**Lehigh Math Contest, Spring 2005**

Two Journeys video: *Math I started from Hendrik Lenstra's work*

B. Dodson

**New Formulas (algorithms)** for computing solutions to hard problems

**Lenstra's best:** LLL for lattice reduction

ECM for finding medium sized prime factors

NFS for breaking RSA keys

LLL: 1st L: Lovasz, 3rd L: Arjen

ECM: small primes? (1) $p < 10000$; (2) ...

medium: (1) $10^{30}$ ; (2) $10^{40}$ ...;

(3) largest prime found by ECM

NFS: Sieving method, broke 512-bits (155-digits)

**Lenstra chronology**

met Hendrik at math conference,
Arcata, CA; Aug 1985

(1) consultation for Theorem in Journal of Algebra article, appeared 1987

(2) copy and explanation of his paper (*Sums of Roots of 1*); method used in my student's Ph.D. Thesis, Lehigh 1994

**subsequent meetings, consultation**

Lecture at Penn, Topic: Runtime of ECM

(Fall 1985?)

Lecture at Lehigh, Topic: NFS (Spring 1990?)

under-grad Algebra assignment:

Attend Lenstra lecture

intended effect: student interest in algebra(?)

side effect: professor interest in computing(!)

**Next Steps:**

(1) email of small ECM results to Arjen (1991/2)

(2) factorization of RSA-120 (old sieving method), paper Aug 1994, AKL Lehigh lecture, spring 1994

(3) first use of NFS (new sieving method), 116-digits Crypto conference lecture, paper (AKL/Dodson), 1995 "*Explosive Experiment*"

(4) 512-bit RSA-key broken by NFS, 1999, paper NY Times article(s), "*International Team breaks Internet Code*", 5-year joint project, AKL, others

(5) Dodson ECM records, 57-digit prime factor 2003; 59-digit prime factor, Feb 20, 2005