TW 314 (Toegepaste Diskrete Wiskunde)

Tutoriaal 10: 4 Mei 2017

---

1. Gebruik die Euklidiese algoritme om ggd(1764, 225) en ggd(1764, 625) te bepaal. Vind dan die multiplikatiewe inverses van 225 en 625 (mod 1764), as hulle bestaan.

2. Bepaal die Euler phi funksies van 1764 en 503.

3. Let op dat 14 en 15 relatief priem is en $14 \times 15 = 210$, en dat $9 \in \mathbb{Z}_{14}^*$ en $1 \in \mathbb{Z}_{15}^*$. Volgens die bewys van Proposisie 7 volg dit dat daar 'n $x \in \mathbb{Z}_{210}^*$ bestaan sodat $x \equiv 9$ $(mod\ 14)$ and $x \equiv 1$ $(mod\ 15)$. Bepaal x.

4. Bewys dat, as m en n relatief priem is, dan is $a \equiv b$ $(mod\ m)$ en $a \equiv b$ $(mod\ n)$ as en slegs as $a \equiv b$ $(mod\ mn)$.

5. Gebruik die **square-and-multiply** algoritme en vind

   (a) 40^{600} $(mod\ 45)$

   (b) 30^{600} $(mod\ 45)$

TW 314 (Applied Discrete Mathematics)

Tutorial 10: 4 May 2017

---

1. Use the Euclidean algorithm to determine gcd(1764, 225) and gcd(1764, 625). Then find the multiplicative inverses of 225 and 625 (mod 1764), if they exist.

2. Determine the Euler phi functions of 1764 and 503.

3. Note that 14 and 15 are relatively prime and $14 \times 15 = 210$, and that $9 \in \mathbb{Z}_{14}^*$ and $1 \in \mathbb{Z}_{15}^*$. According to the proof of Proposition 7, it therefore follows that there exists an $x \in \mathbb{Z}_{210}^*$ such that $x \equiv 9$ $(mod\ 14)$ and $x \equiv 1$ $(mod\ 15)$. Determine x.

4. Prove that, if m and n are relatively prime, then $a \equiv b$ $(mod\ m)$ and $a \equiv b$ $(mod\ n)$ if and only if $a \equiv b$ $(mod\ mn)$.

5. Use the **square-and-multiply** algorithm and find

   (a) 40^{600} $(mod\ 45)$

   (b) 30^{600} $(mod\ 45)$
