Future directions for the areas of mathematics represented in the Lenstra Treurfeest

In the spring of 2003, Hendrik Lenstra retired from his position at the University of California, Berkeley, and moved to the Netherlands, where he took a position at the University of Leiden. In Lenstra's honor, a farewell conference (the *Lenstra Treurfeest*) was held March 21–23 at the Mathematical Sciences Research Institute and on the U.C. Berkeley campus. The themes of the conference were chosen to represent Lenstra's mathematical interests, including algebra, algebraic geometry, algebraic number theory, arithmetic geometry, and computational number theory.

On the first day of the meeting, the conference organizers invited all of the participants to gather over lunch to discuss "the state of the art, current directions, and emerging opportunities" in the fields of interest to Lenstra. This document gives a short summary of the topics and issues that arose during the lunchtime roundtable. There were approximately twenty participants, including William Cherry, Robert Coleman, Bas Edixhoven, John Flynn, Everett Howe, Lily Khadjavi, Peter Montgomery, Frans Oort, Bjorn Poonen, Ed Schaefer, Alice Silverberg, and Hui June Zhu.

Not surprisingly, one of the major topics of the discussion was the computational problems that number theorists will be confronting in the coming years. Three themes emerged:

1. Computing invariants of elliptic curves over number fields,
2. Counting points on higher-genus curves over finite fields, and
3. Finding rational points on surfaces.

The major elliptic curve problem that was mentioned was the computation of the Shafarevich-Tate group of an elliptic curve over the rational numbers. It is likely that algorithms to calculate this group will be tied to better theoretical understanding of the Birch and Swinnerton-Dyer conjecture.

In the past few years there have been many advances in the theory and practice of computing the number of points on a curve over a finite field. A great many researchers have worked on this problem, following the initial advances of Satoh, Kedlaya, Mestre, and Lauder/Wan. All of this recent research has focussed on curves over finite fields of small characteristic, and the advances in theory have led to major improvements in practical algorithms. For example, it is now possible to randomly pick genus-2 curves over large finite fields of small characteristic and compute the group orders of their Jacobians until a curve is found that is suitable for use in hyperelliptic curve cryptography. The consensus at the roundtable discussion was that there will be continued advances in this field in the coming years, and that perhaps there will be theoretical advances in counting points on curves over finite fields of large characteristic.

There are a number of long-standing Diophantine problems that can be interpreted as questions about the existence of integral or rational points on surfaces. For example, two such problems are the question of whether or not there exists a rectilinear box with the property that the distance between every pair of its corners is an integer, and the question of whether there exists a 3×3 magic square, all of whose entries are squares. Participants in the discussion thought that this is an area in which progress is overdue, but that there are significant difficulties to be overcome: for instance, there is no analog for surfaces of the Mordell-Lang conjecture. One participant pointed out that even *rational* surfaces pose computational problems.

The second topic discussed over lunch was the possibility of incremental improvements in current number-theoretic algorithms. For instance, there was discussion on whether it would be possible to choose elliptic curves for the elliptic curve factorization method that would be more likely to have smooth group orders than the curves that are used now. At present, the best method known for obtaining smooth group orders is to use elliptic curves that have large torsion subgroups over the rational numbers. Also, it was suggested that in the number field sieve method of factorization, it would perhaps be better to use two cubic polynomials with a common root modulo the number to be factored, instead of using a linear polynomial and a quintic polynomial, as is currently done. Theory suggests that there exist pairs of cubics that would lead to an improved running time, but there are no good methods for finding these cubics.

With regard to both of these topics, it was observed that Lenstra's work has shown that it is advances in theory, more than anything else, that lead to dramatic improvements in computation.

Social topics were also discussed. One question was how to get students involved in number theory, arithmetic geometry, and computation. Number theory has some innate advantages in generating student interest — for example, elementary number theory is (at least anecdotally) often one of the topics that first draws students to mathematics — but more can be done to attract students to computational problems. The applications of computational number theory and arithmetic geometry to cryptography have created an increased need for mathematicians well-versed in these topics among corporations and government organizations; this increased demand might draw more graduate students to computational topics, and it certainly has increased the interaction between industry and academia. Academic number theorists and arithmetic geometers are becoming more aware of the possibility of practical applications for their work, and they can be inspired by this awareness to learn about the computational aspects of their fields.

Participants were asked to speculate about which well-known conjectures might be proven in the next decade. Only two people were bold enough to make predictions about this, but they suggested that perhaps significant progress would be made on the André-Oort conjecture and the *abc*-conjecture.

Finally, several people pointed out that the answer to the question "What are the current directions of the fields of interest to Lenstra?" is clearly "Eastward, towards Leiden."