AD734836

THEORY OF NUMBERS

Final Technical Report

December 1971

by

H. Halberstam

EUROPEAN RESEARCH OFFICE

United States Army
London, G.B.

Contract Number: DAJA37-71-C-1118

University of Nottingham

The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

24

Security Classification

DOCUMENT CONTROL DATA - R & D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

1. ORIGINATING ACTIVITY (Corporate author) Department of Mathematics University of Nottingham, England.	2a. REPORT SECURITY CLASSIFICATION Unclassified 2b. GROUP N/A
3. REPORT TITLE THEORY OF NUMBERS	
4. DESCRIPTIVE NOTES (Type of report and inclusive dates) Final Technical Report 1 Oct 70 - 31 Sept 71	
5. AUTHOR(S) (First name, middle initial, last name) Professor H. Halberstam	
6. REPORT DATE October 1971	7a. TOTAL NO. OF PAGES 20 / 7b. NO. OF REFS
8a. CONTRACT OR GRANT NO. DAJA37-71-C-1118 b. PROJECT NO. 20061102B14C c. d.	9a. ORIGINATOR'S REPORT NUMBER(S) 9b. OTHER REPORT NO(S) (Any other numbers that may be assigned this report) E - 1339
10. DISTRIBUTION STATEMENT **This document has been approved for public release and sale; its distribution is unlimited.**	
11. SUPPLEMENTARY NOTES	12. SPONSORING MILITARY ACTIVITY **US Army Research & Development Gp (EUR) Box 15, FPO New York 09510**

13. ABSTRACT

(U) The first part deals with a class of divisor problems. The average of the divisor function (the number of representations as a product of k factors) over numbers of the form p-a, p ≤ x (p prime) is tied up with a certain conjecture about the distribution of primes in arithmetic progressions.

(U) The second part describes some interesting numerical work by J.W. Porter in connection with Selberg's sieve which, when joined with some recent theorems of Halberstam and Richert, yields new results in additive prime number theory. This work will appear in Acta Arithmetica. Porter also outlines progress towards an improvement of the Selberg-Buchstab approach to the lower-bound sieve.

(U) The third part is a survey by H. Halberstam of recent progress, largely due to Richert and himself, towards the notorious Hypothesis H of Schinzel concerning prime values assumed simultaneously by numbers of integer valued polynomials.

KEYWORDS: Arithmetic Progressions; (U) Prime Numbers; (U) Sieve Methods

DD FORM 1 NOV 65 1473 REPLACES DD FORM 1473, 1 JAN 64, WHICH IS OBSOLETE FOR ARMY USE.

UNCLASSIFIED
Security Classification

INDEX

Abstract

Chapter 1 deals with a class of divisor problems. The average of the divisor function τ_k (the number of representations as a product of k factors) over numbers of the form $p - a$, $p \leq x$ (p prime) is tied up with a certain conjecture about the distribution of primes in arithmetic progressions. This work is to appear in the Proc. of the London Mathematical Society.

Chapter 2 describes some interesting numerical work by J.W. Porter in connection with Selberg's sieve which, when joined with some recent theorems of Halberstam and Richert, yields several remarkably good new results in additive prime number theory. This work will appear in Acta Arithmetica. In this Chapter, too, Porter outlines some progress he is beginning to make with an improvement of the Selberg-Buchstab approach to the lower-bound sieve.

Chapter 3 is a survey by H. Halberstam of recent progress, largely due to Richert and himself, towards the notorious Hypothesis H of Schinzel concerning prime values assumed simultaneously by numbers of integer valued polynomials. The progress has taken the form of approximating to the classical questions in terms of results about almost-primes; and similar approximations with respect to other questions in prime number theory are described.

1. DIVISOR SUMS

Let k be an integer greater than one, and denote by $\tau_k(n)$ the number of ways of expressing the positive integer n as the product of k positive integers, having regard to the order of the factors. Write $T_{a,k}(x)$ for the sum

$$\sum_{a<p\leq x} \tau_k(p-a)$$

where a is a positive integer.

Porter has obtained an asymptotic formula for $T_{a,k}(x)$ on the basis of the following hypothesis (H_k):

If $\pi(x;d,h)$ denotes the number of primes less than x congruent to h modulo d, then there exists a number $B = B(k)$ such that

$$\sum_{d\leq x^{1-1/k}(\log x)^{-B}} \max_{\substack{1\leq h<d \\ (d,h)=1}} \left|\pi(x;d,h) - \frac{\operatorname{li} x}{\phi(d)}\right| \ll \frac{x}{\log^{k^2-4k+6} x} .$$

<u>Theorem</u>: If (H_k) is true, then, as $x \to \infty$,

$$T_{a,k}(x) \sim \frac{1}{(k-1)!} \prod_{p\nmid a} \left(1 + \frac{p^{k-1}-(p-1)^{k-1}}{p^{k-1}(p-1)}\right) \prod_{p|a} \left(1-\frac{1}{p}\right)^{k-1} x \log^{k-2} x .$$

We begin with the remark that

$$\tau_k(n) = \sum_{t_0 t_1 \ldots t_{k-1}=n} 1$$

$$= k! \sum_{\substack{t_{k-1}<t_{k-2}<\ldots<t_0 \\ t_0 t_1 \ldots t_{k-1}=n}} 1 + O\Big(\sum_{t_1^2 t_2 \ldots t_{k-1}=n} 1\Big)$$

$$= k! \sum_{\substack{t_{k-1}<n^{1/k} \\ t_{k-1}<t_{k-2}<(n/t_{k-1})^{1/(k-1)} \\ \vdots \\ t_2<t_1<(n/t_2 t_3 \ldots t_{k-1})^{1/2} \\ t_0 t_1 \ldots t_{k-1}=n}} 1 + O\Bigl(\sum_{t_1^2 t_2 \ldots t_{k-1}=n} 1 \Bigr)$$

Hence

$$T_{a,k}(x) = k! \sum_{a<p\leq x} \sum_{\substack{t_{k-1}<(p-a)^{1/k} \\ t_{k-1}<t_{k-2}<\{(p-a)/t_{k-1}\}^{1/(k-1)} \\ \vdots \\ t_2<t_1<\{(p-a)/t_2 t_3 \ldots t_{k-1}\}^{1/2} \\ p\equiv a \bmod t_1 t_2 \ldots t_{k-1}}} 1 + O\Bigl(\sum_{n\leq x} \sum_{t_1^2 t_2 \ldots t_{k-1}=n} 1 \Bigr)$$

$$= k! \sum_{t_{k-1}<x^{1/k}} \sum_{t_{k-1}<t_{k-2}<(x/t_{k-1})^{1/(k-1)}} \cdots$$

$$\sum_{t_2<t_1<(x/t_2 t_3 \ldots t_{k-1})^{1/2}} \sum_{\substack{a+t_1^2 t_2 \ldots t_{k-1}<p\leq x \\ p\equiv \bmod t_1 t_2 \ldots t_{k-1}}} 1$$

$$+ O\Bigl(\sum_{t\leq x^{1/2}} \sum_{m\leq x/t^2} \tau_{k-2}(m) \Bigr);$$

that is

$$T_{a,k}(x) = k! \Sigma^* \{ \pi(x; t_1 t_2 \ldots t_{k-1}, a) - \pi(a+t_1^2 t^2 \ldots t_{k-1}; t_1 t_2 \ldots t_{k-1}, a) \}$$

$$+ O\Bigl(\sum_{t\leq x^{1/2}} \frac{x}{t^2} \log^{k-3} x \Bigr) \qquad (1)$$

where we write Σ^* for the $(k-1)$-fold summation symbol

$$\sum_{t_{k-1}<x^{1/k}} \sum_{t_{k-1}<t_{k-2}<(x/t_{k-1})^{1/(k-1)}} \cdots \sum_{t_2<t_1<(x/t_2 t_3 \ldots t_{k-1})^{1/2}} .$$

It follows from (1) that

$$T_{a,k}(x) = k!\,\mathrm{li}\,x.S_1 + k!S_2 - k!S_3 + O(x\log^{k-3}x) \tag{2}$$

where

$$S_1 = \sum_{(t_1 t_2 \ldots t_{k-1}, a)=1}^{*} \frac{1}{\phi(t_1 t_2 \ldots t_{k-1})}, \tag{3}$$

$$S_2 = \sum_{(t_1 t_2 \ldots t_{k-1}, a)=1}^{*} \left\{\pi(x; t_1 t_2 \ldots t_{k-1}, a) - \frac{\mathrm{li}\,x}{\phi(t_1 t_2 \ldots t_{k-1})}\right\} \tag{4}$$

and

$$S_3 = \Sigma^* \; \pi(a+t_1^2 t_2 \ldots t_{k-1}; t_1 t_2 \ldots t_{k-1}, a). \tag{5}$$

We remark that if $t_1, t_2, \ldots, t_{k-1}$ are subject to the conditions of summation of Σ^*,

$$t_1 t_2 \ldots t_{k-1} < x^{1-\frac{1}{k}}. \tag{6}$$

We now prove a lemma (which we shall require in the estimation of S_1 in Lemma 2) concerning sums of the form

$$G(Y) = \sum_{\substack{c<t<Y \\ (t,a)=1}} \frac{1}{t} \prod_{p|bt} (1+f(p)) \tag{7}$$

where b, c are positive integers, $(b,a) = 1$ and $f(p)$ satisfies the inequality

$$0 < f(p) \le \frac{1}{p-1}. \tag{8}$$

Lemma 1.

Under the condition (8),

$$G(Y) = \prod_{p\nmid a}\left(1+\frac{f(p)}{p}\right) \prod_{p|a}\left(1-\frac{1}{p}\right) \prod_{p|b}\left(1+\frac{(p-1)f(p)}{p+f(p)}\right)\log\frac{Y}{c}$$

$$+ O\left(\sum_{d|b} \frac{\mu^2(d)\tau(d)}{\phi(d)}\right). \tag{9}$$

Proof.

Define $f(d)$ for square-free d by demanding that f be multiplicative, so that

$$G(Y) = \sum_{\substack{c<t<Y \\ (t,a)=1}} \frac{1}{t} \sum_{m|bt} \mu^2(m)f(m).$$

In the inner summation write $m = d\delta$, where $d|b$, $\delta|t$, and $(d,t) = 1$. We find

$$G(Y) = \sum_{d|b} \mu^2(d)f(d) \sum_{\substack{c<t<Y \\ (t,ad)=1}} \frac{1}{t} \sum_{\delta|t} \mu^2(\delta)f(\delta)$$

$$= \sum_{d|b} \mu^2(d)f(d)H_d(Y), \tag{10}$$

writing

$$H_d(Y) = \sum_{\substack{c<t<Y \\ (t,ad)=1}} \frac{1}{t} \sum_{\delta|t} \mu^2(\delta)f(\delta)$$

$$= \sum_{\substack{c<t<Y \\ (t,ad)=1}} \frac{1}{t} \prod_{p|t} (1+f(p)).$$

We now define a multiplicative function g on the square-free integers by setting

$$g(p) = \begin{cases} f(p) & \text{if } p\nmid ad \\ -1 & \text{if } p|ad \end{cases}$$

so that

$$H_d(Y) = \sum_{c<t<Y} \frac{1}{t} \prod_{p|t} (1+g(p))$$

$$= \sum_{c<t<Y} \frac{1}{t} \sum_{m|t} \mu^2(m)g(m)$$

$$= \sum_{c<mn<Y} \frac{\mu^2(m)g(m)}{mn}$$

$$= H_1 - H_2 \tag{11}$$

where

$$H_1 = \sum_{mn<Y} \frac{\mu^2(m)g(m)}{mn}$$

and

$$H_2 = \sum_{mn\le c} \frac{\mu^2(m)g(m)}{mn} .$$

Now

$$H_1 = \sum_{n<Y} \frac{1}{n} \sum_{m<Y/n} \frac{\mu^2(m)g(m)}{m}$$

$$= \sum_{m=1}^{\infty} \frac{\mu^2(m)g(m)}{m} \sum_{n<Y} \frac{1}{n} - \sum_{n<Y} \frac{1}{n} \sum_{m\ge Y/n} \frac{\mu^2(m)g(m)}{m}$$

It follows, after some manipulation of the error term, that

$$H_1 = \sum_{m=1}^{\infty} \frac{\mu^2(m)g(m)}{m}\{\log Y + O(1)\} + O(\tau(d))$$

A similar calculation for H_2, together with (11) shows that

$$H_d(Y) = \prod_p\left(1+\frac{g(p)}{p}\right)\left\{\log\frac{Y}{c} + O(1)\right\} + O(\tau(d)) .$$

The conclusion of the Lemma now follows without difficulty from (10).

<u>Lemma 2</u>.

$$S_1 = \frac{1}{k!(k-1)!} \prod_{p\nmid a}\left(1+\frac{p^{k-1}-(p-1)^{k-1}}{p^{k-1}(p-1)}\right)\prod_{p|a}\left(1-\frac{1}{p}\right)^{k-1} \log^{k-1} x + O(\log^{k-2} x) .$$

<u>Proof</u>.

We shall write, for $r = 1,2,\ldots,k-2$, and b,c positive integers coprime to a,

$$T_r(x;b,c) = \sum_{\substack{c<t_r<(x/b)^{1/(r+1)} \\ (t_r,a)=1}} \sum_{\substack{t_r<t_{r-1}<(x/bt_r)^{1/r} \\ (t_{r-1},a)=1}} \cdots$$

$$\sum_{\substack{t_2<t_1<(x/bt_r\ldots t_2)^{1/2} \\ (t_1,a)=1}} \frac{1}{\phi(bt_r\ldots t_1)}$$

We further define $T_{k-1}(x;b,c)$ by the above equation, save that the first summation symbol is replaced by

$$\sum_{c\le t_{k-1}<(x/b)^{1/k}} .$$

We note that $S_1 = T_{k-1}(x;1,1)$. We shall prove by induction on r that

$$T_r(x;b,c) = \frac{C(r)}{b}\prod_{p|b}(1+f_r(p))\log^r\left(\frac{x}{bc^{r+1}}\right)$$

$$+ O\left(\frac{1}{b}\sum_{d|b}\frac{\mu^2(d)\tau(d)}{\phi(d)}\log^{r-1}x\right), \qquad (12)$$

where

$$C(r) = \frac{1}{(r+1)!r!}\prod_{p\nmid a}\left(1+\frac{p^r-(p-1)^r}{p^r(p-1)}\right)\prod_{p|a}\left(1-\frac{1}{p}\right)^r$$

and

$$f_r(p) = \frac{(p-1)^r}{p^{r+1}-(p-1)^r} .$$

The lemma then follows from (12). Thr truth of (12) for $r = 1$ is an immediate consequence of Lemma 1. Suppose therefore that (12) is true for $r = R$. Then

$$T_{R+1}(x;b,c) = \sum_{\substack{c<t<(x/b)^{1/(R+2)}\\(t,a)=1}}\frac{C(R)}{bt}\prod_{p|bt}(1+f_R(p))\log^R\left(\frac{x}{bt^{R+2}}\right)$$

$$+ O\left(\log^{R-1}x\sum_{t<x}\frac{1}{bt}\sum_{d|bt}\frac{\mu^2(d)\tau(d)}{\phi(d)}\right) \qquad (13)$$

If we write, for $R > 0$,

$$G_R(Y) = \sum_{\substack{c<t<Y\\(t,a)=1}}\frac{1}{t}\prod_{p|bt}(1+f_R(p)),$$

we have for the main term of (13)

$$\frac{C(R)}{b}\int_c^{(x/b)^{1/(R+2)}} \log^R\left(\frac{x}{bt^{R+2}}\right) dG_R(t)$$

$$= \frac{C(R)R(R+2)}{b}\int_c^{(x/b)^{1/(R+2)}} G_R(t)\log^{R-1}\left(\frac{x}{bt^{R+2}}\right)\frac{dt}{t}$$

$$= \frac{C(R+1)}{b}\prod_{p|b}(1+f_{R+1}))\log^{R+1}\left(\frac{x}{bc^{R+2}}\right) + O\left(\frac{1}{b}\sum_{d|b}\frac{\mu^2(d)\tau(d)}{\phi(d)}\log^R x\right),$$

on applying Lemma 1.

The error term in (13) can be easily shown to be

$$O\left(\frac{1}{b}\sum_{d|b}\frac{\mu^2(d)\tau(d)}{\phi(d)}\log^R x\right).$$

This completes the induction step and the proof of the Lemma.

<u>Lemma 3</u>.

$$S_3 = O(x\log^{k-3} x).$$

<u>Proof</u>:

By the Brun-Titchmarsh theorem,

$$S_3 \ll \Sigma^* \frac{t_1^2 t_2 \ldots t_{k-1}}{\phi(t_1 t_2 \ldots t_{k-1})\log t_1}$$

whence the result follows without difficulty.

<u>Lemma 4</u>.

On the hypothesis (H_k),

$$S_2 = O\left(x\log^{k-\frac{5}{2}} x\right).$$

<u>Proof</u>:

We remark first that the summation over t_1 in S_2 may be restricted to the range

$$t_2 < t_1 < \left(\frac{x(\log x)^{-2B}}{t_2 \ldots t_{k-1}}\right)^{1/2},$$

since the contribution of the remaining values of t_1 may be shown to be $O(x \log^{k-3} x \log\log\log x)$, by an application of the Brun-Titchmarsh theorem.

If we write

$$E(x,n) = \max_{\substack{1 \le a \le n \\ (a,n)=1}} \left|\pi(x;n,a) - \frac{\operatorname{li} x}{\phi(n)}\right|,$$

we have

$$S_2 \ll \sum_{n < x^{1-\frac{1}{k}}(\log x)^{-B}} \tau_{k-1}(n) E(x,n) + x \log^{k-3} x \log\log\log x \qquad (14)$$

By the Cauchy-Schwarz inequality and Hypothesis (H_k),

$$\sum_{n < x^{1-\frac{1}{k}}(\log x)^{-B}} \tau_{k-1}(n) E(x,n)$$

$$\le \Big(\sum_{n<x} \tau_{k-1}^2(n) E(x,n)\Big)^{1/2} \Big(\sum_{n < x^{1-\frac{1}{k}}(\log x)^{-B}} E(x,n)\Big)^{1/2}$$

$$\ll x^{1/2} \Big(\sum_{n<x} \frac{\tau_{k-1}^2(n)}{n}\Big)^{1/2} x^{1/2} (\log x)^{-\frac{1}{2}(k^2-4k+6)}$$

$$\ll x \log^{k-\frac{5}{2}} x.$$

The theorem now follows from (2) and Lemmas 2, 3 and 4.

2. THE SMALL SIEVE

A. Ankeny and Onishi (Acta Arithmetica, 1964) have shown the importance of the solutions of certain differential-difference equations and parameters defined in terms of them in the Selberg lower-bound sieve method.

For each $\kappa > 0$ let $\sigma_\kappa(u)$ denote the (continuous) solution of the differential-difference equation,

$$(u^{-\kappa}\sigma_\kappa(u))' = -\kappa u^{-\kappa-1}\sigma_\kappa(u-2), \qquad (u \geq 2)$$

$$\sigma_\kappa(u) = \frac{2^{-\kappa}e^{-\gamma\kappa}}{\Gamma(\kappa+1)}u^\kappa. \qquad (0 \leq u \leq 2).$$

Further let ν_κ denote the (unique and positive) solution of the equation

$$\eta_\kappa(x) = \kappa x^{-\kappa}\int_x^\infty \left(\frac{1}{\sigma_\kappa(t-1)} - 1\right)t^{\kappa-1}\, dt = 1.$$

Porter has investigated these functions on a computer and has extended the table of values of ν_κ as far as $\kappa = 16$. He has also found and corrected what appears to be a systematic error in the table of values of $\sigma_2(u)$ given by Ankeny and Onishi.

The results of these calculations have a number of consequences of which some of the most interesting are summarized in the

Theorem:

(i) There are infinitely many primes p such that $(p+2)(p+6)$ is the product of at most 7 prime factors.

(ii) There are infinitely many n such that $(8n+1)(n^2+n+1)$ is the product of at most 6 prime factors.

(iii) There are infinitely many primes p such that $(p+2)(p^2+p+1)$ is the product of at most 9 prime factors.

B. Porter has now obtained a lower bound for the 'non-linear' sieve which is slightly superior to that given in the Third Quarterly Report. As usual, we suppose that we have a sequence $\mathcal{A}$ of integers and a set $\mathcal{P}$ of primes for which we can find a number X, a multiplicative function $\omega(d)$ and numbers R_d satisfying a number of conditions of which the most important are the following:

(i)
$$\sum_{\substack{a\in\mathcal{A}\\ d|a}} 1 = \frac{\omega(d)}{d}X + R_d;$$

(ii) There exists a number $\varkappa > 0$ such that

$$\sum_{p<x} \frac{\omega(p)}{p}\log p = \varkappa \log x + O(1);$$

(iii) There exists a number ξ suxh that

$$\sum_{d<\xi^2} \mu^2(d)3^{\nu(d)}|R_d| = O\left(\frac{X}{\log^{\varkappa+1} X}\right)$$

where $\nu(n)$ denotes the number of prime factors of n.

We seek upper and lower bounds for the quantity

$$S(\mathcal{A}_q;\mathcal{P},z) = \left|\left\{a\in\mathcal{A};\ q|a \text{ and } \left(a, \prod_{\substack{p\in\mathcal{P}\\ p<z}} p\right) = 1\right\}\right|.$$

As before we let, for r = 2,3

$$\eta_{\varkappa,r}(x) = \varkappa x^{-\varkappa}\int_x^\infty t^{\varkappa-1}\eta_{\varkappa,r-1}(t-1)\,dt,$$

interpreting $\eta_{\varkappa,1}(x)$ as $\eta_\varkappa(x)$.

We suppose that the equation

$$\frac{1}{\sigma_\varkappa(x)} = 1 + \eta_{\varkappa,2}(x)$$

has a unique root $\lambda_\varkappa$ (a conjecture that is supported by numerical evidence, at least for small $\varkappa$). Then starting from the second iteration of the Buchstab identity in the form

$$S(\mathcal{A}_q;\mathcal{P},z) = S(\mathcal{A}_q;\mathcal{P},z_1) - \sum_{\substack{z_1 \le p < z \\ p < \xi^{2/(1+\lambda_\varkappa)}}} S(\mathcal{A}_{qp};\mathcal{P},z_1)$$

$$+ \sum_{\substack{z_1 \le p_2 < p_1 < z \\ p_1 < \xi^{2/(1+\lambda_\varkappa)} \\ p_1, p_2 \in \mathcal{P}}} S(\mathcal{A}_{qp_1p_2};\mathcal{P},p_2) - \sum_{\substack{z_1 \le p < z \\ \xi^{2/(1+\lambda_\varkappa)} \le p \\ p \in \mathcal{P}}} S(\mathcal{A}_p;\mathcal{P},p)$$

we obtain the following bounds:

$$S(\mathcal{A}_q;\mathcal{P},z) \le \frac{\omega(q)}{q}X \prod_{p<z}\left(1-\frac{\omega(p)}{p}\right)F_\varkappa\left(\frac{\log \xi^2}{\log z}\right) + \text{ error terms}$$

and

$$S(\mathcal{A}_q;\mathcal{P},z) \ge \frac{\omega(q)}{q}X \prod_{p<z}\left(1-\frac{\omega(p)}{p}\right)f_\varkappa\left(\frac{\log \xi^2}{\log z}\right) + \text{ error terms,}$$

with

$$F_\varkappa(u) = 1 + \eta_{\varkappa,2}(u)$$

and

$$f_\varkappa(u) = \begin{cases} 1 - \eta_\varkappa(u) + \left(\dfrac{\lambda_\varkappa+1}{u}\right)^{\varkappa}\{\eta_\varkappa(\lambda_\varkappa+1) - \eta_{\varkappa,3}(\lambda_\varkappa+1)\} & (u \le \lambda_\varkappa + 1) \\ 1 - \eta_{\varkappa,3}(u) & (u > \lambda_\varkappa + 1) \end{cases}$$

Numerical investigation of these functions and their consequences in the applications of the sieve is in progress.

3. THE SMALL SIEVE: PROGRESS TOWARDS HYPOTHESIS H

(i) Prime number theory studies the distribution of primes in sequences of natural numbers, such as N itself, arithmetic progressions and polynomial sequences (such as $n^2 + 1$, $n = 1, 2, \ldots$). An extensive range of such questions is embraced by

<u>Hypothesis</u> H (Schinzel 1958)

Let $f_1, \ldots, f_g$ be distinct, irreducible polynomials $\in Z[x]$ (with positive leading coefficients) and suppose that $f_1 \ldots f_g$ has no fixed prime divisors. Then there exist infinitely many integers n such that each $f_i(n)$ $(i = 1, \ldots, g)$ is PRIME.

When $g = 1$ and $f_1(n) = an + b$, with $(a, b) = 1$, H asserts in effect that the arithmetic progression $an + b$ $(n = 1, 2, \ldots)$ contains infinitely many primes; this was proved by Dirichlet in 1837 and is the <u>only</u> case of H known to be true!

The general case $g = 1$ was conjectured as long ago as 1857 by Bouniakovsky; an interesting particular case would be $n^2 + 1 = p$ infinitely often (to be written i.o. for short). The case of g <u>linear</u> polynomials was first conjectured by Dickson in 1904; with $g = 2$, $f_1(n) = n$ and $f_2(n) = n + 2$ we should obtain the prime twins conjecture.

Let us write $F_g = f_1 \ldots f_g$, and let P_r denote an <u>almost-prime of order</u> r, that is, a number having at most r prime factors, counted according to multiplicity. Then H asserts, subject to the stated conditions on F_g that

$$F_g(n) = P_g \quad \text{i.o.} \tag{1}$$

Although experimental and heuristic evidence suggests not only that (1) is true but that it is true very often indeed

(H has been formulated in quantitative form by Bateman and Horn), H appears to be, at the present state of knowledge, almost hopelessly difficult. Nevertheless, let us formulate a companion conjecture, H*, which, if anything, lies even deeper!

<u>Hypothesis</u> H*

Let $\rho_g(p)$ denote the number of solutions of the congruence $F_g(x) \equiv 0 \bmod p$, $0 \leq x < p$ and suppose that $\rho_g(p) < p$ for all primes p (as in H), as well as that $\rho_g(p) < p - 1$ if $p \nmid F_g(0)$ (this requirement can be seen to be essentially necessary). Assume that $f_i(n) \neq n$ $(i = 1, \ldots, g)$.

Then

$$(2) \qquad F_g(p) = P_g \quad \text{i.o.}$$

It is easily seen that the case $g = 1$, f_1 linear leads, in particular, to the prime twins conjecture (again) and to Goldbach's conjecture.

The object of this survey is to describe the currently best known approximations to H and H*; though far short of what is probably true these approximations - of type

$$(1') \qquad F_g(n) = P_h \quad \text{i.o.}$$

and

$$(2') \qquad F_g(p) = P_{h*} \quad \text{i.o.,}$$

where $h = h(g,k)$ and $h* = h*(g,k)$ $(k = \deg F_g)$ - are nevertheless of such a quality as to represent, I believe, results of intrinsic interest.

(ii) <u>Results: $g = 1$</u>

Here, for the case of a single irreducible polynomial $F_1 = (f_1)$, we obtain the sharpest results. An account of the method of proof is to be found in H.-E. Richert (Mathematika 1969) where theorem 1 below, as well as the corollaries of theorem 2, are stated explicitly.

<u>Theorem 1</u> <u>If</u> $\deg F_1 = k$, <u>then, under the conditions in</u> H;

$$F_1(n) = P_{k+1} \quad \text{i.o.},$$

<u>and, under the conditions of</u> H*,

$$F_1(p) = P_{2k+1} \quad \text{i.o.}$$

Thus, for example, $n^2 + 1 = P_3$ i.o., and $p^2 + p + 1 = P_5$ i.o.

In the linear case of H* we have

<u>Theorem 2</u> <u>If</u> $ab \neq 0$, $(a,b) = 1$ <u>and</u> $2|ab$,

$$ap + b = P_3 \quad \text{i.o.};$$

<u>of the prime factors of</u> P_3, <u>none is less than</u> $(\ell i\, N)^{1/8}$; <u>in fact</u>, P_3 <u>is either a</u> P_2 <u>or has a (non-repeated) prime factor between</u> $(\ell i\, N)^{1/8}$ and $(\ell i\, N)^{3/8}$. <u>Moreover</u>,

$$|\{p : p \leq x,\ ap + b = P_3\}| \geq \frac{8}{3} \prod_{p>2}\left(1 - \frac{1}{(p-1)^2}\right) \prod_{2<p|ab} \frac{p-1}{p-2}\, \frac{x}{\log^2 x}$$

$$(x \geq x_0).$$

As contributions towards the prime twins and Goldbach conjectures one can show in this way that

<u>Corollary 1</u> $\quad p + 2 = P_3 \quad$ i.o.

and

<u>Corollary 2</u> <u>If</u> n <u>is a large enough even natural number, then</u> n <u>can be represented in the form</u>

$$n = p + P_3 .$$

Let us take $a = 8$ and $b = 1$ in theorem 2. There is an interesting connection here with another old conjecture in multiplicative number theory: namely, that if $d(n)$ is the Dirichlet divisor function, then <u>there exist infinitely many n</u>

<u>such that $d(n+1) = d(n)$</u>. Now if we could be sure in theorem 2 that the P_3 is, i.o., the product of three distinct primes, we should have immediately a proof of this conjecture. As it is, all we can deduce is that either the conjecture is true or $8p + 1 = P_2$ i.o.!

(This observation arose from a conversation with Professor Mirsky and Dr. Vaughan.)

Intuitively, one would expect better results if one considered instead of polynomials in a single variable, forms in several variables. In confirmation we have

<u>Theorem 3</u> (G. Greaves - <u>J. of Number Theory</u> 1971) <u>If</u> F <u>is an irreducible form</u> $\in \mathbb{Z}[x,y]$ <u>of degree</u> $k \geq 3$, <u>without fixed prime divisors, then</u>

$$F(m,n) = P_{[k/2]+1} \quad \text{i.o.}$$

For example, if $k = 3$, $F(m,n) = P_2$ i.o.

(The case of quadratic forms was already settled by de la Vallee Poussin.)

(iii) <u>Results: $g > 1$</u>

H.E. Richert and I have developed and refined the method of Ankeny and Onishi (<u>Acta Arithmetica</u> 1964) to yield all the results listed below; a full account of the method and of the proofs will be given in a forthcoming book by Richert and myself on <u>Sieve Methods</u>. To gain the maximum precision from the method one must have recourse to numerical integration; this has been done for several special problems in the theorem of Section 2A. There is another method which yields results as general as those listed below, due to Miech (<u>Acta Arithmetica</u> 1964); but our results are always at least as good as his, and mostly better.

<u>Theorem 4</u> <u>Let</u> a_i, b_i $(i = 1, \ldots, g)$ <u>be integers satisfying</u>

$$\prod_{i=1}^{g} a_i \prod_{1 \le j < k \le g} (a_j b_k - a_k b_j) \ne 0 .$$

<u>If the polynomial</u> $\prod_{i=1}^{g} (a_i n + b_i)$ <u>satisfies the conditions in</u> H, <u>it is infinitely often a</u> P_h <u>provided</u>

(3) $$h = h(g) > (g+1)\log \nu_g + g - 1 ;$$

<u>and if it satisfies the conditions of</u> H*, <u>then</u> $\prod_{i=1}^{g} (a_i p + b_i)$ <u>is infinitely often a</u> P_{h*} <u>provided</u>

(4) $$h^* = h^*(g) > (g+\tfrac{1}{2}) \log 2\nu_g + 2g - 1 - \tfrac{1}{2}(g/\nu_g)$$

<u>the</u> ν_g <u>occurring in (3) and (4) increases with</u> g, <u>and</u> $\nu_g/g \to 2.44 \ldots$ <u>as</u> $g \to \infty$ (see Table 1 p. 18)

For example, we have $h(3) = 10$ and $h^*(3) = 14$ as admissible choices in theorem 5. Table 2 provides such information for other values of g. For g very large, we see that

$$h(g) \sim g \log g + (1.892\ldots)g$$

Theorem 4 is a special case of the following quite general result.

<u>Theorem 5</u> <u>If</u> F_g <u>satisfies the conditions of</u> H, <u>then</u> infinitely often $F_g(n) = P_h$ <u>provided</u> $(k = \deg F_g)$

$$h = h(g,k) > g\left(1 + \frac{1}{k}\right) \log \left(\frac{\nu_g}{g} k\right) + k - 1 - \frac{k-g}{k} \frac{g}{\nu_g} ;$$

<u>and if</u> F_g <u>satisfies the conditions of</u> H*, <u>then infinitely</u> often, $F_g(p) = P_{h*}$ provided

$$h^* = h^*(g,k) > g\left(1 + \frac{1}{2k}\right) \log \left(2\frac{\nu_g}{g} k\right) + 2k - 1 - \frac{2k-g}{2k} \frac{g}{\nu_g} .$$

With the help of Table 1, many numerical illustrations may be constructed. Here are two special results where maximum precision has been sacrificed to simplicity of form: if $k \geq 5$, we have

$$F_2(n) = P_{[k+2\log k]+1} \quad \text{i.o.}$$

in the case of H; and, in the case of H*,

$$F_2(p) = P_{[2k+2\log k]+3} \quad \text{i.o.}$$

g	ν_g	ν_g/g
1	2.06...	2.06...
2	4.42...	2.21...
3	6.85...	2.28...
4	9.32...	2.33...
5	11.80...	2.36...
6	14.28...	2.38...
7	16.77...	2.39...
8	19.25...	2.40...
9	21.74...	2.41...
10	24.22...	2.42...
11	26.70...	2.42...
12	29.20...	2.43...
13	31.68...	2.43...
14	34.15...	2.43...
15	36.62...	2.44...
16	39.09...	2.44...

Table 1

g	1	2	3	4	5	6	7	8	9	10
h	2	6	10	15	19	24	29	34	39	45
h^*	4	9	14	20	27	33	39	46	53	60

Table 2

(iv) Related results

The methods for proving the results of section 2 (the case $g = 1$) can be made to yield also approximations, in terms of almost-primes, to the famous classical problems concerning gaps between consecutive primes, and the least prime in an arithmetic progression. Theorems 6 and 7 are slight refinements of two theorems in the paper of Richert cited earlier. The refinement amounts to introducing some control on the multiplicity of the prime factors of almost-primes, and is made possible by applying some old results of Roth and Halberstam-Roth on gaps between consecutive k-free numbers (J. London Math. Soc. 1951)

Theorem 6 Let $P_r^{(k)}$ denote a k-free almost-prime of order r. Then there is a

$$P_2^{(2)} \quad \text{in} \quad [x - x^{6/11}, x) \quad \text{for} \quad x \geq x_2,$$

$$P_3^{(3)} \quad \text{in} \quad [x - x^{4/11}, x) \quad \text{for} \quad x \geq x_3,$$

$$P_4^{(2)} \quad \text{in} \quad [x - x^{3/11}, x) \quad \text{for} \quad x \geq x_4,$$

and a

$$P_r^{([\frac{1}{2}(r+1)])} \quad \text{in} \quad [x - x^{\frac{1}{r-(2/7)}}, x) \quad \text{for} \quad x \geq x_r,\ r \geq 5 .$$

These results should be compared with the recent result of H. Montgomery, according to which there is a prime in

$$[x - x^{\frac{3}{5}+\varepsilon}, x) \quad \text{if} \quad x \geq x_0(\varepsilon).$$

Theorem 7 Suppose that a and b are coprime natural numbers. Then the arithmetic progression b mod a contains a

$$P_2^{(2)} \leq a^{11/5} \quad (a \geq a_2),\quad P_3^{(2)} \leq a^{11/7} \quad (a \geq a_3),$$

$$P_4 \leq a^{11/8} \quad (a \geq a_4) \text{ and a } P_r \leq a^{1 + \frac{1}{r-(9/7)}} \quad (a \geq a_r,\ r \geq 5).$$

These results should be measured against Linnik's famous result which, in a later form, states that the progression $b \bmod a$ contains a prime $p \leq a^{777}$; and the result of Elliott and Halberstam according to which the least prime $p(a,b)$ in the arithmetic progression $b \bmod a$ satisfies

$$p(a,b) \leq \phi(a) \log a . \delta(a) \quad (a \geq a_0)$$

with $\delta(a)$ any positive function tending monotonically and arbitrarily slowly to ∞, for asymptotically $\phi(a)$ progressions $b \bmod a$, for almost all a.

Fluch has proved recently that $b \bmod a$ contains a $P_4^{(2)} \leq a^{3/2}$; it would be interesting to see whether the P_4 in theorem 7 could be chosen squarefree - this is probably rather difficult. Not only should we then have an improvement of Fluch's result, but also of the old Prachar-Erdos result concerning the least squarefree number in an arithmetic progression.

To illustrate the versatility of the modern sieve method, let me conclude by quoting the following recent result:

<u>Theorem 8</u> (Deshouillers 1971 - unpublished) <u>If</u> α <u>is irrational, there exist infinitely many integers</u> n <u>such that</u> $[\alpha n^2] = P_6$.

BIBLIOGRAPHY

Chapter 1:

1. P.D.T.A. Elliott and H. Halberstam, 'A conjecture in prime number theory', Ist.Naz. Alta Mat. Symp. Mat. IV (1970) 59-72.

2. H. Halberstam, 'Footnote to the Titchmarsh-Linnik divisor problem', Proc. Amer. Math. Soc. 18, No.1 (1967), 187-88.

3. Ju.V. Linnik, 'The dispersion method in binary additive problems' (Leningrad, 1961; Transl. Math. Monographs, Vol. 4, Amer. Math. Soc. Providence, R.I., 1963, Chapter 8).

4. G. Rodriquez, 'Sul problema dei divisori di Titchmarsh', Boll. Un. Mat. Ital. (3) 20 (1965) 358-66.

Chapter 2:

1. N.C. Ankeny and H. Onishi, 'The general sieve', Acta Arith. 10 (1964) 31-62.

2. W.B. Jurkat and H.-E. Richert, 'An improvement of Selberg's sieve method I', Acta Arith. 11 (1965) 217-240.

Chapter 3:

1. H. Halberstam and K.F. Roth, 'On the gaps between consecutive k-free integers', Jour. Lond. Math. Soc. 26 (1951) 268-73.

2. W. Fluch, 'Bemerkung uber quadratfreie Zahlen in arithmetischen Progressionen', Monatshefte fur Mathematik 72 (1968) 427-430.

3. R.J. Miech, 'Almost primes generated by a polynomial', Acta Arith. 10 (1964) 9-30.

4. H.-E. Richert, 'Selberg's sieve with weights', Mathematika 16 (1969) 1-22.

5. K.F. Roth, 'On the gaps between squarefree integers', Jour. Lond. Math. Soc. 26 (1951) 263-268.