Universiteit van Stellenbosch

Toegepaste Wiskunde 314

Tutoriaaltoets 1b: Donderdag 19 Februarie 2004

US nommer: _____ Voorletters: _____ Van: _____

Die Gebruik van Klasnotas word Verbied

(1) Dekripteer, *met die hand*, die kriptoteks `NQCHJYUEM`, wat met behulp van die additiewe substitusie–stelsel $\Im_{26}^{20}$ gevorm is. Wys u werking volledig. [2]

(2) Die kriptoteks `KAEGFKTWJY` is met behulp van die additiewe substitusie–stelsel gevorm. Ontrafel die sleutel en dekripteer dan die kriptoteks. Wys u werking. [3]

(3) Gebruik die Gewysigde Euklidiese Algoritme om die inverse $a \equiv (19)^{-1} \pmod{36}$ te bepaal. Wys u werking volledig deur die onderstaande tabel in te vul. Toets die korrektheid van u antwoord deur die produk $19a \pmod{36}$ te evalueer. [3]

Algorithm 2-2: Revised Euclidean Algorithm
To calculate a number z that satisfies $az \equiv 1 \pmod{m}$.
1. *Let $p_0 = m$, $q_0 = a$, $x_0 = 0$, $y_0 = 1$ and set $i = 0$.*
2. *Let r_i be the remainder when p_i is divided by q_i, i.e.*

$$\frac{p_i}{q_i} = s_i + \frac{r_i}{q_i},$$

   for some integer $s_i \geq 0$.
3. *Let $p_{i+1} = q_i$, $q_{i+1} = r_i$, $x_{i+1} = y_i$ and $y_{i+1} = x_i - s_i y_i$.*
4. *If $q_{i+1} > 0$, increment the value of i by 1. Return to Step 2.*
5. *Let $z = y_i$. Stop.*

i	p_i	q_i	r_i	s_i	x_i	y_1
1						
2						
3						
4						
5						
6						
7						
8						