Introduction to Modern Cryptography

9th lecture:

Algorithmic Number Theory

Pierre de Fermat

1601 or 1607/8 - 1665

- of Basque origin
- last theorem: $a^n + b^n = c^n$, $n>2$ (proven in 1994 by Andrew Wiles, earning him a silver plaque instead of the fields medal)

- claimed to have proven all his statements, but often communicated them without proofs

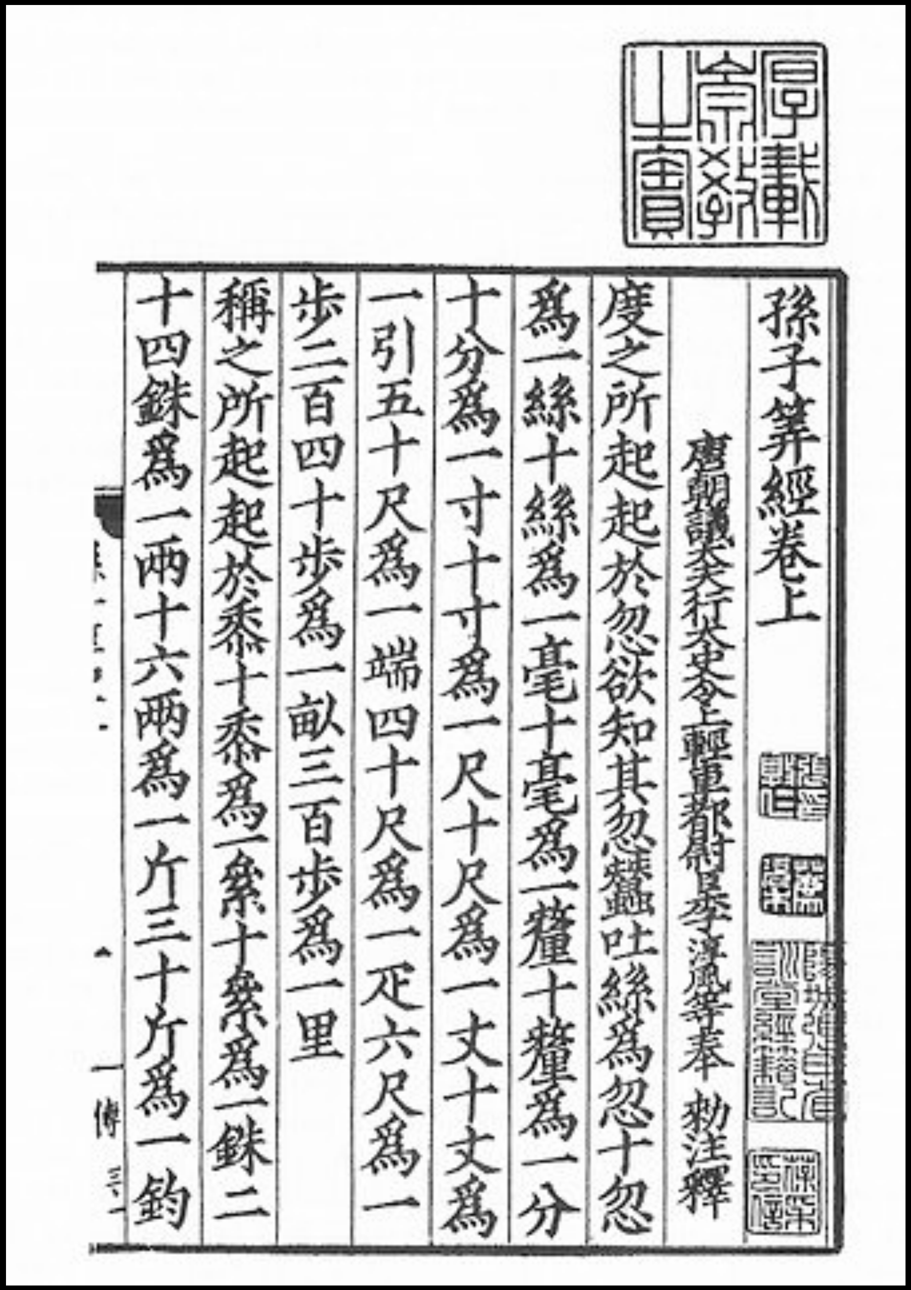
Leonhard Euler

1707 - 1783

- (most?) important mathematician of 18th century
- worked in St. Petersburg and Berlin
- very productive (e.g. in 1775, one math paper per week on average!)
- math notation: $f(x)$, e , $\sum$, i
- analysis: exp , log , trigonometry
- number theory: $\Phi(N)$
- graph theory: $V - E + F = 2$
- applied math, physics, astronomy

Sun Zi

after 300 AD



孫子算經卷上

唐朝議大夫行太史令上輕車都尉臣李淳風等奉 勑注釋

度之所起起於忽欲知其忽蠶吐絲爲忽十忽爲一絲十絲爲一毫十毫爲一氂十氂爲一分十分爲一寸十寸爲一尺十尺爲一丈十丈爲一引五十尺爲一端四十尺爲一疋六尺爲一步二百四十步爲一畝三百步爲一里

稱之所起起於黍十黍爲一絫十絫爲一銖二十四銖爲一兩十六兩爲一斤三十斤爲一鈞

- identity of author unclear

- The Mathematical Classic:
  1. Counting Rods
  2. Fractions
  3. Chinese Remainder Theorem

Gary Lee Miller

* ~1950

- PhD UC Berkeley
- prof at Carnegie Mellon University, Pittsburgh
- deterministic primality test based on Riemann hypoth

Michael O. Rabin

*1931

- PhD Princeton
- Turing Award for “non-deterministic machines”
- 1975: randomized primality test

John M. Pollard

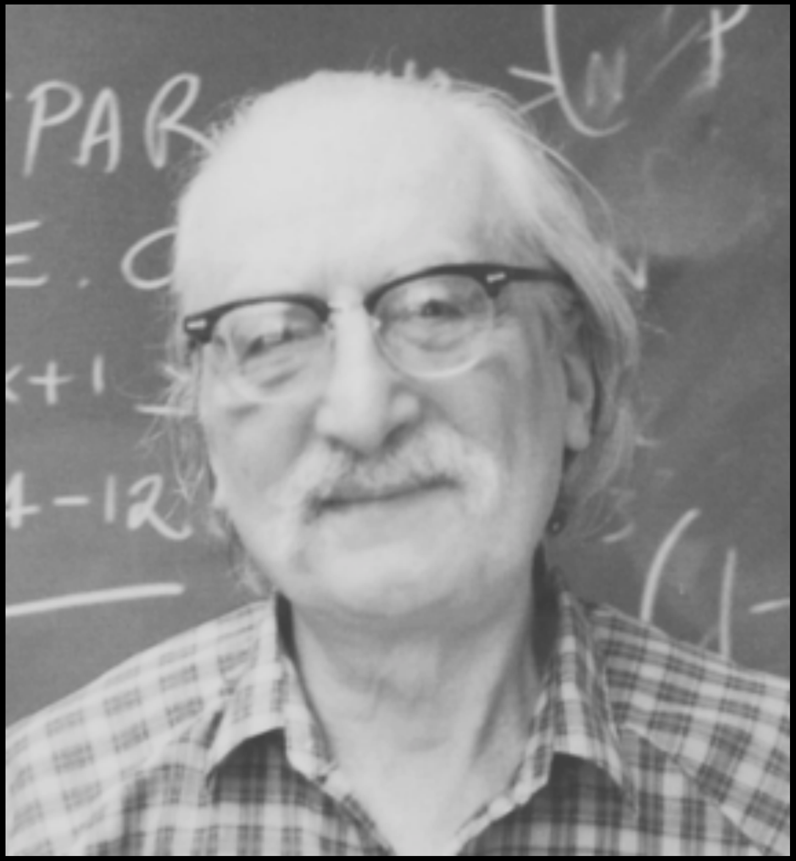
? -

- mathematician
- invented algorithms for factoring and discrete logs
- rho, p-1, kangaroo, number field sieve

- wiki , webpage

Daniel Shanks

1917 - 1996



- PhD University of Maryland
- numerical analysis and number theory
- baby-step giant-step algorithm

- 1962: computed the number π to 100,000 decimals on a computer
- wiki