Universiteit van Stellenbosch

Toegepaste Wiskunde 314

Tutoriaaltoets 4: Donderdag 11 Maart 2004

MEMORANDUM

Tuttoets 4a.

Die inverse van die matriks

$$\mathbf{S} = \begin{bmatrix} 11 & 11 & 11 \\ 12 & 13 & 14 \\ 21 & 1 & 0 \end{bmatrix}$$

in die versameling $\mathcal{Z}_{26}^{3*}$ is

$$\mathbf{S}^{-1} = \begin{bmatrix} 12 & 11 & 11 \\ 8 & 3 & 4 \\ 25 & 12 & 11 \end{bmatrix}$$

Toets:

$$\begin{bmatrix} 11 & 11 & 11 \\ 12 & 13 & 14 \\ 21 & 1 & 0 \end{bmatrix} \begin{bmatrix} 12 & 11 & 11 \\ 8 & 3 & 4 \\ 25 & 12 & 11 \end{bmatrix} = \begin{bmatrix} 495 & 286 & 286 \\ 598 & 339 & 338 \\ 260 & 234 & 235 \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \pmod{26}$$

en

$$\begin{bmatrix} 12 & 11 & 11 \\ 8 & 3 & 4 \\ 25 & 12 & 11 \end{bmatrix} \begin{bmatrix} 11 & 11 & 11 \\ 12 & 13 & 14 \\ 21 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 495 & 286 & 286 \\ 208 & 131 & 130 \\ 650 & 442 & 443 \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \pmod{26}$$

Tuttoets 4b.

Neem as eerste raaiskoot $n = 2$. Dit sou impliseer dat

$$\underbrace{\begin{bmatrix} 4 & 19 \\ \boxed{\text{E}} & \boxed{\text{T}} \\ 10 & 5 \\ \boxed{\text{K}} & \boxed{\text{F}} \end{bmatrix}}_{\mathbf{Y}} \equiv \underbrace{\begin{bmatrix} 11 & 0 \\ \boxed{\text{l}} & \boxed{\text{a}} \\ 13 & 3 \\ \boxed{\text{n}} & \boxed{\text{d}} \end{bmatrix}}_{\mathbf{X}} \mathbf{S} \pmod{26},$$

waaruit volg dat $|\mathbf{X}| = 33 \equiv 7 \pmod{26}$, sodat $|\mathbf{X}|^{-1} \equiv 15 \pmod{26}$. Hieruit volg dat

$$\begin{aligned} \mathbf{S} &= \mathbf{X}^{-1}\mathbf{Y} \\ &= 15 \begin{bmatrix} 3 & 0 \\ -13 & 11 \end{bmatrix} \begin{bmatrix} 4 & 19 \\ 10 & 5 \end{bmatrix} \\ &\equiv \begin{bmatrix} 24 & 23 \\ 12 & 6 \end{bmatrix} \pmod{26}, \end{aligned}$$

wat nie inverteerbaar is nie. Dit beteken dat $n \neq 2$.

Die volgende raaiskoot is dat $n = 3$. Dan is

$$\underbrace{\begin{bmatrix} 4 & 19 & 10 \\ \boxed{\text{E}} & \boxed{\text{T}} & \boxed{\text{K}} \\ 5 & 10 & 4 \\ \boxed{\text{F}} & \boxed{\text{K}} & \boxed{\text{E}} \\ 14 & 15 & 2 \\ \boxed{\text{O}} & \boxed{\text{P}} & \boxed{\text{C}} \end{bmatrix}}_{\mathbf{Y}} \equiv \underbrace{\begin{bmatrix} 11 & 0 & 13 \\ \boxed{\text{l}} & \boxed{\text{a}} & \boxed{\text{n}} \\ 3 & 18 & 14 \\ \boxed{\text{d}} & \boxed{\text{s}} & \boxed{\text{o}} \\ 5 & 6 & 11 \\ \boxed{\text{f}} & \boxed{\text{g}} & \boxed{\text{l}} \end{bmatrix}}_{\mathbf{X}} \mathbf{S} \pmod{26}.$$

Maar nou is $|\mathbf{X}| = 318 \equiv 6 \pmod{26}$, sodat $|\mathbf{X}|^{-1}$ weereens nie bestaan nie. Dit kan beteken dat $n \neq 3$, of moontlik net dat die skoonteks singulier is. As ons by die raaiskoot $n = 3$ hou, maar konsentreer op 'n volgende segmentering van die (skoonteks, kriptoteks)–paar. Dan is

$$\underbrace{\begin{bmatrix} 5 & 10 & 4 \\ \boxed{\text{F}} & \boxed{\text{K}} & \boxed{\text{E}} \\ 14 & 15 & 2 \\ \boxed{\text{O}} & \boxed{\text{P}} & \boxed{\text{C}} \\ 13 & 25 & 9 \\ \boxed{\text{N}} & \boxed{\text{Z}} & \boxed{\text{J}} \end{bmatrix}}_{\mathbf{Y}} \equiv \underbrace{\begin{bmatrix} 3 & 18 & 14 \\ \boxed{\text{d}} & \boxed{\text{s}} & \boxed{\text{o}} \\ 5 & 6 & 11 \\ \boxed{\text{f}} & \boxed{\text{g}} & \boxed{\text{l}} \\ 14 & 17 & 24 \\ \boxed{\text{o}} & \boxed{\text{r}} & \boxed{\text{y}} \end{bmatrix}}_{\mathbf{X}} \mathbf{S} \pmod{26}.$$

Maar nou is $|\mathbf{X}| \equiv 3 \pmod{26}$, sodat $|\mathbf{X}|^{-1} = 9 \pmod{26}$. Gevolglik is

$$\mathbf{X}^{-1} = \begin{bmatrix} 3 & 22 & 12 \\ 20 & 2 & 21 \\ 9 & 15 & 2 \end{bmatrix} \pmod{26}.$$

Gevolglik is

$$\mathbf{S} = \mathbf{X}^{-1}\mathbf{Y} = \begin{bmatrix} 3 & 22 & 12 \\ 20 & 2 & 21 \\ 9 & 15 & 2 \end{bmatrix} \begin{bmatrix} 5 & 10 & 4 \\ 14 & 15 & 2 \\ 13 & 25 & 9 \end{bmatrix} \equiv \begin{bmatrix} 11 & 10 & 8 \\ 11 & 1 & 13 \\ 21 & 1 & 6 \end{bmatrix} \pmod{26}$$

en dus is

$$\mathbf{S}^{-1} \equiv \begin{bmatrix} 3 & 0 & 22 \\ 19 & 14 & 5 \\ 8 & 15 & 9 \end{bmatrix} \pmod{26}.$$

Die dekripsie

$$\mathbf{X} = \mathbf{Y}\mathbf{S}^{-1} = \begin{bmatrix} 25 & 3 & 7 \\ 22 & 20 & 19 \\ 24 & 15 & 16 \\ 23 & 21 & 0 \end{bmatrix} \begin{bmatrix} 3 & 0 & 22 \\ 19 & 14 & 5 \\ 8 & 15 & 9 \end{bmatrix} = \begin{bmatrix} 188 & 147 & 628 \\ 598 & 565 & 755 \\ 485 & 450 & 747 \\ 468 & 294 & 611 \end{bmatrix} \equiv \begin{bmatrix} 6 & 17 & 4 \\ 0 & 19 & 1 \\ 17 & 8 & 19 \\ 0 & 8 & 13 \end{bmatrix} \pmod{26}$$

word verkry, wat as `greatbritain` verletter, oftewel "Great Britain" (ná invoeging van spasies).