Conspectus materiae tomi XXVIII, fasciculi 2

La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисер

L'adresse de la Rédaction et de l'échange
Address of the Editorial Board and of the exchange
Die Adresse der Schriftleitung und des Austausches
Адрес редакции и книгообмена

ACTA ARITHMETICA
ul. Śniadeckich 8, 00-950 Warszawa

Les auteurs sont priés d'envoyer leurs manuscrits en deux exemplaires
The authors are requested to submit papers in two copies
Die Autoren sind gebeten um Zusendung von 2 Exemplaren jeder Arbeit
Рукописи статей редакция просит предлагать в двух экземплярах

PRINTED IN POLAND

WROCŁAWSKA DRUKARNIA NAUKOWA

CTA ARITHMETICA
XXVIII (1975)

Class numbers of elliptic function fields and the distribution of prime numbers

by

LAWRENCE WASHINGTON (Princeton, N. J.)*

An interesting problem in number theory is the determination of vhich integers occur as class numbers of algebraic number fields. In this ote we consider the corresponding question for function fields over inite fields and relate it to a classical problem in the distribution of prime umbers; namely, is there at least one prime between n^2 and $(n+1)^2$ for ll positive integers n?

THEOREM 1. (a) *Suppose that for every positive integer n there is a prime etween n^2 and $(n+1)^2$. Then, for each positive integer m, there exists a prime and an elliptic function field E over F_p (the finite field with p elements) uch that the class number (i.e., the number of divisor classes of degree 0) f E equals m.*

(b) *Conversely, suppose that each positive integer occurs as the class umber of some elliptic function field over some F_p (p prime). Then for ach positive integer n there is a prime between n^2 and $(n+2)^2$.*

THEOREM 2. *Let $H(x)$ be the number of positive integers less than or qual to x which do not occur as class numbers of elliptic function fields over ny F_p. Then*

$$H(x) = O\left(\frac{x}{\log x}\right) \quad \text{as} \quad x \to \infty.$$

n particular, the set of integers which are class numbers has asymptotic ensity 1.

Before proceeding with the proofs, we first need some preliminary emarks. Let E be an elliptic function field over F_p and let h be its class umber. Then the zeta-function of E has the form

$$Z(u) = \frac{P(u)}{(1-u)(1-pu)},$$

* Research supported by a National Science Foundation Graduate Fellowship.

where $P(u) = pu^2+au+1$ for some integer a, and $P(1) = p+a+1 = h$ (see [4], p. 130). By the Hasse–Weil theorem (i.e., the Riemann hypothesis for function fields), $P(u) = (1-\pi u)(1-\pi' u)$ with $|\pi| = |\pi'| = p^{1/2}$, which is equivalent to $|a| \leqslant 2p^{1/2}$. Therefore,

$$p-2p^{1/2}+1 \leqslant h \leqslant p+2p^{1/2}+1. \tag{*}$$

Now, it follows from some results of Deuring on endomorphism rings of elliptic curves that, for $p \geqslant 5$, each value of a with $|a| \leqslant 2p^{1/2}$ occurs for some E over F_p (see [2], pp. 276–279). Therefore each integer h satisfying (*) is a class number.

The proof of Theorem 1 is now immediate. Let m be an arbitrary integer $\geqslant 4$. Choose n such that $n^2 \leqslant m < (n+1)^2$ and let p be a prime ($\geqslant 5$) satisfying $n^2 < p < (n+1)^2$. Then

$$p-2p^{1/2}+1 < (n+1)^2-2(n+1)+1 = n^2 \leqslant m,$$

and

$$p+2p^{1/2}+1 > n^2+2n+1 = (n+1)^2 > m.$$

Therefore m satisfies (*), hence is a class number. The integers 2 and 3 satisfy (*) for $p = 5$ and consequently are also class numbers. The curve $Y^2 = X^3-X-1$ over F_3 is easily seen to give an example of $h = 1$. Therefore every integer m is a class number.

To prove (b), suppose there is no prime between n^2 and $(n+2)^2$. Let p be any prime less than n^2 and let q be any prime greater than $(n+2)^2$. The maximum class number for elliptic function fields over F_p is $[p+2p^{1/2}+1] < (n+1)^2$. The minimum class number for elliptic function fields over F_q is $[q-2q^{1/2}+1]+1 > (n+1)^2+1$. Therefore $(n+1)^2$ cannot be a class number, which is a contradiction.

We note that the assumption of part (b) could be replaced, for example, by the weaker assumption that all perfect squares are class numbers.

In order to prove Theorem 2, we need the following.

LEMMA. *Let $q(x)$ equal the number of positive integers $n \leqslant x$ such that there is no prime between n^2 and $(n+1)^2$. Then*

$$q(x) = O\left(\frac{x}{\log x}\right), \quad \textit{as} \quad x \to \infty.$$

Proof. A. Selberg has proved the following result ([3], p. 104): Let $f(x) > 0$ be increasing and $f(x)/x$ decreasing for $x > 0$ and suppose $f(x)/x \to 0$ and $\liminf\big(\log f(x)/\log x\big) > 19/77$ for $x \to \infty$. Then there exists a set $S \subset (0, \infty)$ such that

(i) $m(S_x) = O\left(\frac{x}{\log x}\right)$, where m is Lebesgue measure and $S_x = S \cap (0, x]$;

(ii) $\pi\big(x+f(x)\big)-\pi(x) = \frac{f(x)}{\log x} + O\left(\frac{f(x)}{\log^2 x}\right)$ as $x \to \infty$, $x \notin S$, where $\pi(x)$ is the number of primes less than or equal to x.

In particular, we may take $f(x) = x^{1/2}$. By (ii), $\pi(x+x^{1/2})-\pi(x) > 0$ for large $x \notin S$, and by suitably modifying S we may assume this inequality holds for all $x \notin S$.

Now, suppose there is no prime between n^2 and $(n+1)^2$. Then $\pi(x+x^{1/2})-\pi(x) = 0$ for $x \in [n^2, n^2+n]$, so $[n^2, n^2+n] \subset S$. Fix an $x > 0$ and let $n_1, \ldots, n_m$ be the set of such n satisfying $\frac{1}{2}x^{1/2} < n \leqslant x^{1/2}-\frac{1}{2}$. Each n_i, $1 \leqslant i \leqslant m$, contributes an interval of length n_i to S_x. Therefore

$$\tfrac{1}{2}x^{1/2}\big(q(x^{1/2}-\tfrac{1}{2})-q(\tfrac{1}{2}x^{1/2})\big) \leqslant \sum_{i=1}^{m} n_i \leqslant m(S_x) = O\left(\frac{x}{\log x}\right),$$

from which it follows that

$$q(y)-q(\tfrac{1}{2}y) \leqslant C\frac{y}{\log y} \quad \text{for} \quad y > 1,$$

for some constant C. Now fix y and let k be the integer such that $2^{-k-1}y \leqslant y^{1/2} < 2^{-k}y$. Then

$$\begin{aligned} q(y) &\leqslant q(y)-q(\tfrac{1}{2}y)+q(\tfrac{1}{2}y)-q(\tfrac{1}{4}y)+\ldots+q(2^{-k}y)-q(2^{-k-1}y)+q(y^{1/2}) \\ &\leqslant C\frac{y}{\log y}+C\frac{\frac{1}{2}y}{\log\frac{1}{2}y}+\ldots+C\frac{2^{-k}y}{\log 2^{-k}y}+y^{1/2} \\ &\leqslant C\frac{y}{\frac{1}{2}\log y}+\ldots+C\frac{2^{-k}y}{\frac{1}{2}\log y}+y^{1/2} \\ &\leqslant 4C\frac{y}{\log y}+y^{1/2} \leqslant 5C\frac{y}{\log y} \quad \text{for large } y. \end{aligned}$$

This completes the proof of the lemma.

It should be noted that Cramér [1] has proved that if the Riemann hypothesis is true, then $q(x) = O(x^{2/3}\log^3 x)$.

The proof of Theorem 2 is now straightforward. The proof of Theorem 1(a) shows that if m is not a class number and $n^2 \leqslant m < (n+1)^2$, then there is no prime between n^2 and $(n+1)^2$. There are $q(x^{1/2})$ such n with $n^2 \leqslant x$ and each n can contribute at most $2n+1$ different integers $m \leqslant x$ which are not class numbers. Therefore,

$$H(x) \leqslant q(x^{1/2})(2x^{1/2}+1) = O\left(\frac{x}{\log x}\right),$$

which completes the proof.

References

[1] H. Cramér, *Some theorems concerning prime numbers*, Arkiv för Mat., Astr., Fys. 15 (5) (1921), pp. 1–33.

[2] Y. Ihara, *Hecke polynomials as congruence ζ functions in elliptic modular case*, Ann. of Math. 85 (1967), pp. 267–295.

[3] A. Selberg, *On the normal density of primes in small intervals, and the difference between consecutive primes*, Arch. Math. Naturvid. 47 (6) (1943), pp. 87–105.

[4] A. Weil, *Basic Number Theory*, New York 1967.

PRINCETON UNIVERSITY

Received on 15. 8. 1973 (449)

ACTA ARITHMETICA
XXVIII (1975)

Bounds on the number of integer valued monotone functions of k integer arguments*

by

AZAD BOLOUR (Berkeley, Calif.)

1. Introduction. Consider the set

$$(0, n-1)^k = \{(x_1, x_2, \ldots, x_k),\ x_i \text{ integer, and } 0 \leqslant x_i \leqslant n-1\} \tag{1}$$

together with the partial order $\leqslant$ given by:

$$\boldsymbol{x} \leqslant \boldsymbol{y} \Leftrightarrow x_i \leqslant y_i\ \forall i, \quad 1 \leqslant i \leqslant k.$$

We say an integer valued function f is monotone on $(0, n-1)^k$ if:

$$\boldsymbol{x} \leqslant \boldsymbol{y} \Rightarrow f(\boldsymbol{x}) \leqslant f(\boldsymbol{y}).$$

The problem we shall be concerned with is to count the number (denoted by $L_k(N, n)$) of monotone functions $f\colon (0, n-1)^k \to (0, 1, 2, \ldots, N)$, to which we refer as N-restricted n^k-partitions (of any integer).

In one dimension ($k = 1$) the problem is trivial, $L_1(N, n) = \binom{N+n}{n}$. The problem for planes and higher dimensional solids was first studied by McMahon [2]. He generalized the concept of partitioning an integer into a linear array, and defined plane partitions and partitions "in solido," as two or more dimensional arrays of integers non-decreasing in each direction and summing up to a given integer m. He also considered partitions with restricted part magnitudes. McMahon was successful in obtaining generating functions for a wide variety of plane partitions (not necessarily rectangular). R. Stanley [3] gives a survey of many of the known results about plane partitions and some of the proofs involved. These proofs appeal to the theory of symmetric functions and the representation theory of symmetric groups. They are quite involved and apparently not trivially generalizable to higher dimensional lattices (except for some particularly simple 3-dimensional figures). Carlitz [1]

* Research conducted in partial fulfillment of the degree of Master of Science at the Department of Electrical Engineering, Massachusetts Institute of Technology.