Summer School
Number Theory for Cryptography

Warwick University, june 2013

Integer factorization

F. Morain

morain@lix.polytechnique.fr

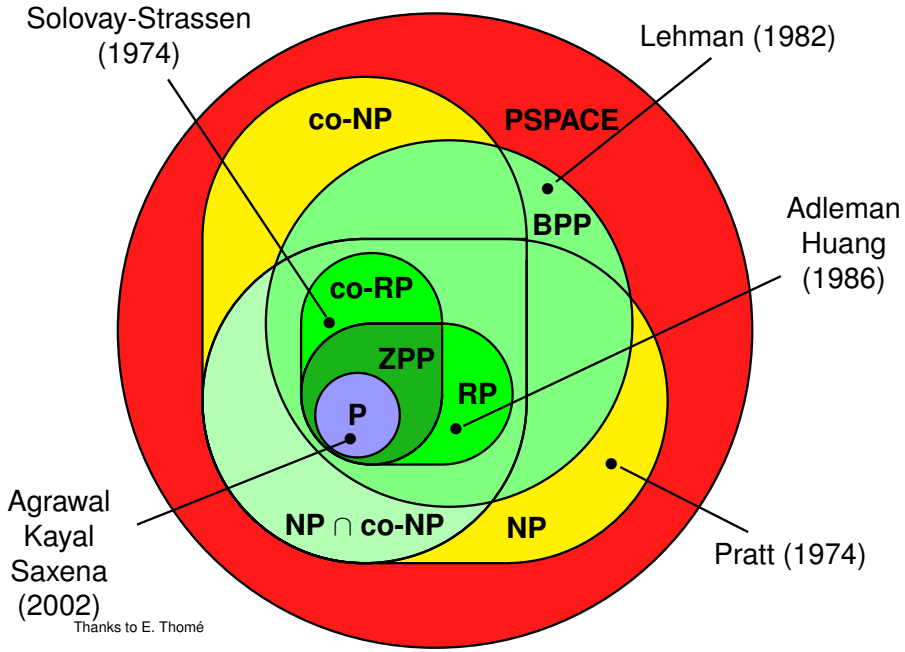
Rules of the game

$$N = \prod_{i=1}^{k} p_i^{\alpha_i}.$$

- What do we do in practice? Which size is doable?
  Factorization : number field sieve
  $O(\exp(c(\log N)^{1/3}(\log\log N)^{2/3}))$; 768 bits (a lot of people, 2010).
  Primality: hopefully without too much factoring, past some easy trial division; 30,000 decimal digits.
- Complexity question: to which class does **isPrime?** belong?

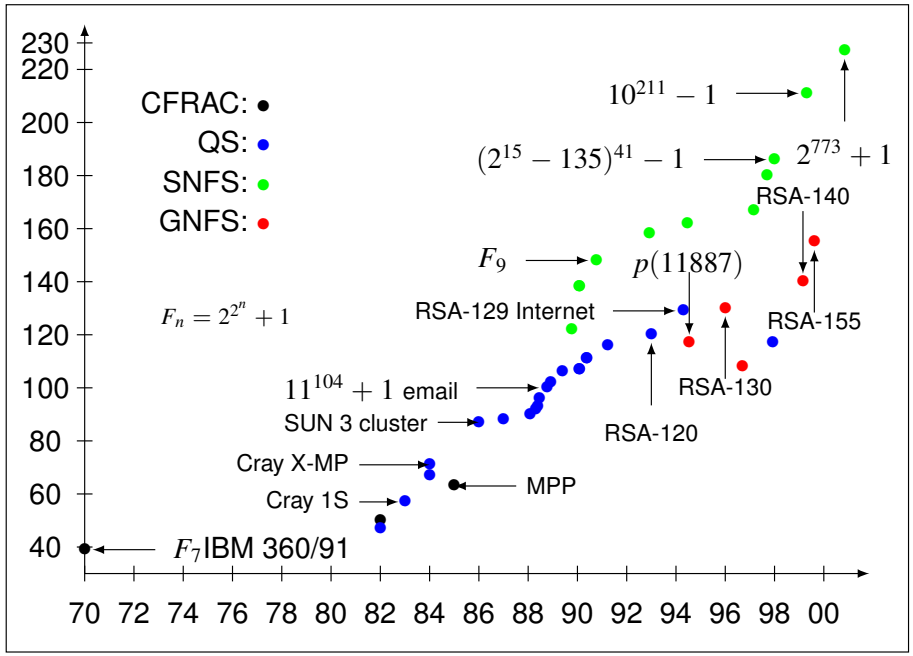
Best : **P** (e.g., integer multiplication).
At least : **RP**.
And: what about proofs?

Complexity classes



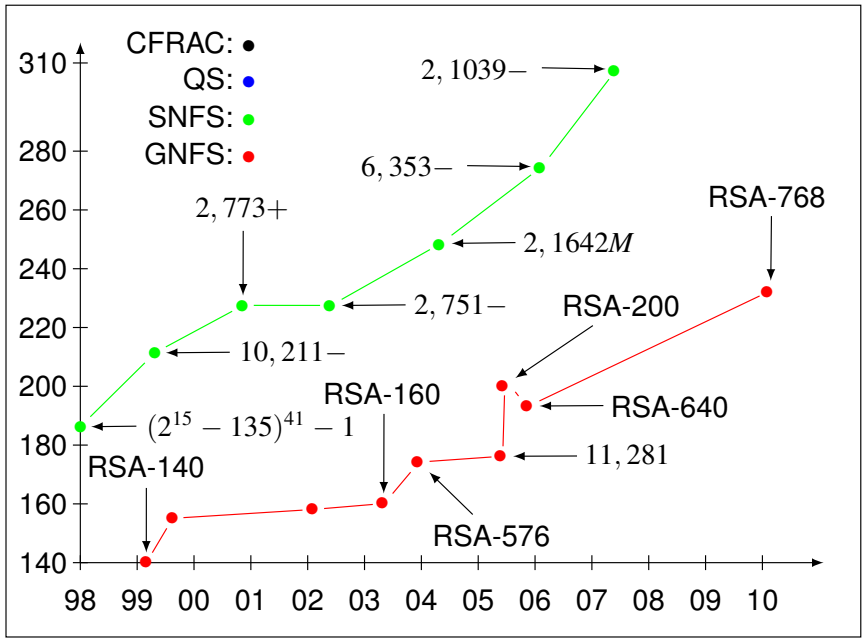
Thanks to E. Thomé

How difficult is factoring?



And alsoi: 03/1991: 2,463+ (c101) on a Cray Y-MP4/464; 04/1992: RSA-110 on a MasPar (16K nodes).

The reign of clusters



Plan

- Today: primality.
- Tomorrow: elementary factoring algorithms.
- Last but not least: powerful factoring.

You must practice with numbers!