Naam:

EXAMEN GETALTHEORIE – 22 JUNI 2020

- Leg je antwoorden helder uit en geef duidelijk aan welke resultaten je gebruikt.
- Dit examen bestaat uit **drie vragen**, genummerd van (1) tot en met (3), die elk bestaan uit verschillende deelvragen. **Elk van de drie vragen** moet op een apart blad worden beantwoord. Vergeet niet om op elk opgavenblad en 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.

(1) Zij $n \in \mathbb{Z}_{\geq 2}$.

(a) **(2 punten)** Zij a een geheel getal. Wanneer zeggen we dat n een Fermat pseudopriem is ten opzichte van a?

(b) **(4 punten)** Zij p een priemgetal. Toon aan dat het aantal oplossingen van de vergelijking $x^{n-1} = 1$ in het veld $\mathbb{F}_p$ gelijk is aan $\text{ggd}(n-1, p-1)$.

(c) **(4 punten)** Zij p een priemdeler van n, en zij $e \in \mathbb{Z}_{>0}$. Toon aan dat het aantal oplossingen van de vergelijking $x^{n-1} = 1$ in de ring $\mathbb{Z}/p^e\mathbb{Z}$ gelijk is aan $\text{ggd}(n-1, p-1)$.

(d) **(4 punten)** Zij $n = p_1^{e_1} \cdots p_r^{e_r}$ de priemontbinding van n, waarbij $p_1, \ldots, p_r$ onderling verschillende priemgetallen zijn, en de exponenten $e_1, \ldots, e_r$ strikt positieve gehele getallen. Zij F de verzameling van restklassen $[a]_n$ in $\mathbb{Z}/n\mathbb{Z}$ zodat n een Fermat pseudopriem is ten opzichte van a. Toon aan dat F precies $\prod_{i=1}^{r} \text{ggd}(n-1, p_i - 1)$ elementen heeft.

Oplossing: (b) Zij g een generator van $\mathbb{F}_p^\times$. Voor elk geheel getal m geldt dat $(g^m)^{n-1} = 1$ als en slechts als $m(n-1)$ een veelvoud is van $p-1$; dus als en slechts als m een veelvoud is van

$$(p-1)/\text{ggd}(n-1, p-1).$$

In de verzameling $\{1, \ldots, p-1\}$ zijn er precies $\text{ggd}(n-1, p-1)$ elementen m die aan deze eigenschap voldoen.

(c) We bewijzen dit via inductie op e. Voor $e = 1$ is dit het resultaat uit (b). Stel dus dat $e > 1$ en dat het aantal oplossingen van de vergelijking $x^{n-1} = 1$ in de ring $\mathbb{Z}/p^{e-1}\mathbb{Z}$ gelijk is aan $\text{ggd}(n-1, p-1)$. Stel $f(x) = x^{n-1} - 1$ in $\mathbb{Z}[x]$ en zij a een element in $\mathbb{Z}$ zodat $f(a) \equiv 0$ modulo p^{e-1}. Dan is a niet deelbaar door p, en ook $n-1$

is niet deelbaar door p omdat p een priemdeler is van n. Hieruit volgt dat $\mathrm{ord}_p f'(a) = 0$. Uit het lemma van Hensel volgt nu dat er een uniek element b in $\mathbb{Z}/p^e\mathbb{Z}$ bestaat zodat $f(b) = 0$ en $a \equiv b$ modulo p^{e-1}. Met andere woorden, elke oplossing modulo p^{e-1} lift naar een unieke oplossing modulo p^e. Hieruit volgt dat het aantal oplossingen van de vergelijking $x^{n-1} = 1$ in de ring $\mathbb{Z}/p^e\mathbb{Z}$ ook gelijk is aan $\mathrm{ggd}(n-1, p-1)$.

(d) Dit volgt uit (c) en de Chinese Reststelling: de verzameling F staat in bijectie met de verzameling van r-tallen

$$([a_1]_{p_1^{e_1}}, \ldots, [a_r]_{p_r^{e_r}})$$

zodat $[a_i]_{p_i^{e_i}}$ een oplossing is van de vergelijking $x^{n-1} = 1$ in $\mathbb{Z}/p_i^{e_i}\mathbb{Z}$ voor elke i in $\{1, \ldots, r\}$.

Naam:

(2) (a) **(2 punten)** Geef de definitie van de complexe Riemann zetafunctie $\zeta(s)$.

(b) **(6 punten)** De *Dirichlet etafunctie* is de holomorfe functie

$$\eta\colon \{s \in \mathbb{C} \mid \Re(s) > 0\} \to \mathbb{C},\ s \mapsto \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n^s}.$$

Je mag vrij gebruiken dat de reeks in deze definitie convergeert voor alle s in het domein. Bewijs dat $\eta(s) = (1 - 2^{1-s})\zeta(s)$ voor alle $s \in \mathbb{C}$ met $\Re(s) > 1$. *Hint: schrijf $\eta(s)$ in termen van L-functies.*

Oplossing: Zij χ_0 het triviale Dirichletkarakter modulo 2. Dan geldt per definitie dat

$$L(s, \chi_0) = \sum_{k=0}^{\infty} \frac{1}{(2k+1)^s}$$

voor alle s in $\mathbb{C}$ met $\Re(s) > 1$. Dus $\eta(s) = 2L(s, \chi_0) - \zeta(s)$. Het Eulerproduct van $L(s, \chi_0)$ wordt gegeven door

$$L(s, \chi_0) = \prod_{p \text{ oneven}} \frac{1}{1 - p^{-s}} = (1 - 2^{-s})\zeta(s),$$

zodat $\eta(s) = 2L(s, \chi_0) - \zeta(s) = (1 - 2^{1-s})\zeta(s)$.

Naam:

(3) (a) **(2 punten)** Zij m een strikt positief geheel getal. Geef de definitie van een *Dirichletkarakter modulo m.*

(b) **(2 punten)** Zij p een oneven priemgetal, en zij a een geheel getal. Definieer het *Legendresymbool* $\left(\frac{a}{p}\right)$.

(c) **(8 punten)** Zij a een oneven natuurlijk getal dat niet deelbaar is door het kwadraat van een priemgetal, en stel $m = 4a$. Toon aan dat er een uniek Dirichletkarakter χ_a modulo m bestaat zodat $\chi_a(p) = \left(\frac{a}{p}\right)$ voor elk priemgetal p dat geen deler is van m. Toon aan dat χ_a niet triviaal is als $a \neq 1$.

(d) **(6 punten)** Zij a een oneven natuurlijk getal dat geen kwadraat is. Bewijs dat er oneindig veel oneven priemgetallen p bestaan zodat $\left(\frac{a}{p}\right) = 1$, en ook oneindig veel oneven priemgetallen q zodat $\left(\frac{a}{q}\right) = -1$.

Oplossing: (c) Uniciteit volgt uit het feit dat we elk element in $(\mathbb{Z}/m\mathbb{Z})^\times$ kunnen schrijven als een product van elementen van de vorm $[p]_m$ met p een priemgetal dat m niet deelt. We tonen het bestaan van χ_a aan met behulp van het Jacobisymbool. We zouden willen schrijven dat

$$\chi_a([x]_m) = \left(\frac{a}{x}\right)$$

voor alle gehele getallen x die onderling ondeelbaar zijn met m, maar dit Jacobisymbook is niet gedefineerd wanneer x even is of $x \leq 1$, en het is ook niet duidelijk dat deze definitie enkel afhangt van x modulo m. We gebruiken daarom kwadratische reciprociteit om het rechterlid te herschrijven in een goed gedefinieerde vorm.

Voor $a = 1$ stellen we χ_a gelijk aan het triviale karakter. Als $a \geq 3$ dan stellen we

$$\chi_a([x]_m) = (-1)^{\frac{a-1}{2}\frac{x-1}{2}} \left(\frac{x}{a}\right)$$

voor elk geheel getal x dat onderling ondeelbaar is met m. Dit is goed gedefinieerd omdat de eerste factor enkel afhangt van x modulo 4, en het Jacobisymbool enkel afhangt van x modulo a, zodat het product enkel afhangt van x modulo $m = 4a$. Aangezien zowel het Jacobisymbool als de factor $(-1)^{\frac{x-1}{2}}$ multiplicatief zijn in x, bekomen we zo een groepshomomorfisme

$$\chi_a \colon (\mathbb{Z}/m\mathbb{Z})^\times \to \{\pm 1\} \subset \mathbb{C}^\times.$$

Als p een oneven priemgetal is dat a niet deelt, dan volgt uit kwadratische reciprociteit dat $\chi_a(p) = \left(\frac{a}{p}\right)$.

We tonen nu aan dat χ_a niet triviaal is als $a \neq 1$. We kiezen een oneven priemgetal q_0 dat a deelt en gebruiken de Chinese Reststelling om een geheel getal x te vinden dat onderling ondeelbaar is met m en voldoet aan $\left(\frac{x}{q_0}\right) = -1$, en zodat x congruent is aan 1 modulo $4a/q_0$. Dan geldt $\chi_a([x]_m) = -1$. We hebben hier gebruikt dat q_0 geen deler

Naam:

is van $4a/q_0$ aangezien a niet deelbaar is door het kwadraat van een priemgetal.

(d) We mogen veronderstellen dat a kwadraatvrij is, omdat a delen door een kwadraat geen invloed heeft op $\left(\frac{a}{p}\right)$ als p een priengetal is dat geen deler is van a. Zij χ_a het Dirichletkarakter modulo $m = 4a$ uit punt (2), en noteer met $H \subset (\mathbb{Z}/m\mathbb{Z})^\times$ de kern van χ_a. Aangezien χ_a niet triviaal is, is H een strikte deelgroep van $(\mathbb{Z}/m\mathbb{Z})^\times$. Voor elk oneven priemgetal p geldt dat $\left(\frac{a}{p}\right) = 1$ als en slechts als $[p]_m \in H$. Elke congruentieklas in H bevat oneindig veel priemgetallen wegens de stelling van Dirichlet, en hetzelfde geldt voor elke congruentieklas in $(\mathbb{Z}/m\mathbb{Z})^\times \setminus H$.

Totaal: 40 punten