February 12, 1998

José Felipe Voloch, University of Texas, Austin and MSRI

``Cellular telephones and elliptic curves over rings''

In some applications, such as in the case of cellular telephones, multiple users need to share a common communication channel. One way to achieve this is by the technique known as code-division multiple access (CDMA), in which each user is assigned a code from a set of sequences of low-correlation (which, loosely speaking, means distinct codewords are almost orthogonal). A basic problem is to find large enough sets of sequences of low-correlation of moderate lenght. This problem is also related to the more classical problem in communication theory of constructing good error-correcting codes. We will discuss these problems and present some new constructions based on elliptic curves over finite rings.