Getaltheorie

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

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

(a) In het bewijs van de reciprociteitswet van Gauss, op pagina 26, de voorlaatste regel, staat er "De te bewijzen gelijkheid volgt nu direct.". Leg dat in detail uit.

(b) Aangaande Eigenschap 6.44, op pagina 37: bewijs in detail waarom $\mathbb{Q}$ dicht ligt in $\mathbb{Q}_p$. (Dat wordt in de cursustekst niet volledig uitgelegd.)

(2) Zij p een oneven priemgetal en $q > 1$ het kleinste kwadratisch nonresidu modulo p. Toon aan dat q priem is, en dat $q < \sqrt{p} + 1$.

(3) Zij $m > 1$ een natuurlijk getal waarvoor geldt dat $\mathbb{Z}_m^\times$ niet cyclisch is. Toon aan dat $a^{\frac{\varphi(m)}{2}} \equiv 1 \bmod m$ voor elke $a \in \mathbb{Z}$ met $\gcd(a, m) = 1$.

(4) Beschrijf alle gehele oplossingen van $x^2 - 2x - 6y^2 = 9$, zodanig dat elke oplossing precies eenmaal voorkomt in je beschrijving.

(5) Zij $a > 2$ een oneven kwadraatvrij geheel getal. We ontbinden a in priemfactoren als $a = r_1 r_2 \cdots r_m$. Zij $q_1, q_2, \ldots, q_k$ onderling verschillende oneven priemgetallen zodanig dat $\left(\frac{a}{q_i}\right) = -1$ voor elke i. Kies tenslotte $c \in \mathbb{Z}$ zodat $\left(\frac{c}{r_m}\right) = -1$ en neem $b > 1$ als oplossing van het stelsel van volgende $k + 1 + m$ congruenties

$$\begin{cases} x \equiv 1 \bmod q_i & \text{voor } i = 1, \ldots, k \\ x \equiv 1 \bmod 4 & \\ x \equiv 1 \bmod r_i & \text{voor } i = 1, \ldots, m-1 \\ x \equiv c \bmod r_m & \end{cases}$$

(a) Toon aan dat b een priemfactor p heeft waarvoor geldt dat $\left(\frac{a}{p}\right) = -1$.

(b) Leid uit (a) af dat er oneindig veel priemgetallen q bestaan met $\left(\frac{a}{q}\right) = -1$.

Voor de ongelijkheid in vraag (2) kon een hint gevraagd worden. Deze luidde als volgt:

Bekijk de rij $q, 2q, \ldots, (q-1)q$.