Proc. Indian Acad. Sci. (Math. Sci.), Vol. 97, Nos 1–3, December 1987, pp. 75–84.

On prime representing polynomials

EMIL GROSSWALD

Department of Mathematics, Temple University, Computer Building 038-16, Philadelphia, Pennsylvania 19122, USA

Abstract. A heuristic method is presented to determine the number of primes $p \leqslant x$, represented by an irreducible polynomial $f(n)$, without non-trivial fixed factor ($f(y) \in Z[y]$; $n \in Z$). The method is applied to two specific polynomials and the results are compared with those of the heuristic approach of Hardy and Littlewood.

Keywords. Primes; polynomials.

1. Introduction

In volume 2 of Ramanujan's Notebooks [4], on page 308 we find lists of primes in certain arithmetic progressions. On page 319 of the same Notebook we find actual counts of primes in different arithmetic progressions to the same modulus. In several instances, Ramanujan studies the representation of primes, belonging to given residue classes of certain moduli, as quadratic forms in 2 variables. Hence, Ramanujan considered primes represented by first degree polynomials in one variable and by second degree polynomials in two variables. Did he ever consider the representation of primes by second degree polynomials in one variable, e.g. by $y^2 + 1$? If he ever did, he did not transcribe anything on that topic in his known notebooks. It is at least conceivable that the difficulty of the subject prevented him from obtaining results that he should consider worthwhile recording. In fact, this problem is still unsolved at present and only conjectural results exist. Did Ramanujan ever discuss this matter with Hardy? This we shall, presumably never know, unless some new, at present "lost" documentary evidence appears sometime in the future.

Be that as it may, it is a fact that shortly after Ramanujan's death, Hardy and Littlewood's famous paper appeared on problems of Partitio Numerorum, Part III [2]. In it the number $N(n)$ of primes $p \leqslant n$, of the form $y^2 + 1$ is discussed. As the authors state, they prove no theorem on this subject, not even a conditional one (i.e. one that assumes the validity of some unproved hypothesis). What they come up with, by using the circle method, earlier developed by Hardy and Ramanujan, is a conjectural asymptotic *formula* for $N(n)$. The procedure is formal and error terms are ignored.

This conjectural result is the following:

Denote by $N(n)$ the number of primes $p \leqslant n$ and of the form $p = y^2 + 1$ and set $C = \prod_{p \geqslant 3} (1 - (-1/p)(p-1)^{-1})$; then, as $n \to \infty$,

$$N(n) \simeq C\frac{\sqrt{n}}{\log n} = N_0(n), \quad \text{say.} \tag{$*$}$$

The authors then compare the figures furnished by (*) with the actual count of primes $p = y^2 + 1 \leqslant n$ and find a most satisfactory agreement.

They generalize their approach to arbitrary, irreducible polynomials without fixed divisor and with integer coefficients, but not to such polynomials, which are integral valued, without having necessarily integer coefficients, such as, e.g. $p = \frac{1}{2}y(y+1)+1$. However, by following their method (more specifically, by use of their "Conjecture F" of [2]), it is not difficult to show that, if one now denotes by $N(n)$ the number of primes $p \leqslant n$, of the form $p = \frac{1}{2}y(y+1)+1$, one obtains

$$N(n) \simeq 2C' \frac{\sqrt{n}}{\log n} = N_0(n), \quad \text{say}, \tag{**}$$

where $C' = \lim_{x\to\infty} \prod_{p\leqslant 3} (1 - \chi(p)(p-1)^{-1})$, $\chi(p) = (p/7)$, the Legendre symbol.

In what follows, we take up once more the problem of the number of primes $p = y^2 + 1 \leqslant n$ and the corresponding one for $p = \frac{1}{2}y(y+1)+1$. We shall treat the first one in detail, the second one more briefly.

The present results are also only conjectural, but the method used is entirely different from that of Hardy and Littlewood. While they use the circle method and a weak form of the generalized Riemann hypothesis and then ignore error terms (as already recalled, they explicitly disclaim any proof and only propose a formula), we shall use a sieve method approach and propose a certain conjectural fudge factor, that should compensate for neglected error terms and also another lack of accuracy that will occur. Some numerical computations are made in order to compare the results of the different proposed formulae with actual counts of primes, but these computations are limited and all were performed on a hand calculator, so that third decimals should not be taken too seriously. While this may not be significant, it turns out that, as far as the computations go, the best fit to actual counts is obtained with the fudge factor $c = 1$.

2. Sketch of the method

Let $f(y)$ be a polynomial, integral valued, irreducible, of arbitrary degree and without non-trivial constant divisor, but not necessarily with integer coefficients. If a prime p divides $f(m)$ for a_p values of m modulo p, then the number of integers represented by $f(m)$, with $m \leqslant x$ and such that $p \nmid f(m)$ equals $x - a_p[x/p] - \varepsilon_p$, where ε_p stands for the number of solutions of $f(m) \equiv 0 (\operatorname{mod} p)$ on the segment $p[x/p] < m \leqslant x$: clearly, $0 \leqslant \varepsilon_p \leqslant a_p$. For simplicity and without loss of generality, we shall assume that x is an integer. By the independence of congruences modulo distinct primes, the number of integers $f(m)$ with $m \leqslant x$, such that no prime $p \leqslant z$ divides $f(m)$ equals

$$x \prod_{p \leqslant z} \left(1 - \frac{a_p}{x}[x/p] - \frac{\varepsilon_p}{x}\right) = x \prod_{p\leqslant z} \left(1 - \frac{a_p}{p} + \delta_p\right), \tag{1}$$

where $|\delta_p| \leqslant a_p/x$. In particular, if $z = \sqrt{f}(x)$, then this sieving process leaves, in principle all (and only) primes represented by $f(m)$, $m \leqslant x$, except that those primes $f(m)$ that are less than z will also have been wrongly removed. It will follow from an easy extension of the present considerations (see especially formulae (5′) and (10)) that, if $f(m)$ is of degree h and $f(x)=n$, then our conjecture implies in particular that the number of those wrongly eliminated primes does not exceed a constant multiple of $n^{1/2h}/\log n$, which is negligible with respect to the principal term of order $n^{1/h}/\log n$. One observes, however, that formally even larger primes, up to $f(x)/2$ may be considered. In fact, even if $[x/p]=0$, in general $\delta_p \neq 0$ and the factor $1+\delta_p$ may affect the product. If we select z so that $\sqrt{f(x)} \leqslant z \leqslant f(x)/2$, the number of $f(m)$ that are primes does not change and (1) appears to remain valid, but the value of the product changes. This vagueness in the selection of z has been pointed out already by Hardy and Littlewood (see [2, p. 37, footnote 1]). Finally, the δ_p's, if taken in absolute value, lead to an error term that swamps the main term. In fact, however, the δ_p's are not of constant sign and it is highly unlikely that the true error term is of an order as high as that of the principal term, but no proof of this conjecture is known.

In what follows we shall ignore the δ_p's and choose $z=(f(x))^{\alpha/2}$. It will turn out that z enters the formula for the number $\tilde{N}(x)$ of primes represented by $f(m)$ with $m \leqslant x$ in the form of a factor $1/\log z = 2/(\alpha \log f(x))$. Hence, the choice of α translates into a multiplicative coefficient α^{-1}, independent of x, for the formula of $\tilde{N}(x)$. We shall make the following *Conjecture*: For every polynomial there exists a fudge factor c, independent of x, such that, if we ignore the δ_p's and take $z=\sqrt{f(x)}$, then $\tilde{N}(x)$ is asymptotically equal to $cx\prod_{p\leqslant z}(1-a_p/p)$.

In some respect it is more satisfactory to ask for the number $N(n)$ of primes represented by $f(m)$, when $f(m)\leqslant n$. It is clear that, if $f(x)=n$, then $\tilde{N}(x)=N(n)$.

Concerning the fudge factor, it is worthwhile to recall that some such non-trivial fudge factors are in fact needed and are well known. Let us consider, e.g. the polynomial $f(y)=y$. In this case, $a_p=1$ for all primes. If in (1) we set $a_p=1$, ignore the δ_p's and take $z=\sqrt{x}$, we obtain

$$\tilde{N}(x)=N(n)\simeq cx\prod_{p\leqslant\sqrt{x}}(1-p^{-1})\simeq cx\frac{e^{-\gamma}}{\log\sqrt{x}}\simeq 2ce^{-\gamma}(x/\log x)=2ce^{-\gamma}(n/\log n).$$

By the prime number theorem we know that $N(n)\simeq n/\log n$; hence, the formula yields the correct result only if we use the fudge factor $c=e^{\gamma}/2\simeq 0{\cdot}8905\ldots\neq 1$.

3. A conjectural theorem

On the basis of the preceding discussion, we state the following

Conjectural Theorem. Let $f(y)$ be an irreducible polynomial, integral-valued and without non-trivial constant divisor, but not necessarily with integer coefficients. Then the number $\tilde{N}(x)$ of primes represented by $f(m)$, $m\in\mathbb{Z}$, $0\leqslant m\leqslant x$, satisfies

$$\tilde{N}(x)\simeq cx\prod_{p<\sqrt{f(x)}}\left(1-\frac{a_p}{p}\right), \tag{2}$$

where c is a fudge factor, independent of x, but which may depend on the polynomial $f(y)$. Also, if $f(x)=n$, then the number of primes not exceeding n and represented by

$f(m)$, $m\in\mathbb{Z}$, is given by

$$N(n) \simeq cx_0 \prod_{p\leqslant\sqrt{n}} \left(1-\frac{a_p}{p}\right), \tag{2'}$$

where x_0 is the solution of $f(x_0)=n$. (This solution is unique for sufficiently large n; if ay^h is the leading term of $f(y)$, then $x_0 \simeq (n/a)^{1/h}$).

The problem arises as to how to determine the value of the factor c. One approach is to consider formulae for $N(n)$ obtained by other considerations (even if only conjectural ones) and then identify them with (2'). Another approach is to compare the numerical results of the conjectured formulae, with actual counts of the primes up to n, represented by $f(y)$. Finally, one may brazenly ignore all inaccuracies and consider (2), or (2'), without any fudge factor, i.e. with $c=1$.

From here on we shall consider only the case of quadratic polynomials (i.e. $h=2$) and, in fact, restrict ourselves to two specific ones, $f(y)=y^2+1$ and $f(y)=1+y(y+1)/2$.

4. The polynomial $f(y)=y^2+1$

Let $x\in\mathbb{Z}$ be large. For odd integer m, $2|(m^2+1)$, so that m^2+1 can be prime only for $m=1$, or for m even. There are $[x/2]+1=(x/2)+1-\varepsilon_2(\varepsilon_2=0$, or $1/2)$ such values $m\leqslant x$. For p odd, $m^2+1\equiv 0 \pmod p$ is possible only for $p\equiv 1 \pmod 4$; therefore, $a_p=0$ for $p\equiv 3 \pmod 4$. On the other hand, if $p\equiv 1 \pmod 4$, then there exist 2 values of $m \pmod p$, such that $m^2+1\equiv 0 \pmod p$; hence, $a_p=2$ for $p\equiv 1 \pmod p$. Formula (2) becomes

$$\tilde{N}(x) \simeq c\frac{x}{2} \prod_{\substack{p\leqslant x\\ p\equiv 1 \pmod 4}} \left(1-\frac{2}{p}\right). \tag{3}$$

We proceed to estimate the product in (3). All congruences without indication of a modulus are understood modulo 4 (in this section only).

$$\prod_{\substack{p\leqslant x\\ p\equiv 1}} \left(1-\frac{2}{p}\right) = \prod_{\substack{p\leqslant x\\ p\equiv 1}} \left(1-\frac{1}{p}\right)^2 \frac{1-2p^{-1}}{(1-p^{-1})^2} = \prod_{\substack{p\leqslant x\\ p\equiv 1}} \left(1-\frac{1}{p}\right)^2 \prod_{\substack{p\leqslant x\\ p\equiv 1}} \left(1-\frac{1}{(p-1)^2}\right).$$

As $x\to\infty$, the last product converges to a constant, say $A=\prod_{p\equiv 1}(1-(p-1)^{-2}) \cong 0{\cdot}927\ldots$ and (3) becomes

$$\tilde{N}(x) \simeq \frac{c}{2} Ax \prod_{\substack{p\leqslant x\\ p\equiv 1}} \left(1-\frac{1}{p}\right)^2.$$

It may be shown (see [1]) that

$$\prod_{\substack{p\leqslant x\\ p\equiv 1}} \left(1-\frac{1}{p}\right)^2 \simeq \frac{8e^{-\gamma}}{\pi} B(\log x)^{-1},$$

where B stands for the convergent infinite product $\prod_{p\equiv 3}(1-p^{-2})^{-1}$. This constant appears in some work of Landau (see [3]). Its value is about 1·1680... We have obtained

$$\tilde{N}(x) \simeq c\frac{4e^{-\gamma}}{\pi}AB\frac{x}{\log x}. \tag{4}$$

Formula (4) can be simplified. In what follows, ratios of semi-convergent, or even divergent products will occur; the ratios themselves will converge. A correct writing is $\lim_{x\to\infty}\{\prod_{\substack{p<x\\ \cdots}}(\cdots)/\prod_{\substack{p\leq x\\ \cdots}}(\cdots)\}$. To avoid this cumbersome writing, this notation will be suppressed, although that will make the intermediate expressions formally invalid.

The constant A may be rewritten as follows:

$$A = \prod_{p\equiv 1}(1-(p-1)^{-1})\prod_{p\equiv 1}(1+(p-1)^{-1})$$

$$= \prod_{p\equiv 1}(1-(p-1)^{-1})\prod_{p\equiv 3}(1+(p-1)^{-1})\frac{\prod_{p\equiv 1}(1+(p-1)^{-1})}{\prod_{p\equiv 3}(1+(p-1)^{-1})}$$

$$= \prod_{p\geq 3}\left(1-\frac{(-1/p)}{p-1}\right)\frac{\prod_{p\equiv 1}\frac{p}{p-1}}{\prod_{p\equiv 3}\frac{p}{p-1}} = C\frac{\prod_{p\equiv 3}(1-p^{-1})}{\prod_{p\equiv 1}(1-p^{-1})} = C\lim_{x\to\infty}\frac{\prod_{p\leq x, p\equiv 3}(1-p^{-1})}{\prod_{p\leq x, p\equiv 1}(1-p^{-1})}.$$

Here C stands for the semiconvergent product $\prod_{p\geq 3}(1-(-1/p)(p-1)^{-1})$. As $x\to\infty$, the last ratio is known to approach the constant $\pi/4B$ (see [1]), so that $A = \pi C/4B$ and $4AB/\pi = C$. It follows that (4) may be written simply as

$$\tilde{N}(x) \simeq ce^{-\gamma}C\frac{x}{\log x}. \tag{5}$$

If we replace x by n as a variable, where $n = x^2+1$, then (5) becomes

$$N(n) \simeq c\cdot 2e^{-\gamma}C\frac{\sqrt{n}}{\log n}. \tag{5'}$$

As already mentioned, Hardy and Littlewood [2] have obtained the conjectural formula

$$N(n) \simeq C\frac{\sqrt{n}}{\log n} = N_0(n) \tag{5''}$$

by an entirely different approach. This suggests that we take the fudge factor $c = e^{\gamma}/2$. For reasons that will become clear immediately, it is worthwhile to consider also

$$N(n) \simeq C_1\frac{\sqrt{n}}{\log n}, \quad \text{with} \quad C_1 = 2e^{-\gamma}C, \tag{5'''}$$

i.e. (5′) with fudge factor $c = 1$. We shall denote the second member of (5‴) by $N_1(n)$.

5. Numerical comparisons

It may be worthwhile to compare the numerical results of (5″) and of (5‴), i.e. of (5′) with the fudge factors $c = e^{\gamma}/2$ and $c = 1$, respectively, with the actual counts of primes. In the computation we use the value $C = 1{\cdot}378\ldots$ It is easier and more accurate to compute C by the formula $C = 4AB/\pi$, than by its defining, very slowly converging product, because A and B are given by relatively fast converging products, which lead to $A = 0{\cdot}927\ldots$ and $B = 1{\cdot}1680\ldots$ If $c = 1$, the constant becomes $C_1 = 2e^{-\gamma}C = 1{\cdot}546\ldots$ In computing table 1, the values of $N_0(n) = C\sqrt{n}/(\log n)$ and of $N_1(n) = C_1\sqrt{n}/(\log n)$ were computed to two decimal places and those values were used in the computation of the ratios $N(n)/N_0(n)$ and $N(n)/N_1(n)$, where $N(n)$ stands for the actual number of primes represented by $m^2 + 1$, with $m^2 + 1 \leqslant n$. In the listings of the $N_0(n)$ and $N_1(n)$, however, the figures have been rounded off to the nearest integer. For that reason the ratios $N(n)/N_0(n)$ and $N(n)/N_1(n)$ computed with the tabulated figures will, in general, differ from the listed ratios.

In [2] one finds on pp. 43–44 a lengthy argument, why, for numerical comparisons of the present kind, the simple asymptotic formulae, like (5), (5′), etc. should be replaced by others, less simple ones, unless one computers these tabulations for very large values of n (when the difference between the two asymptotic formulae becomes irrelevent). The idea is that some of the terms used in the simple formulae are just the leading terms of asymptotic expansions and that the second (and perhaps even the third) terms of those expansions are by no means negligible with respect to the main term—at least for the moderate values of n, likely to be used. Be that as it may, the tabulation does not suggest at all a convergence of the ratios towards unity, but seems to oscillate in the case of (5″) around the simple constant 4/3. Also in the case of (5‴), the ratio $N(n)/N_1(n)$ seems to stay close to 7/6, rather than converge towards unity. Without any theoretical justification and only for illustrative purposes, we add in table 1 also a column $N_2(n)$, with the entries obtained by using in (5″), instead of C, the constant $C_2 = \frac{4}{3}C$ and $N_3(n)$, where the constant $C_3 = \frac{7}{6}C_1$ has been used. Perhaps the fudge factor c should be $7/6(= 1{\cdot}1666\ldots)$, rather than $e^{\gamma}/2(= 0{\cdot}89\ldots)$, or even $c = 1$?

Table 1. Comparison of formula with empirical results for $y^2 + 1$.

n	$\sqrt{n}/\log n$	$N(n)$	$N_0(n)$	$N(n)/N_0(n)$	$N_1(n)$	$N(n)/N_1(n)$	$N_2(n)$	$N_3(n)$	$N(n)/N_3(n)$
10000	10·8	19	15	1·28	17	1·14	20	19	0·975
20000	14·3	26	20	1·32	22	1·18	25	26	1·008
30000	16·8	30	23	1·30	26	1·16	31	30	0·990
40000	18·9	33	26	1·27	29	1·13	35	34	0·968
50000	20·7	36	29	1·26	32	1·125	38	37	0·964
60000	22·2	40	31	1·31	34	1·17	41	40	0·999
70000	23·7	44	33	1·35	37	1·20	44	43	1·029
80000	25·1	46	35	1·33	39	1·19	47	45	1·016
90000	26·3	47	36	1·30	41	1·16	48	47	0·991
100000	27·5	50	38	1·32	43	1·18	51	50	1·008

6. The polynomial $f(y) = 1 + y(y+1)/2$

Clearly, $2f(m) = m^2 + m + 2$ can be a prime only for $m = 0$, because, for $m \in \mathbb{Z}, f(m)$ is even. We therefore consider $f(y)$, which is integral valued, but does not have integer coefficients. For $m \equiv 1 \pmod 4$ $m \equiv 2 \pmod 4$, $f(m)$ is even; therefore, in order to have $f(m)$ prime, we must take $m \equiv 0$, or $m \equiv 3 \pmod 4$. The number of such integers $m \leqslant x$ is asymptotically equal to $x/2$.

For p odd, $8f(m) = 4m^2 + 4m + 8 = (2m+1)^2 + 7$; hence, $f(m) \equiv 0 \pmod p$ if and only if $u^2 \equiv -7 \pmod p$ has solutions, i.e. precisely when $(-7/p) = 1$. By the quadratic reciprocity law, $(-7/p) = (p/7) = 1$ restricts p to the residue classes 1, 2, or 4 modulo 7. The Legendre symbol $(n/7)$ is the non-principal real character $\chi(n)$ modulo 7. We conclude that in (2)

$$a_p = \begin{cases} 2 & \text{if} \quad p \equiv 1, 2, \quad \text{or} \quad 4 \text{ modulo } 7, \; p \geqslant 3, \\ 1 & \text{if} \quad p = 2, \\ 0 & \text{if} \quad p \equiv 3, 5, \quad \text{or} \quad 6 \text{ modulo } 7. \end{cases}$$

Formula (2) now becomes

$$\tilde{N}(x) \simeq c\frac{x}{2} \prod_{\substack{\chi(p)=1 \\ 3 \leqslant p \leqslant z}} \left(1 - \frac{2}{p}\right) \tag{6}$$

where $z = x/\sqrt{2}$.

We proceed to compute the product in (6), just as we did with a similar product in § 4.

$$\begin{aligned} \prod_{\substack{\chi(p)=1 \\ 3 \leqslant p \leqslant z}} (1 - 2p^{-1}) &= \prod_{\substack{\chi(p)=1 \\ 3 \leqslant p \leqslant z}} (1 - p^{-1})^2 \frac{1 - 2p^{-1}}{(1 - p^{-1})^2} \\ &= \prod_{\substack{\chi(p)=1 \\ 3 \leqslant p \leqslant z}} (1 - p^{-1})^2 \prod_{\substack{\chi(p)=1 \\ 3 \leqslant p \leqslant z}} (1 - (p-1)^{-2}). \end{aligned}$$

For $x \to \infty$, also $z \to \infty$ and the second product converges to a constant, say $A = 0{\cdot}983\ldots$ As for the first one, it follows from results in [1] that

$$\prod_{\substack{\chi(p)=1 \\ 3 \leqslant p \leqslant x/\sqrt{2}}} (1 - p^{-1})^2 \simeq k_1^2/\log x, \quad \prod_{\substack{\chi(p)=-1 \\ p \leqslant x/\sqrt{2}}} (1 - p^{-1})^2 \simeq k_{-1}^2/\log x, \tag{7}$$

where

$$\begin{aligned} k_1^2 &= \tfrac{14}{3} e^{-\gamma} L(1,\chi)^{-1} \prod_{\chi(p)=-1} (1 - p^{-2})^{-1}, \\ k_{-1}^2 &= \tfrac{7}{6} e^{-\gamma} L(1,\chi) \prod_{\chi(p)=-1} (1 - p^{-2}), \end{aligned} \tag{8}$$

so that

$$k_{-1}/k_1 = \tfrac{1}{2} L(1,\chi) \prod_{\chi(p)=-1} (1 - p^{-2}). \tag{9}$$

For $\chi(p)=(p/7)$ it may be shown (see [3]) that

$$L(1,x)=\frac{\pi}{2\left(-\sin\frac{\pi}{7}+\sin\frac{2\pi}{7}+\sin\frac{3\pi}{7}\right)}=1{\cdot}18741\ldots$$

Also,

$$\prod_{\chi(p)=-1}(1-p^{-2})^{-1}=1{\cdot}1900\ldots$$

It follows that $\tilde{N}(x)\simeq(c/2)Ak_1^2x/\log x$. Next, if $1+x(x+1)/2=n$, then $x\simeq\sqrt{2n}$ and, passing from $\tilde{N}(x)$ to $N(n)$, we find

$$N(n)\simeq c\sqrt{2}Ak_1^2\frac{\sqrt{n}}{\log n}. \tag{10}$$

This can still be simplified, as was done for $f(y)=y^2+1$. We use once more the simplified writing, when dealing with semiconvergent, or divergent products. We have

$$\begin{aligned}A&=\prod_{\substack{\chi(p)=1\\ p\geqslant 3}}(1-(p-1)^{-2})\\ &=\prod_{p\geqslant 3}(1-\chi(p)(p-1)^{-1})\left\{\prod_{\substack{\chi(p)=1\\ p\geqslant 3}}(1+(p-1)^{-1})\Big/\prod_{\chi(p)=-1}(1+(p-1)^{-1})\right\}.\end{aligned}$$

The first factor converges (conditionally) to a constant $C'=1{\cdot}970\ldots$ After obvious transformations, the second factor is seen to be equal to

$$\lim_{x\to\infty}\left\{\prod_{\substack{\chi(p)=-1\\ p\leqslant x}}(1-p^{-1})\Big/\prod_{\substack{\chi(p)=1\\ 3\leqslant p\leqslant x}}(1-p^{-1})\right\}=k_{-1}/k_1,$$

where we have used (7). By (9) this ratio equals $\frac{1}{2}L(1,\chi)\prod_{\chi(p)=-1}(1-p^{-2})$, so that

$$A=\tfrac{1}{2}C'L(1,\chi)\prod_{\chi(p)=-1}(1-p^{-2}). \tag{11}$$

The constant in (10) becomes

$$c\frac{\sqrt{2}}{2}C'L(1,\chi)\prod_{\chi(p)=-1}(1-p^{-2})k_1^2=c\frac{7\sqrt{2}}{3}e^{-\gamma}C',$$

where we made use of (8).

We have completed the proof of

$$N(n)\simeq K\frac{\sqrt{n}}{\log n}, \tag{12}$$

where $K=c(7\sqrt{2}/3)e^{-\gamma}C'\simeq 3{\cdot}65c$.

According to (**), $K=2C'\simeq 3{\cdot}94\ldots$, the second member of (12), obtained with this constant will be denoted by $N_0(n)$. We also consider in (12) the value K_1 of K, obtained with $c = 1$, i.e. $K_1 \simeq 3{\cdot}65$ and denote the corresponding value of $N(n)$ by $N_1(n)$. Finally, we consider the fudge factor $c = e^\gamma/2 \simeq 0{\cdot}8905\ldots$, which was valid for $f(y) = y$ and (perhaps) for $f(y) = y^2 + 1$; this leads to $K_2 \simeq 3{\cdot}25$ and we denote the corresponding value of $N(n)$ by $N_2(n)$. If we want to identify $K = K_0$ of (12) with the presumed coefficient $2C'$ of Hardy and Littlewood, in $N_0(n)$, then we have to take

$$c = \frac{3\sqrt{2}}{7}e^\gamma = \frac{6\sqrt{2}}{7}(e^\gamma/2) \simeq 1{\cdot}212\ldots(e^\gamma/2) \simeq 1{\cdot}079\ldots$$

rather than $c = e^\gamma/2 \simeq 0{\cdot}8905\ldots$, or $c = 1$.

As in the case of $f(y) = y^2 + 1$, we tabulate the values of (12) (see table 2) obtained with K_0, K_1 and K_2 and compare them with the values $N(n)$, the true number of primes not in excess of n, represented by $f(m)$. As previously, the value $C' \simeq 1{\cdot}970\ldots$ has been computed by use of (11), rather than by the direct evaluation of the defining infinite product, which converges only conditionally and very slowly. The three indicated values of c are too close, to make a significant difference for $n \leqslant 100{,}000$.

We recall that in table 2 the values of the $N_i(n)$ have been rounded off to the nearest integer, while the ratios have been computed with the values furnished by formula (12), with the respective coefficients K_i $(i = 0, 1, 2)$, rounded off to two decimal places.

It appears that the formula that yields the results closest to the true count is obtained by taking the trivial fudge factor $c = 1$ in both cases, $f(y) = y^2 + 1$ and $f(y) = \frac{1}{2}y(y + 1) + 1$.

But one should not be overly impressed by the good fit of the formulae with $c = 1$; as pointed out by Hardy and Littlewood, such considerations can easily be misleading. As long as, e.g. $(\log n)^{-2}$ is not entirely negligible with respect to $(\log n)^{-1}$, one ought to be skeptical. While no amount of computation can decide the validity of any asymptotic formula, more extensive and more accurate computations seem desirable.

At this point it may be worthwhile to recall that in [2; pp. 34–36], Hardy and Littlewood show for the Goldbach problem that, if a formula obtained by sieve methods has the same general structure as one obtained by the circle method, then the constant coefficient can only be the one obtained by the circle method. This reasoning is not immediately applicable to the present situation, but the result of

Table 2. Comparison of formula with empirical results for $\frac{1}{2}y(y + 1) + 1$.

n	$n/\log n$	$N(n)$	$N_0(n)$	$N(n)/N_0(n)$	$N_1(n)$	$N(n)/N_1(n)$	$N_2(n)$	$N(n)/N_2(n)$
10000	10·86	40	43	0·935	40	1·009	35	1·133
20000	14·28	50	56	0·889	52	0·959	46	1·077
30000	16·80	61	66	0·922	61	0·995	55	1·117
40000	18·87	67	73	0·913	69	0·973	61	1·092
50000	20·67	73	81	0·896	75	0·968	67	1·087
60000	22·26	78	88	0·889	81	0·960	72	1·078
70000	23·72	85	93	0·909	87	0·982	77	1·103
80000	25·05	91	99	0·922	91	0·995	81	1·118
90000	26·30	94	104	0·907	96	0·979	85	1·065
100000	27·47	101	108	0·933	100	1·007	89	1·134

Hardy and Littlewood may have a more general validity than for the Goldbach problem alone. If one could show its validity in the present case, then $N_1(n)$ is the correct asymptotic value for both polynomials here considered, regardless of the better fit of $c = 1$ for "small" values of n.

References

[1] Grosswald E, Some number theoretic products (to appear); see also *Notices of the Am. Math. Soc.* **7** (1986) p. 374

[2] Hardy G H and Littlewood J E, Partitio Numerorum III — *Acta Math.* **44** (1923) 1–70

[3] Landau E, *Die Lehre von der Verteilung der Primzahlen* (New York: Chelsea Pub. Co.) 2nd edn (1953)

[4] Ramanujan's *Notebooks* (Bombay: Tata Institute of Fundamental Research) Photostatic edition in 2 volumes (1959)