Math. Proc. Camb. Phil. Soc. (1989), **106**, 7
Printed in Great Britain

The function field abstract prime number theorem

BY STEPHEN D. COHEN

Department of Mathematics, University of Glasgow, Glasgow G12 8QW

(*Received* 15 *August* 1988; *revised* 31 *October* 1988)

1. *Introduction*

For arithmetical semigroups modelled on the positive integers, there is an 'abstract prime number theorem' (see, for example, [1]). In order to study enumeration problems in the several arithmetical categories whose prototype instead is the ring of polynomials in an indeterminate over a finite field of order q, Knopfmacher [2, 3] introduced the following modification. An *additive* arithmetical semigroup G is a free commutative semigroup with an identity, generated by a countable set of 'primes' P and admitting an *integer-valued* degree mapping ∂ with the properties

(i) $\partial(1) = 0, \partial(p) > 0$ for $p \in P$;

(ii) $\partial(ab) = \partial(a) + \partial(b)$ for all a, b in G;

(iii) the number of elements in G of degree n is finite. (This number will be denoted by $G(n)$.)

The investigation described in [3] principally concerned arithmetical semigroups satisfying a precise formulation of (iii) known as Axiom A$^\#$.

Axiom A$^\#$. There exist constants $A > 0$, $q > 1$ and ν with $0 \leqslant \nu < 1$ such that

$$G(n) = Aq^n + O(q^{n\nu}) \quad \text{as} \quad n \to \infty.$$

At its core is an abstract prime number theorem for additive arithmetical semigroups satisfying Axiom A$^\#$. This is an estimate for $P(n)$, the number of primes in P of degree n. It states that, for any $\alpha > 1$,

$$P(n) = \frac{q^n}{n} + O\left(\frac{q^n}{n^\alpha}\right) \quad \text{as} \quad n \to \infty. \tag{1}$$

In this paper we improve (1) by showing that there is a constant θ with $\max(\frac{1}{2}, \nu) < \theta < 1$ such that

$$P(n) = \frac{q^n}{n} + O(q^{n\theta}) \quad \text{as} \quad n \to \infty. \tag{2}$$

Conversely, we show that an estimate of the form (2) for some θ with $0 \leqslant \theta < 1$ implies Axiom A$^\#$ (with $\max(\frac{1}{2}, \theta) < \nu < 1$) and end by summarizing our results in a series of equivalent statements.

To conclude this Introduction, note these conventions. Throughout, G will be an additive arithmetical semigroup. In Sections 2–4, G will be assumed to satisfy Axiom A$^\#$, an assumption which will then be dropped in Sections 5 and 6. The functions and

https://doi.org/10.1017/S0305004100067943 Published online by Cambridge University Press

related power series fully discussed in [1] and [3] will be freely used and we will write Σa_n for $\Sigma_{n=0}^{\infty} a_n$. As in [3], given a function $f(a)$ on G, put

$$f(n) = \sum_{\partial(a)=n} f(a) \quad \text{and} \quad f(y) = \Sigma f(n)\, y^n$$

(although we remark that Knopfmacher generally uses $\bar{f}$ or $f^{\#}$ instead of f).

2. *The divisor function*

By Axiom A$^{\#}$ we can write

$$G(n) = A(q^n + E(n)),$$

where $E(n) = O(q^{n\nu})$ as $n \to \infty$. In particular $\Sigma E(n)/q^n$ is convergent to E (say).

We begin by proving a simple 'Dirichlet type' estimate involving E for $d(n)$, where $d(a)$ denotes the total number of divisors of $a \in G$. It is a sharpened version of [2], lemma 3·3, or [3], proposition 7·1.

THEOREM 1.

$$d(n) = A^2(n+1+2E)\, q^n + O(nq^{n\nu}) \tag{3}$$

$$= A(n+1+2E)\, G(n) + O(nq^{n\nu}) \quad as \quad n \to \infty. \tag{4}$$

Proof. By [1], theorem 3·3·1 we have $d(y) = Z^2(y)$, where $Z(y) = \Sigma G(n)\, y^n$. This immediately implies that

$$\begin{aligned} d(n) &= \sum_{m \leqslant n} G(m)\, G(n-m) \\ &= A^2\{(n+1)\, q^n + 2 \sum_{m \leqslant n} E(m)\, q^{n-m} + \sum_{m \leqslant n} E(m)\, E(n-m)\} \\ &= A^2\{(n+1+2E)\, q^n - 2q^n \sum_{m>n} E(m)/q^m\} + O(nq^{n\nu}). \end{aligned}$$

By Axiom A$^{\#}$ as in [3], pp. 19–20,

$$\sum_{m>n} E(m)/q^m = O\Big(\sum_{m>n} q^{m(\nu-1)}\Big) = O(q^{n(\nu-1)}).$$

Hence (3) is valid and (4) follows by another application of Axiom A$^{\#}$.

3. *Conditional result*

Proposition 2·1 of [3] implies that, in terms of a complex variable y, $Z(y)$ is an analytic function of $y \neq q^{-1}$ in the disc $|y| < q^{-\nu}$ which is non-zero for $|y| < q^{-1}$ and has a simple pole with residue $-q^{-1}A$ at $y = q^{-1}$. Indeed, this all simply follows from the representation

$$Z(y) = A\left[\frac{1}{1-qy} + \Sigma E(n)\, y^n\right]. \tag{5}$$

Consistent with the familiar pattern, there is significant gain in extending the zero-free region of Z onto and beyond the circle $|y| = q^{-1}$. The following theorem is conditional on the existence of such an extension.

https://doi.org/10.1017/S0305004100067943 Published online by Cambridge University Press

THEOREM 2. *Assume that for some* α, *where* $\max(\frac{1}{2}, \nu) \leqslant \alpha < 1$, $Z(y)$ *is non-zero for all* $y(\neq q^{-1})$ *with* $|y| < q^{-\alpha}$. *Then, for any* θ *with* $\alpha < \theta < 1$,

$$P(n) = \frac{q^n}{n} + O(q^{n\theta}) \quad as \quad n \to \infty.$$

Proof. Use (5) to define a function $Z^*(y)$ analytic on the disc $|y| < q^{-\nu}$ by means of $Z^*(y) = (1-qy)\,Z(y)$. Then, by assumption, the function $(1-qy)/Z^*(y)$ is analytic on the disc $|y| < q^{-\alpha}$ (and agrees with $1/Z(y)$ for $y \neq q^{-1}$). However, if $\mu(a)$ is the Möbius function on G, then by [1], theorem 3·3·1, $\mu(y) = 1/Z(y)$ which therefore, as a power series in y, has radius of convergence $q^{-\alpha}$ at least. Thus we deduce in particular that $\Sigma\,\mu(n)\,q^{-n\theta}$ is convergent and certainly that

$$\mu(n) = O(q^{n\theta}). \tag{6}$$

Now let $\Lambda(a)$ be the von Mangoldt function on G, i.e.

$$\Lambda(a) = \begin{cases} \partial(p) & \text{if } a = p^r (\neq 1) \text{ for some } p \in P, \\ 0 & \text{otherwise.} \end{cases}$$

Then, again by [1], theorem 3·3·1,

$$\Lambda(y) = yZ'(y)/Z(y),$$

where Z' denotes the formal derivative of Z. Thus the identity

$$A^{-1}Z(y) - \Lambda(y) - (1+2E) = \mu(y)\,(A^{-1}Z^2(y) - yZ'(y) - (1+2E)\,Z(y))$$

yields

$$A^{-1}G(n) - \Lambda(n) = \sum_{m \leqslant n} \mu(m)\,\delta(n-m) \quad (n \geqslant 1), \tag{7}$$

where

$$\begin{aligned} \delta(n) &= A^{-1}d(n) - (n+1+2E)\,G(n) \quad (n \geqslant 0) \\ &= O(nq^{n\nu}) \end{aligned} \tag{8}$$

by Theorem 1. Applying (6) and (8) with Axiom A$^\#$ to (7) we obtain

$$\begin{aligned} \Lambda(n) - A^{-1}G(n) &= O(q^{n\nu}) + O\Big(n \sum_{m \leqslant n} q^{m\theta + (n-m)\nu}\Big) \\ &= O(nq^{n\theta}) \end{aligned}$$

since $\theta > \nu$. The result follows by Axiom A$^\#$ and lemma 8·4 of [3] which states that

$$P(n) = n^{-1}\Lambda(n) + O(q^{\frac{1}{2}n} \log n) \quad \text{as} \quad n \to \infty.$$

4. *Zero-free region*

THEOREM 3. *For some* α *with* $\nu \leqslant \alpha < 1$, $Z(y)$ *is non-zero for all* $y\,(\neq q^{-1})$ *with* $|y| < q^{-\alpha}$.

Proof. In addition to being analytic on the disc $|y| < q^{-\nu}$, the function $Z^*(y)$ introduced in the proof of Theorem 2 is actually non-zero on the closed disc $|y| \leqslant q^{-1}$ by [3], lemma 8·5, and thus does not vanish on a suitable disc $|y| < R$ where $R > q^{-1}$. Defining α by $q^\alpha = 1/R$ completes the proof.

https://doi.org/10.1017/S0305004100067943 Published online by Cambridge University Press

In summary, we have established the abstract prime number theorem in the form (2) for some unspecified θ. It would, of course, be of interest to be able to describe θ more precisely in terms of ν (and possibly other quantities involved in Axiom A$^\#$).

5. *Converse*

Now, instead of assuming Axiom A$^\#$, we derive it from (2).

THEOREM 4. *Suppose that for some α with $0 \leqslant \alpha < 1$*

$$P(n) = \frac{q^n}{n} + O(q^{n\alpha}) \quad as \quad n \to \infty.$$

Then, for every ν with $\max(\frac{1}{2}, \alpha) < \nu < 1$, Axiom A$^\#$ is valid for some $A > 0$.

Proof. We can assume $\frac{1}{2} \leqslant \alpha < \nu$. From [3], p. 77

$$\Lambda(n) = \sum_{d|n} dP(d).$$

Hence $\Lambda(0) = 0$, while, if $n \geqslant 1$,

$$\Lambda(n) = q^n + O(nq^{n\alpha}) = q^n + O(q^{n\beta}) \quad (\alpha < \beta < \nu).$$

Accordingly, write

$$\Lambda(n) = q^n + F(n) \quad (n \geqslant 1),$$

where $|F(n)| \leqslant Kq^{n\beta}$ for some $K > 0$. Then

$$y^{-1}\Lambda(y) = \frac{Z'(y)}{Z(y)} = \frac{q}{1-qy} + \sum_{r=1}^{\infty} F(r)\, y^{r-1}. \tag{9}$$

Now certainly (9) is valid for real y with $|y| < q^{-1}$ and $Z(0) = 1$. It follows that, for such y, $Z(y)$ does not vanish and

$$\log Z(y) = -\log(1-qy) + L(y),$$

where
$$L(y) = \sum_{r=1}^{\infty} r^{-1}F(r)\, y^r, \tag{10}$$

i.e.
$$Z(y) = (1-qy)^{-1} \exp L(y). \tag{11}$$

Consequently, of course, (11) remains valid for *complex* y with $|y| < q^{-1}$.

Next, set

$$G(n) = Aq^n + E(n),$$

where
$$0 < A = \exp L(q^{-1}) \leqslant (1-q^{\beta-1})^{-K}. \tag{12}$$

Then, by (11),

$$E(y)\,(= \Sigma E(n)\, y^n) = (1-qy)^{-1}(\exp(L(y)) - A). \tag{13}$$

However, (13) (with (10)) can be used to define $E(y)$ as an analytic function on $|y| < q^{-\beta}$ satisfying $E(q^{-1}) = -q^{-1}\exp(\sum_{r=1}^{\infty} F(r)/q^{1-r})$.

https://doi.org/10.1017/S0305004100067943 Published online by Cambridge University Press

By Cauchy's theorem

$$2\pi i E(n) = \int_{|y|=q^{-\nu}} \frac{\exp(L(y))-A}{(1-qy)\,y^{n+1}}\,dy = iq^{n\nu}\int_0^{2\pi} \frac{\exp(L(q^{-\nu}e^{it}))-A}{(1-q^{1-\nu}e^{it})\,e^{int}}\,dt.$$

Hence

$$|q^{-n\nu}E(n)| \leqslant (2\pi)^{-1}.2\pi(1-q^{1-\nu})^{-1}\left\{\exp\left(\sum_{r=1}^{\infty}\frac{|F(r)|}{rq^{r\nu}}\right)+A\right\}$$

$$\leqslant (1-q^{1-\nu})\left\{\exp\left(K\sum_{r=1}^{\infty}\frac{q^{r\beta}}{rq^{r\nu}}\right)+A\right\}$$

$$\leqslant (1-q^{1-\nu})^{-1}\{(1-q^{\beta-\nu})^{-K}+(1-q^{\beta-1})^{-K}\}$$

using (12). The result follows.

6. *Equivalent conditions*

Following a suggestion by Professor Knopfmacher we conclude by listing a series of equivalent statements in the form of a theorem. It involves constants q, ν and A not necessarily the same on each occurrence but always satisfying $q > 1$, $0 \leqslant \nu < 1$ and $A > 0$. $Z(y)$ denotes the power series $\sum G(n)\,y^n$ and $Z^*(y)$ the series $\sum G^*(n)\,y^n$, where $G^*(n) = G(n)-qG(n-1)$ (with $G(-1)=0$), so that, formally, $Z^*(y) = (1-qy)\,Z(y)$ as in the proof of Theorem 2.

THEOREM 5. *The following assertions* (i)–(iv) *are equivalent*:

(i) *there exist* q, ν *and* A *such that*

$$G(n) = Aq^n + O(q^{n\nu}) \quad as \quad n\to\infty;$$

(ii) *there exist* q, ν *such that*

$$P(n) = \frac{q^n}{n} + O(q^{n\nu}) \quad as \quad n\to\infty;$$

(iii) *there exist* q, ν *such that the complex function* Z *is analytic and non-zero for* $|y| < q^{-\nu}$ *except for a simple pole at* $y = q^{-1}$;

(iv) *there exist* q, ν *such that* $Z^*(y)$ *is convergent for* $|y| < q^{-\nu}$ *with* $Z^*(q^{-1}) \neq 0$.

Proof. From our discussion so far the equivalence of (i) and (ii) and the implication (i) $\Rightarrow$ (iii) are clear.

(iii) $\Rightarrow$ (iv). The radius of convergence of $Z^*(y)$ is obviously at least that of $Z(y)$, namely, q^{-1}. Moreover $(1-qy)\,Z(y)$ is analytic for $|y| < q^{-\nu}$ so that in fact $Z^*(y)$ has radius of convergence at least $q^{-\nu}$. Also $Z^*(q^{-1}) \neq 0$ since $y = q^{-1}$ is a pole of Z.

(iv) $\Rightarrow$ (i). Since $Z^*(q^{-1}) \neq 0$ then $G(n)/q^n \not\to 0$ as $n\to\infty$ and so $Z(q^{-1})$ is divergent. However, with ν as in (iv) and any α with $\nu < \alpha < 1$, $G^*(n) = O(q^{n\alpha})$. Hence

$$G(n) = \sum_{m\leqslant n} G^*(m)\,q^{n-m} = O(q^n \sum_{m\leqslant n} q^{m(\alpha-1)}) = O(q^n).$$

We deduce that the radius of convergence of $Z(y)$ is exactly q^{-1}. Thus $Z^*(y)/(1-qy)$

https://doi.org/10.1017/S0305004100067943 Published online by Cambridge University Press

is an extension of $Z(y)$ analytic on $|y| < q^{-\nu}$ except for a simple pole at $y = q^{-1}$ with residue $-q^{-1}A$, where $A = Z^{*\prime}(q^{-1}) \neq 0$. Set

$$G(n) = A(q^n + E(n)).$$

Then
$$E(y) = A^{-1}Z(y) - (1-qy)^{-1}$$

and $E(y)$ is analytic for $|y| < q^{\nu}$, whence, for any α with $\nu < \alpha < 1$, $E(y)$ is convergent for $|y| \leqslant q^{-\alpha}$ and $E(n) = O(q^{n\alpha})$. This completes the proof.

It might be of interest to investigate relationships between the various values of ν occurring in the equivalent statements of Theorem 5 and also what would ensue were the hypothesis that the singularity at $y = q^{-1}$ in (iii) be a simple pole to be relaxed.

REFERENCES

[1] J. KNOPFMACHER. *Abstract analytic number theory* (North-Holland, 1975).
[2] J. KNOPFMACHER. An abstract prime number theorem relating to algebraic function fields. *Arch. Math.* (*Basel*) **29** (1977), 271–279.
[3] J. KNOPFMACHER. *Analytic arithmetic of algebraic function fields*. Lecture Notes in Pure and Applied Math. no. 50 (Marcel Dekker, 1979).

https://doi.org/10.1017/S0305004100067943 Published online by Cambridge University Press