

GETALTHEORIE
(07/06/2010 (14u-18u))

(1) [*Theorie-vraag, mondeling te verdedigen*]

(a) Op pagina 47, Dan heeft $ax^2 + by^2 = z^2$ een oplossing $(x_0, y_0, z_0) \in \mathbf{Z}^3 \setminus p\mathbf{Z}^3$. Leg dat in detail uit.

(b) Op pagina 62, de derde zin. Het is gemakkelijk om in te zien dat s en $\bar{s}$ niet geassocieerd zijn, want anders zou $\bar{s}/s = \pm 1$ of $\pm i$, wat onmogelijk is want $s = x + iy$ met $x, y \in \mathbb{Z}$ en $x^2 + y^2 = p$.

(2) Zij p een priemgetal en beschouw $\mathbb{Z}_p^\times = S_1 \cup S_2$ als disjuncte unie van 2 niet lege verzamelingen waarvoor de volgende eigenschappen gelden:

(a) Het product van 2 elementen uit S_i , $i = 1, 2$, zit in S_1 ,

$$\forall i : \forall a, b \in S_i : a.b \in S_1.$$

(b) Het product van een element uit de ene met een element uit de andere verzameling zit in S_2 ,

$$\forall a \in S_1, \forall b \in S_2 : a.b \in S_2.$$

Toon aan dat S_1 precies de verzameling kwadraten in $\mathbb{Z}_p^\times$ is.

(3) Bekijk de Taylorreeks van $-\log(1-x)$:

$$-\log(1-x) = \sum_{i=1}^{\infty} \frac{x^i}{i}.$$

Toon aan dat het convergentiegebied van deze functie op $\mathbb{Q}_p$ precies $C = \{x \in \mathbb{Q}_p : \text{ord}(x) > 0\}$ is.

(4) Welke priemgetallen p zijn te schrijven als $p = x^2 - 7y^2$ met $x, y \in \mathbb{Q}$. Geef van de twee kleinste zulke p_1 en p_2 telkens een bijbehorende oplossing (x_1, y_1) en (x_2, y_2) .

(5) Zij $p > 5$ een willekeurig priemgetal. Toon het volgende aan:

(a) Als $p \equiv \pm 5 \pmod{5}$, is 5 geen generator van $\mathbb{Z}_p^\times$.

(b) Als $p \equiv \pm 2 \pmod{5}$ en p is van de vorm $2q+1$ met q ook priem, dan is 5 wel een generator van $\mathbb{Z}_p^\times$.