On choisit m de sorte que $mx = t$ s'écrive $\sum_{0}^{\infty} p_k \theta_k$, $p_k \in \mathbf{Z}$. Alors la limite en question vaut, grâce au lemme 2, $(-1)^{\sum_{k\geqslant 0} p_k} \prod_{1}^{\infty} J_{p_k}(2\pi t \eta_k)$. Nous utiliserons le lemme:

LEMME 3. *Quel que soit ε positif et quelle que soit la partie dénombrable D de $\mathbf{R}$ il existe une suite $(\eta_k)_{k\geqslant 1}$ de nombres réels telle que pour tout entier k, tout entier p et tout élément non nul t de D, $J_p(t\eta_k) \neq 0$.*

Soit, en effet, $\Delta(p, t)$ l'ensemble des x réels tels que $J_p(tx) = 0$. Puisque J_p est une fonction entière, $\Delta(p, t)$ est dénombrable et il en est de même de $\Delta = \bigcup_{\substack{p\geqslant 0 \\ 0\neq t\in D}} \Delta(p, t)$. Il suffit de choisir une suite $(\eta_k)_{k\geqslant 1}$ tendant assez rapidement vers 0 pour que $\sum_{k\geqslant 1} |\eta_k| \leqslant \varepsilon$ mais dont les termes n'appartiennent pas à l'ensemble dénombrable Δ ce qui est possible.

Les η_k étant ainsi choisis, lorsque $D = 2\pi \mathscr{A}$, le produit infini $\prod_{1}^{\infty} J_{p_k}(2\pi t \eta_k)$ est convergent et n'est donc pas nul si $t \in \mathscr{A}$.

Travaux cités

[1] M. Mendès-France, *Deux remarques concernant l'équirépartition des suites*, Acta Arith. 14 (1968), p. 163–167.

[2] Y. Meyer, *Nombres algébriques et répartition modulo* 1, C. R. Acad. Sc., Paris, 268 (1969), p. 25–27.

Reçu par la Rédaction le 31. 3. 1969

ACTA ARITHMETICA
XVI (1970)

On the distribution of prime numbers which are of the form x^2+y^2+1

by

YOICHI MOTOHASHI (Tokyo)

1. In 1957 Hooley [2] proved under the extended Riemann Hypothesis the asymptotic formulae for the sums

$$\sum_{p\leqslant N} r(p-a), \qquad \sum_{p<N} r(N-p), \tag{1.1}$$

where a is a fixed non-zero integer and p denotes generally a prime number and further $r(n)$ is the number of representations of n as the sum of two squares.

After Hooley's very interesting proof, in 1960 Linnik [4] proved rigorously these asymptotic formulae applying his very powerful "Dispersion Method". Therefore the longstanding conjecture of Hardy and Littlewood is completely proved.

On the other hand the large sieve method which is created by Linnik is recently astonishingly improved by Bombieri [1], and the extended Riemann Hypothesis which was used by Hooley can be replaced by the mean-value theorem for the remainder terms of the prime number theorem in an arithmetical progression.

Now from the asymptotic formula for the sum (1.1) we can conclude that there are infinitely many prime numbers which are of the form x^2+y^2+1. Then, how many such prime numbers are there up to N? This is the problem that we will treat in this paper.

Let $b(n) = 1$ if n is representable as the sum of two squares, and $= 0$ otherwise. Then the following asymptotic formula of Landau

$$\sum_{n\leqslant N} b(n) \sim \frac{1}{\sqrt{2}} \prod_{p\equiv -1 \,(\mathrm{mod}\, 4)} \left(1-\frac{1}{p^2}\right)^{-1/2} N(\log N)^{-1/2} \tag{1.2}$$

is a well known result. Hence our problem is to study the behaviour of the sum

$$I(N) = \sum_{p\leqslant N} b(p-1),$$

and it is natural from the result (1.2) to expect the asymptotic formula

$$I(N) \sim \mathfrak{S}N(\log N)^{-3/2}, \tag{1.3}$$

where $\mathfrak{S}$ is an absolute constant. Unfortunately we can not prove this, and really this seems very deep. In the last paragraph we will state this conjecture more precisely.

We will prove only the lower estimate of $I(N)$, and by the familiar assertion this can be reduced to the upper estimate of the sum

$$\sum_{p\leqslant N} r^2(p-1).$$

For this sake we must study the behaviour of the sum

$$R(N;\, q, l) = \sum_{\substack{n\equiv l \,(\mathrm{mod}\, q)\\ n\leqslant N}} r^2(n).$$

Namely we must prove the uniformity of the value $r(n)$ in an arithmetical progression, and actually this can be done by the large sieve method.

2. Let χ_q be a character modulo q and ϱ be the non-principal character modulo 4. Further let $R(s, \chi_q)$ be the Dirichlet series

$$\sum_{n=1}^{\infty} r^2(n)\chi_q(n)n^{-s} \qquad (s = \sigma+it),$$

which converges absolutely for $\sigma > 1$.

Let $r(n)/4 = T(n)$, then it is well-known that $T(n)$ is a multiplicative function and has the property

$$T(p^u) = \begin{cases} 1 & \text{for } p = 2,\\ u+1 & \text{for } p\equiv 1 \ (\mathrm{mod}\ 4),\\ 1 & \text{for } p\equiv -1 \ (\mathrm{mod}\ 4) \text{ and even } u,\\ 0 & \text{for } p\equiv -1 \ (\mathrm{mod}\ 4) \text{ and odd } u.\end{cases}$$

Hence we have

$$\begin{aligned}\tfrac{1}{16}R(s,\chi_q) &= \prod_p \Big\{1+\sum_{u=1}^{\infty}\chi_q(p^u)T^2(p^u)p^{-us}\Big\}\\ &= \big(1-\chi_q(2)2^{-s}\big)^{-1}\prod_{p\equiv -1\,(\mathrm{mod}\,4)}\big(1-\chi_q^2(p)p^{-2s}\big)^{-1}\times\\ &\qquad\times\prod_{p\equiv 1\,(\mathrm{mod}\,4)}\Big\{1+\sum_{u=1}^{\infty}(u+1)^2\chi_q^u(p)p^{-us}\Big\}\\ &= \big(1-\chi_q(2)2^{-s}\big)^{-1}\times\\ &\times\prod_{p\equiv 1\,(\mathrm{mod}\,4)}\big(1+\chi_q(p)p^{-s}\big)\big(1-\chi_q(p)p^{-s}\big)^{-3}\prod_{p\equiv -1\,(\mathrm{mod}\,4)}\big(1-\chi_q^2(p)p^{-2s}\big)^{-1},\end{aligned} \tag{2.1}$$

since

$$\sum_{u=0}^{\infty}(u+1)^2x^u = (1+x)(1-x)^{-3} \qquad (|x|<1).$$

On the other hand

$$\begin{aligned}&L^2(s,\chi_q)L^{-1}(2s,\chi_q^2)\\ &\quad = \big(1+\chi_q(2)2^{-s}\big)\big(1-\chi_q(2)2^{-s}\big)^{-1}\prod_{p>2}\big(1+\chi_q(p)p^{-s}\big)\big(1-\chi_q(p)p^{-s}\big)^{-1}\end{aligned}$$

and

$$L^2(s,\varrho\chi_q) = \prod_{p\equiv 1\,(\mathrm{mod}\,4)}\big(1-\chi_q(p)p^{-s}\big)^{-2}\prod_{p\equiv -1\,(\mathrm{mod}\,4)}\big(1+\chi_q(p)p^{-s}\big)^{-2},$$

and so we have

$$\begin{aligned}L^2(s,\chi_q)L^2(s,\varrho\chi_q)L^{-1}(2s,\chi_q^2) &= \big(1+\chi_q(2)2^{-s}\big)\big(1-\chi_q(2)2^{-s}\big)^{-1}\times\\ \times\prod_{p\equiv 1\,(\mathrm{mod}\,4)}\big(1+\chi_q(p)p^{-s}\big)\big(1-\chi_q(p)p^{-s}\big)^{-3}&\prod_{p\equiv -1\,(\mathrm{mod}\,4)}\big(1-\chi_q^2(p)p^{-2s}\big)^{-1}.\end{aligned} \tag{2.2}$$

Therefore from (2.1) and (2.2) we obtain

$$R(s,\chi_q) = 16\big(1+\chi_q(2)2^{-s}\big)^{-1}L^2(s,\chi_q)L^2(s,\varrho\chi_q)L^{-1}(2s,\chi_q^2). \tag{2.3}$$

And hence completely analogously as in our previous paper [5], Lemma 2, we have for arbitrary $M, N > 1$ and $\sigma = \frac{1}{2}+(\log N)^{-1}$ the inequality

$$\sum_{q\leqslant M}\varphi(q)^{-1}\sum_{\chi \bmod q} R(s,\chi_q) \ll M|s|^2\log N\,(\log M|s|)^{26}. \tag{2.4}$$

3. Let us consider the equation

$$\varrho\chi_q = 1. \tag{3.1}$$

If 4 does not divide q, then the congruence

$$\begin{cases} n\equiv 1 \ (\mathrm{mod}\ q),\\ n\equiv -1 \ (\mathrm{mod}\ 4)\end{cases}$$

has a solution, and so if χ_q' satisfies (3.1), then we have

$$1 = \varrho\chi_q'(n) = \varrho(n)\chi_q'(n) = -1.$$

This is a contradiction. Therefore it must be $4|q$, and for this case it is easy to see that (3.1) has only one solution $\varrho\chi_q^0$, where χ_q^0 is the principal character modulo q. Moreover in this case we have

$$R(s,\varrho\chi_q^0) = R(s,\chi_q^0).$$

Now let $R_k(y;q,l)$ be the sum

$$(k!)^{-1}\sum_{\substack{n\equiv l(\mathrm{mod}\,q)\\ n\leqslant y}} r^2(n)\left(\log\frac{y}{n}\right)^k.$$

Then we have

$$R_k(y;q,l)=\varphi(q)^{-1}\sum_{\chi\,\mathrm{mod}\,q}\bar{\chi}_q(l)\frac{1}{2\pi i}\int_{(2)}R(s,\chi_q)\frac{y^s}{s^{k+1}}\,ds.$$

Hence under the above consideration on the characters we have easily from (2.4)

$$\text{(3.2)}\quad \sum_{q\leqslant M}\max_{y\leqslant N}\max_{(q,l)=1}|R_3(y;q,l)-\varepsilon_q\varphi(q)^{-1}\operatorname*{Res}_{s=1}R(s,\chi_q^0)s^{-4}y^s| \ll MN^{1/2}\log N(\log M)^{26},$$

where ε_q is 2 if $4|q$, and 1 otherwise.

4. Now let us calculate the residue of $R(s,\chi_q^0)s^{-4}y^s$ at $s=1$.

We have the following expansions (as $s\to 1$)

$$s^{-4}y^s=y\{1+(\log y-4)(s-1)+O((s-1)^2)\},$$

$$(1+\chi_q^0(2)2^{-s})^{-1} =(1+\chi_q^0(2)2^{-1})^{-1}\{1-(1+\chi_q^0(2)2^{-1})^{-1}\chi_q^0(2)2^{-1}\log 2(s-1)+O((s-1)^2)\},$$

$$\begin{aligned}L^2(s,\chi_q^0)&=\prod_{p|q}(1-p^{-s})^2\zeta^2(s)\\ &=(s-1)^{-2}\prod_{p|q}(1-p^{-1})^2\Big\{1+2\sum_{p|q}\frac{\log p}{p-1}(s-1)+O((s-1)^2)\Big\}\times\\ &\qquad\times\{1+2\gamma(s-1)+O((s-1)^2)\}\\ &=(s-1)^{-2}\prod_{p|q}(1-p^{-1})^2\Big\{1+2\Big(\gamma+\sum_{p|q}\frac{\log p}{p-1}\Big)(s-1)+O((s-1)^2)\Big\},\end{aligned}$$

$$\begin{aligned}L^2(s,\varrho\chi_q^0)&=\prod_{p|q}(1-\varrho(p)p^{-s})^2L^2(s,\varrho)\\ &=\Big(\frac{\pi}{4}\Big)^2\prod_{p|q}(1-\varrho(p)p^{-1})^2\Big\{1+2\sum_{p|q}\varrho(p)\frac{\log p}{p-1}(s-1)+O((s-1)^2)\Big\}\times\\ &\qquad\times\Big\{1+\frac{8}{\pi}L'(1,\varrho)(s-1)+O((s-1)^2)\Big\}\\ &=\Big(\frac{\pi}{4}\Big)^2\prod_{p|q}(1-\varrho(p)p^{-1})^2\Big\{1+2\Big(\frac{4}{\pi}L'(1,\varrho)+\sum_{p|q}\varrho(p)\frac{\log p}{p-1}\Big)(s-1)+\\ &\qquad+O((s-1)^2)\Big\},\end{aligned}$$

and further

$$\begin{aligned}L^{-1}(2s,\chi_q^0)&=\prod_{p|q}(1-p^{-2s})^{-1}\zeta(2s)^{-1}\\ &=\frac{6}{\pi^2}\prod_{p|q}(1-p^{-2})^{-1}\Big\{1-2\sum_{p|q}\frac{\log p}{p^2-1}(s-1)+O((s-1)^2)\Big\}\times\\ &\qquad\times\Big\{1-\frac{12}{\pi^2}\zeta'(2)(s-1)+O((s-1)^2)\Big\}\\ &=\frac{6}{\pi^2}\prod_{p|q}(1-p^{-2})^{-1}\Big\{1-2\Big(\frac{6}{\pi^2}\zeta'(2)+\sum_{p|q}\frac{\log p}{p^2-1}\Big)(s-1)+O((s-1)^2)\Big\}.\end{aligned}$$

Here the number γ in the expansion of $L^2(s,\chi_q^0)$ is Euler's constant.

Hence collecting these expansions we obtain

$$\text{(4.1)}\qquad \operatorname*{Res}_{s=1}R(s,\chi_q^0)s^{-4}y^s=f_1(q)y\log y+f_2(q)y,$$

where

$$\text{(4.2)}\qquad f_1(q)=6(1+\chi_q^0(2)2^{-1})^{-1}\prod_{p|q}\Big(1-\frac{1}{p^2}\Big)^{-1}\Big(1-\frac{1}{p}\Big)^2\Big(1-\frac{\varrho(p)}{p}\Big)^2$$

and

$$\text{(4.3)}\qquad f_2(q)=f_1(q)\Big\{2\sum_{p|q}\frac{\log p}{p-1}\Big(1+\varrho(p)-\frac{1}{p+1}\Big)- -(1+\chi_q^0(2)2^{-1})^{-1}\chi_q^0(2)2^{-1}\log 2+c_0\Big\}.$$

Here c_0 is an absolute constant and is equal to

$$2\gamma-4+\frac{8}{\pi}L'(1,\varrho)-\frac{12}{\pi^2}\zeta'(2).$$

5. Now $R_k(y;q,l)$ is a non-decreasing function of y, and hence for any positive $\lambda<1$, we have the inequality

$$\int_{ye^{-\lambda}}^{y}R_2(\xi;q,l)\frac{d\xi}{\xi}\leqslant\lambda R_2(y;q,l)\leqslant\int_{y}^{ye^{\lambda}}R_2(\xi;q,l)\frac{d\xi}{\xi}.$$

The left integral is equal to

$$\begin{aligned}&R_3(y;q,l)-R_3(ye^{-\lambda};q,l)\\ &\quad=\varepsilon_q\varphi(q)^{-1}\lambda\{f_1(q)y\log y+(f_1(q)+f_2(q))y\}+\\ &\qquad+O\{\lambda^2\varphi(q)^{-1}(f_1(q)y\log y+|f_2(q)|y)\}+\\ &\qquad+O\{\max_{\xi\leqslant y}|R_3(\xi;q,l)-\varepsilon_q\varphi(q)^{-1}(f_1(q)\xi\log\xi+f_2(q)\xi)|\}.\end{aligned}$$

An analogous equality holds for the right integral.

Hence from (3.2) we have

$$\sum_{q\leqslant M}\max_{y\leqslant N}\max_{(q,l)=1}\left|R_2(y;q,l)-\varepsilon_q\varphi(q)^{-1}\big(f_1(q)y\log y+(f_1(q)+f_2(q))y\big)\right| \tag{5.1}$$

$$\ll\lambda^{-1}N^{1/2}M\log N(\log M)^{26}+\lambda\sum_{q\leqslant M}\varphi(q)^{-1}\{f_1(q)N\log N+|f_2(q)|N\}$$

$$=\lambda^{-1}N^{1/2}M\log N(\log M)^{26}+\lambda\Sigma_1,\ \text{say}.$$

Now we have from (4.2)

$$\varphi(q)^{-1}f_1(q)\ll q^{-1}\prod_{p|q}\left(1+\frac{1}{p}\right)\ll q^{-1}\log\log(q+3), \tag{5.2}$$

since

$$\prod_{p|q}\left(1+\frac{1}{p}\right)\leqslant\exp\left\{\sum_{p|q}\frac{1}{p}\right\}\leqslant\exp\left\{\sum_{p\leqslant\log(q+3)}\frac{1}{p}+\big(\log(q+3)\big)^{-1}\sum_{p|q}\log p\right\}$$

$$=\exp\{\log\log\log(q+3)+O(1)\}.$$

Further we have from (4.3)

$$\varphi(q)^{-1}f_2(q)\ll q^{-1}\log\log(q+3)\sum_{p|q}\frac{\log p}{p-1}\ll q^{-1}\{\log\log(q+3)\}^2, \tag{5.3}$$

since

$$\sum_{p|q}\frac{\log p}{p-1}\ll\sum_{p\leqslant\log(q+3)}\frac{\log p}{p}+\big(\log(q+3)\big)^{-1}\sum_{p|q}\log p\ll\log\log(q+3).$$

Hence from (5.2) and (5.3) we have

$$\Sigma_1\ll\log M(\log\log M)^2N\log N$$

and therefore we obtain

$$\sum_{q\leqslant M}\max_{y\leqslant N}\max_{(q,l)=1}\left|R_2(y;q,l)-\varepsilon_q\varphi(q)^{-1}\big\{f_1(q)y\log y+(f_1(q)+f_2(q))y\big\}\right| \tag{5.4}$$

$$\ll\lambda^{-1}N^{1/2}M\log N(\log M)^{26}+\lambda N\log N(\log M)^3.$$

By the same assertion taking $\lambda^{1/2}$ instead of λ we have from (5.4)

$$\sum_{q\leqslant M}\max_{y\leqslant N}\max_{(q,l)=1}\left|R_1(y;q,l)-\varepsilon_q\varphi(q)^{-1}\big\{f_1(q)y\log y+(2f_1(q)+f_2(q))y\big\}\right| \tag{5.5}$$

$$\ll\lambda^{-3/2}N^{1/2}M\log N(\log M)^{26}+\lambda^{1/2}N\log N(\log M)^3.$$

Finally taking $\lambda^{1/4}$ instead of λ we have from (5.5) the fundamental inequality

$$\sum_{q\leqslant M}\max_{y\leqslant N}\max_{(q,l)=1}\left|R(y;q,l)-\varepsilon_q\varphi(q)^{-1}\big\{f_1(q)y\log y+(3f_1(q)+f_2(q))y\big\}\right| \tag{5.6}$$

$$\ll\lambda^{-7/4}N^{1/2}M\log N(\log M)^{26}+\lambda^{1/4}N(\log N)(\log M)^3.$$

6. Let $u>0$ and $k_0>k_1>\ldots>k_u\geqslant 0$. Let γ_s $(0<s\leqslant k_0)$ be real numbers such that $0<\gamma_s<1$. Further we define ϱ_i by

$$\varrho_i=\begin{cases}1 & \text{for}\quad i=0,\\ \displaystyle\sum_{\substack{s_1>s_2>\ldots>s_i>k_i\\ s_j\leqslant k_{\left[\frac{j-1}{2}\right]}}}\gamma_{s_1}\gamma_{s_2}\cdots\gamma_{s_i} & \text{for}\quad 0<i\leqslant 2u,\end{cases}\qquad 0\leqslant m\leqslant u. \tag{6.1}$$

Now if the conditions

$$L_m=\prod_{k_m<s\leqslant k_{m-1}}(1-\gamma_s)\geqslant\tfrac{4}{5}\quad\text{for}\quad 1\leqslant m\leqslant u \tag{6.2}$$

are satisfied, then we have

$$\left|\sum_{i=0}^{2u}(-1)^i\varrho_i\right|<2\prod_{m=1}^{u}L_m. \tag{6.3}$$

The proof of this familiar result can be found in [3].

In the following paragraph we need to improve this as follows. Let Γ be a subset of integers $\{s\}$. Let γ_s^* be defined by

$$\gamma_s^*=\gamma_s\quad\text{for}\quad s\notin\Gamma,$$

$$\gamma_s^*=0\quad\text{for}\quad s\in\Gamma.$$

Further we construct ϱ_i^* and L_m^* analogously as in (6.1) and (6.2). Then we have under the condition (6.2)

$$\left|\sum_{i=0}^{2u}(-1)^i\varrho_i^*\right|<2\prod_{m=1}^{u}L_m^*. \tag{6.3*}$$

7. Now we will prove the upper estimate of the sum

$$\sum_{p\leqslant N}r^2(p-1).$$

From (4.2) we have for $p>7$

$$\frac{f_1(p)}{4\varphi(p)}=\frac{1}{p}\left(1+\frac{1}{p}\right)^{-1}\left(1-\frac{\varrho(p)}{p}\right)^2<\frac{2}{11}. \tag{7.1}$$

Moreover we have

$$\prod_{7<p\leqslant\xi}\left(1-\frac{f_1(p)}{4\varphi(p)}\right)=\prod_{7<p\leqslant\xi}\left(1-\frac{1}{p}\right)\prod_{7<p\leqslant\xi}\left\{\left(1-\frac{1}{p}\right)^{-1}-\frac{1}{p}\left(1-\frac{1}{p^2}\right)^{-1}\left(1-\frac{\varrho(p)}{p}\right)^2\right\},$$

where the last product converges as $\xi\to\infty$, and hence there is an absolute constant $c_1>1$ such that

$$\frac{1}{c_1\log\xi}\leqslant\prod_{7<p\leqslant\xi}\left(1-\frac{f_1(p)}{4\varphi(p)}\right)\leqslant\frac{c_1}{\log\xi}. \tag{7.2}$$

Now we put

$$\alpha=(270c_1^2)^{-1}, \tag{7.3}$$

and let $p_1<p_2<\ldots<p_k$ be all prime numbers that are larger 7 and not larger than N^α.

Let k_1 be the least integer $\geqslant 0$ such that

$$L_1=\prod_{k_1<s\leqslant k}\left(1-\frac{f_1(p_s)}{4\varphi(p_s)}\right)\geqslant\frac{4}{5}.$$

If $k_1>0$, we define k_2 to be the least integer $\geqslant 0$ such that

$$L_2=\prod_{k_2<s\leqslant k_1}\left(1-\frac{f_1(p_s)}{4\varphi(p_s)}\right)\geqslant\frac{4}{5}.$$

In such way we define $k_1>k_2>\ldots>k_u\ (=0)$ inductively.

Then following Brun we obtain

$$\sum_{p\leqslant N}r^2(p-1)\leqslant\sum_{q\epsilon\Omega}\mu(q)R(N;q,-1)+O(N^\alpha\log N), \tag{7.4}$$

where Ω is the set of 1 and all integers q such that

$$q=p_{r_1}p_{r_2}\ldots p_{r_i},\quad r_1>r_2>\ldots>r_i,\ r_j\leqslant k_{\left[\frac{j-1}{2}\right]},\quad 0\leqslant i\leqslant 2u. \tag{7.5}$$

Here the rest term $N^\alpha\log N$ is obtained from the inequality

$$\sum_{p\leqslant N^\alpha}r^2(p-1)\leqslant\sum_{n\leqslant N^\alpha}r^2(n)\ll N^\alpha\log N.$$

On the other hand we have

$$\begin{aligned}&\sum_{q\epsilon\Omega}\mu(q)R(N;q,-1)\\&=(N\log N+3N)\sum_{q\epsilon\Omega}\mu(q)\varphi(q)^{-1}f_1(q)+N\sum_{q\epsilon\Omega}\mu(q)\varphi(q)^{-1}f_2(q)+\\&\quad+O\Big\{\sum_{q\epsilon\Omega}\max_{y\leqslant N}\max_{(q,l)=1}\big|R(N;q,l)-\varphi(q)^{-1}\{f_1(q)y\log y+(3f_1(q)+f_2(q))y\}\big|\Big\}\\&=(N\log N+3N)\Sigma_2+N\Sigma_3+O\{\Sigma_4\},\ \text{say}.\end{aligned}$$

Then by the assertion of the preceding paragraph, considering $4^{-1}\varphi(p_s)^{-1}f_1(p_s)$ as γ_s, we have from (6.3)

$$|\Sigma_2|<8\prod_{m=1}^{u}L_m,$$

where

$$L_m=\prod_{k_m<s\leqslant k_{m-1}}\left(1-\frac{f_1(p_s)}{4\varphi(p_s)}\right).$$

Namely we obtain from (7.2)

$$|\Sigma_2|<8c_1\alpha^{-1}(\log N)^{-1}. \tag{7.6}$$

Now let us consider the sum Σ_3. From (4.3) we have

$$\begin{aligned}\Sigma_3&=(c_0-\tfrac{1}{3}\log 2)\Sigma_2+2\sum_{q\epsilon\Omega}\mu(q)\varphi(q)^{-1}f_1(q)\sum_{p|q}\frac{\log p}{p-1}\left(1+\varrho(p)-\frac{1}{p+1}\right)\\&=O\big((\log N)^{-1}\big)+2\Sigma_5,\ \text{say},\end{aligned}$$

since $2\nmid q$ and the inequality (7.6).

We have

$$\begin{aligned}\Sigma_5&=\sum_{7<p\leqslant N^\alpha}\frac{\log p}{p-1}\left(1+\varrho(p)-\frac{1}{p+1}\right)\Big\{\Sigma_2-\sum_{\substack{q\epsilon\Omega\\p\nmid q}}\mu(q)f_1(q)\varphi(q)^{-1}\Big\}\\&=O\big(\log N(\log N)^{-1}\big)-\sum_{7<p\leqslant N^\alpha}\frac{\log p}{p-1}\left(1+\varrho(p)-\frac{1}{p+1}\right)\sum_{\substack{q\epsilon\Omega\\p\nmid q}}\mu(q)f_1(q)\varphi(q)^{-1}.\end{aligned}$$

Now it is easy to see that the last inner sum can be estimated by the improved form of the assertion of the preceding paragraph. Hence from (6.3)* we have

$$\Big|\sum_{\substack{q\epsilon\Omega\\p\nmid q}}\mu(q)f_1(q)\varphi(q)^{-1}\Big|<8\left(1-\frac{f_1(p)}{4\varphi(p)}\right)^{-1}\prod_{m=1}^{u}L_m\ll(\log N)^{-1}.$$

Therefore we obtain

$$\Sigma_5\ll 1\quad\text{and hence}\quad\Sigma_3\ll 1.$$

At this point we have

$$\sum_{p\leqslant N}r^2(p-1)\ll N+\Sigma_4. \tag{7.7}$$

Now we must estimate the sum Σ_4, and for this sake we must find the size of $q\in\Omega$.

By the construction of k_m we have for $1\leqslant m\leqslant u-1$

$$\left(1-\frac{f_1(p_{k_m})}{4\varphi(p_{k_m})}\right)L_m = \prod_{k_{m-1}<s\leqslant k_m-1}\left(1-\frac{f_1(p_s)}{4\varphi(p_s)}\right) < \frac{4}{5},$$

and so from (7.1) we have

$$L_m < 1-\tfrac{1}{45}.$$

Hence from (7.2) we have

$$\log p_{k_m} \leqslant c_1 \prod_{1\leqslant s\leqslant k_m}\left(1-\frac{f_1(p_s)}{4\varphi(p_s)}\right)^{-1} \leqslant ac_1^2\log N\prod_{i=1}^{m} L_i < ac_1^2\log N(1-\tfrac{1}{45})^m.$$

This gives

$$(7.8)\qquad (p_{k_0}p_{k_1}\dots p_{k_{u-1}})^2 \leqslant N^{90c_1^2a} = N^{1/3}$$

by the definition of a, (7.3).

Now by the definition of $q\in\Omega$, (7.5), we have $q\leqslant N^{1/3}$. Therefore if we put $M = N^{1/3}$ and $\lambda = N^{-1/12}$ in the fundamental inequality (5.6), we obtain, noting that $\varepsilon_q = 1$ for $q\in\Omega$,

$$\Sigma_4 \ll N^{47/48}(\log N)^4.$$

This completes the proof of the following fundamental result:

THEOREM 1. *There is an absolute constant c_2 such that*

$$\sum_{p\leqslant N} r^2(p-1) \leqslant c_2 N.$$

8. Now we will prove our main theorem.

Thanks to Hooley and Linnik we know that

$$\sum_{p\leqslant N} r(p-1) = \pi\prod_p\left(1+\frac{\varrho(p)}{p(p-1)}\right)\frac{N}{\log N} + O\big(N(\log N)^{-(1+\delta)}\big),$$

where δ is an absolute constant $> 1/35$.

Hence applying the Cauchy inequality we have

$$\left(\frac{N}{\log N}\right)^2 \ll \sum_{p\leqslant N} r^2(p-1)\sum_{p\leqslant N} b(p-1).$$

Therefore from Theorem 1 we obtain our main result:

THEOREM 2. *There are infinitely many prime numbers which are of the form x^2+y^2+1. And their number up to large N is larger than*

$$c_3 N(\log N)^{-2},$$

where c_3 is an absolute constant.

9. Remark 1. In the preceding paper [5] we have proved the asymptotic formula for the sum

$$\sum_{n\leqslant N}\tau^2(n)\tau(n+1),$$

where $\tau(n)$ is the number of divisors of n. Hence it may be interesting to consider the same problem for the sum

$$\sum_{n\leqslant N} r^2(n)\tau(n+1).$$

If we can prove the inequality for $(g,l)=1$, $q\leqslant N^{\beta}$,

$$\sum_{\substack{n\equiv l \pmod q\\ n\leqslant N}} r^2(n) \leqslant c_\beta q^{-1}N\log N,$$

where β is an arbitrary positive number < 1 and c_β is a constant depending only on β, then it is possible to deduce the asymptotic formula by virtue of the fundamental inequality (5.6).

Unfortunately we can not prove the above inequality, and so we can prove only the lower estimation:

$$\sum_{n\leqslant N} r^2(n)\tau(n+1) \geqslant 6\big(1+o(1)\big)\prod_p\left\{1-\frac{1}{p}+\left(1+\frac{1}{p}\right)^{-1}\left(1-\frac{\varrho(p)}{p}\right)^2\right\}N(\log N)^2.$$

The right side must be the main term of the asymptotic formula.

10. Remark 2. We will state the conjecture (1.3) more precisely. Following Turán [6] we consider the sum

$$I^*(N) = \sum_{n\leqslant N} b(n)\Lambda(n+1),$$

where $\Lambda(n)$ is the von Mangoldt function. Then we get at once

$$I^*(N) = -\sum_{q\leqslant N+1}\mu(q)\log q\sum_{\substack{n\equiv -1 \pmod q\\ n\leqslant N}} b(n).$$

Hence we must find a heuristical asymptotic formula for the last inner sum $B(N,q)$.

Now let $R^*(s, \chi_q)$ be the Dirichlet series

$$\sum_{n=1}^{\infty} b(n)\chi_q(n)n^{-s},$$

which converges absolutely for $\sigma > 1$. After some easy calculation we can see that

$$\{R^*(s,\chi_q)\}^2 = \big(1-\chi_q(2)2^{-s}\big)^{-1} \prod_{p\equiv -1 (\mathrm{mod}\, 4)} \big(1-\chi_q^2(p)p^{-2s}\big)^{-1} L(s,\chi_q)L(s,\varrho\chi_q).$$

Hence the regularity of $R^*(s, \chi_q)$ in the region $\sigma > 1/2$ depends on the existence of the critical zeros of Dirichlet's L-series. Namely we must assume the extended Riemann Hypothesis.

Then the main term of $B(N, q)$ must be deduced from the integral

$$\varepsilon_q \varphi(q)^{-1} \frac{1}{2\pi i}\int_C R^*(s,\chi_q^0)s^{-1}N^s ds,$$

where the contour C starts at $s = 1/2+(\log N)^{-1}$, encircles $s = 1$ in the positive direction and returns to $s = 1/2+(\log N)^{-1}$ along the real axis. And after some calculation we can conclude that this integral is asymptotically equal to

$$\frac{1}{2}\prod_{p\equiv -1 (\mathrm{mod}\, 4)}\Big(1-\frac{1}{p^2}\Big)^{-1/2}\frac{N}{\sqrt{\log N}}\varepsilon_q^* q^{-1}\prod_{\substack{p\equiv -1 (\mathrm{mod}\, 4)\\ p|q}}\Big(1+\frac{1}{p}\Big),$$

where $\varepsilon_q^* = 2$ for $2\nmid q$ and $4|q$, and $= 1$ otherwise.

Replacing $B(N, q)$ heuristically by the above value we have

$$I^*(N) \sim \frac{1}{2}\prod_{p\equiv -1 (\mathrm{mod}\, 4)}\Big(1-\frac{1}{p^2}\Big)^{-1/2}\frac{N}{\sqrt{\log N}}\times$$
$$\times\Big\{-\sum_{q\leqslant N+1}\mu(q)\varepsilon_q^* q^{-1}\log q\prod_{\substack{p|q\\ p\equiv -1 (\mathrm{mod}\, 4)}}\Big(1+\frac{1}{p}\Big)\Big\}.$$

On the other hand as in [6], Lemma III, we can prove rigorously the following asymptotic formula:

$$-\sum_{q\leqslant N+1}\mu(q)\varepsilon_q^* q^{-1}\log q\prod_{\substack{p\equiv -1 (\mathrm{mod}\, 4)\\ p|q}}\Big(1+\frac{1}{p}\Big)$$
$$= 3\prod_{p\equiv -1 (\mathrm{mod}\, 4)}\Big(1-\frac{1}{p(p-1)}\Big)+O\big((\log N)^{-10}\big).$$

Hence we may introduce the following conjecture:

CONJECTURE J*. *There are infinitely many prime numbers which are of the form x^2+y^2+1. And their number up to large N is asymptotically equal to*

$$\frac{3}{2}\prod_{p\equiv -1 (\mathrm{mod}\, 4)}\Big(1-\frac{1}{p^2}\Big)^{-1/2}\Big(1-\frac{1}{p(p-1)}\Big)N(\log N)^{-3/2}.$$

References

[1] E. Bombieri, *On the large sieve*, Mathematika 12 (1965), pp. 201–225.

[2] C. Hooley, *On the representation of a number as the sum of two squares and a prime*, Acta Math. 97 (1957), pp. 189–210.

[3] E. Landau, *Die Goldbachsche Vermutung und der Schnirelmannsche Satz*, Göttinger Nachr. Math-Phys. Kl. (1930), pp. 255–276.

[4] Ju. V. Linnik, *An asymptotic formula in an additive problem of Hardy and Littlewood* (Russian), Izv. Akad. Nauk SSSR, ser. mat. 24 (1960), pp. 629–706.

[5] Y. Motohashi, *An asymptotic formula in the theory of numbers*, Acta Arith. 16 (1969), pp. 255–264.

[6] P. Turán, *On the twin-prime problem, II*, Acta Arith. 13 (1967), pp. 61–89.

Reçu par la Rédaction le 2. 4. 1969

ACTA ARITHMETICA
XVI (1970)

On sums of four cubes of polynomials

by

L. J. MORDELL (Cambridge)

It is well known that all integers $n \not\equiv \pm 4 \pmod 9$ can be expressed as a sum of four integer cubes, and numerical evidence suggests that this is also true for integers $\equiv \pm 4 \pmod 9$. A method of trying to prove this is to find polynomials P, Q, R, S in x with integer coefficients and degree $\leqslant 4$, such that

$$P^3+Q^3+R^3+S^3 = 9x+4. \tag{1}$$

Schinzel [1] has recently proved the more general result that such a representation with polynomials not all constant cannot hold for

$$P^3+Q^3+R^3+S^3 = Lx+M, \tag{2}$$

where L and M are integer constants and $M \equiv 4 \pmod 9$. Let

$$P = ax^4+bx^3+cx^2+dx+e$$

and write (2) as say,

$$\sum (ax^4+bx^3+cx^2+dx+e)^3 = 3^a Lx+M, \quad a \geqslant 0, \tag{3}$$

where here and throughout, summations will refer to the four sets typified by a, b, c, d, e. Suppose a representation is taken where the product of the leading coefficients of P, Q, R, S, has its least absolute value. Schinzel's proof, which is really a 3-adic one, is rather complicated since it requires the expansion of P^3 in powers of x and so it is not easy to see what underlies his proof.

He shows that $a \equiv 0 \pmod{81}$, $b \equiv 0 \pmod{27}$, $c \equiv 0 \pmod 9$, $d \equiv 0 \pmod 3$. Since obviously $a \geqslant 1$, then on replacing x by $x/3$, we have a representation

$$\sum \left(\frac{a}{81}x^4+\frac{b}{27}x^3+\frac{c}{9}x^2+\frac{d}{3}x+e\right)^3 = 3^{a-1}Lx+M$$

with a smaller product for the leading coefficients.

[1] J. London Math. Soc. 43 (1968), pp. 143–145.