Dr. Ing. Wilfried Dankmeier
FH Frankfurt am Main
Fachbereich 2

Eppstein im Taunus 01.04.2012

Φ_0	=	a_1	·	Φ_1	+	Φ_2
220		8		27		4

Φ_1	=	a_2	·	Φ_2	+	Φ_3
27		6		4		3

Φ_2	=	a_3	·	Φ_3	+	Φ_4
4		1		3		1

Φ_3	=	a_4	·	Φ_4	+	Φ_5
3		3		1		0

→ der EA endet immer mit „0“

$= ggT(\Phi_0, \Phi_1) = ggT(\Phi(n), e)$

m	=	4

= Index von Rest 1

Rekursion:

z_i	=	$-a_{m-i}$	·	z_{i-1}	+	z_{i-2}

mit i = 2, 3, …, m-1 = **2,3**

Startwerte:

z_0 = 1

$z_1 = -a_{m-1} = -a_3$ = **-1**

Durchführung der Rekursion:

z_2	=	$-a_2$	·	z_1	+	z_0
7		-6		-1		1

z_3	=	$-a_1$	·	z_2	+	z_1
-57		-8		7		-1

z_3 ist die gesuchte modulare inverse Zahl

Beachten: $(-57)\ \text{MOD}\ 220 = 163$

Daher: $(-57 \cdot 27)\ \text{MOD}\ 220 = (163 \cdot 27)\ \text{MOD}\ 220 = 1$

Probe mit Scilab: ***pmodulo(-57 * 27, 220) =1***