[4] Ivan Niven and H. S. Zuckerman, *An Introduction to the Theory of Numbers*, New York 1960, pp. 95–96.

KANSAS STATE UNIVERSITY

Received on 17.2.1971 (144)

ACTA ARITHMETICA
XXII (1972)

On Goldbach's problem

by

R. C. VAUGHAN (Sheffield)

1. Introduction. Goldbach conjectured in 1742 that every even number greater than two is the sum of two odd primes.

In 1923 Hardy and Littlewood developed a method ([4], [5]) which enabled them to show that

(i) if no Dirichlet L-function has a zero in the region $\operatorname{Re} s > 3/4$, then every sufficiently large odd natural number is the sum of three odd primes,

and

(ii) if every Dirichlet L-function has all its zeros in the region $\operatorname{Re} s \leqslant 1/2$ and if $E(N)$ is the number of even numbers less than N for which Goldbach's conjecture is false, then

$$E(N) = O_\varepsilon(N^{1/2+\varepsilon})$$

for every positive ε.

In 1937 Vinogradov obtained estimates ([12], [13]) (for an account of which, see [14]) for trigonometric sums of the form

$$\sum_{p\leqslant N} e^{2\pi i x p} \tag{1.1}$$

which, combined with Page's work [9] on the zeros of L-functions, enabled him to show unconditionally by the Hardy–Littlewood method that every sufficiently large odd number is the sum of three odd primes.

Using these ideas, Van der Corput [1], Tchudakoff [11] and Estermann [3] were able to show unconditionally that

$$E(N) = O_A(N\log^{-A} N). \tag{1.2}$$

In the mid 1940's, Linnik [7], [8] and Tchudakoff [10], by finding estimates for the number of zeros of L-functions in certain regions, were able to dispense with Vinogradov's method for sums of the type (1.1) and thus obtained essentially new proofs of the Goldbach–Vinogradov theorem and (1.2).

Let

$$R(n) = \sum_{\substack{p_1, p_2 \\ p_1+p_2=n}} 1,$$

$$J(n) = \sum_{\substack{n_1, n_2 \geq 2 \\ n_1+n_2=n}} (\log n_1 \log n_2)^{-1}$$

and

$$S(n) = (1+(-1)^n)\left\{\prod_{p \geq 3}\left(1-\frac{1}{(p-1)^2}\right)\right\}\prod_{\substack{p \geq 3 \\ p \mid n}} \frac{p-1}{p-2}.$$

In the proofs of (1.2) mentioned above, (1.2) is deduced from a prior estimate of the form

$$\sum_{n \leq N} (R(n)-J(n)S(n))^2 = O_A(N^3 \log^{-A} N).$$

The object of this paper is to show that

$$E(N) = O\big(N\exp(-c(\log N)^{1/2})\big) \tag{1.3}$$

for a suitable positive constant c. The basic idea is to use the Hardy–Littlewood–Vinogradov method to obtain the estimate

$$\sum_{n \leq N} |R(n)-J(n)S(n)-D(N, n)|^2 = O\big(N^3 \exp(-c_1(\log N)^{1/2})\big),$$

where $D(N, n)$ is introduced to take account of possible exceptional Siegel zeros' of L-functions.

2. Notation. Throughout, with or without suffices, the letters x, y, u, σ, t denote real numbers, X, Y denote positive real numbers, N denotes a large real number, h denotes an integer, a, k, l, m, n, q, r denote positive integers and p denotes a prime number. For any number z, $e(z) = e^{2\pi iz}$. $C_1, C_2, \ldots$ are suitable positive numbers which do not depend on the parameters of the expressions in which they appear. The statement $f \ll g$, concerning the function f and a non-negative function g, is taken to mean that there is a positive number C such that $|f| \leq Cg$. If f is also a non-negative function we use $g \gg f$ to mean $f \ll g$.

If χ is a character to the modulus q, $L(s, \chi)$ denotes the function defined for $\sigma > 1$ by

$$L(s, \chi) = L(\sigma+it, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

$\Lambda(m)$ is $\log p$ if $m = p^n$ for some p and n, and is zero otherwise. $\pi(X, q, a)$

denotes the number of primes which do not exceed X and are congruent to a modulo q, and

$$\psi(X, q, a) = \sum_{\substack{m \leq X \\ m \equiv a \pmod q}} \Lambda(m).$$

μ is Möbius' function and φ is Euler's function. $d(n)$ denotes the number of divisors of n and (n, m) denotes the greatest common divisor of n and m. $\|u\|$ denotes the distance of u from the nearest integer.

3. The main theorems.

DEFINITION 3.1. *Let $E(X)$ denote the number of even numbers less than X which are not the sum of two odd primes.*

THEOREM 1.

$$E(X) \ll X\exp(-C_1(\log X)^{1/2}).$$

DEFINITION 3.2. *Let $R(m)$ denote the number of representations of m as the sum of two primes.*

DEFINITION 3.3. *Let $E_1(X)$ denote the number of even numbers m for which $X/2 < m \leq X$ and*

$$R(m) < m\exp(-(\log m)^{1/2}).$$

THEOREM 2.

$$E_1(X) \ll X\exp(-C_2(\log X)^{1/2}).$$

4. Preliminary lemmas.

LEMMA 4.1. *There are positive numbers C_3, C_4 and C_5 such that for every $X > 1$ and every pair a, q with $(a, q) = 1$ and $q \leq \exp((\log X)^{1/2})$ we have*

$$\left|\psi(X, q, a) - \frac{X}{\varphi(q)} + F(X, q, a)\right| < C_3 X\exp(-C_4(\log X)^{1/2}),$$

where $F(X, q, a) = 0$ unless there is a necessarily unique real non-principal character χ modulo q for which $L(s, \chi)$ has a real zero β satisfying

$$\beta > 1 - C_5(\log q)^{-1},$$

in which case

$$F(X, q, a) = \frac{\chi(a)X^\beta}{\varphi(q)\beta}.$$

This is the main result of Chapter 20 of Davenport [2].

LEMMA 4.2 (Page). *There is a positive number C_6 such that of all the real primitive characters χ to moduli $r \leq \exp((\log N)^{1/2})$ there is at most* *one for which $L(s,\chi)$ has a real zero β satisfying $\beta > 1-C_6(\log N)^{-1/2}$, and then $L(s,\chi)$ has only one such zero.*

This follows easily from Lemmas 7 and 8 of Page [9].

LEMMA 4.3 (Siegel). *For every positive number ε there is a positive number $C(\varepsilon)$ such that, if χ is any real non-principal character, with modulus q, then*

$$L(s,\chi)\neq 0$$

for

$$s > 1-C(\varepsilon)q^{-\varepsilon}.$$

For a proof see Chapter 21 of Davenport [2].

LEMMA 4.4. *There are positive numbers C_7, C_8 and C_9 with the following property:*

For every sufficiently large N,

either

(i) *for every q, a such that $q\leqslant \exp\big((\log N)^{1/2}\big)$ and $(a,q)=1$ and for every X such that $N^{1/2}<X\leqslant N$ we have*

$$\left|\psi(X,q,a)-\frac{X}{\varphi(q)}\right| < C_7X\exp\big(-C_8(\log X)^{1/2}\big),$$

or

(ii) *there is just one pair r, β such that for every q, a so that $q\leqslant \exp\big((\log N)^{1/2}\big)$ and $(a,q)=1$, and for every X such that $N^{1/2}<X\leqslant N$, we have*

$$\left|\psi(X,q,a)-\frac{X}{\varphi(q)}\right| < C_7X\exp\big(-C_8(\log X)^{1/2}\big)\qquad (r\nmid q)$$

and

$$\left|\psi(X,q,a)-\frac{X}{\varphi(q)}+\frac{\chi(a)X^\beta}{\varphi(q)\beta}\right| < C_7X\exp\big(-C_8(\log X)^{1/2}\big)\qquad (r|q),$$

where χ is a real non-principal character modulo q induced, in each case, by the same real non-principal primitive character modulo r. Moreover

$$\tfrac{1}{2}\leqslant\beta<1-C_9r^{-1/8}$$

and

$$r>(\log N)^3.$$

Proof. Let $q\leqslant \exp\big((\log N)^{1/2}\big)$. Suppose that $L(s,\chi)$ does not have, for any real non-principal character χ modulo q, a real zero β satisfying $\beta>1-C_6(\log N)^{-1/2}$. Then, by Lemma 4.1,

$$\left|\psi(X,q,a)-\frac{X}{\varphi(q)}\right| < C_3X\exp\big(-C_4(\log X)^{1/2}\big)+X\exp\big(-C_6\log X(\log N)^{-1/2}\big)$$
$$< C_7X\exp\big(-C_8(\log X)^{1/2}\big)\qquad (N^{1/2}<X\leqslant N).$$

Either this is true for every q in the range, in which case we have (i), or there exists a number $q_1\leqslant \exp\big((\log N)^{1/2}\big)$ which has a real non-principal character χ_1 to the modulus q_1 so that $L(s,\chi_1)$ has a real zero β_1 satisfying $\beta_1>1-C_6(\log N)^{-1/2}$. Suppose that χ_1 is induced by the real non-principal primitive character χ_2 modulo q_2. Then $q_2|q_1$ and $L(\beta_1,\chi_2)=0$. Hence the numbers r, β mentioned in Lemma 4.2 exist and since they are then unique we have $r=q_2$ and $\beta=\beta_1$. Thus for every such q_1 we have $r|q_1$.

Now again suppose that $q\leqslant \exp\big((\log N)^{1/2}\big)$. If $r|q$ and χ modulo q is induced by χ_2, then $L(\beta,\chi)=0$. Thus if $r|q$ and $\beta>1-C_5/\log q$ we have, by Lemma 4.1,

$$\left|\psi(X,q,a)-\frac{X}{\varphi(q)}+\frac{\chi(a)X^\beta}{\varphi(q)\beta}\right| < C_3X\exp\big(-C_4(\log X)^{1/2}\big)\qquad (N^{1/2}<X\leqslant N),$$

and if $r|q$ and $\beta\leqslant 1-C_5/\log q$ then, also by Lemma 4.1,

$$\left|\psi(X,q,a)-\frac{X}{\varphi(q)}+\frac{\chi(a)X^\beta}{\varphi(q)\beta}\right| < C_3X\exp\big(-C_4(\log X)^{1/2}\big)+2X^\beta$$
$$< C_7X\exp\big(-C_8(\log X)^{1/2}\big)\quad (N^{1/2}<X\leqslant N),$$

where in each case χ is the character modulo q induced by the real non-principal primitive character χ_2 modulo r for which $L(\beta,\chi_2)=0$.

On the other hand, if $r\nmid q$, it follows that $L(s,\chi)$ does not have, for any real non-principal character χ modulo q, a real zero β satisfying $\beta>1-C_6(\log N)^{-1/2}$ (since we showed above that if it did have, then $r|q$). Thus, as in the first part of the proof,

$$\left|\psi(X,q,a)-\frac{X}{\varphi(q)}\right| < C_7X\exp\big(-C_8(\log X)^{1/2}\big)\qquad (N^{1/2}<X\leqslant N).$$

The assertion that $\beta<1-C_9r^{-1/8}$ is an easy consequence of Lemma 4.3 and then we have

$$1-C_6(\log N)^{-1/2}<1-C_9r^{-1/8},$$

that is,

$$r>C_{10}(\log N)^4>(\log N)^3.$$

This completes the proof of Lemma 4.4.

Let

$$\mathrm{ls}_x(X) = \sum_{2\leqslant m\leqslant X} m^{x-1}(\log m)^{-1} \tag{4.1}$$

and

$$\mathrm{ls}\,X = \mathrm{ls}_1(X). \tag{4.2}$$

We now restate Lemma 4.4 in terms of $\pi(X, q, a)$.

LEMMA 4.5. *There are positive numbers C_{11}, C_{12} and C_{13} such that, for every sufficiently large number N,*
either

(i) *for every q, a such that $q \leqslant \exp\big((\log N^{1/2})\big)$ and $(q, a) = 1$ we have whenever $N^{3/4} < X \leqslant N$,*

$$\left|\pi(X, q, a) - \frac{\mathrm{ls}\,X}{\varphi(q)}\right| < C_{11}X\exp\big(-C_{12}(\log X)^{1/2}\big),$$

or

(ii) *there is just one pair r, β such that for every q, a such that $q \leqslant \exp\big((\log N)^{1/2}\big)$ and $(q, a) = 1$, and every X with $N^{3/4} < X \leqslant N$, we have*

$$\left|\pi(X, q, a) - \frac{\mathrm{ls}\,X}{\varphi(q)}\right| < C_{11}X\exp\big(-C_{12}(\log X)^{1/2}\big) \qquad (r \nmid q)$$

and

$$\left|\pi(X, q, a) - \frac{\mathrm{ls}\,X}{\varphi(q)} + \frac{\chi(a)}{\varphi(q)}\mathrm{ls}_\beta(X)\right| < C_{11}X\exp\big(-C_{12}(\log X)^{1/2}\big) \qquad (r \mid q),$$

where χ is the real non-principal character modulo q induced, in each case, by the same real non-principal primitive character modulo r. Moreover

$$\tfrac{1}{2} \leqslant \beta < 1 - C_{13}r^{-1/8} \tag{4.2A}$$

and

$$r > (\log N)^3. \tag{4.2B}$$

This follows easily from the previous lemma by a partial summation.

LEMMA 4.6 (Vinogradov). *Suppose that $x = a/q + \theta/q^2$, where $|\theta| \leqslant 1$, $(a, q) = 1$ and $1 < q < N$. Then*

$$\sum_{p\leqslant N} e(xp) \ll N(\log N)^{9/2}\Big((q^{-1} + qN^{-1})^{1/2} + \exp\big(-\tfrac{1}{2}(\log N)^{1/2}\big)\Big).$$

This is Theorem 1 of Chapter IX of Vinogradov [14].

Let

$$c_q(h) = \sum_{\substack{a=1\\(a,q)=1}}^{q} e(ah/q). \tag{4.3}$$

LEMMA 4.7. *Suppose that $k = (|h|, q)$ $(h \neq 0)$ and $k = q$ $(h = 0)$. Let $l = q/k$. Then*

$$c_q(h) = \mu(l)\varphi(q)\varphi(l)^{-1}.$$

This is Theorem 272 of Hardy and Wright [6].

Let

$$A(q, m) = \mu(q)^2 c_q(-m)\varphi(q)^{-2}, \tag{4.4}$$

$$S(x, m) = \sum_{q>x} A(q, m) \tag{4.5}$$

and

$$S(m) = S(0, m). \tag{4.6}$$

LEMMA 4.8. $\varphi(m) \gg m(\log\log m)^{-1}$ $(m \geqslant 3)$.

This follows easily from Theorem 328 of Hardy and Wright [6].

LEMMA 4.9. *We have*

$$S(m) = \big(1 + (-1)^m\big)\Big(\prod_{\substack{p\mid m\\ p\geqslant 3}} \frac{p-1}{p-2}\Big)\prod_{p\geqslant 3}\Big(1 - \frac{1}{(p-1)^2}\Big), \tag{4.7}$$

$$S(m) \gg 1 \qquad (m \text{ even}) \tag{4.8}$$

and

$$S(X, m) \ll X^{-1}d(m)\big(\log\log(X+3)\big)^3. \tag{4.9}$$

Proof. (4.7) is Lemma 12 of Hardy and Littlewood [4] with $r = 2$ and (4.8) follows easily from (4.7).

Proof of (4.9). By Lemma 4.7 and (4.4),

$$A(q, m) = \mu(q)^2\mu\big(q/(q, m)\big)\varphi(q)^{-1}\varphi\big(q/(q, m)\big)^{-1}.$$

Thus

$$\sum_{q>X} A(q, m) = \sum_{k\mid m}\sum_{\substack{q>X\\(q,m)=k}} \mu(q)^2\mu(q/k)\varphi(q)^{-1}\varphi(q/k)^{-1}$$

$$= \sum_{k\mid m}\sum_{\substack{q>X/k\\(q,m/k)=1}} \mu(qk)^2\mu(q)\varphi(qk)^{-1}\varphi(q)^{-1}$$

$$= \sum_{k\mid m}\frac{\mu(k)^2}{\varphi(k)}\sum_{\substack{q>X/k\\(q,m)=1}}\frac{\mu(q)}{\varphi(q)^2}.$$

Therefore, by (4.5),

$$S(X, m) = \Sigma_1 + \Sigma_2, \tag{4.10}$$

where

$$\Sigma_1 = \sum_{\substack{k|m\\ k\leqslant X}} \frac{\mu(k)^2}{\varphi(k)} \sideset{}{'}\sum_{\substack{q>X/k\\ (q,m)=1}} \frac{\mu(q)}{\varphi(q)^2}$$

and

$$\Sigma_2 = \sideset{}{'}\sum_{\substack{k|m\\ k>X}} \frac{\mu(k)^2}{\varphi(k)} \sideset{}{'}\sum_{\substack{q\\ (q,m)=1}} \frac{\mu(q)}{\varphi(q)^2}.$$

By Lemma 4.8,

$$\Sigma_1 \ll \sum_{\substack{k|m\\ k\leqslant X}} \frac{\mu(k)^2}{\varphi(k)} \sideset{}{'}\sum_{q>X/k} q^{-2}\big(\log\log(q+2)\big)^2$$

$$\ll X^{-1}\big(\log\log(X+3)\big)^2 \sideset{}{'}\sum_{\substack{k|m\\ k\leqslant X}} \frac{\mu(k)^2 k}{\varphi(k)}$$

$$\ll X^{-1}\big(\log\log(X+3)\big)^3 d(m)$$

and

$$\Sigma_2 \ll X^{-1}\big(\log\log(X+3)\big) d(m).$$

Hence (4.9) follows from (4.10).

5. The Farey dissection. Let

$$C_{14} = \min\left(1, \frac{\sqrt{3}}{2} C_{12}\right), \tag{5.1}$$

$$P_1 = \exp\left(\tfrac{1}{2}C_{14}(\log N)^{1/2}\right) \tag{5.2}$$

and

$$P_2 = P_1^{1/4}. \tag{5.3}$$

DEFINITION 5.1. *If the pair of numbers r, β of* (ii) *of Lemma* 4.5 *does not exist, or if it does and $P_2 < r$, let $P = P_2$. Otherwise we take $P = P_1$.*

Let

$$\varkappa = P/N. \tag{5.4}$$

DEFINITION 5.2. *When $a \leqslant q \leqslant P$ and $(a, q) = 1$, let $M(q, a)$ denote the closed interval $[(a-\varkappa)/q, (a+\varkappa)/q]$.*

Clearly all the $M(q, a)$ are disjoint and contained in the closed interval $[\varkappa, 1+\varkappa]$.

DEFINITION 5.3. *Let T denote the set of those points of the closed interval $[\varkappa, 1+\varkappa]$ which are not in any of the $M(q, a)$.*

Let

$$V(X, x) = \sum_{p\leqslant X} e(xp). \tag{5.5}$$

LEMMA 5.1. *Let $x \in T$. Then*

$$V(N, x) \ll N(\log N)^{9/2}P^{-1/2}.$$

Proof. By a well-known elementary theorem we may choose h, q so that

(i) either $h = 0$, $q = 1$ or $(|h|, q) = 1$,

(ii) $q \leqslant 2N/P$

and

(iii) $|x - h/q| \leqslant \frac{1}{2}P/(Nq)$.

By Definition 5.3, $x \notin M(1, 1)$. Hence, by (5.4),

$$P/N \leqslant x < 1 - P/N.$$

Therefore

$$h/q \leqslant |x-h/q| + x < \tfrac{1}{2}P/N + 1 - P/N < 1$$

and

$$h/q \geqslant x - |x-h/q| \geqslant P/N - \tfrac{1}{2}P/N > 0.$$

Hence $0 < h < q$. Therefore, by (i), (iii), Definition 5.2 and (5.4), if $q \leqslant P$ we would have $x \in M(h, q)$ which, by Definition 5.3, contradicts the fact that $x \in T$. Hence $q > P$.

The lemma now follows easily from Lemma 4.6, (ii), Definition 5.1, (5.3), (5.2) and (5.1).

Let

$$g_u(X, x) = \sum_{2\leqslant m\leqslant X} \frac{e(mx)}{\log m} m^{u-1} \tag{5.6}$$

and

$$V^*(X, x, q, a) = \frac{\mu(q)}{\varphi(q)} g_1(X, x-a/q). \tag{5.7}$$

LEMMA 5.2. *Suppose that $\frac{1}{2} \leqslant u \leqslant 1$ and $X > 1$. Then*

$$g_u(X, x) \ll 1/\max(\|x\|^u, X^{-u}).$$

This is shown easily by a partial summation.

LEMMA 5.3.

$$\int_T |V(N, x)|^4 dx \ll N^3(\log N)^8 P^{-1} \tag{5.8}$$

and

(5.9) $$\int_T \Big|\sum_{q\leqslant P}\sum_{\substack{a=1\\(a,q)=1}}^{q} V^*(N,x,q,a)^2\Big|^2 dx \ll N^3P^{-1}.$$

Proof. (5.8) follows immediately from Lemma 5.1 and the fact that

$$\int_T |V(N,x)|^2dx \leqslant \int_{\varkappa}^{1+\varkappa} |V(N,x)|^2dx = \pi(N) \ll \frac{N}{\log N}.$$

Proof of (5.9). By the definition of T,

(5.10) $$\|x-a/q\| \geqslant \varkappa/q \quad (a\leqslant q\leqslant P,\ (a,q)=1,\ x\in T).$$

Also if $a\leqslant q\leqslant P$, $(a,q)=1$, $l\leqslant k\leqslant P$ and $(l,k)=1$,

(5.11) $$\left\|\frac{a}{q}-\frac{l}{k}\right\| \geqslant \frac{1}{qk} \quad (q,a\neq k,l).$$

Now

(5.12) $$\Big|\sum_{q\leqslant P}\sum_{\substack{a=1\\(a,q)=1}}^{q} V^*(N,x,q,a)^2\Big|^2 = \sum_{q\leqslant P}\sum_{\substack{a=1\\(a,q)=1}}^{q} |V^*(N,x,q,a)|^4 +$$
$$+\sum_{q\leqslant P}\sum_{\substack{a=1\\(a,q)=1}}^{q}\sum_{k\leqslant P}\sum_{\substack{l=1\\(l,k)=1\\k,l\neq q,a}}^{k} V^*(N,x,q,a)^2\,\overline{V^*(N,x,k,l)}^2.$$

By (5.10), (5.7) and Lemma 5.2,

$$\int_T |V^*(N,x,q,a)|^4dx \ll \frac{\mu(q)^2}{\varphi(q)^4}\int_{\varkappa/q}^{1/2} y^{-4}dy \ll \varphi(q)^{-4}q^3\varkappa^{-3}.$$

Hence, by (5.4) and Lemma 4.8,

(5.13) $$\int_T \sum_{q\leqslant P}\sum_{\substack{a=1\\(a,q)=1}}^{q} |V^*(N,x,q,a)|^4dx \ll N^3P^{-1}.$$

Now suppose that $a\leqslant q\leqslant P$, $(a,q)=1$, $l\leqslant k\leqslant P$, $(l,k)=1$ and $q,a\neq k,l$. Then, by (5.7), Lemma 5.2 and (5.11),

$$\int_T V^*(N,x,q,a)^2\,\overline{V^*(N,x,k,l)}^2dx$$
$$\ll \varphi(q)^{-2}\varphi(k)^{-2}\int_T \|x-a/q\|^{-2}\|x-l/k\|^{-2}dx$$
$$\ll \varphi(q)^{-2}\varphi(k)^{-2}\int_{[\varkappa,1+\varkappa]-M(q,a)-M(k,l)} \|x-a/q\|^{-2}\|x-l/k\|^{-2}dx$$
$$\ll \varphi(q)^{-2}\varphi(k)^{-2}\Big\{\int_{\substack{\varkappa\\ \varkappa/q\leqslant\|x-a/q\|\leqslant 1/(2qk)}}^{1+\varkappa} \|x-a/q\|^{-2}q^2k^2dx + \int_{\substack{\varkappa\\ \|x-l/k\|\geqslant\varkappa/k}}^{1+\varkappa} q^2k^2\|x-l/k\|^{-2}dx\Big\}$$
$$\ll \varphi(q)^{-2}\varphi(k)^{-2}\Big\{q^3\varkappa^{-1}k^2+k^2q^2\int_{\varkappa/k}^{1/2}y^{-2}dy\Big\}$$
$$\ll k^2q^2\varkappa^{-1}\varphi(q)^{-2}\varphi(k)^{-2}(q+k).$$

Hence, by (5.4),

$$\int_T\sum_{q\leqslant P}\sum_{\substack{a=1\\(a,q)=1}}^{q}\sum_{k\leqslant P}\sum_{\substack{l=1\\(l,k)=1\\k,l\neq q,a}}^{k} V^*(N,x,q,a)^2\,\overline{V^*(N,x,k,l)}^2dx$$
$$\ll NP^{-1}\sum_{q\leqslant P}\sum_{k\leqslant P}\varphi(q)^{-1}\varphi(k)^{-1}q^2k^2(q+k) \ll N^3P^{-1}.$$

(5.9) follows from this, (5.13) and (5.12).

Lemma 5.4.

$$\sum_{q\leqslant P}\sum_{\substack{a=1\\(a,q)=1}}^{q}\int_{M(q,a)}\Big|\sum_{k\leqslant P}\sum_{\substack{l=1\\(l,k)=1\\k,l\neq q,a}}^{k} V^*(N,x,k,l)^2\Big|^2dx \ll N^3P^{-1}.$$

Proof. Suppose that $a\leqslant q\leqslant P$, $(a,q)=1$, $l\leqslant k\leqslant P$, $(l,k)=1$, $k,l\neq q,a$ and $x\in M(q,a)$. By Definition 5.2 and (5.4),

$$|x-a/q|\leqslant \varkappa/q = PN^{-1}q^{-1}.$$

Hence

$$\left\|x-\frac{l}{k}\right\| \geqslant \left\|\frac{a}{q}-\frac{l}{k}\right\| - \left|x-\frac{a}{q}\right| \geqslant \frac{1}{qk}-\frac{P}{Nq} \gg \frac{1}{qk}.$$

Therefore, by (5.7) and Lemma 5.2,

$$\Big|\sum_{k\leqslant P}\sum_{\substack{l=1\\(l,k)=1\\k,l\neq q,a}}^{k} V^*(N,x,k,l)^2\Big|^2 \ll \Big(\sum_{k\leqslant P}\varphi(k)^{-1}q^2k^2\Big)^2 \ll P^4q^4.$$

Hence, by Definitions 5.1 and 5.2, (5.4), (5.3) and (5.2), the expression we wish to estimate is

$$\ll \sum_{q\leqslant P} q\varkappa q^{-1}P^4q^4 \ll N^3P^{-1}.$$

This proves the lemma.

Let

$$J(N, m) = \sum_{\substack{2\leqslant m_1, m_2\leqslant N\\ m_1+m_2=m}} (\log m_1 \log m_2)^{-1}. \tag{5.14}$$

LEMMA 5.5. *Suppose that $4\leqslant m\leqslant N$. Then*

$$m\log^{-2}N \ll J(N, m) \ll N\log^{-2}N.$$

Proof. The lower bound is trivial. To prove the upper bound, consider the number of solutions of

$$m_1+m_2 = m.$$

The number of solutions with $m_1\leqslant N^{1/2}$ does not exceed $N^{1/2}$. Similarly the number of solutions with $m_2\leqslant N^{1/2}$ does not exceed $N^{1/2}$. Hence we may suppose on the right-hand side of (5.14) that both $m_1 > N^{1/2}$ and $m_2 > N^{1/2}$. The upper bound follows at once.

DEFINITION 5.4. *Let $R(N, m)$ denote the number of representations of m as the sum of two primes, neither of which exceed N.*

LEMMA 5.6. *We have*

$$V(N, x)^2 = \sum_{m\leqslant 2N} R(N, m)e(mx) \tag{5.15}$$

and

$$\sum_{q>v}\sum_{\substack{a=1\\(a,q)=1}}^{q} V^*(N, x, q, a)^2 = \sum_{m\leqslant 2N} J(N, m)S(y, m)e(mx). \tag{5.16}$$

Proof. (5.15) is an immediate consequence of (5.5) and Definition 5.4. By (5.7), (5.6) and (5.14),

$$V^*(N, x, q, a)^2 = \mu(q)^2\varphi(q)^{-2}\sum_m J(N, m)e\big(m(x-a/q)\big).$$

Hence, by (4.3), (4.4) and (4.5),

$$\sum_{q>v}\sum_{\substack{a=1\\(a,q)=1}}^{q} V^*(N, x, q, a)^2 = \sum_m J(N, m)S(y, m)e(mx).$$

This proves (5.16).

LEMMA 5.7.

$$\int_{\varkappa}^{1+\varkappa}\Big|\sum_{q>P}\sum_{\substack{a=1\\(a,q)=1}}^{q} V^*(N, x, q, a)^2\Big|^2 dx \ll N^3P^{-1}.$$

Proof. By the previous lemma the integral in question is just

$$\sum_{m\leqslant 2N} J(N, m)^2|S(P, m)|^2.$$

The lemma follows easily from this, (5.14) and (4.9).

6. The major arcs-I. The proof of Theorem 2 divides into two cases according as $P = P_1$ or $P = P_2$. Throughout this section we assume that

$$P = P_2. \tag{6.1}$$

LEMMA 6.1. *Suppose that $q\leqslant P$, $(a, q) = 1$, and $N^{3/4} < X \leqslant N$. Then*

$$V(X, a/q) - \frac{\mu(q)}{\varphi(q)}\operatorname{ls} X \ll XqP^{-2}.$$

Proof. By Definition 5.1, (6.1), (5.3), (5.2), (5.1) and Lemma 4.5,

$$\sum_{p\leqslant X} e(ap/q) = \sum_{\substack{h=1\\(h,q)=1}}^{q} e(ah/q)\sum_{\substack{p\leqslant X\\ p\equiv h (\mathrm{mod}\, q)}} 1 + O\Big(\sum_{p|q}1\Big)$$

$$= \frac{\operatorname{ls} X}{\varphi(q)}\sum_{\substack{h=1\\(h,q)=1}}^{q} e(ah/q) + O(XqP^{-2}).$$

We now appeal to (5.5), (4.3) and Lemma 4.7 to complete the proof of the lemma.

LEMMA 6.2. *Suppose that $a\leqslant q\leqslant P$, $(a, q) = 1$ and $x\in \mathfrak{M}(q, a)$. Then*

$$V(N, x) - V^*(N, x, q, a) \ll NP^{-1}.$$

Proof. Let $y = x-a/q$. Then, by (5.7), (5.6), (5.5) and a partial summation,

$$V(N, x) - V^*(N, x, q, a)$$
$$= e(yN)\Big(V(N, a/q) - \frac{\mu(q)}{\varphi(q)}\operatorname{ls} N\Big) -$$
$$-2\pi iy\int_1^N e(yu)\Big(V(u, a/q) - \frac{\mu(q)}{\varphi(q)}\operatorname{ls} u\Big)du.$$

Hence, by Lemma 6.1, Definition 5.2 and (5.4),

$$V(N,x)-V^*(N,x,q,a) \ll NqP^{-2}+|y|\Big(N^2qP^{-2}+\int_1^{N^{3/4}} N^{3/4}\,dy\Big) \ll NP^{-1}.$$

Lemma 6.3.

$$\sum_{q\leq P}\sum_{\substack{a=1\\(a,q)=1}}^{q}\int_{M(q,a)}|V(N,x)^2-V^*(N,x,q,a)^2|^2\,dx \ll N^3P^{-1}.$$

Proof. Suppose that $a\leq q\leq P$, $(a,q)=1$ and $x\in M(q,a)$. By (5.7) and Lemma 5.2,

$$V^*(N,x,q,a)\ll N\varphi(q)^{-1}.$$

Hence, by Lemma 6.2,

$$V(N,x)^2-V^*(n,x,q,a)^2 \ll N^2\varphi(q)^{-1}P^{-1}.$$

Therefore, by Definition 5.2 and (5.4),

$$\sum_{q\leq P}\sum_{\substack{a=1\\(a,q)=1}}^{q}\int_{M(q,a)}|V(N,x)^2-V^*(N,x,q,a)^2|^2\,dx$$
$$\ll N^4P^{-2}\sum_{q\leq P}\varphi(q)^{-1}Pq^{-1}N^{-1} \ll N^3P^{-1}.$$

Lemma 6.4.

$$\int_{\varkappa}^{1+\varkappa}\Big|V(N,x)^2-\sum_{q=1}^{\infty}\sum_{\substack{a=1\\(a,q)=1}}^{q}V^*(N,x,q,a)^2\Big|^2\,dx \ll N^3\log^8NP^{-1}.$$

Proof. By Lemma 5.7,

$$\int_{\varkappa}^{1+\varkappa}\Big|V(N,x)^2-\sum_{q=1}^{\infty}\sum_{\substack{a=1\\(a,q)=1}}^{q}V^*(N,x,q,a)^2\Big|^2\,dx \tag{6.2}$$
$$\ll \int_{\varkappa}^{1+\varkappa}\Big|V(N,x)^2-\sum_{k\leq P}\sum_{\substack{l=1\\(l,k)=1}}^{k}V^*(N,x,k,l)^2\Big|^2\,dx+N^3P^{-1}.$$

Let $M=[\varkappa,1+\varkappa]-T$. Then, by Definitions 5.2 and 5.3,

$$M=\bigcup_{q\leq P}\bigcup_{\substack{a=1\\(a,q)=1}}^{q}M(q,a).$$

Thus, by Lemmas 5.3, 5.4 and 6.3,

$$\int_{\varkappa}^{1+\varkappa}\Big|V(N,x)^2-\sum_{k\leq P}\sum_{\substack{l=1\\(l,k)=1}}^{k}V^*(N,x,k,l)^2\Big|^2\,dx$$

$$\ll \int_{M}\Big|V(N,x)^2-\sum_{k\leq P}\sum_{\substack{l=1\\(l,k)=1}}^{k}V^*(N,x,k,l)^2\Big|^2\,dx+$$
$$+\int_{T}|V(N,x)|^4\,dx+\int_{T}\Big|\sum_{k\leq P}\sum_{\substack{l=1\\(l,k)=1}}^{k}V^*(N,x,k,l)^2\Big|^2\,dx$$
$$\ll \int_{M}\Big|V(N,x)^2-\sum_{k\leq P}\sum_{\substack{l=1\\(l,k)=1\\x\in M(k,l)}}^{k}V^*(N,x,k,l)^2\Big|^2\,dx$$
$$+\int_{M}\Big|\sum_{k\leq P}\sum_{\substack{l=1\\(l,k)=1\\x\notin M(k,l)}}^{k}V^*(N,x,k,l)^2\Big|^2\,dx+N^3\log^8NP^{-1}$$
$$=\sum_{q\leq P}\sum_{\substack{a=1\\(a,q)=1}}^{q}\int_{M(q,a)}|V(N,x)^2-V^*(N,x,q,a)^2|^2\,dx+$$
$$+\sum_{q\leq P}\sum_{\substack{a=1\\(a,q)=1}}^{q}\int_{M(q,a)}\Big|\sum_{k\leq P}\sum_{\substack{l=1\\(l,k)=1\\k,l\neq q,a}}^{k}V^*(N,x,k,l)^2\Big|^2\,dx+N^3\log^8NP^{-1}$$
$$\ll N^3\log^8NP^{-1}.$$

This, with (6.2), completes the proof of Lemma 6.4.

7. Proof of Theorem 2 in the case $P=P_2$.

Lemma 7.1.

$$\sum_{m\leq 2N}\big(R(N,m)-J(N,m)\mathfrak{S}(m)\big)^2 \ll N^3\log^8NP^{-1}.$$

Proof. By Lemma 5.6 with $y=0$ and (4.6),

$$V(N,x)^2-\sum_{q=1}^{\infty}\sum_{\substack{a=1\\(a,q)=1}}^{q}V^*(N,x,q,a)^2=\sum_{m\leq 2N}\big(R(N,m)-J(N,m)\mathfrak{S}(m)\big)e(mx).$$

The lemma now follows easily from Parseval's theorem and Lemma 6.4.

By Lemma 5.5 and (4.8),

$$J(N,m)\mathfrak{S}(m)\gg N\log^{-2}N \qquad (\tfrac{1}{2}N<m\leq N,\ 2|m). \tag{7.1}$$

Lemma 7.1 implies that

$$R(N,m)-J(N,m)\mathfrak{S}(m)\ll N\log^{8/3}NP^{-1/3}$$

for all but at most $N\log^{8/3}NP^{-1/3}$ numbers m with $m\leq 2N$. Hence, by (7.1) and since N is large,

$$R(N,m)\gg N\log^{-2}N$$

for all but at most $N\log^{8/3}NP^{-1/3}$ even numbers m with

$$\tfrac{1}{2}N < m \leqslant N.$$

By Definitions 5.4 and 3.2,

$$R(N, m) = R(m) \quad (\tfrac{1}{2}N < m \leqslant N)$$

and hence, by (6.1), (5.3) and (5.2), Theorem 2 with $X = N$ follows if $C_2 < C_{14}/24$.

8. Major arcs-II. We assume here that

$$P = P_1. \tag{8.1}$$

This together with Definition 5.1, implies that the pair of numbers r, β of Lemma 4.5 exists, and since $r \leqslant P_2$ we have, by (5.3),

$$r \leqslant P_1^{1/4}. \tag{8.2}$$

Definition 8.1. *Let χ_1 be that real non-principal primitive character modulo r mentioned in* (ii) *of Lemma* 4.5.

If ψ is a character to the modulus k we put

$$\tau(\psi) = \sum_{m=1}^{k} e(m/k)\psi(m). \tag{8.3}$$

Definition 8.2. *For any given $q \leqslant P$ for which $r|q$ let χ denote that character modulo q induced by χ_1.*

Let

$$\lambda(q, a) = \tau(\chi)\chi(a)\varphi(q)^{-1} \quad (q \leqslant P,\ r|q). \tag{8.4}$$

Lemma 8.1.

$$\sum_{\substack{q\leqslant P\\ r\nmid q}} \sum_{\substack{a=1\\ (a,q)=1}}^{q} \int_{M(q,a)} |V(N, x)^2 - V^*(N, x, q, a)^2|^2 dx \ll N^3P^{-1}.$$

Proof. We note that when $r\nmid q$ Lemma 6.1 remains valid and hence so does Lemma 6.2. Thus we can deduce Lemma 8.1 in a similar manner to Lemma 6.3.

Lemma 8.2. *Suppose that $q \leqslant P$, $r|q$, $(a, q) = 1$ and $N^{3/4} < X \leqslant N$. Then*

$$V(X, a/q) - \frac{\mu(q)}{\varphi(q)}\operatorname{ls} X + \lambda(q, a)\operatorname{ls}_\beta(X) \ll XqP^{-2}.$$

Proof. By Definition 5.1, (8.1), (5.2), (5.1) and Lemma 4.5,

$$\sum_{p\leqslant X} e(ap/q) = \sum_{\substack{h=1\\ (h,q)=1}}^{q} e(ah/q)\left(\frac{\operatorname{ls} X}{\varphi(q)} - \frac{\chi(h)}{\varphi(q)}\operatorname{ls}_\beta(X)\right) + O(XqP^{-2}).$$

The lemma now follows from (8.3), (8.4), (4.3) and Lemma 4.7.

Let

$$V_\beta^*(N, x, q, a) = \lambda(q, a)g_\beta(N, x-a/q). \tag{8.5}$$

Lemma 8.3. *Suppose that $a \leqslant q \leqslant P$, $r|q$, $(a, q) = 1$ and $x \in M(q, a)$. Then*

$$V(N, x) - V^*(N, x, q, a) + V_\beta^*(N, x, q, a) \ll NP^{-1}.$$

Proof. Let

$$b(m) = \begin{cases} 1 & (m \text{ prime}),\\ 0 & (m \text{ not prime}),\end{cases}$$

and $y = x - a/q$. Then, by (8.5), (4.1), (4.2), (5.5), (5.7) and (5.6), the expression we wish to estimate is just

$$\sum_{2\leqslant m\leqslant N}\left(b(m)e(am/q) - \frac{\mu(q)}{\varphi(q)\log m} + \frac{\lambda(q, a)m^{\beta-1}}{\log m}\right)e(ym)$$
$$= e(yN)\left(V(N, a/q) - \frac{\mu(q)}{\varphi(q)}\operatorname{ls} N + \lambda(q, a)\operatorname{ls}_\beta(N)\right) -$$
$$-2\pi i y\int_1^N e(yu)\left(V(u, a/q) - \frac{\mu(q)}{\varphi(q)}\operatorname{ls} u + \lambda(q, a)\operatorname{ls}_\beta(u)\right)du.$$

Hence, by the previous lemma, Definition 5.2 and (5.4),

$$V(N, x) - V^*(N, x, q, a) + V_\beta^*(N, x, q, a)$$
$$\ll NqP^{-2} + |y|\left(\int_{N^{3/4}}^{N} uqP^{-2}du + N^{3/2}\right) \ll NP^{-1}.$$

Lemma 8.4. *Suppose that $r|q$. Then*

$$\tau(\chi) = \mu(q/r)\chi_1(q/r)\tau(\chi_1) \tag{8.6}$$

and

$$|\tau(\chi_1)|^2 = r. \tag{8.7}$$

Proof. Suppose that ψ is any character modulo q and ψ is induced by the primitive character ψ_1 modulo k. Then $k|q$ and it is shown in Chapter 23 of [2] that

$$\tau(\psi) = \mu(q/k)\psi_1(q/k)\tau(\psi_1)$$

and in Chapter 9 of [2] that

$$|\tau(\psi_1)|^2 = k.$$

The lemma follows at once.

LEMMA 8.5. *Suppose that* $(a, q) = 1$, $q \leqslant P$ *and* $r|q$. *Then*

$$\lambda(q, a) = \mu(q/r)\chi_1(q/r)\chi_1(a)\tau(\chi_1)\varphi(q)^{-1}.$$

Proof. By (8.4), Definition 8.2 and Lemma 8.4,

$$\lambda(q, a) = \mu(q/r)\chi_1(q/r)\chi_1(a)\tau(\chi_1)\varphi(q)^{-1},$$

which proves the lemma.

LEMMA 8.6.

$$\sum_{\substack{q\leqslant P\\ r|q}}\sum_{\substack{a=1\\ (a,q)=1}}^{q}\int_{M(q,a)}\left|V(N,x)^2-\big(V^*(N,x,q,a)-V^*_\beta(N,x,q,a)\big)^2\right|^2dx \ll N^3P^{-1}.$$

Proof. Suppose that $a \leqslant q \leqslant P$, $(a, q) = 1$, $r|q$ and $x \in M(q, a)$. By (5.7) and Lemma 5.2,

$$V^*(N, x, q, a) \ll N\varphi(q)^{-1}, \tag{8.8}$$

and by (8.5) and Lemmas 5.2, 8.5 and 8.4,

$$V^*_\beta(N, x, q, a) \ll Nr^{1/2}\varphi(q)^{-1}. \tag{8.9}$$

Hence, by Lemma 8.3,

$$V(N, x) \ll Nr^{1/2}\varphi(q)^{-1}.$$

Therefore, by Lemma 8.3, (8.8) and (8.9),

$$V(N,x)^2-\big(V^*(N,x,q,a)-V^*_\beta(n,x,q,a)\big)^2 \ll N^2P^{-1}r^{1/2}\varphi(q)^{-1}.$$

Thus, by Definition 5.2 and (5.4), the expression we wish to estimate is

$$\ll \sum_{\substack{q\leqslant P\\ r|q}} N^4P^{-2}r\varphi(q)^{-2}PN^{-1}q^{-1}\varphi(q) = N^3P^{-1}\sum_{k\leqslant P/r}k^{-1}\varphi(kr)^{-1} \ll N^3P^{-1}.$$

DEFINITION 8.3. *If* $a \leqslant q \leqslant P$, $(a, q) = 1$, $r|q$ *and* $x \in M(q, a)$ *let*

$$W(N, x) = V^*_\beta(N, x, q, a)^2 - 2V^*_\beta(N, x, q, a)V^*(N, x, q, a).$$

Otherwise, let $W(N, x) = 0$.

LEMMA 8.7.

$$\int_{\varkappa}^{1+\varkappa}\Big|V(N,x)^2-\sum_{q=1}^{\infty}\sum_{\substack{a=1\\ (a,q)=1}}^{q}V^*(N,x,q,a)^2-W(N,x)\Big|^2dx \ll N^3P^{-1}\log^8N.$$

Proof. The lemma can be deduced from Lemmas 5.7, 5.3, 5.4, 8.1 and 8.6 in the same way that Lemma 6.4 is deduced from Lemmas 5.7, 5.3, 5.4 and 6.3.

9. The investigation of $W(N, x)$. Let

$$D(N, h) = \int_{\varkappa}^{1+\varkappa} W(N, x)e(-hx)\,dx. \tag{9.1}$$

LEMMA 9.1.

$$\sum_{m\leqslant 2N}|R(N,m)-J(N,m)S(m)-D(N,m)|^2 \ll N^3P^{-1}\log^8N.$$

Proof. Let

$$F(N, h) = \begin{cases} R(N,h)-J(N,h)S(h)-D(N,h) & (0 < h \leqslant 2N),\\ D(N,h) & (\text{otherwise}).\end{cases}$$

Then, by (9.1) and Lemma 5.6, the $F(N, h)$ are the Fourier coefficients of

$$V(N,x)^2-\sum_{q=1}^{\infty}\sum_{\substack{a=1\\ (a,q)=1}}^{q}V^*(N,x,q,a)^2-W(N,x).$$

Hence, by Bessel's inequality,

$$\sum_{m\leqslant 2N}|R(N,m)-J(N,m)S(m)-D(N,m)|^2 \leqslant \sum_h|F(N,h)|^2$$

$$\leqslant \int_{\varkappa}^{1+\varkappa}\Big|V(N,x)^2-\sum_{q=1}^{\infty}\sum_{\substack{a=1\\ (a,q)=1}}^{q}V^*(N,x,q,a)^2-W(N,x)\Big|^2dx.$$

The result now follows from Lemma 8.7.

Let

$$I_1(n, q, a) = \int_{M(q,a)} V^*(N,x,q,a)V^*_\beta(N,x,q,a)e(-nx)\,dx \quad (r|q), \tag{9.2}$$

$$I_2(n, q, a) = \int_{M(q,a)} V^*_\beta(N,x,q,a)^2e(-nx)\,dx \quad (r|q), \tag{9.3}$$

$$A_1(n, q, a) = \frac{\mu(q)}{\varphi(q)}\lambda(q, a)e(-an/q) \quad (r|q) \tag{9.4}$$

and

$$A_2(n, q, a) = \lambda(q, a)^2e(-an/q) \quad (r|q). \tag{9.5}$$

LEMMA 9.2. *Suppose that* $a \leqslant q \leqslant P$, $r|q$ *and* $(a, q) = 1$. *Then*

$$I_1(n, q, a) = \int_{-\varkappa/q}^{\varkappa/q} g_1(N, y)g_\beta(N, y)e(-ny)\,dy\,A_1(n, q, a) \tag{9.6}$$

and

$$I_2(n,q,a) = \int_{-\varkappa/q}^{\varkappa/q} g_\beta(N,y)^2 e(-ny)\,dy\,A_2(n,q,a). \tag{9.7}$$

Proof. (9.6) follows from (9.4), (9.2), (5.7), (8.5) and Definition 5.2. (9.7) follows similarly from (9.5) and (9.3).

LEMMA 9.3. *Suppose that $q \leqslant P$, $r|q$ and $k = q/r$. Then*

$$\sum_{\substack{a=1\\(a,q)=1}}^{q} A_1(n,q,a) \ll r^{1/2}\varphi(r)\chi_1(k)^2|c_k(-n)|\varphi(q)^{-2}\mu(k)^2 \tag{9.8}$$

and

$$\sum_{\substack{a=1\\(a,q)=1}}^{q} A_2(n,q,a) = \tau(\chi_1)^2\mu(k)^2\chi_1(k)^2 c_q(-n)\varphi(q)^{-2}. \tag{9.9}$$

Proof. By (9.4) and Lemma 8.5,

$$\sum_{\substack{a=1\\(a,q)=1}}^{q} A_1(n,q,a) = \tau(\chi_1)\mu(q)\mu(k)\chi_1(k)\varphi(q)^{-2}\sum_{\substack{a=1\\(a,q)=1}}^{q}\chi_1(a)e(-an/q). \tag{9.10}$$

Clearly, $\chi_1(k) = 0$ unless $(k,r) = 1$. Hence we may suppose that $(k,r) = 1$. Put $a = a_1 r + a_2 k$ with $1 \leqslant a_1 \leqslant k$, $(a_1,k) = 1$, $1 \leqslant a_2 \leqslant r$ and $(a_2,r) = 1$. Then

$$\sum_{\substack{a=1\\(a,q)=1}}^{q}\chi_1(a)e(-an/q) = \sum_{\substack{a_2=1\\(a_2,r)=1}}^{r}\chi_1(a_2k)e(-a_2n/r)\sum_{\substack{a_1=1\\(a_1,k)=1}}^{k}e(-a_1n/k).$$

(9.8) now follows from (9.10), (4.3) and (8.7).

By (9.5) and Lemma 8.5,

$$\sum_{\substack{a=1\\(a,q)=1}}^{q} A_2(n,q,a) = \tau(\chi_1)^2\mu(k)^2\chi_1(k)^2\varphi(q)^{-2}\sum_{\substack{a=1\\(a,q)=1}}^{q}e(-an/q),$$

since $\chi_1(a)^2 = 1$ when $(a,q) = 1$. Hence, by (4.3), we have (9.9).

LEMMA 9.4.

$$\sum_{k\leqslant P/r}\mu(k)^2|c_k(-n)|\varphi(k)^{-2} \ll n/\varphi(n).$$

Proof. By Lemma 4.7,

$$\sum_{k\leqslant P/r}\mu(k)^2|c_k(-n)|\varphi(k)^{-2} = \sum_{k\leqslant P/r}\mu(k)^2\mu\big(k/(k,n)\big)^2\varphi(k)^{-1}\varphi\big(k/(k,n)\big)^{-1}$$
$$= \sum_{m|n}\sum_{\substack{k\leqslant P/r\\(k,n)=m}}\mu(k)^2\mu(k/m)^2\varphi(k)^{-1}\varphi(k/m)^{-1}$$

$$= \sum_{m|n}\sum_{\substack{k\leqslant P/rm\\(k,n/m)=1}}\mu(km)^2\mu(k)^2\varphi(km)^{-1}\varphi(k)^{-1}$$
$$= \sum_{m|n}\mu(m)^2\varphi(m)^{-1}\sum_{\substack{k\leqslant P/rm\\(k,n)=1}}\mu(k)^2\varphi(k)^{-2}$$
$$\ll \sum_{m|n}\mu(m)^2\varphi(m)^{-1} = n/\varphi(n).$$

LEMMA 9.5.

$$\sum_{\substack{q\leqslant P\\r|q}}\sum_{\substack{a=1\\(a,q)=1}}^{q} I_1(n,q,a) \ll N\log^{-2}N r^{1/2}\varphi(r)^{-1}n\varphi(n)^{-1}.$$

Proof. By (5.6) and Schwarz' inequality,

$$\left\{\int_{-\varkappa/q}^{\varkappa/q} g_1(N,y)g_\beta(N,y)e(-ny)\,dy\right\}^2 \ll \int_{-1/2}^{1/2}|g_1(N,y)|^2dy\int_{-1/2}^{1/2}|g_\beta(N,y)|^2dy$$
$$\ll \Big(\sum_{2\leqslant m\leqslant N}\log^{-2}m\Big)^2 \ll N^2\log^{-4}N.$$

Hence

$$\int_{-\varkappa/q}^{\varkappa/q} g_1(N,y)g_\beta(N,y)e(-ny)\,dy \ll N\log^{-2}N.$$

Therefore, by (9.6), (9.8), Lemma 9.4 and noting that $\chi_1(k) = 0$ unless $(k,r) = 1$, we have

$$\sum_{\substack{q\leqslant P\\r|q}}\sum_{\substack{a=1\\(a,q)=1}}^{q} I_1(n,q,a) \ll N\log^{-2}N r^{1/2}\varphi(r)^{-1}\sum_{\substack{k\leqslant P/r\\(k,r)=1}}\mu(k)^2|c_k(-n)|\varphi(k)^{-2}$$
$$\ll N\log^{-2}N r^{1/2}\varphi(r)^{-1}n\varphi(n)^{-1},$$

whence the result.

Let

$$J_\beta(N,m) = \sum_{\substack{2\leqslant m_1,m_2\leqslant N\\m_1+m_2=m}}(\log m_1\log m_2)^{-1}(m_1m_2)^{\beta-1}. \tag{9.11}$$

LEMMA 9.6. *Suppose that $q \leqslant P$. Then*

$$\int_{-\varkappa/q}^{\varkappa/q} g_\beta(N,y)^2e(-ny)\,dy = J_\beta(N,n) + O(Nq/P).$$

Proof. By Lemma 5.2 and (5.4),

$$\int_{\varkappa/q}^{1/2} g_\beta(N, y)^2 e(-ny)\,dy + \int_{-1/2}^{-\varkappa/q} g_\beta(N, y)^2 e(-ny)\,dy \ll \int_{\varkappa/q}^{1/2} y^{-2\vartheta}\,dy \ll q/\varkappa = Nq/P.$$

Hence

$$(9.12)\qquad \int_{-\varkappa/q}^{\varkappa/q} g_\beta(N, y)^2 e(-ny)\,dy = \int_{-1/2}^{1/2} g_\beta(N, y)^2 e(-ny)\,dy + O(Nq/P).$$

By (5.6) and (9.11),

$$g_\beta(N, y)^2 = \sum_m J_\beta(N, m) e(my).$$

This with (9.12) proves the lemma.

Let

$$(9.13)\qquad G(N, n) = \sum_{\substack{q \leqslant P \\ r|q}} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} A_2(n, q, a).$$

Lemma 9.7. *Suppose that $n \leqslant 2N$. Then*

$$\sum_{\substack{q \leqslant P \\ r|q}} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} I_2(n, q, a) = J_\beta(N, n)G(N, n) + O\big(NP^{-1}rd(n)(\log\log N)^4(\log N)^{1/2}\big).$$

Proof. Suppose that $q \leqslant P$ and $r|q$. Then, by (9.7) and Lemma 9.6,

$$\sum_{\substack{a=1 \\ (a,q)=1}}^{q} I_2(n, q, a) - J_\beta(N, n) \sum_{\substack{a=1 \\ (a,q)=1}}^{q} A_2(n, q, a) \ll \Big|\sum_{\substack{a=1 \\ (a,q)=1}}^{q} A_2(n, q, a)\Big| NP^{-1}q.$$

Hence, by (9.9), (9.13), (8.7) and Lemma 4.7,

$$\sum_{\substack{q \leqslant P \\ r|q}} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} I_2(n, q, a) - J_\beta(N, n)G(N, n) \ll \sum_{\substack{q \leqslant P \\ r|q}} |\tau(\chi_1)|^2 \mu(q/r)^2 \chi_1(q/r)^2 |c_q(-n)| \varphi(q)^{-2} NP^{-1} q$$
$$\leqslant NP^{-1} r^2 \varphi(r)^{-1} \sum_{\substack{k \leqslant P/r \\ (k,r)=1}} \mu(k)^2 \mu\big(k/(k, n)\big)^2 k\varphi(k)^{-1} \varphi\big(k/(k, n)\big)^{-1}.$$

Thus

$$(9.14)\qquad \sum_{\substack{q \leqslant P \\ r|q}} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} I_2(n, q, a) - J_\beta(N, n)G(N, n) \ll NP^{-1} r^2 \varphi(r)^{-1} \Sigma_1,$$

where

$$\Sigma_1 = \sum_{\substack{k \leqslant P/r \\ (k,r)=1}} \mu(k)^2 \mu\big(k/(k, n)\big)^2 k\varphi(k)^{-1} \varphi\big(k/(k, n)\big)^{-1}$$
$$= \sum_{\substack{m|n \\ (m,r)=1}} \sum_{\substack{k \leqslant P/rm \\ (k,r)=1 \\ (k,n/m)=1}} \mu(km)^2 \mu(k)^2 km\varphi(km)^{-1} \varphi(k)^{-1}$$
$$= \sum_{\substack{m|n \\ (m,r)=1}} \mu(m)^2 m\varphi(m)^{-1} \sum_{\substack{k \leqslant P/rm \\ (k,rn)=1}} \mu(k)^2 k\varphi(k)^{-2}.$$

Hence, by Lemma 4.8, (8.1) and (5.2),

$$\Sigma_1 \ll d(n)(\log\log N)^3 \sum_{k \leqslant P} 1/k \ll d(n)(\log\log N)^3 (\log N)^{1/2} \qquad (n \leqslant 2N)$$

and, by (8.2),

$$r/\varphi(r) \ll \log\log N.$$

Therefore the result follows from (9.14).

Lemma 9.8. *Suppose that $n \leqslant 2N$. Then*

$$D(N, n) - J_\beta(N, n)G(N, n) \ll NP^{-1}rd(n)(\log\log N)^4(\log N)^{1/2} + Nr^{-1/2}(\log\log N)^2 \log^{-2} N.$$

Proof. By (9.1), Definition 8.3, (9.2) and (9.3),

$$D(N, n) = \sum_{\substack{q \leqslant P \\ r|q}} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \big(I_2(n, q, a) - 2I_1(n, q, a)\big).$$

Lemma 9.8 now follows from Lemmas 9.5, 9.7 and 4.8, (8.2) and (5.2).

10. Proof of Theorem 2 in the case $P = P_1$.

Lemma 10.1. *Suppose that $n \leqslant 2N$ and n is even. Then*

$$|G(N, n)| \leqslant \mathfrak{S}(n) + O\big(P^{-1}rd(n)(\log\log N)^4\big).$$

Proof. By (9.13) and (9.9),

$$G(N, n) = \sum_{\substack{q \leqslant P \\ r|q}} \tau(\chi_1)^2 \mu(q/r)^2 \chi_1(q/r)^2 c_q(-n)\varphi(q)^{-2}.$$

Hence, by Lemma 4.7,

$$G(N, n) = \frac{\tau(\chi_1)^2\mu(r/(r, n))}{\varphi(r)\varphi(r/(r, n))} \sum_{\substack{k\le P/r\\(k,r)=1}} \frac{\mu(k)^2\mu(k/(k, n))}{\varphi(k)\varphi(k/(k, n))}.$$

Therefore, by (8.7),

$$(10.1)\qquad |G(N, n)| \le \frac{r}{\varphi(r)\varphi(r/(r, n))}\left|\sum_{\substack{k\le P/r\\(k,r)=1}} \frac{\mu(k)^2\mu(k/(k, n))}{\varphi(k)\varphi(k/(k, n))}\right|.$$

Clearly

$$\sum_{\substack{k\le P/r\\(k,r)=1}} \frac{\mu(k)^2\mu(k/(k, n))}{\varphi(k)\varphi(k/(k, n))} = \sum_{\substack{m|n\\m\le P/r\\(m,r)=1}} \sum_{\substack{k\le P/rm\\(k,r)=1\\(k,n/m)=1}} \frac{\mu(km)^2\mu(k)}{\varphi(km)\varphi(k)}$$
$$= \sum_{\substack{m|n\\m\le P/r\\(m,r)=1}} \frac{\mu(m)^2}{\varphi(m)} \sum_{\substack{k\le P/rm\\(k,nr)=1}} \frac{\mu(k)}{\varphi(k)^2},$$

and, by Lemma 4.8, when $X\ge 1$,

$$\sum_{\substack{k>X\\(k,n)=1}} \mu(k)\varphi(k)^{-2} \ll \sum_{k>X} (\log\log(k+3))^2 k^{-2} \ll X^{-1}(\log\log(X+3))^2.$$

Therefore, by Lemma 4.8,

$$\left|\sum_{\substack{k\le P/r\\(k,r)=1}} \frac{\mu(k)^2\mu(k/(k, n))}{\varphi(k)\varphi(k/(k, n))}\right|$$
$$\le \sum_{\substack{m|n\\m\le P/r\\(m,r)=1}} \frac{\mu(m)^2}{\varphi(m)}\left\{\left|\sum_{\substack{k\\(k,nr)=1}} \frac{\mu(k)}{\varphi(k)^2}\right| + O\big(P^{-1}rm(\log\log N)^2\big)\right\}$$
$$= \left\{\sum_{\substack{m|n\\m\le P/r\\(m,r)=1}} \frac{\mu(m)^2}{\varphi(m)} \prod_{p\nmid nr}\left(1-\frac{1}{(p-1)^2}\right)\right\} + O\big(P^{-1}rd(n)(\log\log N)^3\big)$$
$$\le \left\{\Big(\prod_{\substack{p|n\\p\nmid r}} \frac{p}{p-1}\Big) \prod_{p\nmid nr} \frac{p(p-2)}{(p-1)^2}\right\} + O\big(P^{-1}rd(n)(\log\log N)^3\big).$$

Hence, by (10.1) and Lemma 4.8,

$$|G(N, n)| \le \left\{\Big(\prod_{\substack{p|r\\p\nmid n}} \frac{1}{p-1}\Big)\Big(\prod_{p|nr} \frac{p}{p-1}\Big) \prod_{p\nmid nr} \frac{p(p-2)}{(p-1)^2}\right\} + O\big(P^{-1}rd(n)(\log\log N)^4\big)$$

and it is easily seen that the first term on the right is

$$\big(1+(-1)^{nr}\big)\Big(\prod_{\substack{p|r\\p\nmid n}} \frac{1}{p-1}\Big)\Big(\prod_{\substack{p|nr\\p\ge 3}} \frac{p}{p-1}\Big)\prod_{\substack{p\nmid nr\\p\ge 3}} \frac{p(p-2)}{(p-1)^2}$$
$$= \big(1+(-1)^{nr}\big)\Big(\prod_{\substack{p|r\\p\nmid n\\p\ge 3}} \frac{1}{p-2}\Big)\Big(\prod_{\substack{p|n\\p\ge 3}} \frac{p-1}{p-2}\Big)\prod_{p\ge 3}\Big(1-\frac{1}{(p-1)^2}\Big)$$
$$\le 2\Big(\prod_{\substack{p|n\\p\ge 3}} \frac{p-1}{p-2}\Big)\prod_{p\ge 3}\Big(1-\frac{1}{(p-1)^2}\Big)$$

which, by (4.7), is equal to $\mathfrak{S}(n)$ when n is even.

This completes the proof of Lemma 10.1.

Lemma 10.2. *Suppose that $n\le 2N$ and n is even. Then*

$$|D(N, n)| \le J_\beta(N, n)\mathfrak{S}(n) + O\big(NP^{-1}rd(n)(\log\log N)^4(\log N)^{1/2}\big) + O\big(Nr^{-1/2}(\log\log N)^2\log^{-2}N\big).$$

Proof. By (9.11), $J_\beta(N, n)\ll N$. The lemma is an immediate consequence of this and Lemmas 9.8 and 10.1.

Lemma 10.3. *There is a positive number C_{15} such that*

$$J(N, m) - J_\beta(N, m) > C_{15}r^{-1/8}J(N, m).$$

Proof. By (4.2A), when $m_1m_2>1$,

$$1-(m_1m_2)^{\beta-1} > 1-\exp(-C_{13}r^{-1/8}\log m_1m_2)$$
$$\ge 1-\exp(-C_{13}r^{-1/8}\log 2) > C_{15}r^{-1/8}.$$

The lemma follows from this, (9.11) and (5.14).

The next lemma is an immediate corollary of the preceding twa.

Lemma 10.4. *Suppose that $m\le 2N$ and m is even. Then*

$$|J(N, m)\mathfrak{S}(m) + D(N, m)| > C_{15}r^{-1/8}J(N, m)\mathfrak{S}(m) + O\big(NP^{-1}rd(m)(\log\log N)^4(\log N)^{1/2}\big) + O\big(Nr^{-1/2}(\log\log N)^2\log^{-2}N\big).$$

Lemma 10.5. *For all but at most $N(\log N)^{8/3}P^{-1/3}$ numbers m with $m\le 2N$,*

$$R(N, m) - J(N, m)\mathfrak{S}(m) - D(N, m) \ll N(\log N)^{8/3}P^{-1/3}.$$

Proof. Immediate from Lemma 9.1.

Lemma 10.6. *For all but at most $N(\log N)^{8/3}P^{-1/3}$ even numbers m with $\frac{1}{2}N < m\le N$,*

$$|J(N, m)\mathfrak{S}(m) + D(N, m)| \gg N(\log N)^{-2}P^{-1/32}.$$

Proof. It is well-known that

$$\sum_{\frac{1}{2}N<m\leqslant N} d(m) \ll N\log N.$$

Hence for all but at most $NP^{-1/3}\log N$ numbers m with $\frac{1}{2}N < m \leqslant N$, $d(m) \leqslant P^{1/3}$. Therefore, by (8.2), (8.1) and (5.2), for all but at most $NP^{-1/3}\log N$ numbers m with $\frac{1}{2}N < m \leqslant N$,

$$(10.2)\qquad NP^{-1}rd(m)(\log\log N)^4(\log N)^{1/2} \ll NP^{-2/3}r(\log\log N)^4(\log N)^{1/2} \ll Nr^{-1}\log^{-2}N.$$

Thus, by Lemma 10.4 and (10.2), for all but at most $NP^{-1/3}\log N$ even numbers m with $\frac{1}{2}N < m \leqslant N$,

$$|J(N,m)S(m)+D(N,m)| > C_{15}r^{-1/8}J(N,m)S(m)+O\big(Nr^{-1/2}(\log\log N)^2\log^{-2}N\big).$$

The lemma now follows from Lemma 5.5, (4.2B), (4.8), (8.1) and (8.2).

Since $R(N,m)$ is non-negative we have

$$R(N,m) = |R(N,m)| \geqslant |J(N,m)S(m)+D(N,m)| - |R(N,m)-J(N,m)S(m)-D(N,m)|.$$

Hence, by (8.1), (5.2) and Lemmas 10.5 and 10.6,

$$(10.3)\qquad R(N,m) \gg N(\log N)^{-2}P^{-1/32}$$

for all but at most $2N(\log N)^{8/3}P^{-1/3}$ even numbers m with $\frac{1}{2}N < m \leqslant N$.

By Definitions 5.4 and 3.2,

$$R(N,m) = R(m) \qquad (\tfrac{1}{2}N < m \leqslant N).$$

When $X = N$, Theorem 2 follows easily from this, (10.3), Definition 3.3, (8.1), (5.2) and (5.1).

This completes the proof of Theorem 2 for all sufficiently large X. The theorem as stated follows at once.

11. Proof of Theorem 1. By Definitions 3.1, 3.2 and 3.3,

$$E(N) \leqslant \sum_{\substack{m\leqslant N/2\\ R(2m)\leqslant 1}} 1 \leqslant 2Y + \sum_{Y<2^h\leqslant N}\ \sum_{\substack{2^h<2m\leqslant 2^{h+1}\\ R(2m)<2m\exp(-(\log 2m)^{1/2})}} 1 \leqslant 2Y + \sum_{h\leqslant 2\log N} E_1(2^{h+1}) \qquad (Y \geqslant C_{16}).$$

Hence, by Theorem 2,

$$E(N) \ll 1 + \sum_{n\leqslant 2\log N} 2^n\exp\big(-C_2(\log 2^{n+1})^{1/2}\big) \ll N\exp\big(-C_1(\log N)^{1/2}\big),$$

and Theorem 1 follows easily.

12. Postscript. It is possible to dispense with Siegel's theorem (Lemma 4.3) and substitute in Lemma 4.5 the weaker inequalities $\beta < 1 - C_{17}r^{-1/2}\log^{-1}r$ (see Chapter 14 of Davenport [2]) and $r > (\log N)^{1/2}$. Then it is only necessary to make the trivial modification to Lemma 10.3:

$$J(N,m) - J_\beta(N,m) > C_{18}r^{-1/2}\log^{-1}r\log NJ(N,m) \qquad (\tfrac{1}{2}N < m \leqslant N)$$

and the proof goes through as before.

The advantage of such an approach is that explicit values can then be given to $C_1, C_2, \ldots$ and the implied constants of the $\ll$ and O symbols. In the method actually used, because of the appeal to Siegel's theorem, we only prove the existence of C_1, C_2, etc.

References

[1] J. G. van der Corput, *Sur l'hypothèse de Goldbach pour presque tous les nombres pairs*, Acta Arith. 2 (1937), pp. 266–290.

[2] H. Davenport, *Multiplicative number theory*, Chicago 1967.

[3] T. Estermann, *On Goldbach's problem: Proof that almost all even positive integers are sums of two primes*, Proc. London Math. Soc. (2), 44 (1938), pp. 307–314.

[4] G. H. Hardy and J. E. Littlewood, *Some problems of 'partitio numerorum'*; III: *On the expression of a number as a sum of primes*, Acta Math. 44 (1923), pp. 1–70.

[5] — — *Some problems of 'partitio numerorum'*; (V): *A further contribution to the study of Goldbach's problem*, Proc. London Math. Soc. (2), 22 (1923), pp. 46–56.

[6] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, fourth edition, Oxford 1965.

[7] Ju. V. Linnik, *On the possibility of a unique method in certain problems of 'additive' and 'multiplicative' prime number theory*, Comptes rendus (Doklady) de l'Académie des Sciences de l'U.R.S.S. (N.S.), 49 (1945), pp. 3–7.

[8] — *A new proof of the Goldbach-Vinogradov theorem*, Recueil Mathématique (Mat. Sbornik) (N.S.) 19 (1946), pp. 3–7.

[9] A. Page, *On the number of primes in an arithmetic progression*, Proc. London Math. Soc. (2), 39 (1935), pp. 116–141.

[10] N. G. Tchudakoff, *On Goldbach-Vinogradov's theorem*, Annals of Math. 48 (1947), pp. 515–545.

[11] — *On the density of the set of even numbers which are not representable as a sum of two odd primes*, Izv. Akad. Nauk SSSR Ser. Nat. 2 (1938), pp. 25–40.

[12] I. M. Vinogradov, *Representation of an odd number as a sum of three primes*, Comptes rendus (Doklady) de l'Académie des Sciences de l'U.R.S.S. 15 (1937), 169–172.

[13] I. M. Vinogradov, *Some theorems concerning the theory of primes*, Recueil Mathématique 2 (44), 2 (1937), pp. 179–195.
[14] — *The method of trigonometrical sums in the theory of numbers*, translated from the Russian, revised and annotated by K. F. Roth and A. Davenport, Interscience Publishers, 1954.

THE DEPARTMENT OF PURE MATHEMATICS
SHEFFIELD UNIVERSITY, Great Britain

Received on 30.3.1971 (149)

ACTA ARITHMETICA
XXII (1972)

Sur les systèmes complets de restes modulo les idéaux d'un corps de nombres

par

D. BARSKY (Paris)

Monsieur Schinzel a posé la question suivante: soient K un corps de nombres, A son anneau des entiers, existe-t-il une suite d'entiers de K $a_0, a_1, \ldots$ telle que $a_0, a_1, \ldots, a_{N(\boldsymbol{m})-1}$ forment un système complet de restes modulo $\boldsymbol{m}$ pour tout idéal entier $\boldsymbol{m}$ de A de norme $N(\boldsymbol{m})$? (cf. [4]).

Nous allons montrer que la réponse est négative si $K \neq Q$.

Notations: K désigne un corps de nombres, A est son anneau des entiers; on désigne par $\boldsymbol{m}$ un idéal entier de A de norme m. On désigne par $v_{\boldsymbol{m}}(x)$ l'exposant de la plus grande puissance de $\boldsymbol{m}$ qui divise l'idéal (x) engendré par x (x est un élément de A), $v_m(n)$ est l'exposant de la plus haute puissance de m qui divise l'entier naturel n (si $\boldsymbol{m}$ est premier $v_{\boldsymbol{m}}(x)$ est la valuation $\boldsymbol{m}$-adique de x, si m est un nombre premier $v_m(n)$ est la valuation m-adique de n). Si a et b sont des entiers naturels $[a/b]$ désigne la partie entière de a/b, c'est-à-dire que $[a/b]$ est un entier tel que: $[a/b] \leqslant a/b < [a/b]+1$. $\boldsymbol{N}$ désigne l'ensemble des entiers naturels.

DÉFINITION. On dira qu'une suite d'entiers $a_0, a_1, \ldots$ d'un corps de nombres $K \neq Q$ *possède la propriété* P pour les idéaux $\boldsymbol{m}'$ et $\boldsymbol{m}''$ de même norme m si $a_0, a_1, \ldots, a_{m^h-1}$ forment un système complet de restes modulo $\boldsymbol{m}'^r\boldsymbol{m}''^s$ pour tout couple d'entiers positifs ou nuls r et s tels que $r+s = h$.

Il est clair que si une suite $a_0, a_1, \ldots$ possède la propriété P, elle est injective.

PROPOSITION 1. *Soit $a_0, a_1, \ldots$ une suite d'entiers d'un corps de nombres $K \neq Q$ possédant la propriété* P *pour deux idéaux premiers distincts $\boldsymbol{m}'$ et $\boldsymbol{m}''$ de même norme m. Alors, étant données deux applications non décroissantes u et t de $\boldsymbol{N}$ dans $\boldsymbol{N}$, telles que $u+t = w$ soit une application strictement croissante de $\boldsymbol{N}$ dans $\boldsymbol{N}$ et que $u(0) = t(0) = 0$, on peut définir une injection g de $\boldsymbol{N}$ dans $\boldsymbol{N}$ telle que si l'on pose $b_i = a_{g(i)}$ on ait:*