where (h,k) equals 1 or 2. Then*

$$\tau(y;h,k) > y^{1-\epsilon} \qquad (y > y_0(k,\epsilon)).$$

This is similar to but slightly weaker than the analogous Lemma 2.1 in I. Anything sharper being unnecessary here, we adopt a method that avoids recourse to analytic methods involving fractional powers of $s-1$ in the neighbourhood of $s=1$; only a sketch is given because the ideas used are familiar.

In the case where $(h,k)=1$ we only consider odd numbers P' that are of type P. Since 1 is a quadratic residue, mod q, the aggregate of these numbers P' is contained in the set of odd square-free numbers M that are counted with a multiplicity

$$m(M) = \prod_{p|M} \left\{ 1 - \left(\frac{p}{q}\right) \right\} \le 2^{\omega_q(M)},$$

where $\omega_q(M)$ is the number of distinct prime factors of M other than q. Then, forming the analogue

$$\tau'(y;h,k) = \sum_{\substack{M \le y \\ M \equiv 1, \bmod k}} m(M)$$

of $\tau(y;h,k)$, we have first that

$$\tau(y;h,k) > y^{-\epsilon}\tau'(y;h,k) \tag{50}$$

since $d(M) = O(y^\epsilon)$ for $M \le y$.

Next take Dirichlet characters χ, mod k, and set

$$\tau'(y,\chi) = \sum_{M \le y} \chi(M) m(M)$$

with the usual inference that

$$\tau'(y;h,k) = \frac{1}{\phi(k)} \sum_{\chi} \overline{\chi}(h)\tau'(y,\chi).$$

The generating function of $\tau'(y,\chi)$ is then the Dirichlet's series

$$\sum_M \frac{m(M)\chi(M)}{M^s} \qquad (\sigma > 1),$$

which by Euler's theorem is the product

$$\prod_{p\neq 2}\left[1+\frac{\chi(p)}{p^s}\left\{1-\left(\frac{p}{q}\right)\right\}\right]$$

that is seen to equal

$$H_6(s)\prod_{p\neq 2}\left\{1+\frac{\chi(p)}{p^s}\right\}\left\{1-\left(\frac{p}{q}\right)\frac{\chi(p)}{p^s}\right\} = \frac{L(s,\chi')H_6(s)}{L(s,\chi^*)L(2s,\chi')}$$

where χ' is the character, mod q or $2q$, induced by χ, $\chi^*(n) = (n|q)\chi'(n)$, and $H_6(s)$ is a regular non-zero bounded function for $\sigma > 1-2\delta$. This function has a pole at $s=1$ only when χ is principal (even though the denominator might have a pole there for other χ) and we deduce by well-known contour integral methods that

$$\tau'(y;h,k) \sim c(h,k)y \qquad (c(h,k)>0)$$

as $y\to\infty$, from which and (50) the result follows when $(h,k)=1$. If $(h,k)=2$, then the conclusion follows by writing P as $2P'$.

We need a corollary of this proposition in the form of

LEMMA 5. *There are numbers of type P as large as we wish that are congruent to h, mod k, for given co-prime numbers h,k and that have no prime factors less than a given number c_9.*

Form the modulus

$$k' = \prod_{\substack{p\leq c_9\\ p\nmid k}} p$$

and the arithmetical progression of numbers n answering to the congruences $n\equiv h$, mod k, $n\equiv 1$, mod k'. Using this progression in Lemma 4, we get the stated result.

Still assuming Hypothesis P, we first dispose of the special case in which $F(x)$ is of the form

$$D(ax+b)^q, \tag{51}$$

where $(a,b)=1$ and D,a are both positive. Taking the number c_9 in Lemma 5 to exceed both q and $\sqrt[q]{2^{q-1}D}$, we find a number n exceeding X_0 for which $an+b$ is a number P without prime divisors less than c_9 and consider the equation

$$rg(r,s) = D(an+b)^q = DP^q \tag{52}$$

that is soluble in r, s under the condition $0 < s < r$. Here, by the preamble in §3, $P \mid r$ so that $r = Pl$; also, by the first part of (1),

$$r^q \leq 2^{q-1} D P^q$$

and thus $r \leq c_9 P$ with the consequence that $0 < l < c_9$. Therefore

$$lg(lP, s) = DP^{q-1},$$

whence, since P is prime to l and the coefficient q of s^{q-1} in $g(lP, s)$, it follows that $P \mid s$ and $s = Pl_1$, with $0 < l_1 < l$. From this we conclude that

$$D = lg(l, l_1) = (l - l_1)^q + l_1^q$$

and

$$F(x) = \{(l - l_1)(ax + b)\}^q + \{l_1(ax + b)\}^q, \tag{53}$$

which identity expresses $F(x)$ in the expected form (if instead of s we used $r - s$, we would obtain this identity with the terms in reverse order).

For the general case in which (51) does not obtain we shall need the services of a lemma that is essentially due to Bombieri and Pila [1] and that will also be implicitly used in §11 later.

LEMMA 6. *Let $\Psi(u, v)$ be an irreducible polynomial of degree greater than* 1 *with integer coefficients. Then the number of integral solutions of the equation $\Psi(u, v) = 0$ for which $|u|, |v| \leq Q$ is $O(Q^{1/2+\epsilon})$, where the constants implied by the O-notation are independent of the coefficients of $\Psi(u, v)$.*

If $\Psi(u, v)$ be absolutely irreducible and of degree d, then the result is that of Bombieri and Pila, where the exponent can actually be taken as $1/\mathrm{d} + \epsilon$. But, in the opposite case, $\Psi(u, v)$ is a product of absolutely irreducible factors none of which is proportional to a polynomial with rational coefficients. The rational zeros of each factor being also those of one of its non-proportional conjugates and therefore $O(1)$ in number, the estimate remains true.

In the case now under review $F(x)$ can be expressed in the not yet necessarily unique form

$$(ax + b)(A_0 x^{q-1} + \cdots + A_q) = (ax + b)F_1(x), \quad \text{say,} \tag{54}$$

where $(a, b) = 1$ and $a, A_0 > 0$. Associated with this polynomial as thus expressed, there are the discriminant Δ of the second factor and the resultant

$$R = A_0 b^{q-1} - A_1 a b^{q-2} + \cdots + A_q a^{q-1} \tag{55}$$

of both factors, neither of which can yet be asserted to be non-zero. Then, to initiate the demonstration, we shall avail ourselves of any suitable sequence $\mathscr{S}$ of positive numbers n up to a large limit X for which $an + b$ is of type P, the number $t(X)$ of such n being constrained by the inequality

$$t(X) > X^{3/4}. \tag{56}$$

For the time being it is enough to know that Lemma 4 ensures the existence of such a sequence, although later it will be specialized in the light of what emerges.

As the equation

$$(an+b)F_1(n) = rg(r,s) \quad (0<s<r)$$

is always soluble for $n > X_0$, we deduce from the preamble in §3 that for any such $n \in \mathscr{S}$ we have $(an+b) \mid r$ and $r = l(an+b)$ for some positive integer l, whence

$$F_1(n) = lg\{l(an+b), s\}$$

for such an integer l. Yet, by the first part of (1), $D_1(an+b)^q > r^q/2^{q-1}$ for a suitable positive number D_1, and then

$$r < \sqrt[q]{2^{q-1}D_1}\,(an+b)$$

with the implication that

$$0 < l < c_{10} = \sqrt[q]{2^{q-1}D_1}.$$

Hence, for some value l_1 of l in this range, the equation

$$F_1(n) = l_1 g\{l_1(an+b), s\} \quad (0<s<l_1(an+b)) \tag{57}$$

is soluble for at least

$$\frac{1}{c_{10}}\{t(X) - X_0\} > X^{3/5}$$

values of n in $\mathscr{S}$. Also regardless of the first condition in parentheses in (57), it is evident that the primary equation connecting n and s implies that ([4])

$$|s| \le c_{11}n \le c_{11}X \tag{58}$$

because its right-hand side contains the term $l_1 q s^{q-1}$ by (0).

Let us view the polynomial

$$h(u,v) = F_1(u) - l_1 g\{l_1(au+b), v\},$$

which is certainly of degree $q-1 > 1$. Then, by Lemma 6, the number of solutions of (57) in n, s not exceeding the apposite bounds $X, c_{11}X$, respectively, is $O(X^{1/2+\epsilon})$ when $h(u,v)$ is a product of irreducible polynomials of degree at least 2. Therefore from (0) we see that $h(u,v)$ has a linear factor containing v of the type $v - a_1u - b_1$ and we get the identity

$$F_1(u) = l_1 g\{l_1(au+b), a_1u+b_1\} \tag{59}$$

containing rational numbers a_1, b_1. Here, since the case (51) has been excluded, the linear polynomial a_1u+b_1 is not proportional to $au+b$ so that, in particular, a_1 and b_1 are not both zero.

([4]) This apparently superfluous observation will be seen to be needed when we move on to consider qth powers that are not of the same sign.

We shew that the number l_1 is unique. First, if $F_1(u,v)$ denote the form $v^{q-1}F_1(u/v)$ of degree $q-1$, the identity may be expressed as

$$F_1(u,v) = l_1 g\{l_1(au+bv, a_1u+b_1v)\},$$

whence, setting $u=-b$, $v=a$, we find that

$$R = F_1(-b,a) = l_1(ab_1-a_1b)^{q-1}q \neq 0 \tag{60}$$

by (55) and (0). Also, since $l_1 g(\Xi, \mathrm{H})$ transforms into $F_1(u,v)$ by the substitution

$$\Xi = l_1(au+bv), \qquad \mathrm{H} = a_1u+b_1v$$

of modulus $l_1(ab_1-a_1b)$, the discriminants Δ and $-q^{q-2}$ of $F_1(u,v)$ and $g(\Xi,\mathrm{H})$ are seen to be connected by the equation

$$\Delta = -l_1^{(q+1)(q-2)}(ab_1-a_1b)^{(q-1)(q-2)}q^{q-2} \neq 0$$

after a short calculation. This and (60) then imply that ([5])

$$\Delta + l_1^{q(q-2)}R^{q-2} = 0 \tag{61}$$

with the implication that l_1 is unique throughout.

We stress that the truth of the identity (59) is absolute and that it is therefore independent of the process that led to it. If a_1, b_1 therein be not both integers, let I be the least positive integer for which $a_2 = Ia_1, b_2 = Ib_1$ are integers so that $(a_2,b_2)=1$; let also I_1 be the product of the distinct prime divisors p of I. Next, since it is easily verified that each of the congruences

$$ax+b \equiv 0, \bmod p, \qquad a_2x+b_2 \equiv 0, \bmod p,$$

has at most one solution, mod p, there exists a residue class $h_p, \bmod p$, for which

$$ah_p+b \not\equiv 0, \bmod p, \qquad a_2h_p+b_2 \not\equiv 0, \bmod p,$$

when p is odd. But, if $p=2$, the second condition is still met with a suitable residue class $h_2, \bmod 2$, for which ah_2+b may be either odd or even. Hence, if H be a simultaneous solution, mod I_1, of all the congruences

$$H \equiv h_p, \bmod p,$$

pertaining to the prime divisors p of I_1, then

$$(aH+b, I_1) = 1 \text{ or } 2, \qquad (a_2H+b_2, I_1) = 1.$$

Through this number H we now impose on n the condition $n \equiv H$, mod I_1, whereby the numbers $an+b$ belong to the arithmetical progression given by the residue class $aH+b, \bmod aI_1$, in which $(aH+b, aI_1) = (aH+b, I_1) = 1$

([5]) Note that when $q=3$ this becomes $\Delta = -Rl_1^3$, which is what (46) in I should state. Obtained in a different way in I, this equality was expressed there with a mistake in the sign.

or 2. Then, by stipulating that $an+b$ be a number of type P and appealing to Lemma 4 with $h = aH + b, k = aI_1$, we identify the sequence $\mathscr{S}$ needed and observe that its members n adhere to the condition $(a_2n + b_2, I_1) = 1$.

We go back to (57), in which l_1 is still given by (61). For some large n in $\mathscr{S}$ this is valid for an integral value of s, as is the parallel equation

$$F_1(n) = l_1 g\{l(an+b), a_1n + b_1\}$$

in virtue of the identity (59). Consequently, by one of our initial remarks in §3, $a_1n + b_1$ equals either s or $l_1(an+b) - s$ and is therefore a positive integer less than $l_1(an+b)$. But here

$$a_1n + b_1 = \frac{1}{I}(a_2n + b_2) \quad \text{and} \quad (a_2n + b_2, I) = 1,$$

which is impossible when $I > 1$. Therefore (59) is an identity in which a_1, b_1 are integers and in which, moreover, $0 < a_1u + b_1 < l_1(au+b)$ for $u > X_0$. Finally via (54) we conclude that

$$\begin{aligned} F(x) &= l_1(ax+b)g\{l_1(ax+b), a_1x + b_1\} \\ &= \{l_1(ax+b) - a_1x - b_1\}^q + (a_1x + b_1)^q, \end{aligned} \tag{62}$$

in which each linear polynomial is positive for sufficiently large values of x.

We have therefore proved

THEOREM 1. *Suppose that $F(x)$ is a polynomial of prime degree $q > 2$ having the property that $F(n)$ is equal to a sum of two positive integral qth powers for all sufficiently large integers n. Then $F(x)$ is identically the sum of two qth powers of polynomials with integral coefficients (in this case linear or constant) that are both positive for sufficiently large values of x.*

In completing this part of our work we must mention that Hypothesis P must fail if the polynomial $F(x)$ within it have a degree r less than q. Obvious for reasons of density when $r < \frac{1}{2}q$, this assertion is easily substantiated by greatly simplified versions of our methods in which exponential sums are absent. Indeed, unless $r = q - 1$ the basic method behind §5 suffices, while in the exceptional case the argument must be augmented by some of the reasoning in §4. Consequently we may replace Theorem 1 by the slightly stronger

THEOREM 1A. *The conclusion of Theorem* 1 *is still valid if it be merely assumed that the total degree of $F(x)$ does not exceed q.*

10. Two qth powers of either sign. In the study of polynomials $F(x)$ that represent sums of two qth powers of either sign the apposite variant of Hypothesis P to be assumed is

HYPOTHESIS P_1. *The conditions of Hypothesis* P *hold except that* $F(n)$ *is now only supposed to be equal to a sum of two perfect non-zero* q*th powers of any sign.*

A moderate change to our proof of Theorem 1 will suffice to demonstrate that Hypothesis P_1 implies that $F(x)$ is equal to the sum of two qth powers of linear polynomials, especially as the previous treatment was so described that it can be readily adapted for the new situation. Yet near the beginning of the exposition we shall need to look at an extra sum that is akin to one introduced at the corresponding stage in I and that therefore can be passed over in a few words.

The polynomial $F(x)$ still being assumed to have a positive leading coefficient, what was said in the preamble in §3 is still applicable save for (3), the second part of (1), and the inequality $0 < s < r$, the last of which should be replaced by the conditions $s < r$, $s \neq 0$ since in the present context the inequalities $s < 0$ and $s > r$ are equivalent.

On the assumption of Hypothesis P_1, the greatest departure from the previous treatment lies in the way that §4 must be modified in order to secure the irreducibility of $F(x)$. The change begins at equation (14), where the appropriate sum $\Upsilon(X)$ to be considered appertains to the new conditions. Then, bringing in the large enough positive constant c_{12}, we divide $\Upsilon(X)$ into two sums $\Upsilon^*(X)$ and $\Upsilon^\dagger(X)$ that answer, respectively, to the two conditions $-c_{12}r \leq s < r$, $s \neq 0$ and $s < -c_{12}r$.

In the former case

$$c_2 n^q < (r-s)^q + s^q \leq \{(1+c_{12})^2 - c_{12}^2\} r^q$$

so that $n \leq c_{13} r$ in place of (3) but still $r \leq c_3 X$ as in (2). The only alteration in the analysis of the earlier sum $\Upsilon(X)$ needed for that of $\Upsilon^*(X)$ being the change of c_4 into c_{13}, we find as before that

$$\Upsilon^*(X) = o(X).$$

As for $\Upsilon^\dagger(X)$, the condition of summations implies

$$\{(1+c_{12})^2 - c_{12}^2\} r^q < (r-s)^q + s^q \leq c_1 X^q$$

with the result that $r \leq \gamma X$ where γ is as small as required provided that c_{12} was chosen suitably. Then, letting $\Upsilon_r^\dagger(X)$ be the contribution to $\Upsilon^\dagger(X)$ due to a given value of r, we write

$$\Upsilon^\dagger(X) = \sum_{r \leq \gamma X} \Upsilon_r^\dagger(X)$$

and continue by handling $\Upsilon_r^\dagger(X)$ by the method used to estimate $\Theta_r^{(2)}$ in I. At this point, by analogy with I, we encounter the equation

$$2^{q-1} F(n) = r 2^{q-1} m,$$

in which, being of the form

$$g(2r,2s)=\frac{1}{2r}\{(2r-2s)^q+(2s)^q\}=\frac{1}{2r}\{(r+(r-2s))^q+(r-(r-2s))^q\},$$

$2^{q-1}m$ is a polynomial in r and $(r-2s)^2$. The method of utilizing the congruence I (58) being therefore applicable to

$$2^{q-1}F(n)\equiv rg(2r,2s),\ \mathrm{mod}\ p,$$

because a congruence $\Omega^2\equiv a$, mod p, normally has two solutions in Ω, mod p, we find that

$$\Upsilon^{\dagger}(X)<\frac{1}{2}X,$$

by following the analysis of I almost verbatim from (55) therein. Hence $\Upsilon(X)<\frac{3}{4}X$ for $X>X_0$ and thus $F(x)$ is irreducible.

Next, owing to the continued validity of the inequality for $\Psi(X)$ in §8, the methods of §§5–8 establish exactly as before the existence of the rational linear factor of $F(x)$.

In deduction of the theorem, the only alteration in the procedure in §9 is the way in which account is taken of the new constraints on s. First, if $0<s<r$ in (52) as before, then (53) is again valid but, if $s<0$, then $l_1<0$ and (53) presents $F(x)$ identically as a sum of two qth powers of opposite signs. Secondly, it is clear from a brief study of the text that the relaxation of the condition on s does not affect the identity (59). In addition, if (57) were valid for some large n in $\mathscr{S}$ with $0<s<r$, each linear factor in (62) would be positive for large x as previously. But, if instead $s<0$ in (57), then either a_1n+b_1 or $l_1(an+b)-a_1n-b_1$ would be negative because a_1n+b_1 equals either s or $l_1(an+b)-s$. Thus in the latter case the identity (62) emerges in a form in which the qth powers are of opposite signs for large x. We therefore obtain

THEOREM 2. *Suppose that $F(x)$ is a polynomial of prime degree $q>2$ having the property that $F(n)$ is equal to a sum of non-zero perfect qth powers for all sufficiently large integers n. Then $F(x)$ is identically the sum of two qth powers of non-zero polynomials with integral coefficients (in this case, linear or constant), having invariable signs for large x.*

As in Theorem 1A, the conclusion of Theorem 2 is still true if it be merely assumed that the degree of $F(x)$ does not exceed q. But the derivation of this extension is somewhat harder than in the previous case.

We end the section by noting an alternative formulation of Theorem 2. In this we shed the condition that the qth powers in the representation of $F(n)$ be both non-zero and impose instead the requirement that $F(x)$ be not identically a perfect qth power. In the consequential situation when (51) is in place the number D is not a perfect qth power, whence $s\neq 0$ in (52),

$l_1 \neq 0$ and (53) still expresses $F(x)$ in the required way. Yet when (51) does not obtain, $a_1u + b_1$ is not proportional to $au + b$ as was deduced from (59), and again we get (62); here identically it is seen that s does not assume the value zero.

11. Polynomials in several variables that are a sum of two qth powers. Advancing to polynomials in several variables, we generalize Hypothesis P_1 by enunciating

HYPOTHESIS P_2. *$F(x_0, \dots, x_r)$ is a polynomial of degree q with integral coefficients that is not identically the qth power of a linear polynomial with integral coefficients and that has the property that it equals the sum of two perfect qth powers for all integral values of $x_0, \dots, x_r$.*

Then almost as Theorem 3 in I was implied by Theorem 2 there, we can obtain the following theorem from the alternative form of Theorem 2 here that was stated at the end of the previous section.

THEOREM 3. *On Hypothesis P_2 the polynomial $F(x_0, \dots, x_r)$ is identically equal to the sum of two qth powers of linear polynomials in $x_0, \dots, x_r$ with integral coefficients.*

The derivation of this is so similar in detail to the exegesis in §6 of I that we need only indicate the two parts of the treatment that need modification. The first change occurs at the point corresponding to the statement of Lemma 6.1 in I, before which we obtain the identity

$$F(\xi, \boldsymbol{t}) = \{B_0\xi + B_1(\boldsymbol{t})\}^q + \{C_0\xi + C_1(\boldsymbol{t})\}^q \tag{63}$$

in ξ that is the analogue of (68) in I. Now, instead of that lemma, we require the fact that a polynomial $\phi(y)$ of degree q has at most one representation (apart from order) as

$$\lambda(y + \alpha)^q + \mu(y + \beta)^q$$

where $\alpha \neq \beta$ and $\lambda, \mu \neq 0$. This follows from Lemma 6.1 of I by considering the cubic polynomial that is the $(q-3)$th derivative of $\phi(y)$.

The second change is needed at the place where equations (73) and (74) were reached in I. In comparing (63) with the identical polynomial expression

$$a\xi^q + l_1(\boldsymbol{t})\xi^{q-1} + \cdots + l_q(\boldsymbol{t}) \tag{64}$$

for $f(\xi, \boldsymbol{t})$, we can no longer easily use the Hessian of $f(\xi, \boldsymbol{t})$ *qua* polynomial in ξ because this is not a quadratic for $q > 3$. Instead, we use the Hessian of the $(q-3)$th derivative $\partial^{q-3}f(\xi, \boldsymbol{t})/\partial\xi^{q-3}$, which by (63) equals

$$q(q-1)\dots4(B_0C_0)^{q-3}\{B_0C_1(\boldsymbol{t}) - C_0B_1(\boldsymbol{t})\}^2\{B_0\xi + B_1(\boldsymbol{t})\}\{C_0\xi + C_1(\boldsymbol{t})\}$$

and which by (64) also equals a polynomial of the form

$$q_1(\boldsymbol{t})\xi^2 + c_1(\boldsymbol{t})\xi + b_1(\boldsymbol{t})$$

as in I (74). From the equality of these representations we then carry on by the methods of I.

As before, we need only assume that the degree of the polynomial in Hypothesis P_2 does not exceed q.

Acknowledgements. We gratefully acknowledge the support given during the creation of this paper by the Heilbronn Institute in the University of Bristol and by the Welsh Institute of Mathematics and Computational Science.

References

[1] E. Bombieri and J. Pila, *The number of integral points on arcs and ovals*, Duke Math. J. 59 (1989), 337–357.
[2] P. Erdős, *On the sum* $\sum_{k=1}^{x} d(f(k))$, J. London Math. Soc. 27 (1952), 7–15.
[3] C. Hooley, *On the distribution of the roots of polynomial congruences*, Matematika 11 (1964), 39–49.
[4] —, *On polynomials that are sums of two cubes*, Rev. Mat. Complut. 20 (2007), 207–238.
[5] —, *On polynomials that equal binary cubic forms*, Hardy–Ramanujan J. 29 (2006), 1–17.
[6] T. Nagell, *Introduction to Number Theory*, Wiley, New York, 1951.
[7] A. Schinzel, *On the relation between two conjectures on polynomials*, Acta Arith. 38 (1980/81), 285–322.
[8] J. D. Vaaler, *Some extremal functions in Fourier analysis*, Bull. Amer. Math. Soc. (N.S.) 12 (1985), 183–216.
[9] B. M. Wilson, *Proofs of some formulae enunciated by Ramanujan*, Proc. London Math. Soc. (2) 21 (1922), 235–255.

C. Hooley
School of Mathematics
Cardiff University
Senghennydd Road
Cardiff CF24 4AG, Wales, UK

Received on 3.6.2009
and in revised form on 25.2.2010 (6047)