

UITWERKINGEN

1. (a) (1 pt) Bepaal een oplossing $x, y \in \mathbb{Z}$ van $25x - 91y = 1$.

We kunnen het Euclidisch algoritme gebruiken. We kunnen ook de congruentievergelijking $25x \equiv 1 \pmod{91}$ oplossen. Maal 4 is $9x \equiv 4 \pmod{91}$. Maal 10: $90x \equiv -x \equiv 40 \pmod{91}$. Dus $x = -40$. De bijbehorende y is $(25 \times (-40) - 1)/91 = -11$.

- (b) (1 pt) Bepaal de volledige oplossingsverzameling van $25x - 91y = 4$ in $x, y \in \mathbb{Z}$.

Eén oplossing wordt gegeven door $x = 4 \times (-40) = -160, y = 4 \times (-11) = -44$. Stel x, y is een willekeurige oplossing. Dan volgt uit $25x - 91y = 4$ na aftrekken van $25(-160) - 91(-44) = 4$ dat $25(x + 160) - 91(y + 44) = 0$. Dus 25 deelt $91(y + 44)$ en omdat $\gcd(25, 91) = 1$ volgt hieruit dat 25 een deler is van $y + 44$. Dus bestaat er een $t \in \mathbb{Z}$ zó dat $y + 44 = 25t$. Hieruit volgt $x + 160 = 91t$. Dus (x, y) is van de vorm $(-160 + 91t, -44 + 25t)$ met $t \in \mathbb{Z}$ is. Omgekeerd is elk zo'n tweetal inderdaad een oplossing.

- (c) (0.5 pt) Los de congruentievergelijking $25x - 91y \equiv 4 \pmod{14}$ op in $x, y \in \mathbb{Z}$.

De vergelijking herschreven: $-3x + 7y \equiv 4 \pmod{14}$. Maal -5 geeft $15x - 35y \equiv -20 \pmod{14}$ ofwel $x - 7y \equiv 8 \pmod{14}$. Hieruit volgt dat $x = 8 + 7y + 14z$ waarin y, z willekeurig gekozen kunnen worden.

2. De functie $\psi : \mathbb{N} \rightarrow \mathbb{N}$ wordt gegeven door $\psi(1) = 1$ en

$$\psi(n) = n \prod_{p \text{ priem}, p|n} \left(1 + \frac{1}{p}\right).$$

Zij μ de Möbius functie gegeven door $\mu(n) = (-1)^t$ als n kwadraatvrij is en bestaat uit t verschillende priemfactoren, $\mu(1) = 1$ en $\mu(n) = 0$ in alle andere gevallen.

(a) (0.5 pt) Bewijs dat ψ een multiplicatieve functies is.

Stel $m, n \in \mathbb{N}$ en $\gcd(m, n) = 1$. Dan geldt voor elke priemdelers $p|mn$ dat $p|m$ of $p|n$, maar niet beide. Gevolg:

$$\psi(mn) = mn \prod_{p|mn} \left(1 + \frac{1}{p}\right) = mn \prod_{p|m} \left(1 + \frac{1}{p}\right) \prod_{p|n} \left(1 + \frac{1}{p}\right) = \psi(m)\psi(n).$$

(b) (1 pt) Bepaal het convolutieproduct $(\mu * \psi)(n)$ als n kwadraatvrij is.

Omdat ψ multiplicatief is, en μ ook, is $\mu * \psi$ multiplicatief. Stel n kwadraatvrij en $n = p_1 \cdots p_r$ met alle p_i priem. Voor een priemgetal p geldt $(\mu * \psi)(p) = \sum_{d|p} \mu(d)\psi(p/d) = p + 1 - 1 = p$. Dus vinden we

$$(\mu * \psi)(n) = \prod_{i=1}^r (\mu * \psi)(p_i) = \prod_{i=1}^r p_i = n.$$

(c) (1 pt) Bepaal $(\mu * \psi)(n)$ voor willekeurige n en bepaal $(\mu * \psi)(10^{40})$. Als $k \geq 2$ geldt

$$(\mu * \psi)(p^k) = \sum_{l=0}^k \mu(p^l)\psi(p^{k-l}) = (p^k + p^{k-1}) - (p^{k-1} + p^{k-2}) = p^k - p^{k-2}.$$

Gevolg, als $n = p_1^{k_1} \cdots p_r^{k_r}$ met p_1, \dots, p_r verschillende priemgetallen, dan geldt

$$n = \prod_{k_i=1} p_i \prod_{k_i>1} p_i^{k_i} (1 - 1/p_i^2) = n \prod_{p \text{ priem}, p^2|n} \left(1 - \frac{1}{p}\right).$$

In het bijzonder, $(\mu * \psi)(10^{40}) = 10^{40}(1 - 1/2^2)(1 - 1/5^2) = 72 \cdot 10^{38}$.

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

Voor elke a geldt $\text{ord}_{23}(a)$ deelt $23-1 = 22$. Dus $\text{ord}_{23}(a)$ is 1, 2, 11 of 22. De enige elementen van orde 1, 2 zijn $a \equiv \pm 1 \pmod{23}$. Als a kwadratische niet-rest is, dan $a^{(p-1)/2} = \left(\frac{a}{23}\right) \equiv -1 \pmod{23}$. Conclusie: elke kwadratische nietrest mod 23 ongelijk aan $-1 \pmod{23}$ is primitieve wortel. Kwadratische niet-resten zijn bijv 5 of -2 .

- (b) (1 pt) Zij p een oneven priemgetal en g een primitieve wortel modulo p . Bewijs dat $-g$ een primitieve wortel modulo p is precies dan als $p \equiv 1 \pmod{4}$.

Omdat g een primitieve wortel, kan g geen kwadraatrest zijn, dus $g^{(p-1)/2} \equiv -1 \pmod{p}$. Stel $-g$ is een primitieve wortel. Dan geldt ook $(-g)^{(p-1)/2} \equiv -1 \pmod{p}$. Samen met $g^{(p-1)/2} \equiv -1 \pmod{p}$, volgt hieruit dat $(-1)^{(p-1)/2} \equiv 1 \pmod{p}$. Dus is $(p-1)/2$ even en $p \equiv 1 \pmod{4}$.

Stel nu $p \equiv 1 \pmod{4}$. Zij k de orde van $-g$. Dat wil zeggen, $(-g)^k \equiv 1 \pmod{p}$, waaruit weer volgt $g^k \equiv (-1)^k \pmod{p}$. Tevens, $g^{2k} \equiv 1 \pmod{p}$. Omdat g primitieve wortel is, volgt hieruit dat $p-1 \mid 2k$. Samen met $k \mid p-1$ geeft dit $k = p-1$ of $k = (p-1)/2$. Als $k = (p-1)/2$, dan $1 \equiv (-g)^{(p-1)/2} \equiv g^{(p-1)/2} \equiv -1 \pmod{p}$. Tegenspraak. Dus $k = p-1$ en $-g$ is primitieve wortel.

4. (a) (1 pt) Voor welke oneven priemgetallen p is -2 een kwadraat-rest modulo p ?

$$p \equiv 1(\text{mod } 8) : \left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{2}{p}\right) = 1 \cdot 1 = 1.$$

$$p \equiv 3(\text{mod } 8) : \left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{2}{p}\right) = (-1) \cdot (-1) = 1.$$

$$p \equiv 5(\text{mod } 8) : \left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{2}{p}\right) = 1 \cdot (-1) = -1.$$

$$p \equiv 7(\text{mod } 8) : \left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{2}{p}\right) = (-1) \cdot 1 = -1.$$

Conclusie: -2 is kwadraatrest modulo $p \iff p \equiv 1, 3(\text{mod } 8)$.

- (b) (1 pt) Stel x is een oneven geheel. Bewijs dat $x^2 + 2$ deelbaar is door een priemgetal p met $p \equiv 3(\text{mod } 8)$.

De primedelers p van $x^2 + 2$ zijn allen oneven en van de vorm $p \equiv 1, 3(\text{mod } 8)$ volgens voorgaand onderdeel. Verder geldt, omdat x oneven, $x^2 + 2 \equiv 3(\text{mod } 8)$. Als alle primedelers van $x^2 + 2$ van de vorm $p \equiv 1(\text{mod } 8)$ zouden zijn, dan ook hun product $x^2 + 2$. In tegenspraak met $x^2 + 2 \equiv 3(\text{mod } 8)$. Dus is er priemdelers $p \equiv 3(\text{mod } 8)$.

- (c) (1 pt) Bewijs dat er oneindig veel priemgetallen van de vorm $p \equiv 3(\text{mod } 8)$ bestaan.

Stel er zijn er eindig veel en noem ze p_1, \dots, p_n . Beschouw hun product $N = p_1 \cdots p_n$. Het getal $N^2 + 2$ is deelbaar door een priemgetal q met $q \equiv 3(\text{mod } 8)$ volgens voorgaand onderdeel. Dus is er i zó dat $q = p_i$. Merk nu op, $p_i | N^2 + 2$ en $p_i | N$. Hieruit volgt $p_i | 2$. Tegenspraak, en we concluderen dat er oneindig veel priemgetallen p zijn met $p \equiv 3(\text{mod } 8)$.