

# 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
- ▶ 11. Prímteszt elliptikus görbékkel
- ▶ 12. Polinomfaktorizálás
- ▼ 13. Az AKS-teszt
  - ▶ `> restart;`
  - ▶ 13.1. Az AKS-teszt alapötlete.
  - ▶ 13.2. Az AKS-tétel.

▼ **13.3. Megjegyzések.**



▶ **13.4. Bernstein tétele.**

▼ **13.5. Megjegyzések.**



▶ **14. A szita módszerek alapjai**