

Examen number theory + oplossingen van student

Funny numbers go brrrr

16 juni 2025

Informatie

Het examen zelf was in het engels opgesteld en moest in het engels beantwoord worden¹. Het examen was gesloten boek en we kregen 4 uur. Achteraan zullen ook oplossingen van de auteur en een vriend toegevoegd worden eens ik daar meer zin in heb, merk wel op dat deze dus fout kunnen zijn.

Vragen

Vraag 1 (3 pt.) Zij p een oneven priemgetal. Toon aan dat er evenveel kwadraten als niet-kwadraten zijn modulo p .

Vraag 2 (3 pt.) Formuleer Hensel's lemma en gebruik het om aan te tonen dat -2 een vierkantswortel heeft in $\mathbb{Z}_3$.

Vraag 3 (2 pt.) Beschouw de rij $a_n := \frac{5^n}{5^n - 1} + 2$. Bepaal de limiet in $\mathbb{Q}_5$ en in $\mathbb{R}$. Geef vervolgens een rationale rij die convergeert naar 0 in zowel $\mathbb{Q}_2$ als $\mathbb{Q}_3$ maar convergeert naar 1 in $\mathbb{R}$.

Vraag 4 (7 pt.) We zullen in deze vraag de oplossingen van de Diophantische vergelijking $y^2 = x^3 - 1$ bepalen in $\mathbb{Z}$.

a) (1 pt.) Toon aan dat voor een oplossing $(x, y) \in \mathbb{Z}^2$ voor de vergelijking geldt dat x oneven is en y even.

b) (1 pt.) Factoriseer $y^2 + 1$ over $\mathbb{Z}[i]$.

c) (3 pt.) Toon aan dat de factoren die je in de vorige deelvraag gevonden hebt relatief priem zijn (d.w.z. geen irreducibele factoren delen) in $\mathbb{Z}[i]$. Je mag hiervoor gebruiken dat de norm $N : \mathbb{Z}[i] \rightarrow \mathbb{Z}$ gedefinieerd door $N(a + bi) = a^2 + b^2$ multiplicatief is.

d) (2 pt.) Concludeer dat een van de factoren een derde macht moet zijn in $\mathbb{Z}[i]$ en bepaal dan alle oplossingen van $y^2 = x^3 - 1$ in $\mathbb{Z}$.

¹Echter zal ik het examen in het nederlands geven gezien mijn engelse spelling famous achteruit gegaan is de afgelopen paar jaren.

Vraag 5 (6 pt.) Zij voor deze oefening p een oneven priem en $a \in \mathbb{Z}$ niet deelbaar door p . We gebruiken voor deze oefening een variant van het delingsalgoritme dat zegt dat er unieke $q, r \in \mathbb{Z}$ zijn en $\epsilon = \pm 1$ zodat $a = qp + \epsilon r$ en $0 \leq r \leq \frac{p}{2}$.

a) (2 pt.) Toon aan dat $\epsilon = (-1)^{\lfloor \frac{2a}{p} \rfloor}$.

b) (3 pt.) Voor elke $k = 1, \dots, \frac{p-1}{2}$ kunnen we nu een $r_k \in \{1, \dots, \frac{p-1}{2}\}$ vinden zodat $ak \equiv (-1)^{\lfloor \frac{2ak}{p} \rfloor} r_k \pmod{p}$. Toon nu aan dat $a^{\frac{p-1}{2}} \equiv (-1)^S \pmod{p}$, waarbij $S = \sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{2ak}{p} \rfloor$.

c) (1 pt.) Concludeer dat $\left(\frac{a}{p}\right) = (-1)^S$.

Vraag 6 (6 pt.) Zij $a_1, a_2, a_3 \in \mathbb{Q}_p^\times$ met p een oneven priem² en stel $f = a_1x_1^2 + a_2x_2^2 + a_3x_3^2$. Toon aan dat f een niet triviaal nulpunt heeft in $\mathbb{Q}_p$ als en slechts als de volgende gelijkheid van Hilbert symbolen geldt:

$$\left(\frac{-1, a_1a_2a_3}{p}\right) = \prod_{i < j} \left(\frac{a_i, a_j}{p}\right).$$

Vraag 7 (3 pt.) Zij p priem zodat $p = a^2 + b^2 = c^2 + d^2$ voor gehele getallen a, b, c en d . Toon aan dat (a, b) en (c, d) op teken en permutatie na gelijk zijn.

Hint (ook op het examen): Factoriseer over $\mathbb{Z}[i]$ en gebruik het feit dat deze ring een UFD is.

²Origineel was de vraag voor algemene p , maar de assistent heeft tijdens het verloop van het examen gezegd dat het voldoende was deze oefening op te lossen voor $p \neq 2$ aangezien dit geval blijkbaar snel ingewikkeld kon worden.