Departement Wiskunde, Faculteit Bètawetenschappen, UU.
In elektronische vorm beschikbaar gemaakt door de TBC van A–Eskwadraat.
Het college WISB321 werd in 2006/2007 gegeven door Frits Beukers.

Elementaire Getaltheorie (WISB321)
17 november 2006

Opgave 1 *(1 punt)*

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

Opgave 2 *(1 punt)*

Bepaal het kleinste positieve gehele getal x zodat x tegelijkertijd aan de volgende vergelijkingen voldoet:

$$x \equiv 5 (\mathrm{mod}\ 9), \quad x \equiv 3 (\mathrm{mod}\ 4), \quad x \equiv 11 (\mathrm{mod}\ 15)$$

Opgave 3 *(2 punten)*

Zij $a, k, l, m \in \mathbb{Z}_{>1}$ en stel dat

$$a^k \equiv 1 (\mathrm{mod}\ m) \quad a^l \equiv 1 (\mathrm{mod}\ m)$$

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

a) Bewijs dat $a^d \equiv 1 (\mathrm{mod}\ m)$

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

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

Opgave 4 *(2 punten)*

Zij $a \in \mathbb{Z}$ en stel dat $\mathrm{ggd}(a, 10) = 1$

a) Bewijs dat $a^{1000} \equiv 1 (\mathrm{mod}\ 10000)$

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

c) Bepaal ook de laatste vier cijfers van $2^{1000} - 1$

Opgave 5 *(2 punten)*

Zij p een oneven priemgetal.

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

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

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

Opgave 6 *(2 punten)*

a) Voor welke priemgetallen is 5 een kwadraatrest?

b) Zij p een priemgetal zodat $q = 2p + 1$ priem is en zodat $p \equiv 1 (\mathrm{mod}\ 5)$.
Bewijs dat 5 een primitieve wortel modulo q is.