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 which integers occur as class numbers of algebraic number fields. In this note we consider the corresponding question for function fields over finite fields and relate it to a classical problem in the distribution of prime numbers; namely, is there at least one prime between \( n^2 \) and \( (n+1)^2 \) for all positive integers \( n \)?

**Theorem 1.** (a) Suppose that for every positive integer \( n \) there is a prime between \( n^2 \) and \( (n+1)^2 \). Then, for each positive integer \( m \), there exists a prime \( \nu \) and an elliptic function field \( E \) over \( \mathbb{F}_p \) (the finite field with \( p \) elements) such that the class number of \( E \), i.e., the number of divisor classes of degree 0, equals \( m \).

(b) Conversely, suppose that each positive integer occurs as the class number of some elliptic function field over some \( \mathbb{F}_p \) (\( p \) prime). Then for each 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 equal to \( x \) which do not occur as class numbers of elliptic function fields over \( \mathbb{F}_p \). Then

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

In particular, the set of integers which are class numbers has asymptotic density 1.

Before proceeding with the proofs, we first need some preliminary remarks. Let \( E \) be an elliptic function field over \( \mathbb{F}_p \) and let \( h \) be its class number. Then the zeta-function of \( E \) has the form

\[
Z(u) = \frac{P(u)}{(1-u)(1-pu)},
\]
where \( P(u) = pu^2 + au + 1 \) for some integer \( a \), and \( P(1) = p + a + 1 = k \)
(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
\( |a| \leq 2p^{1/2} \). Therefore,
\[
(*) \quad p - 2p^{1/2} + 1 \leq k \leq p + 2p^{1/2} + 1.
\]
Now, it follows from some results of Deuring on endomorphism rings of elliptic curves that, for
\( p \geq 5 \), each value of \( a \) with \( |a| \leq 2p^{1/2} \) occurs for some \( E \) over \( F_p \).
(see [2], pp. 276–279). Therefore each integer \( k \) satisfying \((*)\) is a class number.

The proof of Theorem 1 is now immediate. Let \( m \) be an arbitrary integer \( \geq 4 \). Choose \( n \) such that \( n^2 \leq m < (n + 1)^2 \) and let \( p \) be a prime \((\geq 5)\) satisfying \( n^2 < p < (n + 1)^2 \). Then
\[
p - 2p^{1/2} + 1 < (n + 1)^2 - 2(n + 1) + 1 = n^2 \leq m,
\]
and
\[
p + 2p^{1/2} + 1 > n^2 + 2n + 1 = (n + 1)^2 > m.
\]
Therefore \(*\) 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 \( F_p \) 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 \( F_p \) 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 \( q(x) \) denote the number of positive integers \( n \leq x \) such that there is no prime between \( n^2 \) and \( (n + 1)^2 \). Then
\[
q(x) = O\left(\frac{x}{\log x}\right) \quad \text{as} \quad x \to \infty.
\]

**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 \( \lim \inf \log(f(x))/\log x > 79/77 \) for \( x \to \infty \). Then there exists a set \( S \subset (0, \infty) \) such that

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

(ii) \( \pi(x + f(x)) - \pi(x) = f(x)/\log x + O\left(\frac{f(x)}{\log^2 x}\right) \) as \( x \to \infty \), \( x \in S \), 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 \( x \in S \), and by suitably modifying \( S \) we may assume this inequality holds for all \( x \in S \).

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 \([n^2, n^2 + n] \in S \). Fix an \( a > 0 \) and let \( n_1, \ldots, n_m \) be the set of \( n \) satisfying \( \frac{1}{2}a^{1/2} < n < \frac{1}{2}a^{1/2} \). Each \( n_i, 1 \leq i \leq m \), contributes an interval of length \( n_i \) to \( S_x \). Therefore
\[
\frac{1}{2}a^{1/2}(q(x^{1/2} - \frac{1}{2}) - q(x^{1/2} + \frac{1}{2})) \leq \frac{m}{\log x} \Bigg( \frac{x}{\log x} \Bigg),
\]
from which it follows that
\[
q(y) - q(\frac{1}{2}y) \leq C \frac{y}{\log y} \quad \text{for} \quad y > 1,
\]
for some constant \( C \). Now fix \( y \) and let \( k \) be the integer such that \( 2^{-k-1}y \leq y^{1/2} < 2^{-k}y \). Then
\[
q(y) \leq q(y) - q(\frac{1}{2}y) + q(\frac{1}{2}y) - q(\frac{1}{4}y) + \cdots + q(2^{-k}y) - q(2^{-k-1}y) + q(y^{1/2})
\]
\[
\leq C \frac{y}{\log y} + C \frac{y}{\log 2y} + \cdots + C \frac{y}{\log 2^{-k}y} + y^{1/2}
\]
\[
\leq C \frac{y}{\log y} + \cdots + C \frac{y}{\log 2^{-k}y} + y^{1/2}
\]
\[
\leq 4C \frac{y}{\log y} + y^{1/2} \leq 5C \frac{y}{\log y} \quad \text{for large} \ y.
\]

This completes the proof of the lemma.

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

The proof of Theorem 2 is now straightforward. The proof of Theorem 1(a) shows that if \( m \) is not a class number and \( n^2 \leq m < (n + 1)^2 \), then there is no prime between \( n^2 \) and \( (n + 1)^2 \). There are \( q(x^{1/2}) \) such \( n \) with \( n^2 \leq x \) and each \( n \) can contribute at most \( 2n + 1 \) different integers \( m < x \) which are not class numbers. Therefore,
\[
H(x) \leq q(x^{1/2})(2x^{1/2} + 1) = O\left(\frac{x}{\log x}\right),
\]
which completes the proof.
Bounds on the number of integer valued monotone functions of \( k \) integer arguments

by

AZAD BOLOUR (Berkeley, Calif.)

1. Introduction. Consider the set

\[ (0, n-1)^k = \{(x_1, x_2, \ldots, x_k) : x_i \text{ integer, and } 0 \leq x_i \leq n-1 \} \]

together with the partial order \( \preceq \) given by:

\[ x \preceq y \iff x_i \leq y_i \quad \forall i, \quad 1 \leq i \leq k. \]

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

\[ x \preceq y \implies f(x) \preceq f(y). \]

The problem we shall be concerned with is to count the number (denoted by \( L_k(N, n) \)) of monotone functions \( f : (0, n-1)^k \to (0, 1, 2, \ldots, N) \), 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 solidi," as two or more dimensional arrays of integers non-decreasing in each direction and summing up to a given integer \( n \). He also considered partitions with restricted part magnitudes. McMahon was successful in obtaining generating functions for a wide variety of plane partitions (not necessarily rectanglar). 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.