Least primes in arithmetic progressions

Andrew GRANVILLE

Abstract

For a fixed non-zero integer a and increasing function f, we investigate the lower density of the set of integers q for which the least prime in the arithmetic progression $a (mod\, q)$ is less than $qf(q)$. In particular we conjecture that this lower density is 1 for any f with $\log x = o(f(x))$ and prove this, unconditionally, for $f(x) = x/g(x)$ for any g with $\log g(x) = o(\log x)$. Under the assumption of a strong form of the prime k-tuplets conjecture we prove our conjecture and get strong results on the distribution of values of $\pi(\lambda q log\, q, q, a)$ for any fixed λ, as q varies.

1. Introduction

For given integers a and q, $q > 0$, $a \neq 0$, $(a, q) = 1$, we define $p(q, a)$ to be the least prime p that is greater than a and congruent to $a (mod\, q)$. We let $p(q)$ be the largest value of $p(q, a)$ for a in the range

$$1 \leq a \leq q - 1, \qquad (a, q) = 1 \tag{1}$$

In 1944 Linnik [13] gave the remarkable result that there exists an absolute constant c for which $p(q) \ll q^c$, for all positive integers q. Numerous authors have given better and better explicit values for c, and most recently Chen [5] has shown that we may take c to be 17. In 1930 Titchmarsh [20] showed, under the assumption of the Extended Riemann hypothesis, that $p(q) \ll q^2(\log q)^4$. Recently Heath-Brown [11] conjectured that $p(q) \ll q(\log q)^2$, and Wagstaff [22] gave heuristic arguments which support this; more precisely, McCurley noted that an adaptation of his heuristic arguments in [14] suggest that $\overline{\lim}_{q\to\infty} \frac{p(q)}{\phi(q)\log^2 q} = 2$.

Quite a number of authors have been concerned with bounding $p(q)$ for almost all values of q (as we shall explain); but it seems that little work has gone into bounding $p(q,a)$ for almost all values of q, for some fixed value of a. We will do this here.

In 1977 Kumar Murty [15] used the Bombieri-Vinogradov Theorem [3], [21] to show that, for all $\varepsilon > 0$, $p(q) < q^{2+\varepsilon}$ for almost all integers q. Under the assumption of the Elliott-Halberstam conjecture [6] this result may be improved to $p(q) < q^{1+\varepsilon}$ for almost all q. In a series of recent papers, Bombieri, Friedlander and Iwaniec have extended the Bombieri-Vinogradov Theorem 'locally' and this may be used to provide a sharper result for $p(q,a)$.

Theorem 1 *Suppose that a is a given non-zero integer and $g(x)$ is any positive valued function of x, with $\log g(x) = o(\log x)$ and $x^2/g(x)$ increasing for sufficiently large x. Then*

$$p(q,a) < q^2 \ / \ g(q)$$

for almost all positive integers q which are prime to a.

Proof:- Bombieri, Friedlander and Iwaniec [4] have shown

Lemma 1 *Let $a \neq 0$ be an integer and $A > 0$, $2 \leq Q \leq x^{3/4}$ be reals. Let R be the set of all integers q, prime to a, in some interval $Q' \leq q \leq Q$. Then*

$$\sum_{q \in R} |\pi(x;q,a) - \frac{\pi(x)}{\phi(q)}| \leq \{k(\vartheta - \frac{1}{2})^2 x\mathcal{L}^{-1} + O(x\mathcal{L}^{-3}(\log\log x)^2)\} \sum_{q\in R} \frac{1}{\phi(q)} + O(x\mathcal{L}^{-A})$$

where $\vartheta = \log Q \ / \ \log x$, $\mathcal{L} = \log x$, k is an absolute constant, and the O's depend on at most a and A.

Choosing $A = 5$ in Lemma 1, we observe that for $Q = (xg(x))^{1/2}$,

$$\sum_{\substack{2Q > q > Q \\ (a,q)=1}} |\pi(x;q,a) - \frac{\pi(x)}{\phi(q)}| \ll \frac{x}{(\log x)^3}(\log g(x) + \log\log x)^2$$

where $\ll$ depends only on a.

So assume that for at least εQ integers q in the sum we have $p(q,a) \geq q^2/g(q)(> Q^2/g(Q) > x$, for sufficiently large x), so that $\pi(x,q,a) = 0$. Thus

$$\frac{x}{(\log x)^3}(\log g(x) + \log\log x)^2 \gg \sum_{\substack{Q \leq q < 2Q, \ (q,a)=1 \\ p(q,a) \geq q^2/g(q)}} \frac{\pi(x)}{2Q} \geq \frac{\varepsilon}{2}\pi(x),$$

giving a contradiction for sufficiently large values of x. Summing over the intervals $[2^{-i-1}Q, 2^{-i}Q)$ gives the result.

We make the following

Conjecture 1 *Suppose that $f(x)$ is any function that tends to ∞ as $x \to \infty$. For any fixed non-zero integer a, $p(q,a) < q \log q f(q)$ for almost all positive integers q that are prime to a.*

Evidently Conjecture 1 is considerably stronger than Theorem 1. Later in this paper we will show that Conjecture 1 is true under the assumption of a strong form of the prime k-tuplets conjecture (see [2], [19]).

In the other direction to these results, Pomerance [16], extending arguments of Prachar [17] and Schinzel [18], used Jacobsthal's function to show that for any $\varepsilon > 0$,

$$p(q) > (1-\varepsilon)e^{\gamma}\ \phi(q) \log\ q \log_2 q \log_4 q\ /\ (\log_3 q)^2$$

for almost all positive integers q. (By imitating the methods used by Maier and Pomerance for giving lower bounds on Jacobsthal's function (as announced at this meeting) it seems likely that the constant e^{γ} can be improved by a small but significant amount.)

In fact Prachar and Schinzel gave the result that there exists an absolute constant $c > 0$ such that for all non-zero integers a, there exists infinitely many positive integers q, that are prime to a, for which $p(q,a) > cq \log q\ \ \log_2 q \log_4 q\ /\ (\log_3 q)^2$. It would be nice if one could state that a positive density of integers q, prime to a, satisfied, say, $p(q,a) > bq \log q$, for some constant $b > 0$; however, by using the method of Prachar, Schinzel and Pomerance, it is not possible to do better than the statement that $p(q,a) > bq \log q$ for $\gg x/exp(c(\log x)^{1/2})$ values of $q \leq x$, that are prime to a, for some constant $c = c(a,b) > 0$. This restriction is due to the bound $g(m) \ll (\log m)^2$ on Jacobsthal's function given by Iwaniec [12].

In 1950 Erdös [8] considered the question of how often $p(q,a) < bq \log q$, as a varies over the range (1). He showed that, for any fixed $b > 0$ there exists a constant $U(b) > 0$ such that, for all sufficiently large integers q, $p(q,a) < bq \log q$ for least $U(b)\phi(q)$ values of a in the range (1). For fixed values of b and s, $0 < s \leq 1$, we let $D(b,s)$ be the lower density of the set of positive integers q for which $p(q,a) < bq\log q$ for at least $s\phi(q)$ values of a in the range (1). Let $s(b)$ be the supremum of the set of values of s for which $D(b,s)=1$. Clearly $U(b) \le s(b) \le 1$. Pomerance [16] conjectured that $s(b) < 1$ for all values of b, but $s(b) \to 1$ as $b \to \infty$. This conjecture would imply the following theorem, proved independently by Elliott and Halberstam [7] and Wolke [23]:

Suppose that $f(x)$ is any function that tends to ∞ as $x \to \infty$.

For almost all posistive integers q, for almost all a in the range (1),

$$p(q,a) < q\log q f(q).$$

We can see that Conjecture 1 is a 'local' analogue of this theorem. We now make an analogous 'local' conjecture to that of Pomerance.

Conjecture 2 *Suppose that a is a fixed non-zero integer. For any $b > 0$, let $t(a,b)$ be the lower density of the set of positive integers q, (in the set of positive integers q that are prime to a), for which $p(q,a) < bq\log q$. Then $t(a,b) < 1$ for all $b > 0$, but $t(a,b) \to 1$ as $b \to \infty$.*

It is evident that Conjecture 2 would imply Conjecture 1; we will concentrate for the rest of this paper on Conjecture 2 - in giving lower bounds for $t(a,b)$, and showing that, under the assumption of a strong form of the prime k-tuplets conjecture, rather more than Conjecture 2 is true.

For any $\lambda > 0$ and non-negative integer t, define

$$\mathrm{Poisson}\ (\lambda,\mathrm{t}) \ = \ \mathrm{e}^{-\lambda}\lambda^{\mathrm{t}}/\mathrm{t}!.$$

Conjecture 3 *Suppose that a is a fixed non-zero integer. For any $\lambda > 0$, the set of positive integers q, for which $\pi(\lambda\phi(q)\log q, q, a) = t$ has density* Poisson (λ, t), *in the set of positive integers q that are prime to a.*

Conjecture 3 would correspond rather nicely to a result of Gallagher [9] who showed, under the assumption of a similar, strong form of the prime k-tuplets conjecture, that the distribution of primes in an interval of length $\lambda\log x$ is roughly Poisson with parameter λ (i.e. the set of positive integers x, for which the interval $(x, x+\lambda\log x]$ contains precisely

t primes has density Poisson (λ, t)). Using the techniques in this paper we are unable to confirm Conjecture 3, even under the assumption of the prime k-tuplets conjecture, as our method forces us to examine $\pi(\lambda q \log q, q, a)$ rather than $\pi(\lambda\phi(q)\log q, q, a)$.

On the other hand if we assume that a little bit more than Conjecture 3 holds; that the distribution of integers with $\pi(\lambda\phi(q)\log q, q, a) = t$ remains Poisson, independent of the value of $q/\phi(q)$, we see that $d_t(a,\lambda)$, the density of positive integers q for which $\pi(\lambda q \log q, q, a) = t$, takes value

$$d_t(a,\lambda) = \lim_{X\to\infty} \frac{1}{(\phi(a)/a)X} \sum_{\substack{q\le X\\(a,q)=1}} \text{Poisson}(\lambda q/\phi(q), t).$$

This is precisely the result that we get in Theorem 5 from assuming a strong form of the prime k-tuplets conjecture.

2. Lower densities, via second moments.

Throughout this section we will take a to be a fixed non-zero integer. In order to estimate $t(a,b)$ we use a variation of the second moment method, previously used in a paper of Ankeny and Erdös [1] who were considering the set of exponents for which the First Case of Fermat's Last Theorem is true. We will employ a number of well-known sieve results (see [10], Thm.5.7) on prime constellations and also investigate what happens if a strong conjecture on prime constellations is assumed to be true.

Suppose that integers $a, r_1, r_2, \ldots, r_k$, with $(a, r_1 \ldots r_k) = 1$, are given. For each prime p we define $w_r(p)$ to be the number of distinct solutions $q(mod\, p)$ of $\prod_{i=1}^k (qr_i + a) \equiv 0(mod\, p)$. Also let

$$C_\alpha(r_1,\ldots,r_k) = \prod_{p\ prime} (1-1/p)^{-k}(1 - w_r(p)/p).$$

The prime k-tuplets conjecture, in its quantitative form (see [2]) states that, for each $k \ge 1$,

$$\#\{q : x \le q < 2x,\ \text{each } qr_i + a \text{ prime}\} = C_\alpha(r_1,\ldots,r_k)\frac{x}{(\log x)^k}\{1 + o(1)\}.$$

We will assume that this holds whenever each $r_i \le b \log x$, with o dependent only on a, b and k, for any given constant b.

This result is well known to hold for $k = 1$ (Dirichlet's Theorem), and may be stated with error term $O(1/log\, x)$ (the Siegel-Walfisz Theorem). For $k \geq 2$ Selberg's upper bound sieve method gives, for $r =$ the maximum of the r_i's,

$$\#\{q : x \leq q < 2x \text{ each } qr_i + a \text{ prime}\}$$
$$\leq 2^k k! C_\alpha(r_1, \ldots, r_k) \frac{x}{(\log\, x)^k} \{1 + O(\frac{\log\log\, x + \log\log\, r}{\log\, x})\}.$$

We will use the symbol '$\succ$' to mean '$=$' under the assumption of the k-tuplets conjecture and for $k = 1$, and '$\leq$' otherwise. Also $D_k = 1$ under the assumption of the k-tuplets conjecture, and $D_k = 1$ $(k = 1)$, $2^k k!$ $(k \geq 2)$, otherwise. Thus, for each k,

$$\#\{q : x \leq q < 2x, \text{ each } qr_i + a \text{ prime}\} \succ D_k C_\alpha(r_1, \ldots, r_k) \frac{x}{(\log\, x)^k} \{1 + o(1)\}.$$

We define $B(x, g)$ to be the number of integers q, $x \leq q < 2x$, for which there are exactly g distinct positive integers $r_1, r_2, \ldots, r_g$, each less than or equal to $b \log\, x$, with $qr_i + a$ prime for each i.

Note that

$$\sum_{g \geq 1} B(x, g) = \#\{q : \ x \leq q < 2x, \ p(q, a) < bq \log\, x\}$$
$$\leq \#\{q : \ x \leq q < 2x, \ p(q, a) < bq \log\, q\}$$

Now, for any positive integer k,

$$\sum_{g \geq k} \binom{g}{k} B(x, g) = \#\{(q, r_1, r_2, \ldots, r_k) : \ x \leq q < 2x, \ 1 \leq r_1 < r_2 < \cdots < r_k \leq b \log\, x,$$
$$\text{and } qr_i + a \text{ prime for each } i\}$$
$$= \sum_{1 \leq r_1 < r_2 < \cdots < r_k \leq b \log\, x} \{q : x \leq q < 2x, \text{ and } qr_i + a$$
$$\text{prime for each } i\}$$
$$\succ D_k \frac{x}{(\log\, x)^k} \sum_{1 \leq r_1 < r_2 < \cdots < r_k \leq b \log\, x} C_\alpha(r_1, \ldots, r_k)\{1 + o(1)\}$$
$$\succ D_k \frac{\phi(a)}{a} x \frac{b^k}{k!} \prod_{p \nmid a} (1 + \frac{p^k - (p-1)^k}{p(p-1)^k}) \ \{1 + o(1)\} \qquad (2)_k$$

by Theorem 6, which we shall prove in Section 4.

Let $u = b\prod_{p\not| a}(1+1/p(p-1))$ and $v = D_2\frac{b^2}{2!}\prod_{p\not| a}(1+(2p-1)/p(p-1)^2)$. Let $\alpha = (u^2+4uv)/(u+2v)^2$ and $\beta = 2u^2/(u+2v)^2$ so that, for any integer g, $\alpha g - \beta\binom{g}{2} = 1-(1-gu/(u+2v))^2 \le 1$. Then

$$\begin{aligned}\sum_{g\ge 1} B(x,g) \ge\ & \alpha\sum_{g\ge 1} gB(x,g) - \beta\sum_{g\ge 2}\binom{g}{2}B(x,g)\\ &\ge \alpha\frac{\phi(a)}{a}xu\{1+o(1)\} - \beta\frac{\phi(a)}{a}xv\{1+o(1)\}\\ &\ge \frac{u^2}{u+2v}\frac{\phi(a)}{a}x\{1+o(1)\}.\end{aligned}$$

This immediately gives the result that $t(a,b)\ge u^2/(u+2v)$, so we may state

Theorem 2 *For any given non-zero integer a, the lower density of integers q, prime to a, for which $p(q,a) < bq\ \log\ q$, is at least*

$$\prod_{p\not| a}(1+1/p(p-1))^2\ /\ \{b^{-1}\prod_{p\not| a}(1+1/p(p-1)) + D_2\prod_{p\not| a}(1+(2p-1)/p(p-1)^2)\}.$$

In particular, this tends to

$$\frac{1}{D_2}\prod_{p\not| a}\frac{1+\frac{2}{p(p-1)}+\frac{1}{p^2(p-1)^2}}{1+\frac{2}{p(p-1)}+\frac{1}{p(p-1)^2}},$$

as $b\to\infty$. Of course we may take $D_2 = 8$ unconditionally, and $D_2 = 1$ assuming the prime k-tuplets conjecture.

Evidently the result in Theorem 2, even under the assumption of the prime k-tuplets conjecture, is slightly weaker than that required for a proof of Conjecture 2. However we shall look again, using the criteria $(2)_k$ for each $k\ge 1$ (instead of just for $k=1$ and 2, as in the proof of Theorem 2).

By using the same arguments as above but taking $\alpha=\beta=1$, it is easy to show

Theorem 3 *Suppose that a is a given non-zero integer and $f(x)$ is a function that tends to ∞ as $x\to\infty$, is strictly increasing for sufficiently large values of x and that $f(x) = o(\log\ x)$. Then the number of positive integers $q\le x$, prime to a, for which $p(q,a) < qf(q)$ is*

$$x\frac{\phi(a)}{a}\prod_{p\not| a}(1+1/p(p-1))(f(x)/\log\ x)\{1+o(1)\}.$$

3. Densities, via the prime k-tuplets conjecture

Theorem 4 *Suppose that the prime k-tuplets conjecture as stated above, is true. Let a be a fixed non-zero integer. For any real number $b > 0$, the set of positive integers q, prime to a, for which $p(q, a) < bq \log q$, has density*

$$\begin{aligned} d(a,b) &= \sum_{k\geq 1} (-1)^{k+1} \frac{b^k}{k!} \prod_{p \not| a} \left(1 + \frac{p^k - (p-1)^k}{p(p-1)^k}\right) \\ &= 1 - \lim_{z\to 1^+} d(a,b,z), \end{aligned}$$

where

$$d(a,b,z) = \frac{a}{\phi(a)} \zeta(z)^{-1} \sum_{\substack{n\geq 1 \\ (n,a)=1}} \frac{exp(-bn/\phi(n))}{n^z},$$

and $\zeta(z)$ is the Riemann-zeta function.

In particular $0 < \lim_{z\to 1^+} d(a,b,z) < exp(-b)$; so that $1 - e^{-b} < d(a,b) < 1$, and $\lim_{b\to\infty} d(a,b) = 1$. Thus Conjectures 1 and 2 both hold.

The main ingredients of the proof of Theorem 4, are the combinatorial identity, $B(x,0) = \sum_{k\geq 0} (-1)^k \sum_{g\geq k} \binom{g}{k} B(x,g)$, together with the uniform estimates for $\sum_{g\geq k} \binom{g}{k} B(x,g)$ given by prime k-tuplets conjecture in $(2)_k$ (for each $k \geq 1$). If instead we were to use the more general identity $B(x,t) = \sum_{k\geq t} (-1)^{k-t} \binom{k}{t} \sum_{g\geq k} \binom{g}{k} B(x,g)$, we could derive the following stronger result. (N.B. As the details of the proof of Theorem 5 are essentially the same as those for Theorem 4, we shall omit them.)

Theorem 5 *Suppose that the prime k-tuplets conjecture, as stated above, is true. Let a be a fixed non-zero integer. For any real number $b > 0$, and non-negative integer t, the density, $d_t(a,b)$, of the set of positive integers q, prime to a, for which $\pi(bq \log q;\ q, a) = t$, exists and equals*

$$\begin{aligned} d_t(a,b) &= \sum_{k\geq t} (-1)^{k-t} \binom{k}{t} \frac{b^k}{k!} \prod_{p \not| a} \left(1 + \frac{p^k - (p-1)^k}{p(p-1)^k}\right) \\ &= \lim_{z\to 1^+} \frac{a}{\phi(a)} \zeta(z)^{-1} \sum_{\substack{n\geq 1 \\ (n,a)=1}} \frac{Poisson(bn/\phi(n), t)}{n^z} \\ &= \lim_{X\to\infty} \frac{a}{\phi(a)} X^{-1} \sum_{\substack{n\leq X \\ (n,a)=1}} Poisson(bn/\phi(n), t). \end{aligned}$$

If we let $c_n = Poisson(bn/\phi(n),t)$ $((a,n)=1)$, 0 (otherwise) then by Ikehara's theorem for Dirichlet series that converge to the right of 1, we see that $\lim_{X\to\infty} \frac{1}{X}\sum_{n\le X} c_n$ exists and equals $\lim_{s\to 1^+}(s-1)\sum_{n\ge 1}\frac{c_n}{n^s} = \lim_{s\to 1^+} \zeta(s)^{-1}\sum_{n\ge 1}\frac{c_n}{n^s}$, which confirms the last equality in the statement of Theorem 5.

Proof of Theorem 4:- Let $c_k = \prod_{p \not| a}(1+\frac{p^k-(p-1)^k}{p(p-1)^k})$, $d_k = \frac{b^k}{k!}c_k$ and $S_n = \sum_{k=1}^n (-1)^{k+1} d_k$. It is easy to show that for each $k\ge 4$ and $p>2k$, we have $(1+\frac{p^{k+1}-(p-1)^{k+1}}{p(p-1)^{k+1}}) < (1-p^{-3/2})^{-1}(1+\frac{p^k-(p-1)^k}{p(p-1)^k})$, and so, there exists $c_o>0$ such that

$$c_k < c_o\zeta(3/2)^k \prod_{p\le 2k}\{1-\frac{1}{p}+\frac{1}{p}(\frac{p}{p-1})^k\}.$$

But $1-\frac{1}{p}+\frac{1}{p}(\frac{p}{p-1})^k < (\frac{p}{p-1})^k$ and so, by Mertens' Theorem, $c_k < c_o\zeta(3/2)^k\{\prod_{p\le 2k}(1-\frac{1}{p})^{-1}\}^k < (A\log 3k)^k$ for each $k\ge 1$, for some constant A. Now as $k! \gg (k/e)^k$ we see that $d_k \to 0$ as $k\to\infty$, and that $\sum_{k=1}^{\infty}(-1)^{k+1}d_k$ converges absolutely to some limit S.

Fix $\varepsilon > 0$ and choose n to be an integer such that $|S-S_n|, d_n < \varepsilon/4$. Define $C(x) = \sum_{g\ge 1} B(x,g)/\frac{\phi(a)}{a}x$ and

$$\begin{aligned} A(x) &= \sum_{k=1}^{n}(-1)^{k+1}\sum_{g\ge k}\binom{g}{k}B(x,g) - \sum_{g\ge 1}B(x,g) \\ &= \sum_{g\ge 1}\left[\sum_{k=0}^{n}(-1)^{k+1}\binom{g}{k}\right]B(x,g), \end{aligned}$$

and as $\left|\sum_{k=0}^n(-1)^{k+1}\binom{g}{k}\right| \le \binom{g}{n}$ for all integers g and $n\ge 1$, we see that

$$\begin{aligned} |A(x)| \le \sum_{g\ge n}\binom{g}{n}B(x,g) &= \frac{\phi(a)}{a}x d_n\{1+o(1)\}, \qquad \textit{by } (2)_n \\ &< \frac{\varepsilon}{2}\frac{\phi(a)}{a}x, \quad \text{for sufficiently large values of } x. \end{aligned}$$

Similarly, by $(2)_k$, for $k=1,2,\dots,n$ we see that

$$\frac{\phi(a)}{a}x\{S_n - C(x)\} = A(x) + o(\frac{\phi(a)}{a}x) < A(x) + \frac{\varepsilon}{4}\frac{\phi(a)}{a}x$$

for x sufficiently large. Therefore $|C(x)-S| \le |S_n - S| + |S_n - C(x)| \le \frac{\varepsilon}{4}+\frac{\varepsilon}{4}+\frac{\varepsilon}{2} = \varepsilon$ for sufficiently large values of x, so that $C(x)\to S$ as $x\to\infty$, and so $d(a,b)$ exists and is equal to $\sum_{k\ge 1}(-1)^{k+1}\frac{b^k}{k!}\prod_{p\not| a}(1+\frac{p^k-(p-1)^k}{p(p-1)^k})$.

Now define, for $x \geq 1$,

$$S(a,b,z) = \prod_{p|a} \frac{p^z - 1}{p^{z-1}(p-1)} \sum_{k\geq 0} (-1)^k \frac{b^k}{k!} \prod_{p \not| a} (1 + \frac{p^k - (p-1)^k}{p^z (p-1)^k}).$$

It is evident that $d(a,b) = 1 - S(a,b,1) = 1 - \lim_{z\to 1^+} S(a,b,z)$. Now

$$\begin{aligned} S(a,b,z) =& \prod_{p|a} \frac{p^z - 1}{p^{z-1}(p-1)} \sum_{k\geq 0} \frac{(-b)^k}{k!} \sum_{\substack{d\geq 1\\ (d,a)=1}} \frac{\mu(d)^2}{d^z} \prod_{p|d} ((\frac{p}{p-1})^k - 1) \\ =& \prod_{p|a} \frac{p^z - 1}{p^{z-1}(p-1)} \sum_{\substack{n\geq 1\\ (n,a)=1}} \mu(n) \sum_{k\geq 0} \frac{(-b)^k}{k!} (\frac{n}{\phi(n)})^k \sum_{\substack{d\geq 1, n|d\\ (d,a)=1}} \frac{\mu(d)}{d^z} \\ =& \frac{a}{\phi(a)} \zeta(z)^{-1} \sum_{\substack{n\geq 1\\ (n,a)=1}} \frac{\mu(n)^2}{\prod_{p|n}(p^z - 1)} exp(-bn/\phi(n)) \\ =& d(a,b,z). \end{aligned}$$

Now, for any integer n, $n/\phi(n) \geq 1 + \sum_{p|n} 1/p$, and so

$$\begin{aligned} d(a,b,z) &< \frac{a}{\phi(a)} \zeta(z)^{-1} e^{-b} \sum_{\substack{n\geq 1\\ (n,a)=1}} \mu(n)^2 \prod_{p|n} \frac{exp(-b/p)}{(p^z - 1)} \\ &= \prod_{p|a} \frac{p^z - 1}{p^{z-1}(p-1)} e^{-b} \prod_{p \not| a} \{1 - \frac{(1 - exp(-b/p))}{p^z}\} \\ &\to e^{-b} \prod_{p \not| a} \{1 - \frac{(1 - exp(-b/p))}{p}\} \qquad as\ z \to 1 \\ &< e^{-b} \ \to\ 0\ as\ b \to \infty. \end{aligned}$$

Finally, by observing that there exists a constant c for which $n/\phi(n) < 1 + c\sum_{p|n} 1/p^{1/2}$ for all integers n, we may use essentially the same method (with the inequalities reversed) to show that $d(a,b) \geq e^{-b} \prod_{p \not| a} \{1 - \frac{(1 - exp(-cb/p^{1/2}))}{p}\} > 0$.

4. Technical stuff

In this section we prove the following result which was used in Section 2 to give the equations $(2)_k$.

Theorem 6 *For given integers a and k, with $a \neq 0$, $k > 0$, and $\varepsilon > 0$,*

$$F_{k,a}(x) \ = \ \frac{\phi(a)}{a} \frac{x^k}{k!} \prod_{p \not| a} (1 + \frac{p^k - (p-1)^k}{p(p-1)^k}) \{1 + O_{k,a}(x^{\varepsilon - 1/2})\},$$

where $F_{k,a}(x) = \sum_1 C_a(r_1,\ldots,r_k)$ *and, henceforth* $\sum_1$ *is the sum over* $1 \le r_1 < r_2 < \cdots < r_k \le x$ *with* $(r_i,a)=1$ *for each* i.

In order to prove this we will start with some technical lemmas. First we note that if $p|a$ then $w_r(p)=1$ and if $p \not| a$ then $w_r(p)$ is precisely the number of distinct non-zero residue classes $(mod\, p)$ containing an r_i. Let $\lambda_k(p) = \sum_{0\le r_1,\ldots,r_k\le p-1} w_r(p)$.

Lemma 2 *If* p *does not divide* a *then* $\lambda_k(p) = (p-1)(p^k-(p-1)^k)$.

Proof: - Define $\lambda_{k,j}(p)$ to be the number of $(r_1,\ldots,r_k)$, $0\le r_i\le p-1$, with entries in exactly j distinct non-zero residue classes $(mod\, p)$. We note the recurrence relation $\lambda_{k+1,j}(p) = (j+1)\lambda_{k,j}(p) + (p-j)\lambda_{k,j-1}(p)$, so that

$$\begin{aligned}\lambda_{k+1}(p) &= \sum_{j=0}^{k+1} j\lambda_{k+1,j}(p) = (p-1)\lambda_k(p) + (p-1)\sum_{j=0}^{k}\lambda_{k,j}(p)\\ &= (p-1)[\lambda_k(p)+p^k].\end{aligned}$$

Now $\lambda_o(p)=0$ and so the result follows easily by induction on k.

For each positive integer k define $\phi_k(n) = \prod_{\substack{p|n\\ p>k}}(p-k)$.

Lemma 3 *For positive integer* k, *and* $\varepsilon,\delta>0$, *if* n *is a sufficiently large squarefree integer then*

$$\sum_{d|n,\ d>n^\varepsilon} k^{\nu(d)}/\phi_k(d) < n^{\delta-\varepsilon}.$$

Proof: - If d divides n then it is clear that $d/\phi_k(d) \le n/\phi_k(n)$ and $\nu(d)\le\nu(n)$. Therefore

$$\begin{aligned}\sum_{d|n,\ d>n^\varepsilon} k^{v(d)}/\phi_k(d) &\le \sum_{d|n,\ d>n^\varepsilon}(n/d)k^{\nu(n)}/\phi_k(n)\\ &< n^{1-\varepsilon}(k^{\nu(n)}/\phi_k(n))\sum_{d|n}1\\ &= n^{-\varepsilon}(2k)^{\nu(n)}(n/\phi_k(n)).\end{aligned}$$

Now, $\nu(n) \ll \log n/\log\log n$, by the prime number theorem, and $n/\phi_k(n) \ll_k (\log\log n)^k$ by an immediate application of the prime number theorem and Mertens' theorem, and so the result follows immediately.

Proof of Theorem 6: - Define $\vartheta(r)=\prod_{i=1}^k r_i \prod_{1\le i<j\le k}(r_j-r_i)$ and $u_k(p)=p-\phi_k(p)$. Then

$$F_{k,a}(x)=(a/\phi(a))^{k-1}\prod_{p\,\not|a}\{(1-u_k(p)/p)(1-1/p)^{-k}\}G_{k,a}(x) \qquad (3)$$

where

$$\begin{aligned} G_{k,a}(x) &= \sum\nolimits_1 \prod_{p\,\not|a,\ p|\vartheta(r)}(1+\frac{u_k(p)-w_r(p)}{p-u_k(p)}) \\ &= \sum\nolimits_1 \sum_{d|\vartheta(r),\ (d,\ell)=1} \mu(d)^2\{\prod_{p|d} u_k(p)-w_r(p)\}/\phi_k(d) \\ &= \sum\nolimits_1 \sum_{\substack{d|\vartheta(r)\\ (d,\ell)=1,\ d\le x^{1/2}}} \mu(d)^2\{\prod_{p|d} u_k(p)-w_r(p)\}/\phi_k(d)\{1+O(x^{\varepsilon-1/2})\} \end{aligned}$$

by Lemma 3 as $\vartheta(r)<x^{k(k+1)/2}$, for each choice of the r_i's. Thus

$$G_{k,a}(x) = \sum_{d\le x^{1/2},\ (d,\ell)=1} \mu(d)^2/\phi_k(d) \sum_{d|\vartheta(r)}{}_1 \{\prod_{p|d} u_k(p)-w_r(p)\}\{1+O(x^{\varepsilon-1/2})\} \qquad (4)$$

Note that there are at most $\binom{k}{2}x^{k-1}$ possible vectors $\mathbf{r}$ where $1\le r_1,\ldots,r_k\le x$, with $r_i=r_j$ for some $i\ne j$; so, as $\prod_{p|d} u_k(p)-w_r(p)\le k^{\nu(d)}$ and $\nu(d)\ll \log x/\log\log x$, for $d\le x^{1/2}$, we have

$$\sum_{\substack{1\le r_1,\ldots,r_k\le x\\ r_i=r_j \text{ for some } i\ne j}} \prod_{p|d} u_k(p)-w_r(p)=O_k(x^{k-1+\varepsilon}).$$

Therefore

$$\sum_{d|\vartheta(r)}{}_1 \prod_{p|d} u_k(p)-w_r(p)=\frac{1}{k!}\sum_{d|\vartheta(r)}{}_2 \prod_{p|d} u_k(p)-w_r(p)+O_k(x^{k-1+\varepsilon}) \qquad (5)$$

where $\sum_2$ is the sum over $1\le r_1,\ldots,r_k\le x$, with $(r_i,a)=1$ for each i.

Now, if $r_i\equiv s_i (mod\, d)$ for each i then $\prod_{p|d} u_k(p)-w_r(p)=\prod_{p|d} u_k(p)-w_s(p)$, so that

$$\begin{aligned} \sum_{d|\vartheta(r)}{}_2 \prod_{p|d} u_k(p)-w_r(p) &= \sum_{\substack{1\le r_i\le ad,\ (r_i,a)=1\\ \text{for each } i,\ d|\vartheta(r)}} \prod_{p|d} u_k(p)-w_r(p)\{\frac{x}{ad}+O(1)\}^k \\ &= (\frac{x\phi(a)}{ad})^k \sum_{\substack{d|\vartheta(r)\\ 1\le r_1,\ldots,r_k\le d}} \prod_{p|d} u_k(p)-w_r(p)\{1+O_{k,a}(x^{-1/2})\}. \end{aligned}$$

Now

$$\sum_{\substack{d|\vartheta(r)\\ 1\le r_1,\ldots,r_k\le d}} \prod_{p|d} u_k(p)-w_r(p) = \prod_{p|d} \sum_{1\le r_1,\ldots,r_k\le p} u_k(p)-w_r(p)$$

$$= \prod_{p|d} p^k u_k(p) - \lambda_k(p)$$

$$= \prod_{p|d} p^k u_k(p) - (p-1)(p^k-(p-1)^k), \qquad (6)$$

by Lemma 2.

Now $p^k u_k(p) - (p-1)(p^k-(p-1)^k) = \binom{k+1}{2} p^{k-1} + O_k(p^{k-2})$ so that

$$\sum_{\substack{d|\vartheta(r)\\ 1\le r_1,\ldots,r_k\le d}} \prod_{p|d} u_k(p)-w_r(p) \gg_k d^{k-1}.$$

Therefore

$$\sum_{d|\vartheta(r)}{}_2 \prod_{p|d} u_k(p)-w_r(p) \gg_{k,a} x^k/d \ \ge x^{k-1/2},$$

so that, by (5) and (6),

$$\sum_{d|\vartheta(r)}{}_1 \prod_{p|d} u_k(p)-w_r(p) = \frac{1}{k!}\Big(\frac{x\phi(a)}{ad}\Big)^k \prod_{p|d} p^k u_k(p) - (p-1)(p^k-(p-1)^k)$$
$$\times \{1+O_{k,a}(x^{\varepsilon-1/2})\}.$$

Therefore, by (4),

$$G_{k,a}(x) = \frac{1}{k!}\Big(\frac{x\phi(a)}{a}\Big)^k \sum_{\substack{d\le x^{1/2}\\ (d,\ell)=1}} \frac{\mu(d)^2}{\phi_k(d)d^k} \prod_{p|d} p^k u_k(p) - (p-1)(p^k-(p-1)^k)$$
$$\times \{1+O_{k,a}(x^{\varepsilon-1/2})\} \qquad (7)$$

Now $\prod_{p|d} p^k u_k(p) - (p-1)(p^k-(p-1)^k) \ll_k \ k^{2\nu(d)} d^{k-1} \ll d^{k-1+\varepsilon}$ and so

$$\sum_{\substack{d\ge x^{1/2}\\ (d,\ell)=1}} \frac{\mu(d)^2}{\phi_k(d)d^k} \prod_{p|d} p^k u_k(p) - (p-1)(p^k-(p-1)^k) \ll \sum_{\substack{d\ge x^{1/2}\\ (d,\ell)=1}} d^{\varepsilon-2} \ll x^{(\varepsilon-1)/2} \qquad (8)$$

Also

$$\sum_{\substack{d\ge 1\\ (d,\ell)=1}} \frac{\mu(d)^2}{\phi_k(d)d^k} \prod_{p|d} p^k u_k(p) - (p-1)(p^k-(p-1)^k) = \prod_{p\nmid a} \frac{p^k+(p-1)^{k+1}}{p^k(p-u_k(p))}.$$

Finally combining this with (3), (7) and (8) gives the result.

Acknowledgements I'd like to thank Dom de Caen for useful discussions concerning the power series in Theorem 4, and Kevin McCurley for a number of interesting observations.

5. References

1. Ankeny N.C., Erdös P., *The insolubility of classes of Diophantine equations*, Amer. J. Math., 76, 1954, 488-496.
2. Bateman P.T., Horn R.A., *A heuristic asymptotic formula concerning the distribution of prime numbers*, Math. Comp., 16, 1962, 363-367.
3. Bombieri E., *On the large sieve*, Mathematika, 12, 1965, 201-225.
4. Bombieri E., Friedlander J.B., Iwaniec H., *Primes in Arithmetic Progressions to Large Moduli. III*, to appear.
5. Chen Jing-Run, *On the least prime in an arithmetic progression and theorems concerning the zeros of Dirichlet's L-function II*, Sci. Sinica, 22, 1979, 859-889.
6. Elliott P.D.T.A., Halberstam H., *A conjecture in prime number theory*, Symp. Math., 4, 1968-69, 59-72.
7. Elliott P.D.T.A., Halberstam H., *The least prime in an arithmetic progression*, in *Studies in Pure Mathematics*, Academic Press, London/New York, 1971, 59-61.
8. Erdös P., *On some applications of Brun's method*, Acta Sci. Math. (Szeged), 13, 1949-50, 57-63.
9. Gallagher P.X., *On the distribution of primes in short intervals*, Mathematika, 23, 1976, 4-9.
10. Halberstam H., Richert H.E., *Sieve Methods*, Academic Press, New York, 1974.
11. Heath-Brown D.R., *Almost-primes in arithmetic progressions and short intervals*, Math. Proc. Camb. Phil. Soc., 83, 1978, 357-375.
12. Iwaniec H., *On the problem of Jacobsthal*, Demonstratio Math., 11, 1978, 225-231.
13. Linnik U.V., *On the least prime in an arithmetic progression II, The Deuring -Heilbronn phenomenon*, Rec. Math. [Mat. Sb.] N.S., 15(57), 1944, 347-368.

14. McCurley K.S., *The least r-free number in an arithmetic progression*, Trans. Amer. Math. Soc., 293, 1986, 467-475.

15. Murty V. Kumar, *The least prime in an arithmetical progression and an estimate of Linnik's constant*, BSc. thesis, Carleton University, Ottawa, 1977, 45pp.

16. Pomerance C., *A Note on the Least prime in an Arithmetic Progression*, J. No. Thy., 12, 1980, 218-223.

17. Prachar K., *Über die kleinste Primzahl einer arithmetischen Reihe*, J. Reine Angew. Math., 206, 1961, 3-4.

18. Schinzel A., *Remark on the paper of K. Prachar " Über die kleinste primzahl einer arithmetischen Reihe"*, J. Reine Angew. Math., 210, 1962, 121-122.

19. Schinzel A., Sierpiński W., *Sur certaines hypothèses concernant les nombres premiers*, Acta Arith., 4, 1958, 185-208; erratum 5, 1959, 259.

20. Titchmarsh E.C., *A divisor problem*, Rend. Circ. Mat. Palermo, 54, 1930, 414-429.

21. Vinogradov A.I., *On the density hypothesis for Dirichlet L-functions*, Izv. Akad. Nauk. SSSR Ser. Mat., 29, 1965, 903-934; erratum 30, 1966, 719-720.

22. Wagstaff S.S. Jr., *Greatest of the least primes in arithmetic progressions having a given modulus*, Math. Comp., 33, 1979, 1073-1080.

23. Wolke D., *Farey-Brüche mit primem Nenner und das grosse sieb*, Math. Z., 114, 1970, 145-158.

Andrew Granville

Department of Mathematics

University of Toronto

Toronto, Canada M5S 1A1