OpenUniversiteitNederland

Cursus	Inleiding Informatica, IB0102
Tentamencode	VOORBEELDTENTAMEN
Datum	4 juli 2017
Duur	3 uur

De opgaven van dit tentamen zijn gebaseerd op het cursusmateriaal dat behoort bij de cursus Inleiding Informatica (IB0102).
U mag gebruiken: een schoon exemplaar van het cursusmateriaal, een woordenboek en een zakrekenmachine (simpel, niet-programmeerbaar).

Dit tentamen bestaat uit 22 pagina's met in totaal 45 multiple choice vragen, met daarna 1 pagina met errata. Iedere vraag heeft 4 antwoorden, waarvan 3 fout zijn en 1 goed. De voorlopige cesuur van dit tentamen is vastgesteld op 29/30. Dit betekent dat u slaagt indien u 30 of meer vragen goed beantwoordt. Deze norm is **voorlopig** en kan ingevolge Art. 4 lid 3 van de '*Nadere regels inrichting tentamen en examen*' nog worden bijgesteld.

Aan het eind van dit tentamen bevindt zich een bijlage met de op het moment van het tentamen bekende errata in de lesstof.

Veel succes!

Opgave 1.
Welke van de volgende uitspraken over Software Engineering is waar?

a. De ontwikkeling van methoden als het Unified Process behoort tot het vakgebied Software Engineering.
b. Een belangrijke doelstelling van Software Engineering is de ontwikkeling van nieuwe programmeertalen.
c. Het vakgebied Software Engineering is ontstaan toen er door de opkomst van het web (midden jaren negentig) een heel nieuw type informatiesysteem nodig werd.
d. Sinds de opkomst van de Software Engineering behoort de software crisis tot het verleden.

Opgave 2.
Het boeken van vliegtickets gebeurt in toenemende mate via webgebaseerde systemen. Op een website geeft de boeker aan hoeveel zitplaatsen deze wil boeken voor welke vlucht, plus gegevens over de klasse (economy, business,...) en over eventuele kortingen (bijvoorbeeld voor kinderen). De controle of alle gegevens zijn ingevuld, gebeurt meestal lokaal (op de client-computer); de feitelijke boeking gebeurt op de server (die beschikt over alle boekingsgegevens). Welke omschrijving karakteriseert dit webgebaseerde boekingssysteem het best?

a. Dit is een administratief gedistribueerd systeem.
b. Dit is een embedded gedistribueerd systeem.
c. Dit is een embedded real-time systeem
d. Dit is een kritisch real-time systeem.

Opgave 3.
In een bedrijf wordt een nieuw informatiesysteem ontwikkeld, waarin onder meer gegevens van het personeel worden opgenomen. In het kader daarvan worden diverse discussies gehouden. Een van die discussies gaat over de vraag of ook het burgerservicenummer van de personeelsleden moet worden opgenomen. Een andere discussie gaat over de vraag of er gekozen zal worden voor een relationele database. Stel dat de ontwikkeling van het systeem gebeurt volgens de watervalmethode.

Bepaal dan of de volgende beweringen waar zijn.

I De discussie over het al dan niet opnemen van het burgerservicenummer vindt plaats in de analysefase.
II De discussie over het al dan niet kiezen van een relationele database vindt plaats in de implementatiefase.

a. I en II zijn beide waar.
b. Alleen I is waar.
c. Alleen II is waar.
d. I en II zijn geen van beide waar.

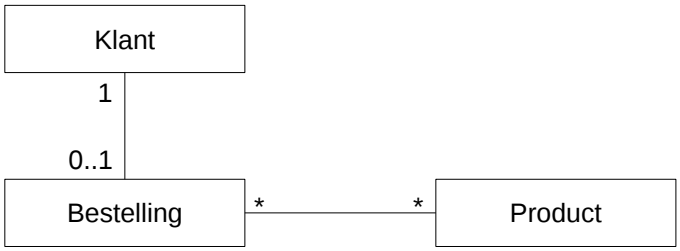
Opgave 4.
Een student krijgt een huiswerkvraag om een use case te maken voor het gebruik van een geldautomaat. Hij maakt de volgende use case:

> **Use case: Geld opnemen uit geldautomaat**
>
> **Primaire actor:** Rekeninghouder, hierna aan te duiden als gebruiker
> **Doel:** geld opnemen van de rekening met behulp van een pinpas
> **Hoofdsuccesscenario:**
> 1. Gebruiker voert de pinpas in in de gleuf rechtsboven.
> 2. Gebruiker typt pincode in.
> 3. Systeem controleert de pincode.
> 4. Gebruiker drukt de knop naast één van de getoonde bedragen in.
> 5. Gebruiker drukt op de knop met OK.
> 6. Systeem geeft geld uit.

Hij krijgt van een medestudent onderstaande vier opmerkingen als feedback. Welke van deze opmerkingen is *onterecht*?

a. Het teruggeven van het pasje aan de gebruiker ontbreekt.
b. De beschrijving bevat te veel details over de gebruikersinterface.
c. Er moet beschreven worden wat er gebeurt als de pincode niet klopt.
d. Het systeem zorgt niet dat het opgenomen bedrag van de rekening van de gebruiker wordt afgeschreven.

Opgave 5.
Klanten doen bestellingen; een bestelling heeft betrekking op producten. Iemand modelleert de onderlinge relatie tussen Klant, Bestelling en Product als volgt in een klassendiagram.

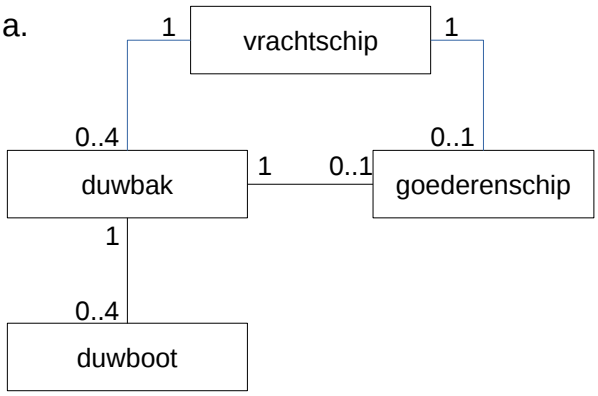


Welke van de volgende uitspraken is in overeenstemming met dit diagram?
(NB: Of de modellering in het diagram klopt met de werkelijke gang van zaken, doet er in deze opgave niet toe).

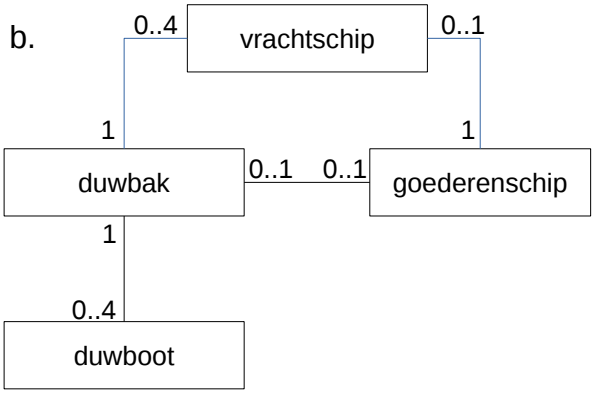
a. Een klant kan meer dan één bestelling doen.
b. Alle producten zijn wel eens besteld.
c. Er kunnen bestellingen zijn die op geen enkel product betrekking hebben.
d. Er kunnen bestellingen zijn die door geen enkele klant zijn gedaan.

Opgave 6.
We stellen een domeinmodel op voor de opbouw van een vrachtschip op rivieren. Een vrachtschip bestaat uit 0 tot 4 duwbakken en een boot. Duwbakken kunnen niet zelf varen, dus daar moet per se een boot bij. Bij een duwboot mogen tot 4 duwbakken, bij een goederenschip (dat zelf laadruimte heeft) mag nog maximaal 1 duwbak worden aangekoppeld. Een duwboot heeft geen laadruimte, dus zonder duwbakken is een duwboot geen vrachtschip.
Welke van onderstaande modellen is in overeenstemming met deze beschrijving?

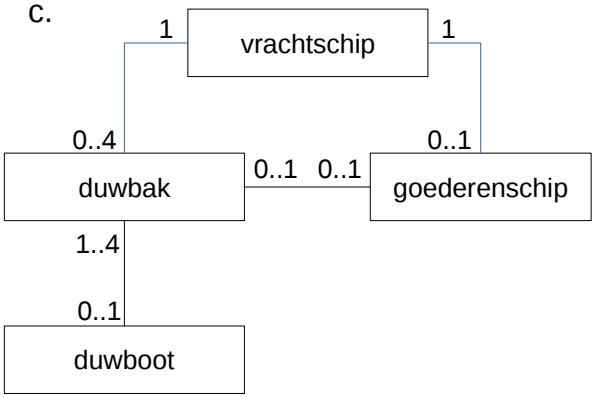
a.



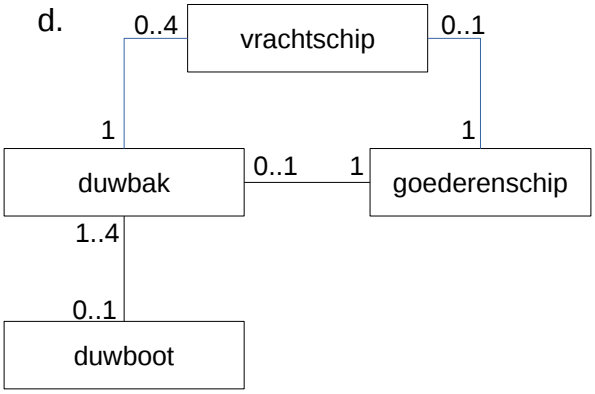
b.



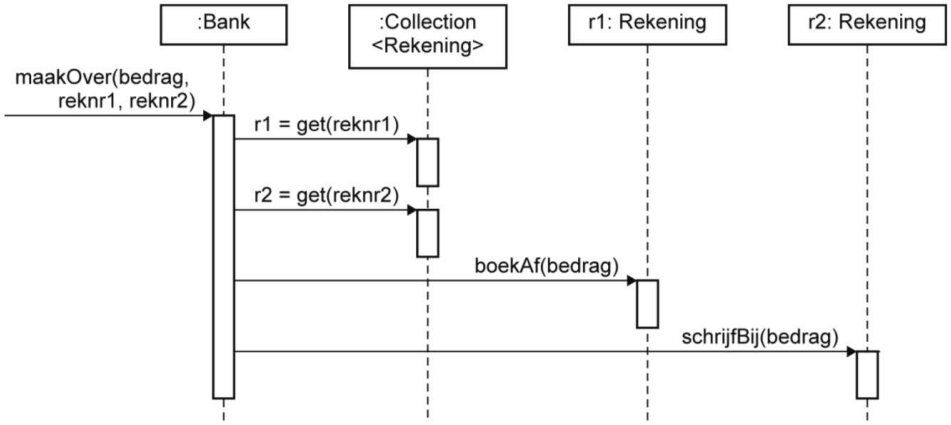
c.



d.



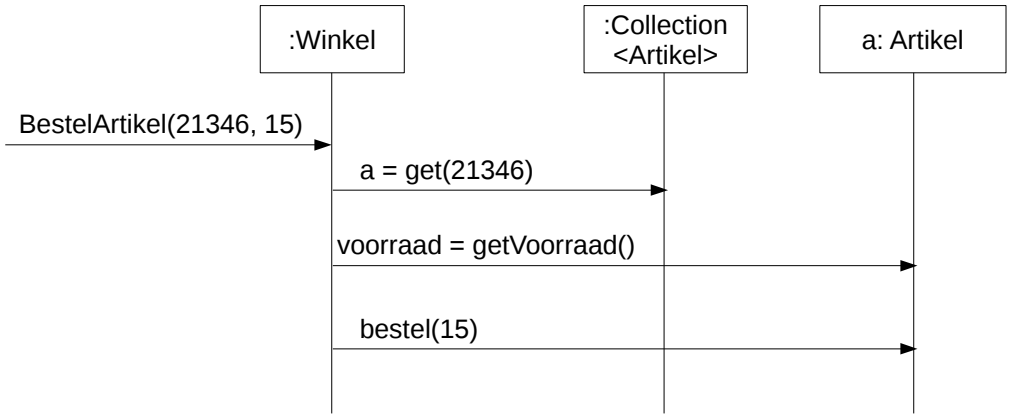
Opgave 7.
Onderstaand sequentiediagram beschrijft hoe een overschrijving door de bank wordt verwerkt.



Welke van onderstaande uitspraken is in overeenstemming met dit sequentiediagram?

a. Object :Bank heeft een methode boekAf().
b. r1 is een klasse van het type Rekening.
c. r1 heeft een methode boekAf().
d. r2 is een ouderklasse van Collection.

Opgave 8.
Gegeven is onderstaand sequentiediagram.

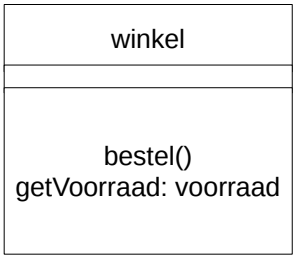


Over welke methode(n) moet de klasse Winkel op basis van dit diagram zeker beschikken?

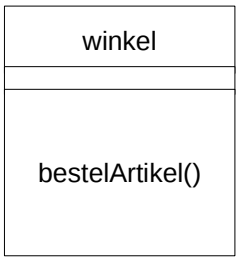
a.

b.

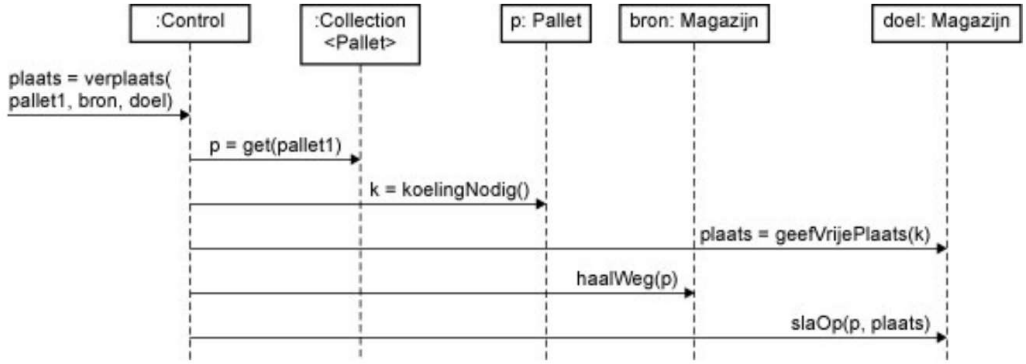
c.



d.



Opgave 9.
Gegeven is onderstaand sequentiediagram. Toelichting: een pallet moet verplaatst worden van het ene magazijn (het bronmagazijn) naar het andere magazijn (het doelmagazijn). Er moet eerst onderzocht worden of de pallet koeling nodig heeft, vervolgens waar in het gewenste magazijn plaats vrij is. Tenslotte moet de pallet worden verplaatst en toont het systeem de gebruiker de nieuwe plaats.



Geef van elk van de volgende uitspraken aan, of deze in overeenstemming is met dit diagram:

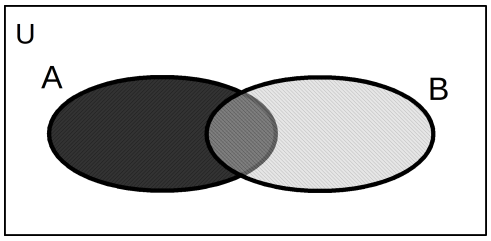
I De methode verplaats heeft één parameter.
II De naam p verwijst naar een instantie van de klasse Pallet.

a. Beide uitspraken zijn in overeenstemming met het diagram.
b. Alleen uitspraak I is in overeenstemming met het diagram.
c. Alleen uitspraak II is in overeenstemming met het diagram.
d. Geen van beide uitspraken is in overeenstemming met het diagram.

Opgave 10.
Welke van onderstaande is een deelverzameling van de verzameling
{tentamen, maken, {is, leuk, {in, de}}, leuk, zomer }?

a. {tentamen, maken, is, leuk}
b. {{in, de}, zomer, {is}, leuk}
c. {de, zomer, {is, leuk}}
d. {zomer, {is, leuk, {in, de}}}

Opgave 11.
Beschouw het onderstaande Venn-diagram van verzamelingen A en B in universum U.



We nemen het complement van de doorsnede van A en B. Welke van onderstaande formules beschrijft dit deel van het Venn-diagram?

a. $A^c \cup B^c$
b. $A^c \cap B^c$
c. $(A \cup B^c) \cap A^c$
d. $A \cup (B^c \cap A^c)$

Opgave 12.
Beschouw de volgende verzameling: { i | $i \in \mathbb{N} \wedge i \bmod 3 = 0$ }.
Welke van onderstaande beweringen is correct?

a. Dit is de verzameling van alle veelvouden van 3.
b. Dit is de verzameling van oneven getallen.
c. Dit is dezelfde verzameling als $\{i | i \in \mathbb{N} \wedge i | 3\}$
d. Dit het complement van de verzameling als $\{i | i \in \mathbb{N} \wedge i | 3\}$

Opgave 13.
Wat is de binaire representatie van de optelling (in het tientallig talstelsel) van 65 + 62?

a. $0011\ 1111_2$
b. $0111\ 1111_2$
c. $1111\ 1100_2$
d. $1111\ 1110_2$

Opgave 14.
Welke van onderstaande twee beweringen is waar? Let op: $0 \in \mathbb{Q}$!

I De verzameling $\mathbb{Q}$ is gesloten onder deling.
II De verzameling $\mathbb{Q}$ is gesloten onder vermenigvuldigen.

a. Beweringen I en II zijn beide juist.
b. Alleen bewering I is juist.
c. Alleen bewering II is juist.
d. Beweringen I en II zijn beide onjuist.

Opgave 15.
Stel dat twee getallen a en b geen enkele priemfactor in overeenstemming hebben. Welke uitspraak is dan correct?

a. ggd(a, b) = $a \cdot b$
b. kgv(a, b) = $a \cdot b$
c. a | b
d. b | a

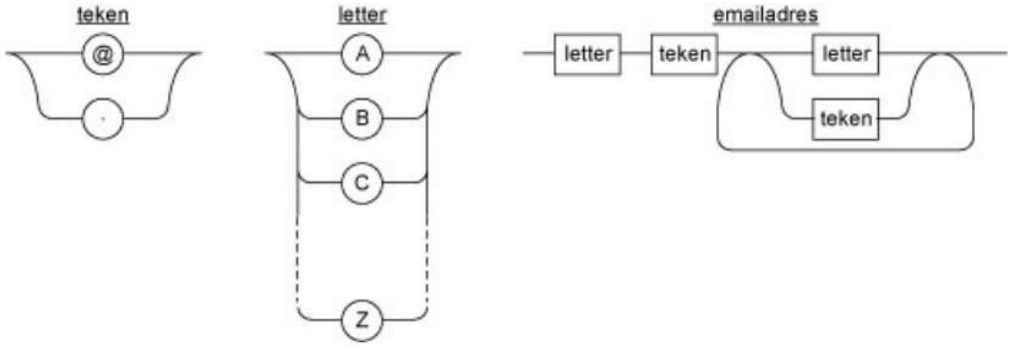
Opgave 16.
Beschouw de volgende grammatica:

<getal> → <cijfer> | <cijfer> <getal>
<cijfer> → 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9
<woord> → <letter> | <letter> < woord>
<letter> → A | B | C | D | E | F | G | H | I | J | K | L | M | N | P | Q | R | S | T | U | V | X | Y | Z

We willen de grammatica uitbreiden zodat deze tenminste postcodes in Nederland beschrijft (vier cijfers, gevolgd door twee letters). Welke van de onderstaande uitbreidingen kan dit *niet*, oftewel: welke uitbreiding kan *geen* geldige postcodes produceren?

a. <uitbreiding> → <getal> <woord> <letter>
b. <uitbreiding> → <cijfer> <getal> <cijfer> <letter> <woord> <letter>
c. <uitbreiding> → <getal> <letter> <letter>
d. <uitbreiding> → <getal> <cijfer> <woord> <letter>

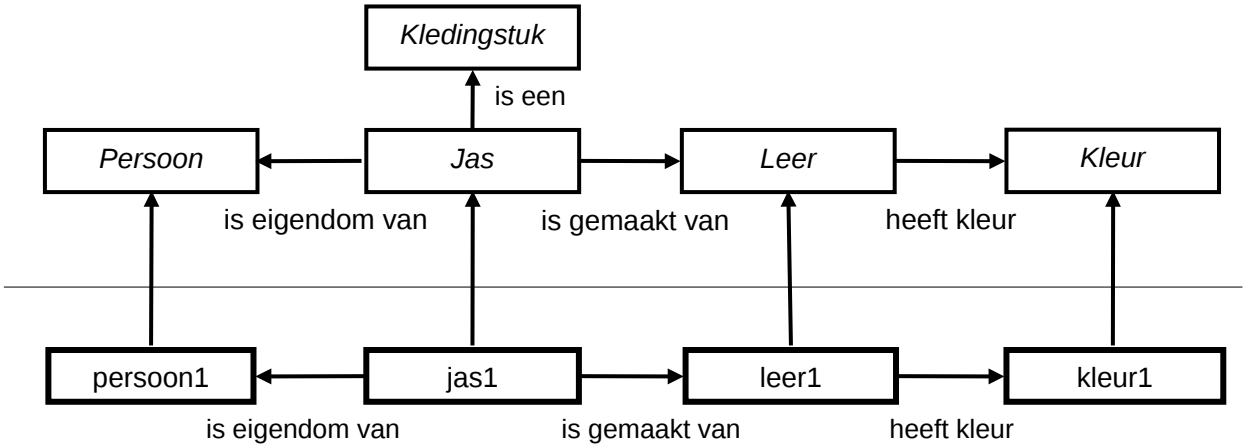
Opgave 17.
Beschouw onderstaand syntaxdiagram.



Welke van onderstaande email adressen is *niet* in overeenstemming met dit syntaxdiagram?

a. Hugo@ou.nl
b. H.u.g.o@ou.nl
c. H@ugo@ou.nl
d. h.a.h.a.

Opgave 18.
Gegeven is onderstaand semantisch netwerk:



Welke uitspraak is juist op basis van dit semantisch netwerk?

a. Alle kledingstukken zijn van persoon1.
b. jas1 heeft kleur kleur1.
c. Kleur is een instantie van kleur1.
d. jas1 is een instantie van Jas.

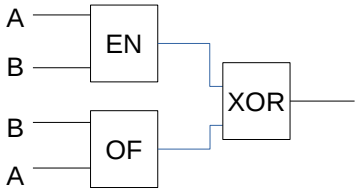
Opgave 19.
In het beschrijven van logische formules kunnen ook symbolen worden gebruikt. In de tabel hieronder staan de symbolen zoals in deze opgave gebruikt.

Symbool	functie
$p \wedge q$	p EN q
$p \vee q$	p OF q
$\neg p$	NIET p
$p \Rightarrow q$	ALS p DAN q
$p \Leftrightarrow q$	q DAN-EN-SLECHTS-DAN-ALS p

Welke van onderstaande uitspraken is correct?

a. $(\neg p) \wedge q$ is hetzelfde als $p \Rightarrow q$
b. $(\neg p) \vee q$ is hetzelfde als $p \Rightarrow q$
c. $p \wedge (\neg q)$ is hetzelfde als $p \Rightarrow q$
d. $p \vee (\neg q)$ is hetzelfde als $p \Rightarrow q$

Opgave 20.
Beschouw de schakeling hieronder.



Deze schakeling is hetzelfde als:

a. A EN B
b. A OF B
c. A XOR B
d. NIET A

Opgave 21.
Midas heeft een predikaatlogisch model gemaakt van computerprogramma's. Hij heeft onder andere de volgende verzamelingen gevuld:

is-besturingssysteem(x), is-browser(x) en is-printerdriver(x).

Welke uitspraak is juist?

a. De bewering is-printerdriver(Windows) is niet toegestaan omdat Windows geen printerdriver is.
b. In de bewering is-browser(Firefox) is 'Firefox' het predikaat.
c. In de bewering is-besturingssysteem(Firefox) is 'Firefox' het argument.
d. Het predikaat is-printerdriver verwijst naar een specifiek object.

Opgave 22.
Beschouw onderstaande tabel van procesadministraties met hun toestanden hieronder.

Proces	Status	Toegewezen voorzieningen	Wachtend op
1	Wacht	c	a
2	Actief	a, b	
3	Pauze		
4	Wacht		b, c

Welke van onderstaande uitspraken is correct?

a. Bij de volgende toestand moet proces 3 actief geworden zijn.
b. Het is onvermijdelijk dat deze procestabel leidt tot processen die wederzijds wachten.
c. Proces 4 zal pas aan de beurt komen als alle andere processen een beurt hebben gehad.
d. Bij de volgende toestand zal ofwel proces 1 ofwel proces 3 actief geworden zijn.

Opgave 23.
Bij veel online spellen kunt u tegen andere spelers spelen. In zo'n geval liggen er een aantal taken, waaronder:
1. er wordt bijgehouden wie wie aanvalt,
2. er wordt bijgehouden hoe hard iemand wordt geraakt,
3. er wordt bijgehouden hoevaak iemand nog geraakt kan worden,
4. de acties worden op het scherm getoond,
5. de acties worden naar de andere spelers gecommuniceerd,
6. animaties behorende bij acties worden van schijf geladen.

Welke van deze acties zal gebruik moeten maken van systeemverzoeken?

a. 1, 2, 3
b. 1, 2, 3 en 4
c. 5 en 6
d. 4, 5 en 6

Opgave 24.
Op Windows-systemen staat vaak een *swapfile* die gebruikt wordt voor niets anders dan om feitelijk het geheugen te vergroten. Op Linux-systemen is er vaak een apart stukje harddisk gereserveerd als “swap space”. In allebei de gevallen is er dus ruimte op de harddisk om het geheugen op de een of andere manier “uit te breiden”. Hoe gebruikt het besturingssysteem deze ruimte op de harddisk om het interne geheugen uit te breiden?

a. Daarin worden geheugenpagina's opgeslagen die op dit moment niet in gebruik zijn door actieve processen.
b. Daarin worden alle bestanden die een proces nodig heeft, naartoe gekopieerd zodat het proces veel sneller bij die bestanden kan.
c. Daarin wordt alle machine-code van een proces neergezet, zodat het besturingssysteem het altijd makkelijk terug kan vinden.
d. Als het gewone geheugen helemaal vol is, dan worden volgende verzoeken voor geheugenruimte verwerkt door deze ruimte te gebruiken.

Opgave 25.
Hieronder staat het begin van een programma om alle delers van een natuurlijk getal naar het scherm uit te voeren.

```
1. def print_divisors(x):
2.     for i in range(1,x):
3.         ……
```

Hoe moet het programma worden afgemaakt?

(Let op dat in Python “a % b” betekent “a modulo b”.)

a. if i % x == 0:
       print(i)
b. if i % x != 0:
       return i
c. if x % i == 0:
       print(i)
d. if x % i != 0:
       return i

Opgave 26.
In de programmeertaal Prolog bestaat een programma uit een aantal zogenaamde 'facts' van zaken die waar zijn. Dat kunnen op zichzelf staande feiten zijn (`het_regent.`) maar ook relaties tussen zulke feiten (`is_dier(hond).` of `fietst_graag_naar(werk, hugo).`) Tot slot kan Prolog afleidingen maken door middel van 'regels' die vertellen hoe je iets uit feiten mag afleiden, bijvoorbeeld een programma dat kan beredeneren of iemand nu aan het fietsen is:

```
fietst_nu_naar(X,Y):- fietst_graag_naar(X,Y), mooi_weer, op_tijd(Y).
```

Op wat voor programmeerparadigma is Prolog gebaseerd?

a. Imperatief programmeren.
b. Functioneel programmeren.
c. Object-geörienteerd programmeren.
d. Logisch programmeren.

Opgave 27.
Beschouw de reeks getallen opgebouwd als volgt: begin met een 1 gevolgd door nog een 1. Ieder volgend getal is dan de optelling van de 2 voorafgaande getallen. Het begin ziet er dus als volgt uit:

1, 1, 2 (=1+1), 3 (=2+1), 5 (=3+2), 8 (=5+3), 13 (=8+5), 21 (=13+8), 34 (=21+13), ….

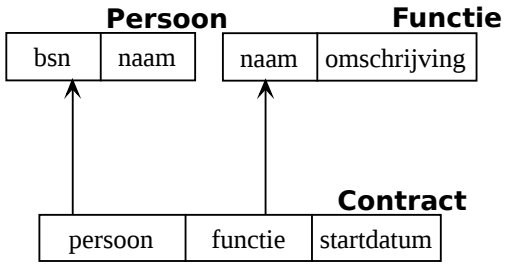
Deze reeks getallen heet de Fibonacci reeks.
Beschouw onderstaand Python programma dat bedoeld is om het N^e getal in deze reeks te berekenen. We weten niet zeker of het programma correct is, of dat er een fout in zit.

```
1  def fib(n):
2          fibmineen = 1
3          fibmintwee = 1
4          retval = 1
5
6          for i in range(3, n+1):
7                  retval = fibmineen + fibmintwee
8                  fibmintwee = fibmineen
9                  fibmineen = retval
10
11         return retval
```

Stel we voeren dit programma uit voor de getallen 1 t/m 9. Welke getallen krijgen we dan als uitvoer?

a. 1, 1, 1, 2, 3, 5, 8, 13, 21
b. 1, 2, 3, 5, 8, 13, 21, 34, 55
c. 1, 1, 1, 1, 1, 1, 1, 1, 1
d. 1, 1, 2, 3, 5, 8, 13, 21, 34

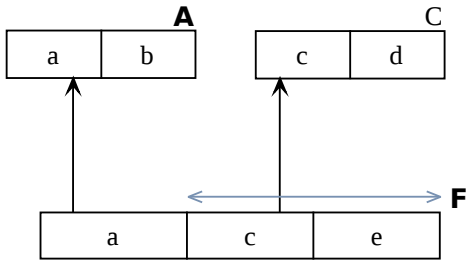
Opgave 28.
Gegeven is het volgende strokendiagram, zonder uniciteitsregels.



Welke van onderstaande regels zorgt ervoor dat contracten alleen verwijderd kunnen worden als de betreffende persoon niet meer in de database zit?

a. een cascading update op de verwijzing van Contract naar Persoon
b. een cascading delete op de verwijzing van Contract naar Persoon
c. de referentiële-integriteitsregel
d. een uniciteitsregel op Contract.persoon

Opgave 29.
Bekijk het volgende abstracte strokendiagram:



Gegeven zijn twee uitspraken over dit diagram:

I Bij iedere waarde van e hoort precies één rij van A.
II Bij iedere rij van A hoort precies één rij van C.

Geef van beide uitspraken aan of ze waar of onwaar zijn.

a. Beweringen I en II zijn beide juist.
b. Alleen bewering I is juist.
c. Alleen bewering II is juist.
d. Beweringen I en II zijn beide onjuist.

Opgave 30.
Gegeven is de volgende niet-genormaliseerde structuur:

Boekenplank

nr	maxKg	steunJN	boeken		
			titel	auteur	jaar
1	20	j	Pietje Puk	Arnoldus	1958
			Pietje Puk wordt agent	Arnoldus	1958
			Pietje Puk viert feest	Arnoldus	1959
2	15	n	De avonturen van Pinkeltje	Laan	1939
			Pinkeltje en zijn vriendjes	Laan	1949
			Pietje Puk	Arnoldus	1958

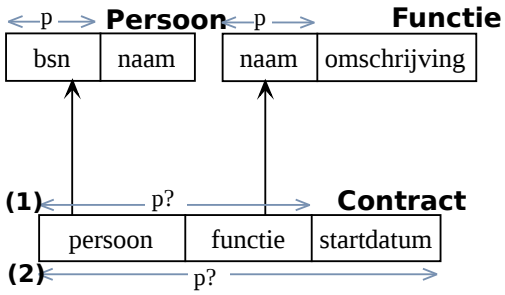
Hieronder geven we twee conclusies die misschien uit de gegeven populatie getrokken zouden kunnen worden:

I Verschillende exemplaren van hetzelfde boek kunnen op verschillende planken staan.
II Twee verschillende auteurs kunnen niet allebei een boek met dezelfde titel geschreven hebben.

Geef aan of dit inderdaad conclusies zijn die uit deze populatie getrokken kunnen worden, of niet.

a. Beweringen I en II zijn beide juist.
b. Alleen bewering I is juist.
c. Alleen bewering II is juist.
d. Beweringen I en II zijn beide onjuist.

Opgave 31.
Gegeven is onderstaande structuur, waarin nog niet duidelijk is wat de primaire sleutel van de tabel Contract wordt: dat kan (1) of (2) zijn.

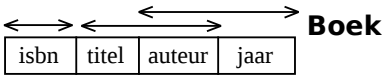


Welke van onderstaande beweringen is waar?

I Als de primaire sleutel is over “persoon” en “functie”, dan kan een persoon meerdere startdatums hebben voor dezelfde functie.
II Als de primaire sleutel is over “persoon”, “functie” en “startdatum”, dan kan een persoon meerdere startdatums hebben voor dezelfde functie.

a. Beweringen I en II zijn beide juist.
b. Alleen bewering I is juist.
c. Alleen bewering II is juist.
d. Beweringen I en II zijn beide onjuist.

Opgave 32.
Gegeven is de volgende structuur, met de aangegeven uniciteitsregels:

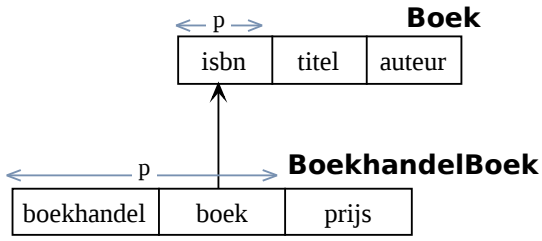


Welke uitspraak klopt, gegeven deze uniciteitsregels?

a. Een auteur kan hoogstens één boek per jaar schrijven
b. Een auteur kan best meerdere boeken met dezelfde titel schrijven, maar dan niet in hetzelfde jaar
c. Er kunnen meerdere boeken met hetzelfde isbn zijn
d. Iedere titel kan maar eens per jaar gebruikt worden

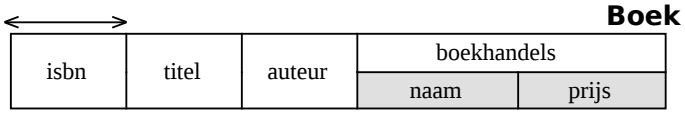
Opgave 33.
Gegeven is onderstaande structuur, waarin informatie kan worden opgeslagen over boeken die bij verschillende boekhandels verkrijgbaar kunnen zijn, eventueel tegen verschillende prijzen:

(*)

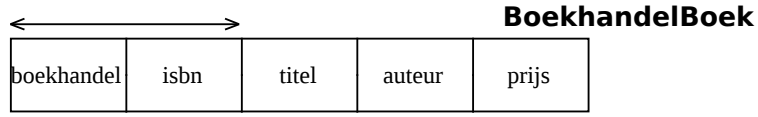


Deze structuur is verkregen door vanuit een zekere startsituatie bepaalde ongewenste structuur te elimineren. We geven twee mogelijke startsituaties, (i) en (ii):

(i)



(ii)



Uit welke van de twee startsituaties kan de structuur (*) worden verkregen, en hoe?

a. alleen door het elimineren van de herhalende groep uit (i).
b. zowel door het elimineren van de herhalende groep uit (i) als door het elimineren van de redundantie uit (ii).
c. alleen door het elimineren van de redundantie uit (ii).
d. geen van beide startsituaties kan leiden tot de structuur.

Opgave 34.
In 1997 werd begonnen met de zoektocht naar een vervanger voor het DES encryptiealgoritme. Waarom was DES toe aan vervanging?

a. DES was te traag voor de huidige computers.
b. Het algoritme van DES was openbaar geworden.
c. De sleutel van DES was gevonden.
d. DES was te makkelijk te kraken.

Opgave 35.
We willen RSA gebruiken en kiezen
$p = 2 \cdot 11 \cdot 31 \cdot 53 \cdot 61 \cdot 79$,
$q = 7 \cdot 23 \cdot 43 \cdot 59 \cdot 67 \cdot 73$, en
$e = 13$.

Merk op dat alle factoren priemgetallen zijn. Welke van onderstaande uitspraken is correct?

a. p en q hebben gemeenschappelijke factoren.
b. Deze p en q zijn geen priemgetallen en mogen daarom niet worden gebruikt.
c. De getallen e en $n = p \cdot q$ hebben een gemeenschappelijke factor.
d. Het getal e kan verder ontbonden worden (het is dus geen priemgetal) en mag daarom niet worden gebruikt.

Opgave 36.
Wat is de inverse van 3 mod 7?

a. 3
b. 4
c. 5
d. 6

Opgave 37.
Recentelijk bleek dat internetcriminelen alweer gebruik maken van domeinnamen die erg lijken op bekende namen, maar gebruik maken van andere tekens (bijv. g00gle.com in plaats van google.com). Stel dat zo'n frauduleuze website een certificaat heeft.

Zou uw browser een SSL-certificaat voor zo'n frauduleuze website weigeren?

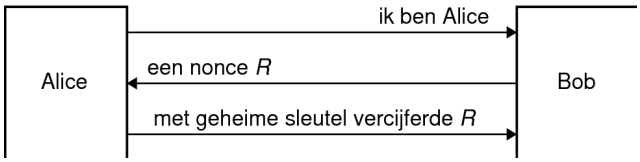
a. Ja, want de criminelen kunnen geen certificaat getekend door een CA verkrijgen.
b. Ja, want de URL van het certificaat kan niet matchen met die van de website (g00gle.com ipv google.com)
c. Ja, want de digitale vingerafdruk van het certificaat zal niet kloppen.
d. Nee, uw browser zal het certificaat accepteren.

Opgave 38.
Alice wil een digitaal document ondertekenen. Daartoe stuurt ze het document op, met daarbij een digitale handtekening van het document: de versleuteling van dat document met haar privésleutel. We nemen aan dat de cryptografie niet gebroken kan worden door Charlie.

Stel dat Mallory deze berichten onderschept en wil zorgen, dat het bericht anders aankomt dan het verstuurt is. Wat moet hij dan doen om het document aan te passen, zonder dat dat gedetecteerd kan worden?

a. Hij hoeft alleen het document aan te passen
b. Hij moet het document aanpassen en daarna de handtekening zo wijzigen dat deze bij het gewijzigde document klopt.
c. Mallory wijzigt de digitale handtekening en vervolgens ontcijfert hij deze met de publieke sleutel van Alice. Daarmee krijgt hij een nieuw document met legitieme handtekening – maar hij kan niet bepalen wat er in het document staat.
d. Hij kan niets doen zonder dat dit gedetecteerd kan worden: de digitale handtekening zoals hier gebruikt garandeert dat het document ongewijzigd is.

Opgave 39.
Beschouw onderstaand protocol, waarin Alice en Bob een geheime sleutel delen.



Welke van onderstaande uitspraken over dit protocol is correct?

a. Bob weet na afloop zeker dat Alice zijn bericht heeft gezien.
b. Alice weet na afloop zeker dat Bob haar berichten heeft gezien.
c. Bob weet zeker dat er geen berichten worden afgeluisterd.
d. Alice weet zeker dat er geen berichten worden afgeluisterd.

Opgave 40.
Is DNS een protocol?

a. Nee, want de syntax van berichten in DNS is niet vastgelegd.
b. Nee, want de volgorde van berichten in DNS is niet vastgelegd.
c. Ja, DNS is een peer-to-peer protocol.
d. Ja, DNS is een client-server protocol.

Opgave 41.
De webmail van de OU laat gebruikers mails versturen en ontvangen, ook met attachments. Via de webinterface kunnen gebruikers tevens hun mailbox organiseren in folders.

Welke van onderstaande technieken wordt hier zeker *niet* voor gebruikt?

a. SMTP
b. POP3
c. DNS
d. MIME

Opgave 42.
Op veel websites komt u tegenwoordig bij het eerste bezoek een cookie-waarschuwing tegen. Als u de cookies accepteert, verdwijnt deze waarschuwing en wordt hij ook bij volgende bezoeken vanaf dezelfde computer niet getoond. Als u echter een andere computer gebruikt, of de gehele browsergeschiedenis verwijdert, dan krijgt u de cookie-waarschuwing weer te zien.

Hoe herkent de server dat u cookies hebt geaccepteerd?

a. Via een GET parameter van het HTTP protocol.
b. Aan de hand van het IP adres van uw computer.
c. Via een HTTP-cookie.
d. Doordat u op de website ingelogd bent.

Opgave 43.
Een bedrijf heeft een netwerk 145.20.0.0/22. Hoeveel IP adressen heeft het tot zijn beschikking (bij IP versie 4)?

a. $2^{10} = 1,024$
b. $2^{11} = 2,048$
c. $2^{21} = 2,097,152$
d. $2^{22} = 4,194,304$

Opgave 44.
Beoordeel de juistheid van de volgende twee beweringen:

I De netwerklaag biedt een datagram aan aan de datalinklaag.
II De user agent van een e-mailsysteem biedt een bericht aan aan de transportlaag.

a. Beweringen I en II zijn beide juist.
b. Alleen bewering I is juist.
c. Alleen bewering II is juist.
d. Beweringen I en II zijn beide onjuist.

Opgave 45.
Wat is een voordeel van pakketschakelen boven circuitschakelen?

a. Op een ster-netwerk kan je niet circuitschakelen.
b. Bij circuitschakelen moet een bericht in kleine stukjes worden gesplitst.
c. Bij pakketschakelen kunnen meerdere verbindingen tegelijk gebruik maken van dezelfde lijnen.
d. Bij circuitschakelen wordt het bericht naar iedere computer in het netwerk verstuurd, bij pakketschakelen niet.

Errata

LE 3:

- Uitwerking opgave 3.6: de nummering herstart (1,2,1,2,3,4,5,6). Dit is fout, de nummering moet doorlopen (1,2,3,4,5,6,7,8).
- opgave 3.17: hier moet verwezen worden naar opgave 3.16 (dus niet 3.15).
- De laatste paragraaf van 3.1 ("UML is zo ontworpen...komen deze uitbreidingen niet voor") is een oud overblijfsel van de vorige versie en dient u te negeren.

LE 5:

- Antwoord 5.9b: ipv. "{}" nemen we "{$}".
- opgave 5.22b: de stelling moet zijn "Het aantal elementen van {∅} is nul."
- vraag 5.24d: in de definitie van verzameling A is een stuk weggevallen. Dit moet zijn "A = {x ∈ Z | ..."

LE6:

- Antwoord 6.6: hier staat een 1 teveel - er moet "1111" staan en niet "11111".
  Antwoord 6.7b: dit moet 232 zijn (231 in het viertallig stelsel is 45 in het 10tallig stelsel).

LE 8:

- opgave 8.8: hier wordt verwezen naar "de vorige opgave". Die is helaas weggevallen in de eerste druk. De PDF bevat de juiste opgave: PDF leereenheid 8

LE9:

- tabel 9.2: 2 2e rij van de tabelkopjes is verkeerd - onder "status" hoort niets te staan, en de rest hoort opgeschoven te zijn, oftewel:

```
opdracht-   status     urgentie  aantal   aantal  kleur    formaat  formaat
nummer                 gewenst   gewenst  klaar   papier   papier   afdruk
```

LE10:

- opgave 10.22, voorbeeld 3 moet zijn:
  `print("3. >" + nextstring("a*bc**efg") + "<")`
- uitwerking opgave 10.22: hier ontbreekt de truc met de extra spaties. De uitwerking in het boek is hierdoor fout. De verbeterde versie is als volgt:

```
def nextstring(string):
    widestr = " " + string + " "
    retstr = ""
    for i in range(1, len(widestr) - 1):
        retstr += widestr[i]
        stars = numstars(widestr[i-1:i+2])
        if widestr[i] == '*':
           for i in range(stars):
               retstr += '*'
    return retstr
```

LE 12

- Opgave 12.6: Antwoord J ontbreekt. Het antwoord moet zijn:
  `j. Foutmelding omdat Gerecht.bereidingstijd verplicht is.`

LE 13

- *Antwoord op opgave 13.6a: hier staat* $24 + 32 = 56 = 9 \cdot 5 + 1 \bmod 5$. *Dit moet zijn:* $24 + 32 = 56 = 11 \cdot 5 + 1 \bmod 5$
- *Antwoord op opgave 13.11b: hier staat* $10^{19} / 3 \cdot 10^{13} = 3 \cdot 10^{6} = 3\ 000\ 000$. *Dit is fout, dit moet natuurlijk zijn:* $10^{19} / 3 \cdot 10^{13} = 10^{6} / 3 = 333\ 333$.