Wanneer is een getal priem?

Inhoud

- Definitie
- Methodes
  - Naieve methodes
  - Probabilistische tests
  - Deterministische methodes
- Besluit

Definitie priemgetal

Een priemgetal is een natuurlijk getal groter dan 1 dat slechts deelbaar is door 1 en door zichzelf.

Methodes

- 3 soorten
  - Naieve methodes
  - Probabilistische methodes
  - Deterministische methodes

Naieve methodes

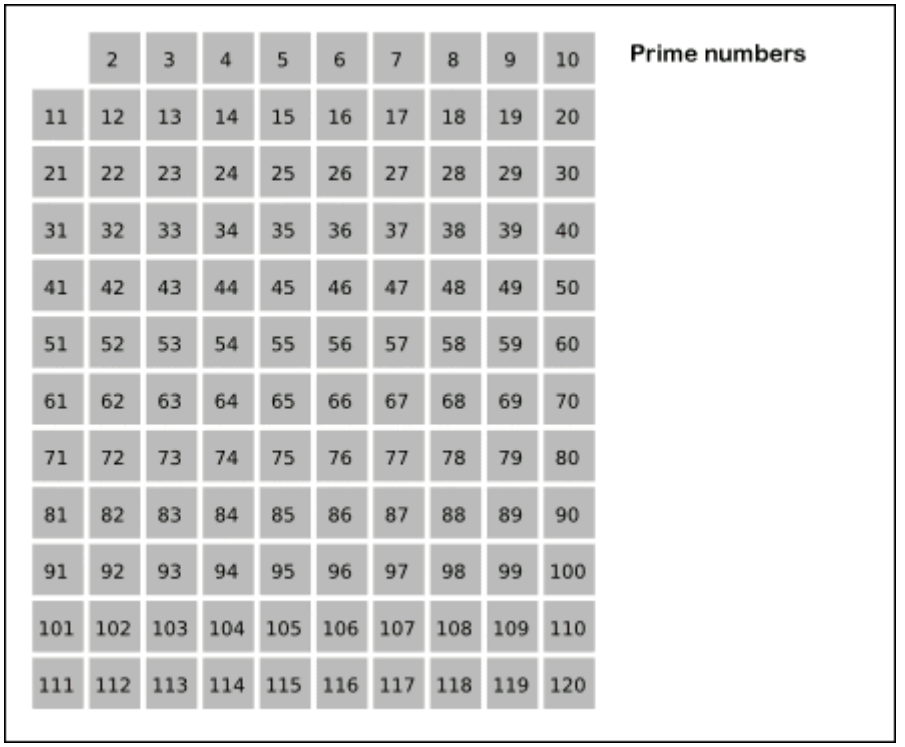
- Principe: kleinere getallen aflopen opzoek naar een deler
- Eenvoudig (+)
- 100% zekerheid correcte oplossing (+)
- Veel werk (-)

Naive methodes

- N | M met 2<M<N-1
  - Alle getallen aflopen
  - Zeer veel werk
  - Nodig?
- N | M met 2<M<sqrt(N)
  - Verbetering : getallen aflopen, stoppen bij wortel
  - Immers als deler > wortel => quotiënt < wortel
  - Quotiënt ook een deler => reeds gepasseerd.

Naive methodes

- N | M met 2<M<sqrt(N)
  M ook priem
  - Sneller
  - Alle kleinere priemgetallen moeten gekend zijn
- Zeef van Eratosthenes
  - Alles aflopen
  - 'Priemveelvouden' schrappen



Probabilistische tests

- “Waarschijnlijk” priem
- Samengesteld getal
  - Positief geheel getal deelbaar door minstens 2 priemgetallen
  - Bv 15 = 3 x 5
- Snel (+)
- Foute oplossing mogelijk (-)

Structuur Probabilistisch testen

- Aantal waarden a
- Voor elke waarde/getuige een gelijkheid testen
- Gelijkheid afhankelijk van algoritme
- Gelijkheid klopt niet => getal is zeker niet priem
- Herhalen -> zekerheid verbetere
  -> gelijkheid klopt niet

Probabilistische test

- Priemtest van Fermat (vb RSA encryptie)
- Miller-Rabin

Priemtest van Fermat

- Gebaseerd op de kleine stelling van fermat.
- Reeks getallen a, deze zijn de 'getuigen'
- Kleine stelling van fermat: als een getal priem is dan geldt:

$a^p \equiv a \pmod p \iff a^{(p-1)} \equiv 1 \pmod p$

- Als priem dan geldt vgl, niet omgekeerd

Aantonen stelling van Fermat

- Getal a => positief, niet deelbaar door p
- Beschouw de reeks : a,2a,3a,...,(p-1)a
- Rest na gehele deling = permutatie van 1,2,3,..,(p-1)

  Dit kan aangetoond worden met het dilemma van Euclides
- Hierdoor geldt :

  $a*2a*3a*...(p-1)a \equiv 1*2*3*...(p-1) \pmod{p}$

Aantonen stelling van Fermat

- Uitwerken geeft:

  $a*2a*3a*...(p-1)a \equiv 1*2*3*...(p-1) \pmod p$

  $a^{(p-1)} * (p-1)! \equiv (p-1)! \pmod p$

- (p-1)! Wegdelen, dit mag want:

  $ux \equiv uy \pmod p \Leftrightarrow u(x-y) \equiv 0 \pmod p$

  $p \mid u(x-y) \Rightarrow p \mid (x-y)$ (altijd)

  OF $p \mid u \Rightarrow$ na deling : $u \equiv 0 \pmod p$

- Zo krijgen we $a^{(p-1)} \equiv 1 \pmod p$

Voorbeeld bewijs

- vb a=3, p=7
- eerste reeks veelvouden:

  3,6,9,12,15,18
- rest na deling door 7

  3,6,2,5,1,4
- Dat is dus een permutatie van

  1,2,3,4,5,6

Voorbeeld bewijs

- Als we deze getallen vermenigvuldigen krijgen we:

  $3*6*9*12*15*18 \equiv 3*6*2*5*1*4 \equiv 1*2*3*4*5*6 \pmod 7$

- Vereenvoudigen geeft

  $3^6 * (1*2*3*4*5*6) \equiv (1*2*3*4*5*6) \pmod 7$

  $3^6 \equiv 1 \pmod 7$

Voorbeeld stelling

- Is p = 221 priem?
- Stel a = 38 (gekozen)
- Test gelijkheid
  - a^(p-1) ≡1 (mod p) => 38^220 ≡1 (mod 221)
  - Priem ?
- 2e test a=26
  - 26^220 ≡169 !≡ 1 (mod 221)
  - P is niet priem! => 13*17 = 221

Deterministische methodes

- Trager dan probabilistisch (-)
- Zeker van oplossing (+)

Priemtest van fermat

- Is gebaseerd op de kleine stelling van fermat (fermat's little theorem)
- Kleine stelling van fermat => als een getal priem is dan geldt X

Deterministische methodes

- Miller-test
  - Riemann-hypothese (onbewezen)
- AKS test
  - Origineel
  - Verbeteringen

Besluit

- Niet zo eenvoudig
- Afweging eenvoud, tijd en juistheid oplossing