Herkansing Elementaire Getaltheorie (WISB321)

Tentamen, 21 december 2015, 9:00 -12:00 uur

Bij dit tentamen is gebruik van boeken, dictaat of aantekeningen niet toegestaan. Als rekenhulp kun je een eenvoudige calculator gebruiken (dus geen GR of smartphone). Als je een onderdeel mist mag je wel het resultaat ervan in de volgende onderdelen gebruiken.
Motiveer je antwoorden!
Veel succes!

1. (a) (1 pt) Bepaal de kleinste $x \in \mathbb{N}$ zó dat

$$3x \equiv 7 \pmod{35}, \qquad 4x \equiv 31 \pmod{45}, \qquad x \equiv 28 \pmod{63}$$

   (b) (1 pt) Zij $a_1, a_2 \in \mathbb{Z}$ en $m_1, m_2 \in \mathbb{N}$. Bewijs dat het stelsel congruetievergelijkingen

$$x \equiv a_1 (\text{mod } m_1) \qquad x \equiv a_2 (\text{mod } m_2)$$

   een oplossing heeft dan en slechts dan als $\text{ggd}(m_1, m_2)$ een deler is van $a_1 - a_2$.

2. (a) (1 pt) Bepaal een primitieve wortel modulo 23.

   (b) (1 pt) Zij q een priemgetal van de vorm $q = 2p + 1$ met p oneven priem. Zij $a \in \mathbb{Z}$ met $a \neq 0, \pm 1 (\text{mod } q)$. Bewijs dat

$$a \text{ is primitieve wortel modulo } q \iff -a \text{ is géén primitieve wortel modulo } q.$$

3. Zij gegeven $a, m \in \mathbb{N}$.

   (a) (1 pt) Bepaal de oplossing van $x^2 - 14y^2 = 1$ in $x, y \in \mathbb{N}$ met minimale y.

   (b) (1 pt) Bepaal $\alpha \in \mathbb{R}$ zó dat α de zuiver periodieke kettingbreuk $[\overline{3, 1, 2}]$ heeft.

4. (2 pt) Geef met $P(n)$ de grootste priemdeler van n aan. Zij $A \in \mathbb{N}$. Neem aan dat het abc-vermoeden waar is. Bewijs dat $P(x^2 + a)$ naar ∞ gaat als $x \in \mathbb{N}$ naar ∞ gaat.

   Beschouw eerst het geval $\text{ggd}(x^2, a) = 1$ (3/2 pt) en daarna het algemene geval.

5. In de volgende opgaven mag je de priemgetalstelling gebruiken.

   (a) (1 pt) Bewijs dat er een $A > 0$ en een $n_1 > 0$ bestaat zó dat

$$\text{kgv}(1, 2, 3, \ldots, n) < A^n \qquad \text{voor alle } n > n_1.$$

   (b) (1 pt) Bewijs dat er een $B > 1$ en een $n_2 > 0$ bestaat zó dat

$$\text{kgv}(1, 2, 3, \ldots, n) > B^n \qquad \text{voor alle } n > n_2.$$