Mathematisches Forschungsinstitut Oberwolfach

Report No. 54/2004

Finite Fields: Theory and Applications

Organised by
Joachim von zur Gathen (Paderborn)
Igor E. Shparlinski (Sydney)
Henning Stichtenoth (Essen)

December 5th – December 11th, 2004

Abstract. Finite fields are the focal point of many interesting geometric, algorithmic and combinatorial problems. The workshop was devoted to progress on these questions, with an eye also on the important applications of finite field techniques in cryptography, error correcting codes, and random number generation.

Mathematics Subject Classification (2000): 11Txx, 14Gxx, 68W30.

Introduction by the Organisers

The workshop *Finite Fields: Theory and Applications* was organized by Joachim von zur Gathen (Bonn), Igor Shparlinski (Sydney), and Henning Stichtenoth (Essen), and ran from 5 to 11 December 2004. Its forty participants, with a wide geographical distribution, enjoyed the hospitality of the Mathematical Research Institute, and its beautiful surroundings. Two previous meetings on the topic had been held in 1997 and 2001. The schedule consisted of three plenary talks each morning, and specialized sessions later in the day, with vast time for discussions and collaborative work. The traditional Wednesday afternoon hike was blessed with wonderful sunny weather and the compulsory Black Forest cake reward at the end.

Very broadly, we can distinguish seven subject areas:

- structure of finite fields,
- field towers,
- points on varieties,
- error-correcting codes,

- computation,
- combinatorics,
- cryptography.

Of course, many of the results presented bridge between two or more of these areas. The abstracts that follow speak for themselves. Avoiding an exhaustive discussion, we now mention one particular talk from each of the seven areas.

The *structure theory* includes questions about polynomials. The well-known Hansen-Mullen conjecture (whose second author was in the audience) was stated in 1992 and asserts that for any finite field $\mathbb{F}_q$, integers n and m with $0 < m < n$ and $a \in \mathbb{F}_q$, there exists a monic primitive polynomial in $\mathbb{F}_q[x]$ of degree n having a as the coefficient of x^m; there are a few well-known exceptional cases where this fails to hold. Cohen presented a proof of this conjecture at degrees $n \geq 9$, assuring the audience that smaller values of n are also under consideration.

Towers of function fields are of great interest because they may yield good algebraic-geometric codes. Beelen introduced a recursive construction of such towers, using a certain type of Fuchsian differential equations. They can be obtained from modular curves, and in some cases can be shown to be asymptotically optimal (in terms of the parameters of the resulting codes).

A conjecture concerning *points on varieties* was stated by Heath-Brown. Namely, he considers a nonsingular nonlinear hypersurface X in $\mathbb{P}^n$ defined over $\mathbb{Q}$, considers the number $N(B)$ of points on X with rational integral coefficients absolutely bounded by B, and conjectures that this number is $O(B^{n-1+\epsilon})$ for any positive ϵ. Browning presented his proof of this conjecture in all cases, with the possible exceptions $d = 3, 4$ and $n = 7, 8$.

In the theory of *error-correcting codes*, finite fields were fundamental from its beginning in the 1940s. Their importance was heightened by the construction of codes from algebraic curves over finite fields. Voloch discussed a different connection: the quadratic residue codes. It is unknown whether subfamilies of them can yield asymptotically good codes. Voloch showed that there exist subfamilies that do not yield good codes. This is based on an expression of the minimal distance by exponential sums, due to Helleseth, and estimates on the smallest prime that splits completely in a number field.

For *computation*, a difficult class of objects are bivariate polynomials presented in a particularly generous format, namely as a sum of terms where the exponents are written in binary (or decimal). Thus we look at polynomials of humongous degrees. Kaltofen presented two results which illuminate the wide range of behavior for questions about such polynomials. Over the rational numbers, he can compute the linear and quadratic factors in polynomial time. Over a large finite field, testing irreducibility is NP-hard (under randomized reductions).

As a question from *combinatorics*, we give the following illustrative example. A sum-free set A in an additive group G is such that $x+y \neq z$ for all $x, y, z \in A$. For instance the additive group $G = \mathbb{Z}_p$ for a prime p and $A = \{n, n+1, \ldots, 2n-1\}$ for $n = \lfloor (p+1)/3 \rfloor$ is a sum-free set. We can also multiply each element of A by a fixed nonzero element of $\mathbb{Z}_p$. When $p \equiv 2 \bmod 3$, no other sum-free subsets of $\mathbb{Z}_p$

exist. Lev shows that assumption $\#A \geq 0.33p$ implies that A is contained in the corresponding interval or a dilation of it.

In *cryptography*, a central question is the conjectured difficulty of computing the discrete logarithm in certain groups. The method of index calculus provides a subexponential algorithm in the unit groups of finite fields. Elliptic curves owe their popularity in cryptography to the absence, so far, of any discrete logarithm computation of comparable efficiency. Semaev presented an approach, rather speculative at this point, aimed at finding such a method; it works with the new notion of summation polynomials which vanish at the x-coordinates of points that sum to 0 on the curve.