

# Számítógépes számelmélet

Járai Antal

Ezek a programok csak szemléltetésre szolgálnak

- ▶ 1. A prímek eloszlása, szitálás
- ▶ 2. Egyszerű faktorizálási módszerek
- ▶ 3. Egyszerű prímtesztelési módszerek
- ▶ 4. Lucas-sorozatok
- ▶ 5. Alkalmazások
- ▶ 6. Számok és polinomok
- ▶ 7. Gyors Fourier-transzformáció
- ▶ 8. Elliptikus függvények
- ▶ 9. Számolás elliptikus görbéken
- ▼ 10. Faktorizálás elliptikus görbékkel
  - [ > restart;
  - ▼ 10.1. Kötegelt végrehajtás.
    - [ >
  - ▼ 10.2. Szorzás egészekkel.
    - [ >
  - ▼ 10.3. Projektív reprezentáció.



#### ▼ 10.4. Második lépcső.



- ▶ 11. Prímteszt elliptikus görbékkel
- ▶ 12. Polinomfaktorizálás
- ▶ 13. Az AKS-teszt
- ▶ 14. A szita módszerek alapjai