

Kenmerk: TW08/DWMP/GP/08-01

Tentamen Discrete Wiskunde II (152162)

Maandag 31 maart 2008, 13:30 - 16:30 uur (sportcentrum)

Alle antwoorden dienen te worden gemotiveerd!
Gebruik van een rekenmachine is niet toegestaan!

- (a) Bepaal met behulp van het algoritme van Euclides de grootste gemene deler ('gcd') van 888 en 108.
(b) Voor welke $c \in \mathbb{Z}$ bestaan er gehele getallen x en y zodat:

$$888x + 108y = c.$$

Motiveer het antwoord.

- (c) Schrijf 6137 octaal (8-tallig).
- Voor een reëel getal a , en een $n \in \mathbb{Z}^+$, is in de onderstaande procedure de eindwaarde van 'Result' gelijk aan a^n .

```
procedure Power(a: real; n: positive integer)
begin
  Result := 1.0
  for i := 1 to n do
    Result := Result * a
  end
```

- (a) Hoeveel vermenigvuldigingen, afhankelijk van n , vinden in de procedure plaats? Geef ook een grote orde ('big-O') representatie van dit aantal.
(b) Geef een verbeterde procedure waarbij het aantal vermenigvuldigingen $O(\log(n))$ is. Geef een bovengrens voor het aantal vermenigvuldigingen, waaruit dit orde gedrag blijkt.
- (a) Bepaal de oplossing van de recurrente betrekking

$$a_{n+2} - 4a_{n+1} + 8a_n = 12 \cdot 2^n$$

$$a_0 = 3, \quad a_1 = 2.$$

- (b) We bekijken binaire strings van lengte n , waarin *geen* opeenvolgende enen voorkomen. Het aantal van deze strings noemen we a_n . Bereken a_1 en a_2 , en geef een recurrente betrekking voor a_n .

Z.O.Z.

4. (a) Gegeven is een volledige ('complete') m -aire boom, met ℓ bladeren ('leaves'), en i interne punten.
Toon aan dat:

$$\ell = (m - 1)i + 1.$$

- (b) Construeer een optimale prefix code voor $\{a, b, c, d, e, f\}$ met frequenties respectievelijk 20, 12, 5, 16, 14 en 10.

5. (a) Zoals gebruikelijk is U_{24} de groep van inverteerbare elementen in \mathbb{Z}_{24} .
Bepaal alle elementen van U_{24} , en geef van elk element de inverse.

- (b) Is U_{24} een cyclische groep? Motiveer het antwoord.

6. Zoals gebruikelijk is S_5 de groep van permutaties van $\{1, 2, 3, 4, 5\}$. Verder zijn $\sigma, \rho \in S_5$ gegeven door:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$$

en

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix}$$

- (a) Bepaal de kleinste subgroep H in S_5 , waarvoor geldt dat $\sigma, \rho \in H$.

- (b) In S_5 is er een subgroep K met 24 elementen. Hoeveel linker cosets van K in S_5 zijn er?

7. De RSA methode met $n = 91$ en $e = 29$ is gebruikt om $M \in \mathbb{Z}_{91}$ te coderen tot $C \in \mathbb{Z}_{91}$ door:

$$C \equiv M^e.$$

Bepaal M als $C = 4$.

Normering:

- 1.(a): 2 2.(a): 1 3.(a): 4 4.(a): 3 5.(a): 3 6.(a): 3 7.: 4
 (b): 2 (b): 3 (b): 3 (b): 3 (b): 2 (b): 1
 (c): 2

Totaal: 36 + 4 = 40 punten