

Uitbreidingen op de congruentie van Euler

Joeri Verscheure

1 Wat als $\text{ggd}(a, n)$ niet gelijk is aan 1?

Stelling 1.1 Zij $n \in \mathbb{N}_0$ en $a \in \mathbb{Z}$. Stel d gelijk aan het getal dat je bekomt door uit de priemfactorisatie van n alle priemfactoren te **schrapen** die **geen** deler van a zijn. (Als alles geschrapt moet worden, blijft natuurlijk '1' over.) Dan is

$$a^{\varphi(n)} \bmod n = d \left(d^{-1} \bmod \frac{n}{d} \right)$$

met $d^{-1} \bmod \frac{n}{d}$ de inverse van d modulo $\frac{n}{d}$

bewijs:

- $0 \leq d^{-1} \bmod \frac{n}{d} < \frac{n}{d}$, dus $0 \leq d(d^{-1} \bmod \frac{n}{d}) < n$, dus is VTB: $a^{\varphi(n)} \equiv d(d^{-1} \bmod \frac{n}{d}) \bmod n$

- Om VTB te bewijzen is het voldoende om volgende twee dingen te bewijzen

TB1: $d | a^{\varphi(n)}$

TB2: $a^{\varphi(n)} \equiv 1 \bmod \frac{n}{d}$

want: TB1 \Rightarrow neem die $k \in \mathbb{Z}$ zodat $a^{\varphi(n)} = dk$

TB2 $\Rightarrow dk \equiv 1 \bmod \frac{n}{d}$

$\Rightarrow k \equiv (d^{-1} \bmod \frac{n}{d}) \bmod \frac{n}{d}$ (omdat de inverse uniek is)

$\Rightarrow dk \equiv d(d^{-1} \bmod \frac{n}{d}) \equiv a^{\varphi(n)} \bmod n$

- Bewijs van TB1:

gegeven: $p|d \Rightarrow p|a$

\Rightarrow VTB: $\varphi(n) \geq \#$ priemfactoren in de priemfactorisatie van d

\Rightarrow VTB: $\varphi(n) \geq \#$ priemfactoren in de priemfactorisatie van n

argumenteer dit vanuit de formule voor $\varphi(n)$

- Bewijs van TB2:

Uit de congruentie van Euler volgt dat

$a^{\varphi(\frac{n}{d})} \equiv 1 \bmod \frac{n}{d}$ (want $\text{ggd}(a, \frac{n}{d}) = 1$, omdat geg.: als $p|\frac{n}{d}$, dan $p \nmid a$, voor elke p priem)

$\Rightarrow a^{\varphi(n)} \equiv 1 \bmod \frac{n}{d}$ (argumenteer dat $\varphi(\frac{n}{d}) | \varphi(n)$, omdat $\frac{n}{d} | n$, vanuit formule voor $\varphi(n)$)

Gevolg 1.2 Zij $n \in \mathbb{N}_0$ en $a, b \in \mathbb{Z}$. Dan geldt

$$a^{\varphi(n)} \equiv b^{\varphi(n)} \pmod{n} \iff \forall p \text{ priem, } p|n : (p|a \iff p|b)$$

bewijs:

Zij d_a de ‘ d die hoort bij a en n ’, zoals gedefinieerd voor de vorige stelling en d_b de ‘ d die hoort bij b en n ’.

• \Leftarrow

In dit geval is $d_a = d_b$ per definitie; noem $d = d_a = d_b$. Dan is

$$a^{\varphi(n)} \pmod{n} = d \left(d^{-1} \pmod{\frac{n}{d}} \right) = b^{\varphi(n)} \pmod{n}$$

• \Rightarrow

Uit het ongerijmde: stel $\exists p$ priem, $p|n$: $p|a$ en $p \nmid b$, neem die p . (Deze p bestaat (uit het ongerijmde), na eventueel omwisselen van de rol van a en b .) Pas nu stelling 1.1 toe:

$$a^{\varphi(n)} \pmod{n} = d_a \left(d_a^{-1} \pmod{\frac{n}{d_a}} \right)$$

|| gegeven

$$b^{\varphi(n)} \pmod{n} = d_b \left(d_b^{-1} \pmod{\frac{n}{d_b}} \right)$$

dan is $p|d_a$ en $p \nmid d_b$

$d_b^{-1} \pmod{\frac{n}{d_b}}$ heeft een inverse modulo $\frac{n}{d_b}$ (namelijk $d_b \pmod{\frac{n}{d_b}}$)

dus is $\text{ggd}(d_b^{-1}, \frac{n}{d_b}) = 1$

maar $p|\frac{n}{d_b}$ (omdat $p|n$ en $p \nmid d_b$)

$p|d_b^{-1}$ (omdat L.L.= $d_a(d_a^{-1} \pmod{\frac{n}{d_a}}) = d_b(d_b^{-1} \pmod{\frac{n}{d_b}})$ =R.L.; $p|$ L.L., dus $p|$ R.L. en $p \nmid d_b$)

Voorbeeld 1.3

$$a^{\varphi(n)} \equiv \text{ggd}(a, n)^{\varphi(n)} \pmod{n}$$

Dit is eigenlijk sowieso niet moeilijk te bewijzen.

Voorbeeld 1.4

$$a^{k\varphi(n)} \equiv a^{l\varphi(n)} \pmod{n}, \forall k, l \in \mathbb{N}_0$$

2 Uitbreiding op de reductie van de exponent modulo $\varphi(n)$

Stelling 2.1 Zij $n, l \in \mathbb{N}_0$, $a \in \mathbb{Z}$ en $k \in \mathbb{N}$. Dan geldt

$$a^{l\varphi\left(\frac{n}{\text{ggd}(a^k, n)}\right)+k} \equiv a^k \pmod{n} \quad (1)$$

$$\Leftrightarrow \text{ggd}\left(a, \frac{n}{\text{ggd}(a^k, n)}\right) = 1 \quad (2)$$

$$\Leftrightarrow \exists e \in \mathbb{N}_0 : a^{k+e} \equiv a^k \pmod{n} \quad (3)$$

bewijs:

$$\begin{aligned} (3) \Rightarrow (2) \text{ gegeven: } n | a^k(a^e - 1) \\ \Rightarrow \frac{n}{\text{ggd}(a^k, n)} | a^e - 1 \\ \Rightarrow a^e \equiv 1 \pmod{\frac{n}{\text{ggd}(a^k, n)}} \\ \Rightarrow a^{e-1} \text{ is inverse voor } a, \text{ modulo } \frac{n}{\text{ggd}(a^k, n)} \\ \text{dus } \text{ggd}\left(a, \frac{n}{\text{ggd}(a^k, n)}\right) = 1 \end{aligned}$$

(2) \Rightarrow (1) uit de congruentie van Euler:

$$\begin{aligned} a^{\varphi\left(\frac{n}{\text{ggd}(a^k, n)}\right)} &\equiv 1 \pmod{\frac{n}{\text{ggd}(a^k, n)}} \\ \Rightarrow a^{l\varphi\left(\frac{n}{\text{ggd}(a^k, n)}\right)} &\equiv 1 \pmod{\frac{n}{\text{ggd}(a^k, n)}} \\ \Rightarrow \frac{n}{\text{ggd}(a^k, n)} | a^{l\varphi\left(\frac{n}{\text{ggd}(a^k, n)}\right)} - 1 \\ \Rightarrow n | a^k(a^{l\varphi\left(\frac{n}{\text{ggd}(a^k, n)}\right)} - 1) \end{aligned}$$

$$(1) \Rightarrow (3) \text{ neem } e = l\varphi\left(\frac{n}{\text{ggd}(a^k, n)}\right)$$

Opmerking 2.2 Deze stelling gaat samen met voorbeeld 1.4 omdat $\varphi(n) \geq \#$ priemfactoren in de priemfactorisatie van d of van n . (Zie het bewijs bij stelling 1.1.)

Oefening 2.3 Zij $n, l, l', l'', l''' \in \mathbb{N}_0$, $a \in \mathbb{Z}$ en $k \in \mathbb{N}$. Dan geldt

$$a^{l'\varphi\left(\frac{n}{\text{ggd}(a^k, n)}\right)+k} \equiv a^k \text{ggd}\left(a^{l'''}, \frac{ln}{\text{ggd}(a^k, n)}\right)^{l''\varphi\left(\frac{n}{\text{ggd}(a^k, n)}\right)} \pmod{n}$$

Oplossing:

Vraag: Voor welke $b \in \mathbb{Z}$ is $a^{l'\varphi\left(\frac{n}{\text{ggd}(a^k, n)}\right)+k} \equiv a^k b^{l''\varphi\left(\frac{n}{\text{ggd}(a^k, n)}\right)} \pmod{n}$?

$$\begin{aligned} \Leftrightarrow n | a^k(a^{l'\varphi\left(\frac{n}{\text{ggd}(a^k, n)}\right)} - b^{l''\varphi\left(\frac{n}{\text{ggd}(a^k, n)}\right)}) \\ \Leftrightarrow \frac{n}{\text{ggd}(a^k, n)} | a^{l'\varphi\left(\frac{n}{\text{ggd}(a^k, n)}\right)} - b^{l''\varphi\left(\frac{n}{\text{ggd}(a^k, n)}\right)} \\ \Leftrightarrow a^{l'\varphi\left(\frac{n}{\text{ggd}(a^k, n)}\right)} \equiv b^{l''\varphi\left(\frac{n}{\text{ggd}(a^k, n)}\right)} \pmod{\frac{n}{\text{ggd}(a^k, n)}} \end{aligned}$$

wegens voorbeeld 1.4 is het voldoende dat

$$\begin{aligned} a^{\varphi\left(\frac{n}{\text{ggd}(a^k, n)}\right)} &\equiv b^{\varphi\left(\frac{n}{\text{ggd}(a^k, n)}\right)} \pmod{\frac{n}{\text{ggd}(a^k, n)}} \\ \Leftrightarrow \forall p \text{ priem, } p | \frac{n}{\text{ggd}(a^k, n)} : p | a &\Leftrightarrow p | b \text{ (dit volgt uit het gevolg 1.2)} \\ b = \text{ggd}\left(a^{l'''}, \frac{ln}{\text{ggd}(a^k, n)}\right) &\text{ voldoet} \end{aligned}$$