Universiteit van Stellenbosch

Toegepaste Wiskunde 314

Tutoriaaltoets 8: Donderdag 29 April 2004

MEMORANDUM

Tuttoets 8a.

Sien bladsye 151–152 van die klasnotas.

Tuttoets 8b.

Pollard se algoritme kan gebruik word om $n = 6\,887$ te faktoriseer met gladheidsgrens $B = 5$ (byvoorbeeld) en aanvanklike waarde $a = 10$ (byvoorbeeld):

q	$\lfloor \ln n / \ln q \rfloor$	a
2	12	3 915
3	8	583
5	5	971

Met hierdie afvoer word die nie–triviale faktor $\gcd(970, n) = 97$ van n verkry. Die volledige priemfaktorisering is $n = \underbrace{71}_{p} \times \underbrace{97}_{q}$.

Gevolglik is $\phi(n) = (p-1)(q-1) = 70 \times 96 = 6\,720$. Om die dekripsie–ekspronent $d \equiv e^{-1} \pmod{\phi(n)}$ te bereken, word die gewysigde Euklidiese algoritme gebruik:

i	p_i	q_i	r_i	s_i	x_i	y_i
0	6 720	4 567	2153	1	0	1
1	4 567	2 153	261	2	1	–1
2	2 153	261	65	8	–1	3
3	261	65	1	4	3	–25
4	65	1	0	65	–25	$\boxed{103}$
10	1	0	–	–	–	–

Die dekripsie–eksponent is dus $d = 103$. Die onderliggende skoonteks is gevolglik

$$x \equiv y^d \equiv 5\,564^{103} \equiv 520 \pmod{n},$$

en die verlettering daarvan is $\underbrace{\texttt{E}}_{05}\underbrace{\texttt{T}}_{20}$.