# Universiteit van Stellenbosch

## Toegepaste Wiskunde 314

### Tutoriaaltoets 2: Donderdag 26 Februarie 2004

**MEMORANDUM**

**Tuttoets 1a.**

Die grootste gemene deler van 4 en 26 is 2, wat 'n deler is van 6. Dus besit die kongruensie volgens Stelling 2-4 twee verskillende oplossings in $\mathbb{Z}_{26}$. Hulle is:

$$\begin{aligned} x &= \left(\frac{4}{2}\right)^{-1}\left(\frac{6}{2}\right) + k\left(\frac{26}{2}\right) \\ &= (7)(3) + 13k, \quad k = 0, 1 \\ &= 8, 21. \end{aligned}$$

**Tuttoets 1b.**

Die letterfrekwensies in die kriptoteks is:

| | | | | | |
|---|---|---|---|---|---|
| A: | 18 | J: | 67 | S: | 15 |
| B: | 3 | K: | 36 | T: | 20 |
| C: | 102 | L: | 0 | U: | 0 |
| D: | 1 | M: | 18 | V: | 11 |
| E: | 55 | N: | 39 | W: | 50 |
| F: | 54 | O: | 15 | X: | 11 |
| G: | 7 | P: | 55 | Y: | 4 |
| H: | 39 | Q: | 9 | Z: | 11 |
| I: | 39 | R: | 14 | | |

Hierdie frekwensies suggereer dat `e` enkripteer na `C`, en dat `t` enkripteer na `J`, wat impliseer dat die sleutelpaar $(a, b)$ die lineêre sisteem

$$\begin{cases} 4a + b \equiv 2 \pmod{26} \\ 19a + b \equiv 9 \pmod{26} \end{cases}$$

bevredig. Die unieke oplossing tot hierdie sisteem is dus $(a, b) \equiv (23, 14)$, wat nie die korrekte sleutelpaar is nie, aangesien die kriptoteks nie na verstaanbare Engels dekripteer as hierdie waardes gebruik word nie. As tweede probeerslag kan verwag word dat `e` steeds enkripteer na `C`, maar dat `t` moontlik enkripteer na `E`, wat impliseer dat die sleutelpaar $(a, b)$ die lineêre sisteem

$$\begin{cases} 4a + b \equiv 2 \pmod{26} \\ 19a + b \equiv 4 \pmod{26} \end{cases}$$

bevredig. Die unieke oplossing tot hierdie sisteem is dus $(a, b) \equiv (14, 24)$, wat nie die korrekte sleutelpaar is nie, aangesien $\text{ggd}(14, 26) = 2 \neq 1$. As derde probeerslag kan verwag word dat `e`

steeds enkripteer na `C`, maar dat `t` moontlik enkripteer na `P`, wat impliseer dat die sleutelpaar $(a, b)$ die lineêre sisteem

$$\begin{cases} 4a + b & \equiv & 2 \pmod{26} \\ 19a + b & \equiv & 15 \pmod{26} \end{cases}$$

bevredig. Die unieke oplossing tot hierdie sisteem is dus $(a, b) \equiv (13, 2)$, wat nie die korrekte sleutelpaar is nie, aangesien $\text{ggd}(13, 26) = 13 \neq 1$. As vierde probeerslag kan verwag word dat `e` steeds enkripteer na `C`, maar dat `t` moontlik enkripteer na `F`, wat impliseer dat die sleutelpaar $(a, b)$ die lineêre sisteem

$$\begin{cases} 4a + b & \equiv & 2 \pmod{26} \\ 19a + b & \equiv & 5 \pmod{26} \end{cases}$$

bevredig. Die unieke oplossing tot hierdie sisteem is dus $(a, b) \equiv (21, 22)$, wat die volgende skoonteks na dekripsie oplewer:

"The nine Rings given to Men ensnared their users, and they became the Nazgûl; the Dwarves proved indomitable, and the Rings could not control them; the Elves escaped Saurons trap when Celebrimbor realized the treachery and hid the Elven Rings. In this way, the Elven Rings – which had never been touched by Sauron – escaped his taint, and were never subject directly to the control of the One. With his deceptions laid bare, Sauron resorted to force, and invaded the West, destroying Eregion and overrunning much of Eriador, before being stopped by an alliance of Elves and Men from Númenor. Sauron retreated to the east to consolidate his power, but after donning the title King of Men, he aroused the anger and pride of Ar-Pharazôn, King of Númenor, who landed a great host on the shores of Middle Earth, humbled Sauron, and took him back to Númenor as a prisoner."

(na invoeging van spasies, leestekens en aksente)