Uitwerkingen tentamen Algebra 1, 27 juni 2013

Opmerkingen in het rood zijn geen onderdeel van de oplossing.

Opgave 1

a) We definiëren

$$a = 20^{13^{27^6}} = 20^{\left(13^{\left(27^6\right)}\right)}.$$

Wat is de rest van a bij deling door 27? Laat uiteraard ook je berekening zien.

Uitwerking. We gebruiken herhaaldelijk dat voor gehele getallen b, n met $\gcd(b,n) = 1$ en gehele exponenten k, l met $k \equiv l \pmod{\varphi(n)}$ geldt $b^k \equiv b^l \pmod{n}$. Dit volgt uit Stelling 6.17.

Omdat $\gcd(20, 27) = 1$, willen we dus eerst de exponent $e = 13^{27^6}$ bepalen modulo $\varphi(27) = \varphi(3^3) = (3-1)\cdot 3^2 = 18$. Omdat $\gcd(13, 18) = 1$, willen we dus eerst de exponent $f = 27^6$ bepalen modulo $\varphi(18) = \varphi(2\cdot 3^2) = \varphi(2)\cdot\varphi(3^2) = 6$. Voor de berekening van $\varphi(18)$, zie Stelling 6.15. Omdat $\gcd(27, 6) \neq 1$, kunnen we niet de allereerste opmerking gebruiken! Er geldt $f \equiv 0 \pmod 3$ en $f \equiv 1 \pmod 2$, dus (vanwege de Chinese Reststelling) $f \equiv 3 \pmod 6$. Je kunt het ook direct uitrekenen: modulo 6 geldt $27 \equiv 3$, dus $27^6 \equiv 3^6 \equiv (3^3)^2 \equiv 27^2 \equiv 3^2 \equiv 3$. Gegeven onze eerste opmerking volgt dus $e \equiv 13^3 \equiv (-5)^3 \equiv -125 \equiv 1 \pmod{18}$. Wegens diezelfde eerste opmerking volgt dus ook $a \equiv 20^1 \equiv 20 \pmod{27}$.

b) Bewijs dat voor $m = 15^3 = 3^3 \cdot 5^3 = 3375$ geldt $a \equiv 5^5 \pmod m$.

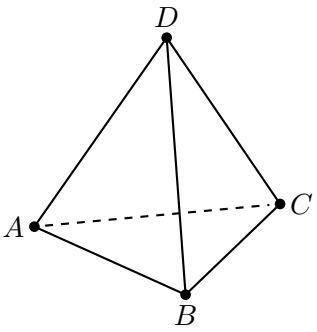
Uitwerking. Het is voldoende om te laten zien dat a en 5^5 congruent zijn modulo $27 = 3^3$ en ook modulo $125 = 5^3$, want wegens $\gcd(3^3, 5^3) = 1$ en de Chinese Reststelling zijn ze dan ook congruent modulo het product $3^3 \cdot 5^3 = 15^3$. Modulo 27 geldt $5^2 \equiv -2$, dus inderdaad

$$5^5 \equiv (5^2)^2 \cdot 5 \equiv (-2)^2 \cdot 5 \equiv 20 \equiv a.$$

Omdat 5 een deler is van 20 en $e \geq 3$, geldt $5^5 \equiv 0 \equiv a \pmod{5^3}$. Hiermee is het gevraagde bewezen.

Opgave 2

Zij T de tetraëder met hoekpunten A, B, C en D zoals in de figuur.
Zij $G = \mathrm{Sym}(T)$ de symmetriegroep van T.
Zij $g_0 \in G$ de spiegeling in het vlak door C, D en het midden van AB.
Zij $g_1 \in G$ de spiegeling in het vlak door A, B en het midden van CD.
Zij ℓ de lijn door D die loodrecht staat op het vlak door A, B en C.
Zij $g_2 \in G$ de draaiing om ℓ die A stuurt naar B.
Definieer $g_3 = g_1 \circ g_0$ en $g_4 = g_2 \circ g_1$.



a) Geef voor elke $0 \leq i \leq 4$ de permutatie van de hoekpunten die g_i induceert (als product van disjuncte cykels in $S(\{A, B, C, D\})$).

Uitwerking. De spiegelingen g_0 en g_1 corresponderen met respectievelijk (AB) en (CD). De draaiing g_2 correspondeert met (ABC) en de producten g_3 en g_4 krijgen we door de permutaties samen te stellen; die corresponderen dus met respectievelijk $(CD)(AB)$ en $(ABC)(CD) = (ABCD)$.

b) Voor elke $0 \leq i \leq 4$, zij $G_i = \langle g_i \rangle$ de ondergroep van G voortgebracht door g_i. Geef voor elke $0 \leq i \leq 4$ de banen van de werking van G_i op de verzameling $X = \{AB, AC, AD, BC, BD, CD\}$ van de zes zijden van T.

Uitwerking. We passen herhaaldelijk g_i toe op de zijden om de banen te vinden. De banen

zijn as volgt.

$$\begin{array}{ll} G_0 & \{AB\},\{CD\},\{AD,BD\},\{AC,BC\} \\ G_1 & \{AB\},\{CD\},\{AC,AD\},\{BC,BD\} \\ G_2 & \{AD,BD,CD\},\{AB,BC,AC\} \\ G_3 & \{AB\},\{CD\},\{AC,BD\},\{AD,BC\} \\ G_4 & \{AB,BC,CD,AD\},\{AC,BD\} \end{array}$$

c) Wat is de orde van G?

Uitwerking. We hebben al vaak gezien dat de groep G isomorf is met S_4 (zie bijvoorbeeld de eerste bladzijde van hoofdstuk 5 van het dictaat), dus de orde is 24.

d) Een Tibetaanse Tetraëder is een tetraëder waarvan alle zijvlakken geel zijn en elk van de zes zijden een kleur rood, blauw of groen heeft. We noemen twee Tibetaanse Tetraëders hetzelfde als ze door een symmetrie in elkaar over te voeren zijn. Hoeveel echt verschillende Tibetaanse Tetraëders zijn er?

Uitwerking. Met de banenformule vinden we dat het aantal gelijk is aan

$$\frac{1}{24}\sum_{g\in G}\chi(g),$$

waarbij $\chi(g)$ het aantal dekpunten is van g in de verzameling van alle 3^6 kleuringen van de tetraëder $ABCD$. Voor elementen g,h in dezelfde conjugatieklasse geldt $\chi(g)=\chi(h)$. In het dictaat worden de conjugatieklassen van S_4 expliciet gegeven, zie Voorbeeld 5.11. In de volgende tabel staan in de eerste twee kolommen een representant van elke conjugatieklasse en de grootte van de klasse. De elementen $\mathrm{id}, g_0, g_2, g_3, g_4$ zijn de gekozen representanten. De laatste kolom bevat $\chi(g)$, wat precies gelijk is aan 3^r met r gelijk aan het aantal banen zoals bepaald in **(b)**, want als een gekleurde tetraëder een dekpunt is van g_i, dan hebben de zijden in elke baan van X onder de werking van G_i dezelfde kleur.

g	#(klasse van g)	$\chi(g)$
id	1	3^6
g_0	6	3^4
g_2	8	3^2
g_3	3	3^4
g_4	6	3^2

We vinden dus

$$\frac{1}{24}\sum_{g\in G}\chi(g)=\frac{1}{24}\left(1\cdot 3^6+6\cdot 3^4+8\cdot 3^2+3\cdot 3^4+6\cdot 3^2\right)=66.$$

Opgave 3
Geef voor elke uitspraak óf een bewijs óf een tegenvoorbeeld. (Dit kan in een paar regels.)
Voor de zekerheid: de orde van een eenheidselement is 1; en 1 is een macht van 2, want $2^0 = 1$.
a) In elke abelse groep vormen de elementen van eindige orde een ondergroep.
b) In elke abelse groep vormen de elementen van oneindige orde samen met het eenheidselement een ondergroep.
c) In elke abelse groep vormen de elementen van (eindige) even orde samen met het eenheidselement een ondergroep.
d) In elke abelse groep vormen de elementen van (eindige) oneven orde een ondergroep.
e) In elke abelse groep vormen de elementen waarvan de orde een macht van 2 is een ondergroep.
f) In elke groep vormen de elementen waarvan de orde een macht van 2 is een ondergroep.
Uitwerking. In een abelse groep met elementen x en y van orde m en n geldt $(xy)^{mn} = x^{mn}y^{mn} = (x^m)^n(y^n)^m = e$, dus de orde van xy is een deler van mn. De inversen van x en y hebben ordes respectievelijk m en n. Omdat delers van oneven getallen oneven zijn en delers van machten van 2 zelf ook een macht van 2, volgt dat **(a), (d), (e)** waar zijn. Dit was zo goed als gelijk aan het argument voor huiswerkopgave 4.56. Voor de andere drie geven we een tegenvoorbeeld.
b) Neem bijvoorbeeld $\mathbb{R}^*$. Dan hebben alle elementen oneindige orde, behalve ± 1, dus zitten bijvoorbeeld $x = 2$ en $y = -2$ wel in de genoemde verzameling, maar $xy^{-1} = -1$ niet. De verzameling is dus geen ondergroep.
c) Neem bijvoorbeeld $\mathbb{Z}/6\mathbb{Z}$. Dan heeft $a = \overline{1}$ wel even orde (namelijk orde 6), maar $a + a = \overline{2}$ heeft orde 3 en zit dus niet in de genoemde verzameling, die dus geen ondergroep is.
f) Neem bijvoorbeeld S_3. De elementen waarvan de orde een macht van 2 is zijn, naast het eenheidselement, de transposities. Maar deze elementen vormen geen ondergroep; het product van twee transposities in S_3 heeft namelijk orde 3.

Opgave 4
a) Zij n een positief geheel getal en $g \in \mathbb{Z}/n\mathbb{Z}$ een element. Laat zien dat g een voortbrenger is van de additieve groep $\mathbb{Z}/n\mathbb{Z}$ dan en slechts dan als er geldt $g \in (\mathbb{Z}/n\mathbb{Z})^*$.
Uitwerking. Omdat $\overline{1}$ de additieve groep $\mathbb{Z}/n\mathbb{Z}$ voortbrengt, is een element g een voortbrenger dan en slechts dan als $\overline{1}$ bevat is in de additieve groep voortgebracht door g, dus dan en slechts dan als $\overline{1}$ een veelvoud is van g, dus dan en slechts dan als er een geheel getal a is zodanig dat

$$\overline{1} = \underbrace{g + g + \cdots + g}_{a} = \overline{a} \cdot g,$$

dus dan en slechts dan als g een eenheid is in $(\mathbb{Z}/n\mathbb{Z})^*$.
b) Zij n een positief geheel getal en C_n een cyclische groep van orde n. Concludeer uit **(a)** dat het aantal elementen $g \in C_n$ waarvoor geldt $C_n = \langle g \rangle$ gelijk is aan $\varphi(n)$.
Uitwerking. De groep C_n is isomorf met $\mathbb{Z}/n\mathbb{Z}$, dus het aantal elementen dat C_n voortbrengt is wegens **(a)** gelijk aan $\#(\mathbb{Z}/n\mathbb{Z})^* = \varphi(n)$.
c) Zij $p = 61$. Hoeveel primitieve wortels bevat het lichaam $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$?
Uitwerking. De groep $\mathbb{F}_p^*$ is cyclisch van orde $p - 1$, dus het aantal voortbrengers is wegens **(b)** gelijk aan $\varphi(p-1) = \varphi(60) = \varphi(3) \cdot \varphi(4) \cdot \varphi(5) = 16$ (Zie Stelling 6.15).
d) Is $\overline{2} \in \mathbb{F}_{61}$ een primitieve wortel?
Uitwerking. De orde k van het element $\overline{2}$ is een deler van de orde $p - 1 = 60 = 2^2 \cdot 3 \cdot 5$ van

de groep $\mathbb{F}_p^*$, dus als de orde k niet gelijk is aan 60, dan is k een deler van $60/2 = 30$ of van $60/3 = 20$ of van $60/5 = 12$. Modulo 61 geldt

$$\begin{aligned} 2^6 &\equiv 64 \equiv 3, \\ 2^{12} &\equiv (2^6)^2 \equiv 3^2 \equiv 9 \not\equiv 1, \\ 2^{20} &\equiv 2^{12} \cdot 2^6 \cdot 2^2 \equiv 9 \cdot 3 \cdot 4 \equiv 47 \not\equiv 1, \\ 2^{30} &\equiv (2^6)^5 \equiv 3^5 \equiv 243 \equiv -1 \not\equiv 1. \end{aligned}$$

De orde k is dus blijkbaar geen deler van 12, 20 of 30, dus geldt $k = 60$. Dat betekent dat $\overline{2}$ inderdaad een primitieve wortel is.

Opgave 5

a) Zij $f\colon G_1 \to G_2$ een homomorfisme van groepen. Laat $N \triangleleft G_2$ een normale ondergroep van G_2 zijn waarvoor het quotient G_2/N abels is. Bewijs dat het inverse beeld $f^{-1}(N)$ een normale ondergroep van G_1 is en dat de commutator ondergroep $[G_1, G_1]$ bevat is in $f^{-1}(N)$.

Uitwerking. Zij $\varphi\colon G_1 \to G_2/N$ de samenstelling van f met de quotiëntafbeelding $\pi\colon G_2 \to G_2/N$. Omdat N de kern is van π, volgt $f^{-1}(N) = f^{-1}(\pi^{-1}(0)) = \varphi^{-1}(0) = \ker\varphi$, dus $f^{-1}(N)$ is normaal wegens Propositie 4.12. Uit Stelling 8.5 (of zelfs de regel daarboven) volgt dat de commutatorondergroep $[G_1, G_1]$ bevat is in $\ker\varphi = f^{-1}(N)$. Je mag hier **niet** gebruik maken van een inverse f^{-1} van f, want die hoeft niet te bestaan!

b) Zij $\mathrm{GL}_2(\mathbb{R})$ de groep van inverteerbare reële 2×2-matrices en $\mathrm{SL}_2(\mathbb{R})$ de ondergroep van matrices van determinant 1. Zij n een positief geheel getal. Zoals gebruikelijk schrijven we S_n voor de permutatiegroep van $\{1, 2, \ldots, n\}$ en A_n voor de ondergroep van alle even permutaties. Stel $g\colon S_n \to \mathrm{GL}_2(\mathbb{R})$ is een homomorfisme. Bewijs dat $g(A_n)$ bevat is in $\mathrm{SL}_2(\mathbb{R})$.

Uitwerking. De groep $\mathrm{SL}_2(\mathbb{R})$ is de kern van de determinant-afbeelding $\det\colon \mathrm{GL}_2(\mathbb{R}) \to \mathbb{R}^*$, dus $\mathrm{SL}_2(\mathbb{R})$ is normaal in $\mathrm{GL}_2(\mathbb{R})$ wegens Propositie 4.12. Wegens de Isomorfiestelling 4.9 is het quotiënt $\mathrm{GL}_2(\mathbb{R})/\mathrm{SL}_2(\mathbb{R})$ isomorf met het beeld van de determinant-afbeelding in de abelse groep $\mathbb{R}^*$, dus dit quotiënt is zelf ook abels. Het quotiënt is isomorf met $\mathbb{R}^*$, want de determinant-afbeelding is surjectief. We mogen dus onderdeel **(a)** toepassen op de afbeelding $g\colon S_n \to \mathrm{GL}_2(\mathbb{R})$ met $G_1 = S_n$ en $G_2 = \mathrm{GL}_2(\mathbb{R})$ en $N = \mathrm{SL}_2(\mathbb{R})$. We concluderen dat de commutatorondergroep $[S_n, S_n]$ bevat is in $g^{-1}(N)$. Er geldt $[S_n, S_n] = A_n$ (zie Gevolg 8.6), dus geldt $A_n \subset g^{-1}(N)$ en dus $g(A_n) \subset N = \mathrm{SL}_2(\mathbb{R})$. Je kunt dit ook zonder onderdeel **(a)** bewijzen door te laten zien dat alle commutatoren in S_n een beeld onder g in $\mathrm{GL}_2(\mathbb{R})$ hebben dat determinant 1 heeft en dan te gebruiken dat $[S_n, S_n] = A_n$.