

# Deeltentamen Elementaire Getaltheorie, 17-11-2006, 14-17 uur

Tijdens dit tentamen mogen boek en aantekeningen niet gebruikt worden. Alleen een eenvoudige calculator is toegestaan. Geef een goede onderbouwing van je antwoorden. Succes!

1. (1 pt) Bepaal alle  $x, y \in \mathbb{Z}$  die voldoen aan de vergelijking  $13x + 49y = 1$ .

2. (1 pt) Bepaal het kleinste positief gehele getal  $x$  zó dat  $x$  tegelijkertijd aan de volgende vergelijkingen voldoet,

$$x \equiv 5 \pmod{9}, \quad x \equiv 3 \pmod{4}, \quad x \equiv 11 \pmod{15}.$$

3. (2 pt) Zij  $a, k, l, m \in \mathbb{Z}_{>1}$  en stel dat

$$a^k \equiv 1 \pmod{m} \quad a^l \equiv 1 \pmod{m}.$$

Zij  $d = \text{ggd}(k, l)$ .

(a) Bewijs dat  $a^d \equiv 1 \pmod{m}$ .

(b) Bewijs, gebruikmakend van onderdeel (a), dat voor elk drietal  $a, k, l \in \mathbb{Z}_{>1}$  geldt dat

$$\text{ggd}(a^k - 1, a^l - 1) = a^{\text{ggd}(k, l)} - 1.$$

4. (2 pt) Zij  $a \in \mathbb{Z}$  en stel dat  $\text{ggd}(a, 10) = 1$ .

(a) Bewijs dat  $a^{1000} \equiv 1 \pmod{10000}$ .

(b) Bepaal de laatste vier cijfers van  $7^{1000}$ .

(c) Bepaal ook de laatste vier cijfers van  $2^{1000}$ .

5. (2 pt) Zij  $p$  een oneven priemgetal.

(a) Zij  $g \in \mathbb{Z}$  zó dat  $g \pmod{p}$  een primitieve wortel modulo  $p$  is. Bewijs dat  $\text{ord}_{p^2}(g)$  gelijk is aan  $p - 1$  of aan  $p(p - 1)$ .

(b) Bewijs dat  $\text{ord}_{p^2}(p + 1) = p$ .

(c) Bewijs, gebruikmakend van de vorige twee onderdelen, dat er een primitieve wortel modulo  $p^2$  bestaat.

6. (2pt)

- (a) Voor welke priemgetallen is 5 een kwadraatrest ?
- (b) Zij  $p$  een priemgetal zó dat  $q = 2p + 1$  priem is en zo dat  $p \equiv 1 \pmod{5}$ . Bewijs dat 5 een primitieve wortel modulo  $q$  is.