

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
 - [> restart;
 - ▶ 11.1. Tétel.
 - ▶ 11.2. Tétel.
 - ▼ 11.3. A prímtesztek vázlata.
 - [>

▼ **11.4. A Goldwasser-Kilian teszt.**



▼ **11.5. Atkin tesztje.**



- ▶ **12. Polinomfaktorizálás**
- ▶ **13. Az AKS-teszt**
- ▶ **14. A szita módszerek alapjai**