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

```
> restart; with(numtheory);
```

[*GIgcd*, *bigomega*, *cfrac*, *cfracpol*, *cyclotomic*, *divisors*, *factorEQ*, *factorset*, *fermat*, *imagunit*, *index*, *integral_basis*, *invcfrac*, *invphi*, *issqrfree*, *jacobi*, *kronecker*, λ, *legendre*, *mcombine*, *mersenne*, *migcdex*, *minkowski*, *mipolys*, *mlog*, *mobius*, *mroot*, *msqrt*, *nearestp*, *nthconver*, *nthdenom*, *nthnumer*, *nthpow*, *order*, *pdexpand*, ϕ, π, *pprimroot*, *primroot*, *quadres*, *rootsunity*, *safeprime*, σ, *sq2factor*, *sum2sqr*, τ, *thue*] (5.1)

▶ 5.1. Fermat–számok.

▶ 5.2. Feladat.

▼ 5.3. Feladat.

```
> interface(verboseproc=2);
```

1 (5.3.1)

```
> print(fermat);
```

proc(*n*::(Or(*nonnegint*, Not(*constant*))), *_info*) ... **end proc** (5.3.2)

▼ 5.4. Mersenne–számok.

```
> mersennes:=[2,3,5,7,13,17,19,31,61,89,107,127,521,607,1279,
  2203,2281,3217,4253,4423,9689,9941,11213,19937,21701,23209,
  44497,86243,110503,132049,216091,756839,859833,1257787,
  1398269,2976221,3021377,6972593,13466917,20996011,24036583,
  25964951,30402457,32582657,37156667,42643801,43112609];
```

$$mersennes := [2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859833, 1257787, 1398269, 2976221, 3021377, 6972593, 13466917, 20996011, 24036583, 25964951, 30402457, 32582657, 37156667, 42643801, 43112609] \quad (5.4.1)$$

▶ 5.5. Feladat.

▼ 5.6. Feladat.

```
> interface(verboseproc=2);
```

$$2 \quad (5.6.1)$$

```
> print(mersenne);
```

$$\mathbf{proc}(n::(\{posint, [posint]\})) \ldots \mathbf{end\ proc} \quad (5.6.2)$$

▶ 5.7. h*2^m+-1 alakú prímek keresése.

▶ 5.8. Feladat.

▶ 5.9. Feladat.

▶ 5.10. Ikerprímek.

▶ 5.11. Feladat.

▶ 5.12. Feladat.

▶ 5.13. Sophie Germain prímek.

▶ 5.14. Ikerprím, amely Sophie Germain prím is.

▶ 5.15. n^2+1 es n^4+1 alakú prímek.

▶ 5.16. Egyéb speciális alakú prímek.

5.17. Kátai egy problémája.

5.18. Példa.

```
> #
  # This is a simple factorization
  # procedure using trial division.
  # The result is a sequence of pairs
  # [p,e] where the p's are the prime
  # factors and the e's are the exponents.
  # The factors are anyway in increasing order.
  # Only primes <= P are tried, hence the
  # last "factor" may composite, if
  # it is greater then P^2;
  #

  trialdiv:=proc(n::posint,P::posint) local L,p,i,d,nn;
  L:=[]; nn:=n;
  if type(nn,even) and 2<=P then
    for i from 0 while type(nn,even) do nn:=nn/2; od;
    L:=[[2,i]];
  fi;
  if nn mod 3=0 and 3<=P then
    for i from 0 while nn mod 3=0 do nn:=nn/3; od;
    L:=[op(L),[3,i]];
  fi;
  d:=2; p:=5;
  while p<=P and nn>=p^2 do
    if nn mod p=0 then
      for i from 0 while nn mod p=0 do nn:=nn/p; od;
      L:=[op(L),[p,i]];
    fi;
    p:=p+d; d:=6-d;
  od;
  if nn>1 then L:=[op(L),[nn,1]] fi;
  L;
  end;
```

$$trialdiv := \mathbf{proc}(n::posint,\ P::posint) \tag{5.18.1}$$

$$\mathbf{local}\ L,\ p,\ i,\ d,\ nn;$$

$$L := [\,];$$

$$nn := n;$$

$$\mathbf{if}\ type(nn,\ even)\ \mathbf{and}\ 2 <= P\ \mathbf{then}$$

$$\mathbf{for}\ i\ \mathbf{from}\ 0\ \mathbf{while}\ type(nn,\ even)\ \mathbf{do}$$

$$nn := 1 / 2 * nn$$

```
        end do;
        L := [[2, i]]
    end if;
    if mod(nn, 3) = 0 and 3 <= P then
        for i from 0 while mod(nn, 3) = 0 do
            nn := 1 / 3 * nn
        end do;
        L := [op(L), [3, i]]
    end if;
    d := 2;
    p := 5;
    while p <= P and p^2 <= nn do
        if mod(nn, p) = 0 then
            for i from 0 while mod(nn, p) = 0 do
                nn := nn / p
            end do;
            L := [op(L), [p, i]]
        end if;
        p := p + d;
        d := 6 - d
    end do;
    if 1 < nn then
        L := [op(L), [nn, 1]]
    end if;
    L
end proc
```

```
> trialdiv(2^107-2^54+1,1000);
```

$$[[5, 1], [857, 1], [37866809061660057264219253397, 1]] \tag{5.18.2}$$

```
> n0:=%[3][1];
```

$$n0 := 37866809061660057264219253397 \tag{5.18.3}$$

```
> modp(3&^(n0-1),n0);
```

$$1 \tag{5.18.4}$$

```
> trialdiv(n0-1,1000);
```

(5.18.5)

$$[[2, 2], [19, 1], [107, 1], [353, 1], [1319127075410822604930 1, 1]] \quad (5.18.5)$$

```
> n1:=%[5][1];
```

$$n1 := 1319127075410822604930 1 \quad (5.18.6)$$

```
> modp(3&^(n1-1),n1);
```

$$1234633084201536400878 9 \quad (5.18.7)$$

```
> trialdiv(n1,100000);
```

$$[[91813, 1], [143675413657196977, 1]] \quad (5.18.8)$$

```
> n2:=%[2][1];
```

$$n2 := 143675413657196977 \quad (5.18.9)$$

```
> modp(3&^(n2-1),n2);
```

$$1 \quad (5.18.10)$$

```
> trialdiv(n2-1,1000);
```

$$[[2, 4], [3, 2], [547, 1], [1824032775457, 1]] \quad (5.18.11)$$

```
> n3:=%[4][1];
```

$$n3 := 1824032775457 \quad (5.18.12)$$

```
> modp(3&^(n3-1),n3);
```

$$1527852257227 \quad (5.18.13)$$

```
> trialdiv(n3,10000);
```

$$[[1103, 1], [1653701519, 1]] \quad (5.18.14)$$

```
> n4:=%[2][1];
```

$$n4 := 1653701519 \quad (5.18.15)$$

```
> modp(3&^(n4-1),n4);
```

$$1 \quad (5.18.16)$$

```
> trialdiv(n4-1,1000);
```

$$[[2, 1], [7, 1], [19, 1], [23, 1], [137, 1], [1973, 1]] \quad (5.18.17)$$

```
> trialdiv(2^107+2^54+1,1000);
```

$$[[162259276829213381405976519770113, 1]] \quad (5.18.18)$$

```
> n5:=%[1][1];
```

$$n5 := 162259276829213381405976519770113 \quad (5.18.19)$$

```
> modp(3&^(n5-1),n5);
```

$$4336417956002695231751729995458 3 \quad (5.18.20)$$

```
> trialdiv(2^107+2^54+1,1000000);
```

$$[[843589, 1], [192343993140277293096491917, 1]] \quad (5.18.21)$$

```
> n6:=%[2][1];
```

$$n6 := 192343993140277293096491917 \quad (5.18.22)$$

```
> modp(3&^(n6-1),n6);
```

$$1817058975461650342105193 86 \quad (5.18.23)$$

▶ 5.19. Feladat.

▶ 5.20. Prímszámkódolás.

▼ 5.21. Feladat.

```
> p:=safeprime
  (156345678881425617888676566155526134298764532134566543212345678877209127512109876123212233332123343412343212334445432123432094872546784546778885981236317);
  log[2.](p);
  q:=safeprime
  (298415244751590016765614534678909876512342543214564909987676267881825143256789099872365142341542323965878747789933777220049883766678827671563638883776266778035);
  log[2.](q);
  n:=p*q;

  e:=28763541324536789099876534321234098876354231;
  igcdex(e,(p-1)*(q-1),'d'); d; d*e mod (p-1)*(q-1);
```

$p :=$

1563456788814256178886765661555261342987645321345665432134566\
5432123456788772091275121098761232122333321233434123432123344454321234320948725467845467788598123631\
9

508.8997379

$q :=$

2984152447515900167656145346789098765123425432145649099876762678818251432567890998723651423415423239658787477899337772200498837666788276715636388837762667778035

533.0858164

$n :=$

4665593402925412424182224876400472112892773327813449453351019945622674603742441009009573960222116531745940349543348422686605488315168714111637189152515088066784280437895008728635106433568269208177093161333726686766786948651055587128221671065756262163287553843459697677813058212618640366396927023748196137495

$$31132333$$

$$e := 28763541324536789099876534321234098876354231251$$

$$1$$

$$-$$

$$19571296224782863766115725725015334897792399314971 1\backslash$$
$$21641988678455206712513618206283545841523296400649 7\backslash$$
$$16177866942346404406822149320841232735686385789371 5\backslash$$
$$80723723234575994248299711996592194896514013640002 6\backslash$$
$$27815342349450815296557183224098089584202366964815 6\backslash$$
$$87137436801012046525167327207531798560080732689144 2\backslash$$
$$00483831$$

$$1 \qquad (5.21.1)$$

5.22. Feladat.

```
> M:="Mint víz alatti, elmerült harangok
  hintáznak-e hajnalonként ágyadnál
  a tizennyolc éves iskolások
  kiket felakasztattál";

  convert(M,'bytes');
  m:=sum(%[i]*256^(i-1),i=1..nops(%));

  c:=m&^e mod n;
```

$M := $ "Mint víz alatti, elmerült harangok

hintáznak-e hajnalonként ágyadnál

a tizennyolc éves iskolások

kiket felakasztattál"

[77, 105, 110, 116, 32, 118, 195, 173, 122, 32, 97, 108, 97, 116, 116, 105, 44, 32, 101, 108, 109, 101, 114, 195, 188, 108, 116, 32, 104, 97, 114, 97, 110, 103, 111, 107, 10, 10, 104, 105, 110, 116, 195, 161, 122, 110, 97, 107, 45, 101, 32, 104, 97, 106, 110, 97, 108, 111, 110, 107, 195, 169, 110, 116, 32, 195, 161, 103, 121, 97, 100, 110, 195, 161, 108, 10,

10, 97, 32, 116, 105, 122, 101, 110, 110, 121, 111, 108, 99, 32, 195, 169, 118, 101, 115, 32, 105, 115, 107, 111, 108, 195, 161, 115, 111, 107, 10, 10, 107, 105, 107, 101, 116, 32, 102, 101, 108, 97, 107, 97, 115, 122, 116, 97, 116, 116, 195, 161, 108]

$m :=$

19528680046240611054074111890960392345823897844641211123261273221169061744378240835537054015631394774815478298280810507336262895468621974609594430591383125353255019845996711281074221991389403117085548216837925027178277690153125688091048976590489549780975327596948774377394853498167317079965301261688579165618893

$c :=$ (5.22.1)

77524849422698264675685168880311738340989858492575204736838157266495122850646492987180503005220451702860034067164181214844639064979047472769226268742097472469920105274607963793029286873545335759860402064934473111621907313764067661760881559786294085051219059843276417291174148333238132265864884154324488973755321 8

```
> c&^d mod n; convert(%,base,256); convert(%,'bytes');
```

19528680046240611054074111890960392345823897844641211123261273221169061744378240835537054015631394774815478298280810507336262895468621974609594430591383125353250198459967112810742219913894031170855482168379250271782776901531256880910489765904895497809753275969487743773948534981673170799653012616885791655618893

[77, 105, 110, 116, 32, 118, 195, 173, 122, 32, 97, 108, 97, 116, 116, 105, 44, 32, 101, 108, 109, 101, 114, 195, 188, 108, 116, 32, 104, 97, 114, 97, 110, 103, 111, 107, 10, 10, 104, 105, 110, 116, 195, 161, 122, 110, 97, 107, 45, 101, 32, 104, 97, 106, 110, 97, 108, 111, 110, 107, 195, 169, 110, 116, 32, 195, 161, 103, 121, 97, 100, 110, 195, 161, 108, 10, 10, 97, 32, 116, 105, 122, 101, 110, 110, 121, 111, 108, 99, 32, 195,

169, 118, 101, 115, 32, 105, 115, 107, 111, 108, 195, 161, 115, 111, 107, 10, 10, 107, 105, 107, 101, 116, 32, 102, 101, 108, 97, 107, 97, 115, 122, 116, 97, 116, 116, 195, 161, 108]

"Mint víz alatti, elmerült harangok (5.22.2)

hintáznak-e hajnalonként ágyadnál

a tizennyolc éves iskolások

kiket felakasztattál"

▶ 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

▶ 14. A szita módszerek alapjai