Universiteit van Stellenbosch

Toegepaste Wiskunde 314

Tutoriaal 1: Donderdag 19 Februarie 2004

MEMORANDUM

(1) (a) 14 ($m = 26$)
(b) 2 ($m = 16$)
(c) 3 ($m = 16$)
(d) 24 ($m = 26$)
(e) 2 ($m = 17$)

(2) Gestel $a \equiv b \pmod{m}$ en $c \equiv d \pmod{m}$. Dan bestaan daar heelgetalle p en q sodat $a = b + pm$ en $c = d + qm$. Gevolglik is

$$\begin{aligned} ac &= (b + pm)(d + qm) \\ &= bd + bqm + dpm + pqm^2 m \\ &= bd + m(bq + dp + pqm). \end{aligned}$$

Omdat $bq + dp + pqm$ 'n heelgetal is, volg dit dus dat $ac \equiv bd \pmod{m}$.

(3)

Skoonteks:	r	o	m	a	n	e	m	p	i	r	e
$x \rightarrow$	17	14	12	0	13	4	12	15	8	17	4
$y = x + 15 \pmod{26} \rightarrow$	6	3	2	15	2	19	1	4	23	6	19
Kriptoteks:	G	D	B	P	C	T	B	E	X	G	T

(4)

Kriptoteks:	M	X	O	L	X	V
$y \rightarrow$	12	23	14	11	23	21
$x = y - 3 \pmod{26} \rightarrow$	9	20	11	8	20	18
Skoonteks:	j	u	l	i	u	s

(5)

Kriptoteks:	U	K	N	M	N	L
$y \rightarrow$	20	10	13	12	13	11
$x = y - 19 \pmod{26} \rightarrow$	1	17	20	19	20	18
Skoonteks:	b	r	u	t	u	s

(6) $s = 1$: `oiuighig`
$s = 2$: `nhthfghf`
$s = 3$: `mgsgefge`
$s = 4$: `lfrfdefd`
$s = 5$: `keqecdec`
$s = 6$: `jdpdbcdb`
$s = 7$: `icocabca`
$s = 8$: `hbnbzabz`

$s = 9$: `gamayzay`
$s = 10$: `fzlzxyzx`
$s = 11$: `fzlzxyzx`
$s = 12$: `dxjxvwxv`
$s = 13$: `cwiwuvwu`
$s = 14$: `bvhvtuvt`
$s = 15$: `augustus` $\rightarrow$ "Augustus" $\Rightarrow s = 15$.

(7) Euklidiese Algoritme:

(a) $\text{ggd}(3\,699, 264) = 3$:

i	p_i	q_i	r_i	s_i
0	3 699	264	3	14
1	264	3	0	88
2	$\boxed{3}$	0	–	–

(b) $\text{ggd}(2\,090, 1\,862) = 38$:

i	p_i	q_i	r_i	s_i
0	2 090	1 862	228	1
1	1 862	228	38	8
2	228	38	0	6
3	$\boxed{38}$	0	–	–

(8) Gewysigde Euklidiese Algoritme:

(a) $5^{-1} \equiv 5 \pmod{24}$:

i	p_i	q_i	r_i	s_i	x_i	y_i
0	24	5	4	4	0	1
1	5	4	1	1	1	–4
2	4	1	0	4	–4	$\boxed{5}$
3	1	0	–	–	–	–

(b) $5^{-1} \equiv 3 \pmod{14}$:

i	p_i	q_i	r_i	s_i	x_i	y_i
0	14	5	4	2	0	1
1	5	4	1	1	1	–2
2	4	1	0	4	–2	$\boxed{3}$
3	1	0	–	–	–	–

(c) $14^{-1} \pmod{24}$ bestaan nie, want $\text{ggd}(14, 24) = 2 \neq 1$.