Vak	:	**Algebra voor TW/INF/BIT**
Vakcode	:	**151039 en 151139**
Datum	:	23 augustus 2005
Tijd	:	9.00 - 11.00 uur

Alle antwoorden dienen gemotiveerd te worden.
Onderdelen waar u niet geheel uitkomt, kunt u zonder meer toch in het vervolg gebruiken. Mocht u door onverschillig welke omstandigheid een onderdeel niet geheel kunnen behandelen, dan verdient het in ieder geval aanbeveling om de aanpak te beschrijven.

1. (a) Gegeven zijn de getallen $a = 108$ en $b = 35$.
Bepaal met behulp van het algoritme van Euclides de GGD (a, b) en gehele getallen s en t zodat $GGD(a, b) = sa + tb$.

   (b) Het RSA-cryptosysteem is onder andere gebaseerd op de stelling van Euler.
Formuleer deze stelling.

   (c) Gegeven is $n = p \cdot q$ met p en q priemgetallen en $p \neq q$. In het RSA-cryptosysteem coderen we via $[B]_n \mapsto [B]_n^e$ en decoderen we via $[C]_n \mapsto [C]_n^d$ voor zekere d. Zij nu $n = 133, e = 35$. Bepaal d en decodeer vervolgens $[2]_{133}$.

2. Beschouw de deelverzameling S_1 van de 2×2-matrices $M_2(\mathbb{R})$ met coëfficiënten uit $\mathbb{R}$ gegeven door

$$S_1 = \left\{ \begin{pmatrix} \alpha & \beta \\ 2\beta & \alpha \end{pmatrix} | \alpha \in \mathbb{Q}, \beta \in \mathbb{Q} \right\} .$$

   (a) Laat zien dat S_1 een deelring is van $M_2(\mathbb{R})$.

   (b) Wat is de definitie van eeen lichaam?

   (c) Gegeven is dat $\alpha^2 - 2\beta^2 \neq 0$ voor $(\alpha, \beta) \in \mathbb{Q}^2$ met $(\alpha, \beta) \neq (0, 0)$.
Bewijs dat S_1 een lichaam is.

3. (a) In $\mathbb{Z}_2[x]$ beschouwen we het polynoom $g(x) = x^3+x^2+1$. Laat zien dat $g(x)$ irreducibel is over $\mathbb{Z}_2$.

   (b) Zij $F = \mathbb{Z}_2[x]/(g(x))$ de quotiëntring naar het ideaal $(g(x))$. We geven de met x corresponderende coset $[x]_g$ voor het gemak aan met α.
Laat zien dat de elementen $\{1, \alpha, \alpha^2\}$ een basis van F vormen.

   (c) Bepaal voor elke $f \in F, f \neq 0$, een $h \in F$ met $fh = 1$.

1	a	:	2	2	a	:	3	3	a	:	2
	b	:	1		b	:	1		b	:	1
	c	:	2		c	:	2		c	:	2

totaal = 16 + 4 = 20 punten