EXAMEN GETALTHEORIE – 9 JUNI 2020

- Leg je antwoorden helder uit en geef duidelijk aan welke resultaten je gebruikt.
- Dit examen bestaat uit **vier vragen**, genummerd van (1) tot en met (4), die elk bestaan uit verschillende deelvragen. **Elk van de vier vragen** moet op een apart blad worden beantwoord. Vergeet niet om op elk antwoordblad je naam te schrijven, en de bladen te nummeren. Je kladpapier hoef je **niet** in te dienen.
- Zelfs als je een onderdeel van een oefening niet kan oplossen, mag je het resultaat gebruiken in het vervolg van de oefening.
- Je mag je antwoorden schrijven in het Nederlands of in het Engels, zoals je verkiest.
- Je hebt voor dit examen **3 uur** de tijd (4 uur voor studenten met faciliteiten).

(1) (a) Zij a en b gehele getallen, niet beide 0; zij p een priemgetal, en zij $n \geq 3$ een oneven geheel getal.

(i) **(1 punt)** Definieer het Legendresymbool $\left(\frac{a}{p}\right)$ onder de veronderstelling dat p oneven is.

(ii) **(1 punt)** Definieer het Jacobisymbool $\left(\frac{a}{n}\right)$.

(iii) **(1 punt)** Definieer het Hilbertsymbool $\left(\frac{a,b}{p}\right)$.

(b) **(6 punten)** Zij a een geheel getal verschillend van 0. Toon voor elk geheel getal $b \geq 3$ dat onderling ondeelbaar is met $2a$ de volgende gelijkheid aan:

$$\left(\frac{a}{b}\right) = \prod_{p|2a} \left(\frac{a,b}{p}\right)$$

Hier loopt het product over alle priemgetallen p die $2a$ delen.

Oplossing: Beide leden van de gelijkheid zijn multiplicatief in b; we mogen dus veronderstellen dat b een priemgetal is dat geen deler is van $2a$. Omdat b positief is, geldt dat $\left(\frac{a,b}{\infty}\right) = 1$. Er volgt nu uit Hilbertreciprociteit dat

$$\prod_{p|2a} \left(\frac{a,b}{p}\right) = \prod_{p\nmid 2a} \left(\frac{a,b}{p}\right)$$

waar we in het rechterlid het product nemen over de priemen p die $2a$ niet delen. Voor zulke priemen geldt dat $\left(\frac{a,b}{p}\right) = 1$ als $p \neq b$ en $\left(\frac{a,b}{p}\right) = \left(\frac{a}{p}\right)$ als $b = p$.

(2) (a) **(6 punten)** Zij $r \in \mathbb{N} \setminus \{0\}$ en zij $p_1, \ldots, p_r$ priemgetallen congruent aan 4 modulo 5. Toon aan dat het natuurlijk getal

$$N = (2p_1 \cdots p_r)^2 - 5$$

deelbaar is door een priemgetal p dat congruent is aan 4 modulo 5.

(b) **(2 punten)** Toon nu aan dat er oneindig veel priemgetallen bestaan die congruent zijn aan 4 modulo 5, *zonder de stelling van Dirichlet te gebruiken.*

Oplossing: de oplossing is gelijkaardig aan het bewijs van Stelling 6.2.1 in de cursustekst.

(a) Het getal N is congruent aan 4 modulo 5 omdat $p_1, \ldots, p_r$ congruent zijn aan 4 modulo 5. Omdat $N > 1$ heeft N zeker een priemdeler p. Voor zo'n priemdeler p geldt dat $5 \equiv (2p_1 \cdots p_r)^2$ modulo p, zodat 5 een kwadratisch residu is modulo p. Uit kwadratische reciprociteit volgt nu dat p ook een kwadratisch residu is modulo 5. Dus p is congruent aan 1 of 4 modulo 5. Als alle priemdelers van N congruent zijn aan 1 modulo 5, dan is ook N congruent aan 1 modulo 5, wat in tegenspraak is met het feit dat $N \equiv 4$ modulo 5. Dus N heeft minstens één priemdeler die congruent is aan 4 modulo 5.

(b) Zij $p_1, \ldots, p_r$ priemgetallen die congruent zijn aan 4 modulo 5. Het volstaat aan te tonen dat er een priemgetal bestaat dat congruent is aan 4 modulo 5 en niet tot de verzameling $\{p_1, \ldots, p_r\}$ behoort. Definieer N als in (a) en zij p een priemdeler van N die congruent is aan 4 modulo 5. Dan kan p geen deler zijn van $p_1 \cdots p_r$, en dus ook niet tot de verzameling $\{p_1, \ldots, p_r\}$ behoren.

(3) (a) **(2 punten)** Formuleer het lemma van Hensel-Rychlik voor veeltermen in één veranderlijke.

(b) **(3 punten)** Zij p een priemgetal zodat $p \neq 3$. Zij a een element van $\mathbb{Q}_p^\times$ en stel $m = \mathrm{ord}_p(a)$. We noteren met b het beeld van $p^{-m}a$ onder de projectie-afbeelding

$$\pi\colon \mathbb{Z}_p \to \mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p.$$

Toon aan dat a een derde macht is in $\mathbb{Q}_p$ als en slechts als m deelbaar is door 3 en b een derde macht is in $\mathbb{F}_p$.

(c) **(6 punten)** Zij a een element in $\mathbb{Q}_3^\times$ en stel $m = \mathrm{ord}_3(a)$. Toon aan dat a een derde macht is in $\mathbb{Q}_3$ als en slechts als m deelbaar is door 3, en $3^{-m}a - 1$ of $3^{-m}a - 8$ deelbaar is door 9.

Oplossing: de oplossing is gelijkaardig aan het resultaat voor kwadraten in $\mathbb{Q}_p$ (lemma 4.3.4 in de cursustekst).

(b) "slechts als" : als $a = x^3$ met $x \in \mathbb{Q}_p^\times$ dan geldt $m = 3\mathrm{ord}_p(x)$, zodat m deelbaar is door 3. Omdat π een ringhomomorfisme is, geldt bovendien dat $b = (\pi(p^{-m/3}x))^3$ in $\mathbb{F}_p$, zodat b een derde macht is in $\mathbb{F}_p$.

"als" : omdat m deelbaar is door 3, is a een derde macht in $\mathbb{Q}_p$ als en slechts als $p^{-m}a$ een derde macht is in $\mathbb{Q}_p$. Door a te vervangen door $p^{-m}a$ mogen we dus veronderstellen dat $m = 0$. Kies een element c in $\mathbb{Z}_p^\times$ zodat $\pi(c)^3 = b$. Stel $f(x) = x^3 - a$ in $\mathbb{Z}_p[x]$. Dan geldt $f(c) \equiv 0$ modulo p terwijl $f'(c) = 3c^2 \not\equiv 0$ modulo p aangezien $p \neq 3$ en c niet deelbaar is door p in $\mathbb{Z}_p$. Uit het lemma van Hensel volgt nu dat de vergelijking $f(x) = 0$ een oplossing heeft in $\mathbb{Z}_p$; dus a is een derde macht in $\mathbb{Q}_p$.

(c) We bewijzen eerst een hulpresultaat: de derde machten in $(\mathbb{Z}/27\mathbb{Z})^\times$ zijn de elementen van de vorm $[u]_{27}$ met $u \equiv 1 \mod 9$ of $u \equiv 8 \mod 9$. Inderdaad, voor alle gehele getallen v en k geldt dat $(v + 9k)^3 \equiv v^3 \mod 27$, dus om alle derde machten te vinden in $(\mathbb{Z}/27\mathbb{Z})^\times$ hoeven we enkel de derde machten te berekenen van $[n]_{27}$ met $n \in \{1, 2, 4, -1, -2, -4\}$. Dit levert het gewenste resultaat op.

We bewijzen nu de "slechts als" implicatie: als $a = x^3$ met $x \in \mathbb{Q}_3^\times$ dan geldt $m = 3\mathrm{ord}_3(x)$, zodat m deelbaar is door 3. Omdat de projectie-afbeelding $\pi_3\colon \mathbb{Z}_3 \to \mathbb{Z}/27\mathbb{Z}$ gegeven door reductie modulo 27 een ringhomomorfisme is, moet $\pi_3(3^{-m}a)$ een derde macht zijn in $(\mathbb{Z}/27\mathbb{Z})^\times$. Uit ons hulpresultaat volgt nu dat $3^{-m}a - 1$ of $3^{-m}a - 8$ deelbaar is door 9.

We bewijzen ten slotte de "als" implicatie: we mogen opnieuw veronderstellen dat $m = 0$. Dankzij ons hulpresultaat kunnen we een element c in $\mathbb{Z}_3^\times$ kiezen zodat $\pi_3(c)^3 = \pi_3(a)$. Stel $f(x) = x^3 - a$ in $\mathbb{Z}_3[x]$. Dan geldt $f(c) \equiv 0$ modulo 3^3 terwijl $\mathrm{ord}_3(f'(c)) = \mathrm{ord}_3(3c^2) = 1$. Uit het lemma van Hensel-Rychlik (met $e = 1$) volgt nu dat de vergelijking $f(x) = 0$ een oplossing heeft in $\mathbb{Z}_3$; dus a is een derde macht in $\mathbb{Q}_3$.

(4) Zij P een eindige verzameling priemgetallen.

(a) **(2 punten)** Zij x_p een element in $\mathbb{Z}_p$, voor elke p in P. Toon aan dat er voor elke $m \in \mathbb{N}$ een geheel getal a bestaat zodat $\mathrm{ord}_p(x_p - a) \geq m$ voor alle p in P.

(b) **(2 punten)** Voor elke p in P noteren we met $|\cdot|_p$ de p-adische absolute waarde op $\mathbb{Q}_p$. Zij x_p een element in $\mathbb{Q}_p$, voor elke p in P. Toon aan dat er voor elke $\varepsilon > 0$ een rationaal getal a bestaat zodat $|x_p - a|_p < \varepsilon$ voor alle p in P.

(c) **(8 punten)** Verfijn nu je resultaat uit de vorige oefening op de volgende manier. We noteren met $|\cdot|_\infty$ de gebruikelijke absolute waarde op $\mathbb{R}$. Zij x_∞ een reëel getal, en zij x_p een element in $\mathbb{Q}_p$, voor elke p in P. Toon aan dat er voor elke $\varepsilon > 0$ een rationaal getal b bestaat zodat $|x_p - b|_p < \varepsilon$ voor alle p in $P \cup \{\infty\}$.

Oplossing: (a) Voor elke p in P kiezen we een geheel getal y_p zodat $y_p - x_p$ deelbaar is door p^m in $\mathbb{Z}_p$. Uit de Chinese reststelling volgt dat er een geheel getal a bestaat zodat $y_p \equiv a$ modulo p^m voor alle p in P. Dan geldt ook dat $x_p \equiv a$ modulo p^m voor alle p in P, of dus $\mathrm{ord}_p(x_p - a) \geq m$ voor alle p in P.

(b) Zij m een natuurlijk getal zodat $p^{-m} < \varepsilon$ voor alle p in P. We kiezen ook een natuurlijk getal n zodat $p^n x_p$ in $\mathbb{Z}_p$ ligt voor alle p in P. Uit (a) volgt dat we een geheel getal b kunnen vinden zodat $\mathrm{ord}_p(p^n x_p - b) \geq m + n$ voor alle p in P. Voor $a = p^{-n} b$ geldt dan dat

$$|x_p - a|_p = p^n |p^n x_p - b|_p \leq p^n p^{-m-n} < \varepsilon.$$

(c) Zij m een natuurlijk getal zodat $p^{-m} < \varepsilon$ voor alle p in P. Wegens (b) kunnen we een element a in $\mathbb{Q}$ kiezen zodat $|x_p - a|_p \leq p^{-m} < \varepsilon$ voor alle p in P. Als r een rationaal getal is van de vorm $(\prod_{p \in P} p^m)u/v$ met u en v gehele getallen zodat v niet deelbaar is door een priemgetal in P, dan zal $|r|_p \leq p^{-m} < \varepsilon$ voor alle p in P. Dus voor $b = a + r$ geldt dan dat

$$|x_p - b|_p \leq \max\{\, |x_p - a|_p,\, |r|_p \,\} < \varepsilon.$$

We gaan nu u en v kiezen zodat $|x_\infty - b|_\infty < \varepsilon$.

Zij q een priemgetal dat niet tot P behoort. Voor elk geheel getal $n > 0$ en elk reëel getal z kunnen we $d \in \mathbb{Z}$ vinden zodat $|z - d/q^n|_\infty < 1/q^n$. We kiezen n voldoende groot zodat $q^{-n} < \varepsilon / \prod_{p \in P} p^m$ en we stellen $z = (x_\infty - a)/\prod_{p \in P} p^m$. Kies $d \in \mathbb{Z}$ zodat $|z - d/q^n|_\infty < 1/q^n$. Voor $u = d$, $v = q^n$ en $r = (\prod_{p \in P} p^m)u/v$ voldoet $b = a + r$ aan

$$|x_\infty - b|_\infty = |z - \frac{d}{q^n}|_\infty \prod_{p \in P} p^m < \varepsilon.$$

Totaal: 40 punten