Reprinted from

Analytic Number Theory

Proceedings of a Conference in Honor of Paul T. Bateman

Edited by
Bruce C. Berndt Harold G. Diamond
Heini Halberstam Adolf Hildebrand

1990

Birkhäuser
Boston • Basel • Berlin

Some Conjectures in Analytic Number Theory And their Connection With Fermat's Last Theorem

ANDREW GRANVILLE

Dedicated to P. Bateman on his retirement

1. Introduction

The first case of Fermat's Last Theorem is the assertion:

For all odd primes p there are no integer solutions x, y, z to

$$x^p + y^p + z^p = 0 \quad \text{with } p \nmid xyz. \qquad (1)_p$$

In 1823 Sophie Germain showed that if $2p + 1$ is also prime then $(1)_p$ has no solutions and this has been generalized as follows (see [15]):

Lemma 1. *For any fixed positive integer m, with $m \equiv 2$ or $4 (\mathrm{mod}\ 6)$, define N_m to be the product, over all pairs α, β of mth roots of unity, of $(1 + \alpha + \beta)$. If p and $q = mp+1$ are both primes, where p does not divide m and q does not divide N_m, then $(1)_p$ has no solutions in integers x, y and z.*

By finding prime pairs of the form p, $q = mp+1$ one hopes to be able to use Lemma 1 to establish the first case of Fermat's Last Theorem. Unfortunately it is not presently known how to formulate a 'reasonable' conjecture in analytic number theory that would achieve this goal; however, in this paper, we examine what exactly a number of quite different conjectures of analytic number theory actually imply about the set of primes p for which there is an integer solution x, y, z of $(1)_p$.

This paper may be seen as a continuation of [8] where we investigated the consequences (for Fermat's Last Theorem) of a variety of conjectures from algebraic, combinatorial and transcendental number theory.

2. Statement of Results

In order to exploit Lemma 1 it is obviously necessary to obtain information about primes q in the arithmetic progression $1(\text{mod} p)$, for which 3 does not divide $q-1$. A famous result of Linnik [13] implies that there exists a constant $L>0$ such that the least such prime q is $<p^L$. A recent result of Bombieri, Friedlander and Iwaniec [3] implies that we may take $L=2$ for almost all primes p. However we actually need to use stronger estimates than these. We start by assuming a conjecture that has been formulated by each of Heath-Brown [12], McCurley [14] and Wagstaff [17] independently.

Conjecture 1. *There exists a constant* $c_1 > 0$ *such that, for any given integer* d, *the least prime in the arithmetic progression* $a(\text{mod } d)$ *is less than* $c_1\phi(d) \log^2 d$ *whenever* $(a, d) = 1$.

From this we will deduce

Theorem 1. *If Conjecture 1 is true then*

$$\#\{\textit{primes } p \leq x\text{: } (1)_p \textit{ has solutions}\} \ll \log^7 x.$$

In a recent paper Adleman and Heath-Brown [1] showed what effect three conjectures in analytic number theory have on $(1)_p$. The third of these conjectures was proved by Fouvry [6] and allowed them to state that $(1)_p$ has no solutions for $\gg x^{2/3}$ prime exponents $p \leq x$. Michael Filaseta has noted that their results imply that there exist arbitrarily large values of x for which this can be improved to $\gg x/\log x$ prime exponents $p \leq x$ (we give his proof in Section 5). We now state a new conjecture, which is a modification of the one that Fouvry proved. Define, as usual, $\pi(x;d,a)$ to be the number of primes $\leq x$ that are $\equiv a(\text{mod} d)$, and let

$$\pi^*(x;d) = \pi(x;d,1) - \pi(x;3d,1) .$$

$$(= \#\{\text{primes } q \leq x\text{: } q \equiv 1(\text{mod} d),\ q \not\equiv 1(\text{mod} 3d)\})$$

Conjecture 2. *There exists* θ, $2/3 < \theta < 1$, *such that*

$$\sum_{x^\theta<p<2x^\theta} \pi^*(x; p) \gg x/\log^2 x.$$

Of the three approaches presented in this paper, perhaps this one has the greatest chance of success (in the sense that we have real hope of Conjecture 2 being proved in the forseeable future). We will show

Theorem 2. *If Conjecture 2 is true then* $(1)_p$ *does not have solutions for* $\gg \pi(x)$ *primes* $p \le x$.

A minor modification of the proof of Theorem 2 leads to a new and shorter proof of the results of Adleman and Heath-Brown, and of Filaseta (see section 5).

As early as 1904, Dickson [4] had conjectured that, with certain obvious restrictions, an arbitrary set of linear polynomials will simultaneously take on prime values infinitely often. Hardy and Littlewood conjectured asymptotic formulae for how often this happens for various sets of polynomials in [11]. These conjectures were extended to arbitrary sets of polynomials by Schinzel and Sierpinski [16] and then modified to obtain greater accuracy by Bateman and Horn [2]. An explicit form of these conjectures restricted to certain linear polynomials is given here:

Conjecture 3. *Suppose that* $m_1, m_2, ..., m_k$ *are given positive integers and let* $N(x; m_1, m_2, ..., m_k)$ *be the number of primes* p, $x < p \le 2x$, *for which* $m_1p{+}1, m_2p{+}1, ..., m_kp{+}1$ *are also prime. Then*

$$N(x; m_1, m_2, ..., m_k) \;=\; C(m_1, ..., m_k)\frac{x}{(\log x)^{k+1}}\{1 + o(1)\}, \tag{2}$$

where $C(m_1, ..., m_k) = \prod_{p\ prime} \dfrac{(1-w_m(p)/p)}{(1-1/p)^{k+1}}$ *and* $w_m(p)$ *is the number of distinct solutions* $y(\mathrm{mod}\ p)$ *of* $y(ym_1{+}1)(ym_2{+}1)\ ...\ (ym_k{+}1) \equiv 0 \ (\mathrm{mod}\ p)$.

Just as one should view Conjecture 3 as a generalization of Dirichlet's Theorem (for primes in arithmetic progressions) from one to many linear polynomials, so one should view the next conjecture as a generalization of a weak form of the Siegel-Walfisz Theorem from one to many linear polynomials.

Conjecture 3^u. *For any fixed integer* k *and positive real* d, *the error term* $o(1)$ *in (2) depends only on* k *and* d *whenever each* $m_i \le d \log x$.

A consequence of our Proposition 2 is that Conjecture 3^u implies

Conjecture 3*. *For any given* $\varepsilon > 0$, *there exists a constant* $c(\varepsilon) > 0$ *such that if* x *is sufficiently large then there are less than* $\varepsilon\pi(x)$ *primes* $p \le x$ *with* $mp{+}1$ *composite for every* $m \le c(\varepsilon)\log x$ *and not divisible by 3.*

In Section 6 we will deduce from Conjecture 3* and Lemmas 1 and 2 that

$$\#\{\text{primes } p \le x\text{: } (1)_p \text{ has solutions}\} \;=\; o(\pi(x)) .$$

Thus we will have proved

Theorem 3. *If Conjecture* 3^u *is true then* $(1)_p$ *has no solutions for almost all primes* p; *that is* $\#\{$*primes* $p \le x$: $(1)_p$ *has solutions*$\}$ $= o(\pi(x))$.

In [9] we saw how the methods used in proving Sophie Germain's Theorem could be applied to studying any Diophantine Equation. For the rest of this section suppose that $f(X_1, ..., X_n) \in \mathbf{Z}[X_1, ..., X_n]$ is a given homogenous polynomial. For a given prime p we investigate whether there are integer solutions $x_1, x_2, ..., x_n$ to

$$f(x_1^p, x_2^p, ..., x_n^p) = 0 . \tag*{$(3)_p$}$$

In [9] we proved a rather technical analogue to Lemma 1:

Lemma 1'. *For any given homogenous polynomial f in n variables, there is a finite (computable) set of positive integers β such that if m is a positive, even integer, not divisible by any element of β, then there exists a non-zero integer $N_m (= N_m(f))$ such that if p and $q = mp + 1$ are both primes, and q does not divide N_m then $(3)_p$ has no 'non-trivial' integer solutions. Moreover there are $\ll_f m^{n-1}$ primes q that divide N_m.*

It is clear that Lemma 1' is useless if 1 or 2 are in the set β (for then all positive even integers m are divisible by an element of β!). We call f "admissible" if neither 1 nor 2 are elements of β (it is easily shown that there are relatively few inadmissible polynomials f).

Now, as any integer ≥ 3 is divisible by some element of $Q := \{4\} \cup \{\text{the odd primes}\}$, we can certainly replace β in Lemma 1' by a finite subset $\beta(f)$ of Q, whenever f is admissible. Then, by the methods used to prove Theorems 1, 2 and 3 (and by the methods of [1]) we are able to give various results on $(3)_p$.

Theorem 1 generalized. *If f is an admissible polynomial and Conjecture 1 is true then*

$$\#\{\textit{primes } p \leq x : (3)_p \textit{ has non-trivial solutions}\} \ll \log^{2n+1} x .$$

For any odd prime p, $p \notin \beta(f)$, define

$$\begin{aligned} \pi_\beta(x;p) &= \#\{\text{primes } q \leq x : p \mid q-1 \text{ but } b \nmid q-1 \text{ for all } b \in \beta\} \\ &= \sum_{\substack{d \mid \prod b \\ b \in \beta}} \mu(d)\, \pi(x; 2dp, 1) . \end{aligned}$$

Conjecture 2'. *For a given finite subset β of Q and positive integer $n \geq 3$, there exists θ, $1-1/n < \theta < 1$, for which*

$$\sum_{x^\theta < p < 2x^\theta} \pi_\beta(x;p) \gg x/\log^2 x .$$

Theorem 2 generalized. *If f is an admissible polynomial and Conjecture 2' is true then $(3)_p$ does not have non-trivial solutions for $\gg \pi(x)$ primes $\leq x$.*

Theorem 3 generalized. *If f is an admissible polynomial and Conjecture 3^u is true then $(3)_p$ has no non-trivial integer solutions for almost all primes p; that is*

$$\#\{\textit{primes } p \leq x : \ (3)_p \ \textit{ has non-trivial solutions}\} \ = \ o(\pi(x)) .$$

In a similar fashion we may use Lemma 1' to apply the ideas of Adleman and Heath-Brown [1] and of Filaseta, to equation $(3)_p$. The conjectures of [1] (given below as Conjecture 5) can be generalized as follows:

Conjecture 4. *For a given finite subset β of Q and integer $n \geq 3$, there exists θ, $1 - 1/n < \theta < 1$ for which*

(a) $$\sum_{\substack{2<p<x^\theta \\ p\notin\beta(f)}} \left| \pi_\beta(x;p) - \rho(\beta)\frac{\pi(x)}{(p-1)} \right| \ll x/\log^3 x$$

where $\rho(\beta) = \prod_{b\in\beta}\{1 - 1/\phi(b)\}$; and

(b) $$\sum_{x^\theta<p\leq x} \pi_\beta(x;p) \gg x/\log x.$$

Evidently the Elliott-Halberstam conjecture implies (a) which itself implies (b). Moreover, as in [1], we can show

Theorem 4. *If f is an admissible polynomial and Conjecture 4(a) is true then*

$$\#\{\textit{primes } p \leq x : \ (3)_p \ \textit{ has non-trivial solutions}\} \ll x/\log^2 x .$$

Let T be the set of primes for which $(3)_p$ has no solutions, and let

$$\pi_T(x) = \sum_{p\in T, p\leq x} 1 .$$

Theorem 5. *If f is an admissible polynomial and Conjecture 4(b) is true then*

(i) $$\sum_{p\in T, p\leq x} \frac{\log p}{p} \gg \log x$$

(ii) $$\pi_T(x) \gg x^\theta$$

(iii) *There are arbitrarily large values of x for which $\pi_T(x) \gg \pi(x)$.*

Theorems 5(i) and (ii) generalize results in [1] while Theorem 5(iii) generalizes Lemma 4(iii) (due to Filaseta) given below.

3. Exceptional Prime Pairs p,q

In order to be able to apply lemma 1 it is evidently necessary to estimate how many values of q divide N_m.

Lemma 2. *There exists a constant* $c_2 > 0$ *such that*

$$\#\{\textit{prime pairs } p,\, q = mp + 1\text{: } p|m \textit{ or } q|N_m\} \ \leq\ c_2m^2,$$

for all positive integers $m \equiv 2$ *or* 4 *(mod 6).*

Proof: For each α and β, $|1 + \alpha + \beta| \leq 3$ and so $|N_m| \leq 3^{m^2}$. Therefore there are $0(m^2)$ distinct primes q dividing N_m, and trivially $0(m)$ dividing m.

4. The Proof of Theorem 1

Proof: For a given prime p in the range $x < p \leq 2x$, we know, by Conjecture 1, that there is a prime $q_p < 7c_1x \log^2x$ in the arithmetic progression a_p (mod 3p) where $a_p = p+1$ if $p \equiv 1$ (mod 3), $2p+1$ otherwise. So if $q_p = mp+1$ then $m \equiv 2$ or 4 (mod 6) and $m < 7c_1\log^2x$. Therefore, by Lemmas 1 and 2 we have

$$\#\{\text{primes } p\text{: } x < p \leq 2x \text{ and } (1)_p \text{ has solutions}\} \ \leq \sum_{\substack{m<7c_1\log^2x \\ m\equiv 2 \text{ or } 4 \text{ (mod 6)}}} c_2m^2$$
$$\ll \log^6x.$$

Summing over the intervals $[2^{-i-1}x, 2^{-i}x]$ gives the result.

5. The Adleman-Heath-Brown approach

The Bombieri-Vinogradov Theorem states that for any $\varepsilon, A > 0$,

$$\sum_{q\leq Q} \max_{(a,q)=1} \max_{y\leq x} |\pi(y;\, q,a) - \frac{\pi(y)}{\phi(q)}| \ll_{A,\varepsilon} x/\log^Ax$$

where $Q = x^{1/2-\varepsilon}$. Elliott and Halberstam [3] conjectured that this can be extended to $Q = x^{1-\varepsilon}$. This implies the case $\beta = \{3\}$, n=3 of Conjecture 4a), namely

Conjecture 5a. *There exists* θ, $2/3 < \theta < 1$, *such that*

$$\sum_{3<p\leq x^\theta} |\pi^*(x;\, p) - \frac{\pi(x)}{2(p-1)}| \ll x/\log^3x\,.$$

This, in turn, implies the case $\beta = \{3\}$, n=3 of Conjecture 4b):

Conjecture 5b. *There exists* θ, $2/3 < \theta < 1$, such that

$$\sum_{x^\theta < p \leq x} \pi^*(x; p) \gg x/\log x\,.$$

Adleman and Heath-Brown [1] showed

Lemma 3. *If Conjecture 5a) is true then* $(1)_p$ *has solutions for* $\ll x/\log^2 x$ *prime exponents* $p \leq x$.

Let T be the set of primes for which $(1)_p$ has no solutions. Adleman and Heath-Brown [1] also showed the first two parts of Lemma 4; the last part is due to Filaseta.

Lemma 4. *If Conjecture 5b) is true then*

(i) $\displaystyle\sum_{x^\theta < p \leq x, p \in T} \frac{\log p}{p} \gg \log x$;

(ii) $\pi_T(x) \gg x^\theta$.

(iii) *There are arbitrarily large values of* x *for which* $\pi_T(x) \gg \pi(x)$.

Lemma 4(iii) follows immediately from Lemma 4(i) and

Lemma 5. *If* T *is a set of primes such that* $\displaystyle\sum_{p \leq x, p \in T} \frac{\log p}{p} > c_3 \log x$ *for all* $x > x_0$ *(for some constant* $c_3 > 0$*) then there are arbitrarily large values of* x *for which* $\pi_T(x) > \dfrac{c_3}{2}\,\dfrac{x}{\log x}$.

Proof. Suppose not, so that $\pi_T(x) \leq \dfrac{c_3}{2}\,\dfrac{x}{\log x}$ for all $x > x_1 (> x_0)$. Then, by forming a Riemann-Stieltjes integral, we have

$$\begin{aligned}\sum_{p \leq x, p \in T} \frac{\log p}{p} &= \int_{x_1}^{x} \frac{\log z}{z}\, d\pi_T(z) + O(1)\\ &= \frac{\log x}{x}\,\pi_T(x) + \int_{x_1}^{x} \frac{(\log z - 1)}{z^2}\,\pi_T(z) dz + O(1)\\ &\leq \frac{c_3}{2}\int_{x_1}^{x} \frac{\log z}{z^2}\,\frac{z}{\log z}\, dz + O(1)\\ &< \frac{c_3}{2}\log x + O(1)\,,\end{aligned}$$

giving a contradiction.

In 1985, Fouvry [6] showed that Conjecture 5b) holds for some $\theta > 0.6687$. From Lemma 4 one can immediately deduce a number of consequences for the set T.

Our approach here (that is, through Conjecture 2) evidently corresponds to assuming Conjecture 5b) on diadic intervals. This slight strengthening of the (already proved) Conjecture 5b) implies a significantly stronger result.

The next result not only implies Theorem 2 but also a different proof of Lemmas 4(ii) and (iii).

Proposition 1. *Suppose that* $c_4 > 0$ *and* $1 < \lambda < 3/2$ *are fixed constants. If, for given values of* z *and* x, *with* $x \leq z^{\lambda}$, *we have*

$$\sum_{z<p\leq 2z} \pi^*(x; p) \geq c_4 x/\log^2 x \tag{4}$$

then

$$\#\{z < p \leq 2z\colon\ p \text{ prime and } p \in T\} \gg z/\log z$$

We see that Theorem 2 follows immediately by taking $\lambda = 1/\theta$ in Proposition 1. Moreover Conjecture 5b) implies that, for any given x, there are $\gg \log x$ values of z of the form 2^k, satisfying (4), in the range $x^{\theta} < z < x$. Therefore we see, from Proposition 1:

Corollary 1. *If Conjecture 5b) is true then (ii) and (iii) follow.*

Proof of Proposition 1: Let $y = x/z$ so that

$$S_1 := \sum_{m\leq y,\ 3\nmid m} \#\{p \text{ prime: } z<p<2z,\ q = mp+1 \quad \text{is prime},\ p\nmid m,\ q\nmid N_m\}$$

$$= \sum_{z<p\leq 2z} \#\{m \leq y\colon 3\nmid m \text{ and } mp+1 \text{ is prime}\} + O\Big(\sum_{m\leq y} m^2\Big)$$

by Lemma 2

$$\geq \sum_{z<p\leq 2z} \pi^*(x;p) + O(y^3) \gg x/\log^2 x$$

by (4), as $y^3 = o(x/\log^2 x)$. On the other hand, it is well known that if $r < s \leq y$ then $N(z;r,s) \ll C(r,s)\, z/\log^3 z$ (see [10], Theorem 5.7). Therefore for $\beta = \{3\}$,

$$S_2 := \sum_{\substack{r<s\leq y \\ 3\nmid rs}} N(z;\, r,\, s)$$

$$\ll F_{2,\beta}(y) z/\log^3 z$$

where $F_{2,\beta}(y) = \sum_{r<s\leq y,\ 3\nmid rs} C(r,s)$. In Proposition 3 below we shall accurately estimate $F_{2,\beta}(y)$, but here a crude argument suffices:

By noting that, for $d = s-r > 0$,

$$C(r,s) \ll \frac{r}{\phi(r)}\frac{d}{\phi(d)}\frac{r+d}{\phi(r+d)},$$

we see that

$$\begin{aligned} F_{2,\beta}(y) &\ll \sum_{d\leq y}\frac{d}{\phi(d)}\sum_{r\leq y}\frac{r}{\phi(r)}\frac{r+d}{\phi(r+d)} \\ &\ll \sum_{d\leq y}\frac{d}{\phi(d)}\left[\sum_{r\leq y}\left[\frac{r}{\phi(r)}\right]^2\right]^{1/2}\left[\sum_{r\leq y}\left[\frac{r+d}{\phi(r+d)}\right]^2\right]^{1/2} \end{aligned}$$

by Cauchy's inequality,

$$\leq \left[\sum_{n\leq 2y}\left[\frac{n}{\phi(n)}\right]^2\right]^2$$

$$\ll y^2$$

from elementary considerations. Thus $S_2 \ll y^2z/\log^3 z$, and so by Cauchy's inequality and Lemma 1, we have

$$\pi_T(2z) - \pi_T(z) \gg S_1^2/S_2 \gg z/\log z.$$

6. The Number of Small Primes in Arithmetic Progressions

In order to prove Theorem 3, we will use Conjecture 3" to count, in a very precise way, the number of "small" primes in the arithmetic progression $1 (\mathrm{mod}\, p)$. More precisely, for given subset β of Q and $d > 0$ we define, for each $g \geq 0$, $B(x, g)$ to be the number of primes p, $x < p \leq 2x$, for which there are exactly g distinct integers $m_1, \ldots, m_g$, not divisible by any $b \in \beta$ and less than $d \log x$, such that each of $m_1p+1, m_2p+1, \ldots, m_gp+1$ is prime. We shall prove:

Proposition 2. *Suppose that Conjecture* 3" *is true. Given any finite subset* β *of* Q *and* $d > 0$ *we have*

$$B(x, t) \sim \frac{e^{-\lambda}\lambda^t}{t!}\frac{x}{\log x} \quad (as\ x \to \infty)$$

for any fixed non-negative integer t, *where* $\lambda = d\rho(\beta)$.

Assuming Proposition 2 we can now give the

Proof of Theorem 3: Fix $\varepsilon > 0$. By taking $\beta = \{3\}$, $t = 0$ and $d = -4\log\varepsilon$ $(= c(\varepsilon))$ in Proposition 2, we see that Conjecture 3^* follows from Conjecture $3^{\prime\prime}$.

Now by taking the integers $m \equiv 2$ or $4 \pmod 6$ with $m < d\log x$ in Lemma 1 we have

$$\#\{\text{primes } p\text{:}\ \ x < p \leq 2x \ \text{ and } \ (1)_p \text{ has solutions}\}$$

$$\leq \#\{\text{primes } p\text{:}\ \ x < p \leq 2x\text{and there } \textbf{does not} \text{ exist a prime } mp{+}1$$
$$\text{with } m < d\log x \ \text{ and } \ m \equiv 2 \ \text{ or } \ 4 (\text{mod } 6)\}$$
$$+ \sum_{m < d\log x,\ m\equiv 2 \text{ or } 4 (\text{mod } 6)} \#\{\text{primes } p\text{:}\ \ p|m \ \text{ or } \ q = mp{+}1 \mid N_m\}$$
$$\leq \ \varepsilon\pi(x) + O(\log^3 x)$$

by Conjecture 3^* and Lemma 2,

$$\leq \ 2\varepsilon\pi(x)$$

for all sufficiently large x. Summing over the intervals $[2^{-i-1}x, 2^{-i}x]$ gives the result.

The proof of Proposition 2 is very similar to that of Theorem 5 in [7] where we estimated, for any fixed $a \neq 0$, the number of integers n, $x < n \leq 2x$, for which there are exactly g integers $m_1, \ldots, m_g$, each less than $d\log x$, such that each of $m_1n{+}a, m_2n{+}a, \ldots, m_gn{+}a$, is prime. In our proof we shall miss out some technical details that are identical to the proof of that result.

Now, for any fixed k,

$$\sum_{g\geq k} \begin{bmatrix} g \\ k \end{bmatrix} B(x, g) \ = \ \sum_{\substack{1\leq m_1<\ldots<m_k<d\log x \\ b\nmid m_i \text{ for all } b\in\beta}}{}_{1} \ N(x; m_1, m_2, \ldots, m_k)$$

$$= \ F_{k,\beta}(d\log x)\frac{x}{(\log x)^{k+1}} \ \{1 + o(1)\} \tag{5}$$

by Conjecture $3^{\prime\prime}$, where $F_{k,\beta}(y) \ = \ \sum_1 C(m_1, \ldots, m_k)$ and $\sum_1$ is the sum over sets of k positive integers $m_1 < m_2 < \cdots < m_k \leq y$, none of which are divisible by any $b \in \beta$.

In Section 7 we will prove

Proposition 3. *For any fixed subset* β *of* Q, *integer* $k \geq 1$ *and real* $\varepsilon > 0$, *we have the estimate*

$$F_{k,\beta}(x) = \frac{1}{k!}\,(\rho(\beta)x)^k\,\{1 + O(x^{\varepsilon-1/2})\}\,. \tag{6}$$

The main idea of the proof of Proposition 2 is to use the combinatorial identity

$$B(x,\,t) = \sum_{k\geq t} A_k(x), \text{ where } A_k(x) = (-1)^{k-t}\binom{k}{t}\sum_{g\geq k}\binom{g}{k} B(x,\,g), \tag{7}$$

for each $t \geq 0$, together with the estimates (5) and (6). Unfortunately, as the o(1) in (2) depends on k, we cannot use the infinite sum in (7), **but** we are able to approximate $B(x,\,t)$ by $\sum_{k=t}^{n} A_k(x)$ for n large to prove the result.

Now, by (2) and (6) we have

$$A_k(x) = \frac{\lambda^t}{t!}\,\frac{(-\lambda)^{k-t}}{(k-t)!}\,\frac{x}{\log x}\,\{1 + o_k(1)\}. \tag{8}$$

Moreover, as $\left|\sum_{k=0}^{r}(-1)^{k+1}\binom{s}{k}\right| \leq \binom{s}{r}$ for any integers $r, s \geq 1$, we have, for any fixed $n \geq t+1$,

$$\begin{aligned}\left|B(x,\,t) - \sum_{k=t}^{n} A_k(x)\right| &= \left|\sum_{g\geq n+1}\left[\sum_{k=0}^{n-t}(-1)^{k+1}\binom{g-t}{k}\right]\binom{g}{t} B(x,\,g)\right| \\ &\leq \sum_{g\geq n+1}\binom{g-t}{n-t}\binom{g}{t} B(x,\,g) \\ &\leq \binom{n}{t}\sum_{g\geq n}\binom{g}{n} B(x,\,g) \\ &\leq \frac{\lambda^n}{t!}\,\frac{1}{(n-t)!}\,\frac{x}{\log x}\,\{1 + o(1)\}\end{aligned} \tag{9}$$

by (8). Define $s_n = \sum_{k\geq n}(-\lambda)^k/k!$ which tends to 0 as $n \to \infty$. Then

$$\left|B(x,\,t) - e^{-\lambda}\frac{\lambda^t}{t!}\,\frac{x}{\log x}\right| \leq \left|B(x,\,t) - \sum_{k=t}^{n} A_k(x)\right|$$

$$+ \left|\sum_{k=t}^{n}\{A_k(x) - \frac{\lambda^t}{t!}\,\frac{(-\lambda)^{k-t}}{(k-t)!}\,\frac{x}{\log x}\}\right| + \frac{\lambda^t}{t!}\,\frac{x}{\log x}\left|e^{-\lambda} - \sum_{k=t}^{n}\frac{(-\lambda)^{k-t}}{(k-t)!}\right|$$

$$\leq \frac{\lambda^t}{t!}\,\frac{x}{\log x}\,\{\frac{\lambda^{n-t}}{(n-t)!} + o_n(1) + |s_{n-t+1}|\}$$

by (8) and (9),

7. Technical stuff: The Proof of Proposition 3

We evaluate $F_{k,\beta}(x)$ as $x \to \infty$, using essentially the same method as in the proof of Theorem 6 of [7]. In keeping control of the error term the details become extremely technical. We avoid these details here as they are very similar and refer the reader to [7].

Now $w_m(p)$ counts precisely the number of distinct residue classes (mod p) that contain an m_i $(i = 0, 1, ..., k)$ where $m_0 = 0$.

We define $\phi_k(d) = \prod_{p|d, p>k} (p-k)$ for each $d \geq 1$, and

$$c_5 = \prod_p \frac{\phi_{k+1}(p)/p}{(1-1/p)^{k+1}} .$$

It is easy to see that

$$C(m_1, ..., m_k) = c_5 \prod_{p|\theta(m)} \frac{p - w_m(p)}{\phi_{k+1}(p)} \tag{10}$$

where $\theta(m) = \left[\prod_{i=1}^{k} m_i\right] \left[\prod_{1\leq i<j\leq k} (m_j - m_i)\right]$, and so the product in (10) is finite. Therefore

$$\begin{aligned} F_{k,\beta}(x) &= c_5 \sum\nolimits_1 \sum_{d|\theta(m)} \mu^2(d) \prod_{p|d} \left[\frac{p - \phi_{k+1}(p) - w_m(p)}{\phi_{k+1}(p)}\right] \\ &= g_{k,\beta} \frac{x^k}{k!} \{1 + O_{k,\beta}(x^{\varepsilon-1/2})\} \end{aligned}$$

after a considerable amount of rearrangement (exactly as in [7]) where

$$g_{k,\beta} = c_5 \sum_{d\geq 1} \frac{\mu^2(d)}{\phi_{k+1}(d)} \frac{1}{(ad)^k} \sum\nolimits_{2\, d|\theta(m)} \prod_{p|d} [p - \phi_{k+1}(p) - w_m(p)] , \tag{11}$$

$a = \prod_{b\in\beta} b$ and $\sum_2$ is the sum over $1 \leq m_1, ..., m_k \leq ad$ with $b \nmid m_i$ for each i and $b \in \beta$.

Now, in order to evaluate the sum in (11) we need:

Lemma 6. *For each* $k \geq 1$ *we have*

(a) $\lambda_k(p) \;=\; \sum_{0 \leq m_1, \dots, m_k \leq p-1} w_m(p) \;=\; p^{k+1} - (p-1)^{k+1},$

(b) $\bar{\lambda}_k(p) \;=\; \sum_{1 \leq m_1, \dots, m_k \leq p-1} w_m(p) \;=\; p(p-1)^k - (p-1)(p-2)^k,$ and

(c) $\sum_{1 \leq m_1, \dots, m_k \leq 3} w_m(2) \;=\; 2.3^k - 1.$

Proof: (a) Let $\lambda_{k,j}(p)$ denote the number of k-tuples $(m_1, \dots, m_k)$, with $0 \leq m_1, \dots, m_k \leq p-1$, for which there are **exactly** j non-zero residue classes (mod p) that contain an m_i. We shall prove our result by induction on k: For $k = 1$,

$$\lambda_1(p) \;=\; 2.\lambda_{1,1}(p) + 1.\lambda_{1,0}(p) \;=\; 2(p-1) + 1 \;=\; p^2 - (p-1)^2 .$$

Now, by using the identity

$$\lambda_{k+1,j}(p) \;=\; (j+1)\,\lambda_{k,j}(p) + (p-j)\,\lambda_{k,j-1}(p)\,, \tag{12}$$

we have

$$\lambda_{k+1}(p) \;=\; \sum_{j=0}^{k+1} (j+1)\,\lambda_{k+1,j}(p)$$

$$=\; \sum_{j=0}^{k} \big(p + (p-1)(j+1)\big)\,\lambda_{k,j}(p)\,,$$

using (12),

$$=\; p^{k+1} + (p-1)\,\lambda_k(p) \;=\; p^{k+2} - (p-1)^{k+2}\,,$$

by the induction hypothesis.

(b) It is easy to see that $\lambda_h(p) = \sum_{j=0}^{h} \binom{h}{j} \bar{\lambda}_j(p)$ and so,

$$\bar{\lambda}_k(p) \;=\; \sum_{h=0}^{k} \binom{k}{h} (-1)^{k-h}\,\lambda_h(p)$$

$$=\; \sum_{h=0}^{k} \binom{k}{h} (-1)^{k-h} \left(p^{h+1} - (p-1)^{h+1}\right)$$

by (a),

$$=\; p(p-1)^k - (p-1)(p-2)^k .$$

(c) As $w_m(2) = 2$ unless each m_i equals 2, the result is immediate.

Now, for a fixed value of d we have

$$\underset{d|\theta(m)}{\textstyle\sum_2} \prod_{p|d} \Big[p - \phi_{k+1}(p) - w_m(p)\Big] = \Pi_1\, \Pi_2\, \Pi_3\, \Pi_4 \tag{13}$$

where

$$\Pi_1 = \prod_{\substack{p\nmid a \\ p|d}} \sum_{\substack{0\le m_1, \,\ldots,\, m_k\le p-1 \\ p|\theta(m)}} \Big[p - \phi_{k+1}(p) - w_m(p)\Big]$$

$$= \prod_{\substack{p\nmid a \\ p|d}} \Big[p^k\big(p-\phi_{k+1}(p)\big) - \lambda_k(p)\Big] = \prod_{\substack{p\nmid a \\ p|d}} \Big[(p-1)^{k+1} - p^k\, \phi_{k+1}(p)\Big]$$

by Lemma 6(a),

$$= \prod_{\substack{p|d \\ p\nmid a}} \big(-p^k\phi_{k+1}(p)\big)\left[1 - \frac{(p-1)}{\phi_{k+1}(p)}\left(\frac{p-1}{p}\right)^k\right];$$

$$\Pi_2 = \prod_{\substack{b\in\beta \\ (b,d)=1}} \sum_{1\le m_1, \,\ldots,\, m_k\le b-1} 1 = \prod_{\substack{b\in\beta \\ (b,d)=1}} (b-1)^k;$$

$$\Pi_3 = \prod_{\substack{p|(a,d) \\ p\ge 3}} \sum_{\substack{0\le m_1, \,\ldots,\, m_k\le p^2-1 \\ p\nmid m_1 \ldots m_k}} \Big[p - \phi_{k+1}(p) - w_m(p)\Big]$$

$$= \prod_{\substack{p|(a,d) \\ p\ge 3}} p^k\Big[(p-1)^k\big(p-\phi_{k+1}(p)\big) - \bar\lambda_k(p)\Big]$$

$$= \prod_{\substack{p|(a,d) \\ p\ge 3}} p^k\Big[(p-1)(p-2)^k - (p-1)^k\, \phi_{k+1}(p)\Big]$$

by Lemma 6(b),

$$= \prod_{\substack{p|(d,a) \\ p\ge 3}} \big(-p^k(p-1)^k\phi_{k+1}(p)\big)\left[1 - \frac{(p-1)}{\phi_{k+1}(p)}\left(\frac{p-2}{p-1}\right)^k\right];$$

$$\Pi_4 = \sum_{\substack{0\le m_1,\ldots,m_k\le 7\\ 4m_1,\ldots,m_k}} \Big[1 - w_m(p)\Big] = 2^k[1-3^k],$$

by Lemma 6(c), if $4\in\beta$ and $2|d$; $\pi_4 = 1$ otherwise.

Therefore, by (11) and (13), and a little rearrangement, we have

$$g_{k,\beta} = c_5 \prod_{b\in\beta}\Big(1-\frac{1}{b}\Big)^k \sum_{d\ge 1}\mu(d)\cdot\prod_{p|d}\left[1-\frac{(p-1)}{\phi_{k+1}(p)}\Big(1-\frac{1}{p-\varepsilon_p}\Big)^k\right]\cdot r_d$$

where $r_d = 1 - 1/3^k$ if $4\in\beta$ and $2|d$, 1 otherwise, and $\varepsilon_p = 1$ if $p|a$, 0 otherwise,

$$= c_5 \prod_{b\in\beta}\Big(1-\frac{1}{b}\Big)^k\left[\prod_p \frac{(p-1)}{\phi_{k+1}(p)}\Big(\frac{p-1}{p}\Big)^k\right]\left[\prod_{\substack{p|a\\ p\ge 3}}\Big(\frac{p(p-2)}{(p-1)^2}\Big)^k\right] s_\beta$$

where $s_\beta = (2/3)^k$ if $4\in\beta$, 1 otherwise,

$$= \prod_{b\in\beta}\Big(1-\frac{1}{\phi(\beta)}\Big)^k = \rho(\beta)^k.$$

The result follows immediately.

Acknowledgements: I'd like to thank Michael Filaseta for allowing me to include his unpublished results (Lemma 4(iii) and Lemma 5) in this paper; and the referee for a number of thoughtful comments.

REFERENCES

[1] Adleman, L.M. and Heath-Brown, D.R., The first case of Fermat's last theorem, Invent. Math., **79** (1985) 409-416.

[2] Bateman, P.T. and Horn, R.A., A heuristic asymptotic formula concerning the distribution of prime numbers, Math. Comp., **16** (1962), 363-367.

[3] Bombieri, E., Friedlander, J.B. and Iwaniec, H., Primes in arithmetic progressions to large moduli, III, J. Amer. Math. Soc., **2** (1989) 215-224.

[4] Dickson, L.E., A new extension of Dirichlet's theorem on prime numbers, Messenger of Math., **33** (1904) 155-161.

[5] Elliott, P.D.T.A. and Halberstam, H., A conjecture in prime number theory, Symp. Math., **4** (1968-9), 59-72.

[6] Fouvry, E., Théorème de Brun-Titchmarsh, application au théorème de Fermat, Invent. Math., **79** (1985), 383-407.

[7] Granville, A., Least Primes in Arithmetic Progressions, in: J.-M. de Koninck and C. Levesque (eds.), Théorie des nombres (Proceedings of the International Number Theory Conference at Laval, Quebec, 1987), de Gruyter, New York 1989, pp. 306-321.

[8] Granville, A., Some conjectures related to Fermat's Last Theorem, to appear in the Proceedings of the First Conference of the Canadian Number Theory Association, 1988.

[9] Granville, A., Diophantine Equations with varying exponents, (Ph.D. Thesis, Queen's University), 1987.

[10] Halberstam, H. and Richert, H.-E., Sieve Methods, (Academic Press), 1974.

[11] Hardy, G.H. and Littlewood, J., Some problems of partitio numerantium III. On the expression of a number as a sum of primes, Acta Math., **44** (1923), 1-70.

[12] Heath-Brown, D.R., Almost primes in arithmetic progressions and short intervals, Math. Proc. Camb. Phil. Soc., **83** (1978) 357-375.

[13] Linnik, U.V., On the least prime in an arithmetic progression II, The Deuring-Heilbronn phenomenon, Rec. Math. [Math. 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] Ribenboim, P., 13 Lectures on Fermat's Last Theorem, (Springer-Verlag, New York) 1979.

[16] Schinzel, A and Sierpinski, W., Sur certaines hypothèses concernant les nombres premiers, Acta Arith. **4** (1958), 185-208; erratum **5** (1959), 259.

[17] Wagstaff, S.S. Jr., Greatest of the least primes in arithmetic progresssions having a given modulus, Math. Comp., **33** (1979) 1073-1080.

Andrew Granville
School of Mathematics
Institute for Advanced Study
Princeton, NJ 08540