Tentamen ~~Alg~~ Alg. 1, 28 juni 2012, Uitwerkingen.

1. $\sigma = (5\,7\,9)(7\,2\,1)(1\,7\,2\,3\,4\,9\,8)(5\,6)$
$= (1\,2\,3\,4\,5\,6\,7)(8\,9)$

(5) (a) $\text{orde}(\sigma) = 7 \cdot 2 = 14$

(10) (b) $7 / 2012 \backslash 287$ dus in $\mathbb{Z}/7\mathbb{Z}$: $\overline{2012} = \overline{3}$. Omdat 7 priem: $\overline{3}^6 = \overline{1}$,

14
61
56
52
49
3

$2011 \equiv 1 (2)$, $2011 \equiv 1(3)$, dus $2011 \equiv 1(6)$, dus $\overline{3}^{2011} = \overline{3}^1 = \overline{3}$.
som v.d. cijfers; Chinese rest. Ook: $2012^{2011} \equiv 0\,(2)$

$\sigma^{2012^{2011}} = (1\,2\,3\,4\,5\,6\,7)^3 \cdot (8\,9)^0 = (1\,4\,7\,3\,6\,2\,5)$.

(5) (c) $\varepsilon(\sigma) = \varepsilon(7\text{-cykel}) \cdot \varepsilon(2\text{-cykel}) = 1 \cdot -1 = -1$.
Als $\sigma = \tau^2$, dan $\varepsilon(\sigma) = \varepsilon(\tau)\cdot\varepsilon(\tau) = 1$, dus er is niet zo'n τ.

(5) (d) Ja, want orde(σ) is onderling priem met 3, in $\mathbb{Z}/7\mathbb{Z}$: $\overline{3}\cdot\overline{5} = 1$,
en in $\mathbb{Z}/2\mathbb{Z}$: $\overline{3} = \overline{1}$, dus $\tau = (1\,6\,4\,2\,7\,5\,3)(8\,9)$.

2. $255 = 5 \cdot 51 = 5 \cdot 3 \cdot 17$.

$13/255\backslash 19$
13
125
117
8

(5) (a) $\text{ggd}(13, 255) = 1$, dus er is zo'n a. (of meer?)

$(L1): 1 \cdot 255 + 0 \cdot 13 = 255$
$(L2): 0 \cdot 255 + 1 \cdot 13 = 13$
$(L1) - 19\cdot(L2) = (L3): 1 \cdot 255 - 19 \cdot 13 = 8$
$(L2) - (L3) = (L4): -1 \cdot 255 + 20 \cdot 13 = 5$
$(L3) - (L4) = (L5): 2 \cdot 255 - 39 \cdot 13 = 3$
$(L4) - (L5) = (L6): -3 \cdot 255 + 59 \cdot 13 = 2$
Ik neem $\boxed{a = -98}$ $\quad (L5) - (L6) = (L7): 5 \cdot 255 - 98 \cdot 13 = 1$

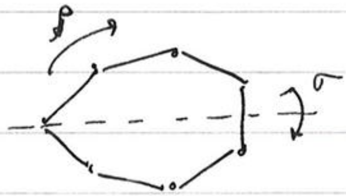
(5) (b) Chinese rest stelling: $(\mathbb{Z}/255\mathbb{Z})^*$ is isom. met $(\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^* \times (\mathbb{Z}/17\mathbb{Z})^*$.
$\varphi(3) = 2$, $\varphi(5) = 4$, $\varphi(17) = 16$, alle drie 2-machten.
$\#(\mathbb{Z}/255\mathbb{Z})^* = 2 \cdot 4 \cdot 16$, (Gev. 6.16 gebruikt)
Voor $x \in (\mathbb{Z}/255\mathbb{Z})^*$: $\text{orde}(x) \mid 2 \cdot 4 \cdot 6$, dus orde($x$) is een 2-macht.
Het antwoord is <u>nee</u>.

(5) (c) orde($\overline{7}$): beeld in $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z}$: $(\overline{1}, \overline{2}, \overline{7})$
$\text{orde}(\overline{2} \text{ in } (\mathbb{Z}/5\mathbb{Z})^*) = 4$ want $\overline{2}^2 \neq 1$.
in $\mathbb{Z}/17\mathbb{Z}$: $\overline{7}^2 = \overline{49} = -\overline{2}$, $\overline{7}^4 = \overline{4}$, $\overline{7}^8 = \overline{16} = -\overline{1}$, $\overline{7}^{16} = \overline{1}$.
dus $\text{orde}(\overline{7} \text{ in } (\mathbb{Z}/17\mathbb{Z})^*) = 16$. Dus $\overline{7}^{16} = 1$ in $\mathbb{Z}/255\mathbb{Z}$, $\overline{7}^8 \neq 1$ in $\mathbb{Z}/255\mathbb{Z}$,
dus $\text{orde}(\overline{7} \text{ in } (\mathbb{Z}/255\mathbb{Z})^*) = 16$.

3. Ik gebruik de kleurformule v.d. formulekaart.

$\# G = \# D_7 = 2 \cdot 7 = 14$: $G = \{1, \rho, \ldots, \rho^6, \sigma, \sigma\rho, \ldots, \sigma\rho^6\}$

g	1	ρ	ρ^2	ρ^3	ρ^4	ρ^5	ρ^6	σ	$\sigma\rho$	$\ldots$	$\sigma\rho^6$
$\# \langle g \rangle \backslash Z$	7	1	1	1	1	1	1	4	4		4



$$\# G \backslash \{f : Z \to \{1, 2, \ldots, n\}\} = \frac{1}{14} \cdot \left(n^7 + 6 \cdot n + 7 \cdot n^4\right).$$

4.(a) $\# G = 77 = 7 \cdot 11$. De lengte van een baan is in $\{1, 7, 11, 77\}$. 77 kan niet: is te groot. Stel $X^G = \emptyset$, dan hebben de banen lengte 7 of 11. ~~[illegible]~~ Dus $30 = 7 \cdot a + 11 \cdot b$, $a, b \geq 0$.
30 is geen 7-voud, dus $b > 0$, maar ook 30 is geen 11-voud, dus $a > 0$
$12 = 7 \cdot (a-1) + 11 \cdot (b-1)$, zelfde argument. Tegenspraak. Dus $X^G \neq \emptyset$.

~~(b) Neem $h \in G$ met $g_2 = h g_1 h^{-1}$. Stel $g_1 x = x$, dan $g_2 h x = h g_1 h^{-1} h x = h g_1 x = h x$, dus $h x$.~~
Beter: laat $x \in X$, $g_2 x = x \iff h g_1 h^{-1} x = x \iff$ ~~$g_1 h^{-1} x = h^{-1} x \iff$~~
$\iff g_1 \cdot (h^{-1} x) = h^{-1} x$

5. $\# \mathrm{Hom}(C_7, S_9) = 1 + \#\, 7$ cykels in S_9 $= 1 + \binom{9}{2} \cdot 6! =$
$= 1 + \frac{9 \cdot 8}{2 \cdot 1} \cdot 6!$ is niet uit te schrijven.

$\# \mathrm{Hom}(C_6, A_5)$ (~~S_5~~)

$5 = 5$ ~~4+1~~ ~~3+2 ✓~~ 3+1+1 ✓ 2+2+1 ✓ ~~2+1+1+1 ✓~~ 1+1+1+1+1 ✓

6 = 6 ✓ ~~5+1 ✗~~ 4+2 ✗ ~~4+1+1 ✗~~ ~~3+3 ✓~~

~~3+2: 10·2~~
3+1+1: 10·2
2+2+1: 5·3 !!
~~2+1+1+1: 10~~
1 - 1 1

66. 76