

/^ všOE o K8 t}OE | vÀ]OE }vu vš ^µOE À
(}OE Z] ( u] K8 U ^‰OE]vP îìíï v ^

## /všŒ}µŸ}v

d} šZ ]OE i} • Á ooU •š + v •쉉}OEŸÀ v }oo }OE ŸÀ Á}OEI v À oµ v šOEµ•š X ^]v îììñU šZ /^ všOE o K8 t}OEI vÀ]OE}vu vš š} P šZ OE ]v(}OEu Ÿ}v }µš Á}OEI‰o }v ]Ÿ}v• OE o š š} o OE•Z]% ‰}o] ]• v ‰OE} µOE•U ( ]o]Ÿ• v OE•}µOE •U Á}OEIPOE}µ‰ Çv u] (}oo}Á]vP OE ‰}OEš ‰OE• vš• šZ Á}OEI vÀ]OE}vu vš•µOEÀ Ç OE•µoš• ( Z] ( u] K8 u‰o}Ç•X

## ^µŒÀÇZ•µoš•Ç:}>}Ÿ}v

		îìíï	îìíð
	]o]vPµ o	V	ôì9
íX dZ •š + v •µ‰ 0EÀ]•}0E∼•• Z	∧‰ 10 и Ÿ}v	ó ï 9	ò ñ 9
	Z] ( u] • VKR8šZ	Œv	ôï9
	Z]( u]•vK&oo	ô ñ 9	ó õ 9
	]o]vPµ o	V	ò ì 9
	^‰]o µ Ÿ}v	ñ ñ 9	ñ ì 9
îX dZ Œ ]• v šu}•‰Z Œ }(šŒ	µ•s v uµsµ o cz •‰ Z]( u]•vKK8šZ	°CE ` v	ó ô 9
	Z]( u]•vK&oo	ó ò 9	ó í 9
	]o]vPµ o	v	òì9
ïX ^š + ( o }u()Œš o Œ ]•]vP	^‰]oµŸ}v	ô î 9	ðï9
šZš OE ]u‰}OEšvšš}šZuX	Z] ( u] • vKK8šZ	Œ v	ó ó 9
	Z]( u]•vK&oo	ô î 9	òõg
	]o]vPµ o	V	ñò9
ĂΧ ∧μ‰ (ŒÀl•}(Œ• }ν•l•š νšοC•μ	^‰ ] o µ Ÿ}v	òð9	ò î 9
ðX ^µ‰ ŒÀ]∙}Œ∙ }v∙]•š všoÇ •µ	Z] ( u] • vKk8š Z	0E v	ô í 9
	Z]( u]•vK&oo	ô í 9	óñ9
	]o]vPµ o	V	õ ì 9
ñX^š+ Œ Z o š} Z]PZ ‰Œ}(•	^‰]oµŸ}v	ó ï 9	ô í 9
	Z] ( u] • vKk8š Z	Œ v	õòS
	Z]( u]•vK&bo	õ ì 9	õï9
	]o]vPµ o	V	òóS
òX ^š + ‰ Œ(}Œu v ]• •• •• }	^‰ ]ο μ Ϋ}ν ι ι ΑυζΑ	ô ì 9	ò ó 9
	Z] ( u] • vKk8š Z	Œv	ô ò 9
	Z] ( u] • vK & o	ô ð 9	ô í 9
	]o]vPµ o	V	ò ì 9
óX^š+Œ]À ( IšZš v 2	^‰]o µ Ÿ}v	òð9	ðó9
šZ]CEÁ}CEIX	Z] ( u] • vKK8šZ	Œ v	ôðg
	Z]( u]•vK&oo	ô ð 9	óò9
ôXdZ‰Œ}μŒ•(}ŒÀομŸ}	]o]vPµ o	V	ó ñ 9
	^‱]oµŸ}v	ô ì 9	ò ï 9
$0 \land 0 2 \mod p \square p$	Z] ( u] • vKK8šZ	Œv	ô ï 9
	Z]( u]•vK&bo	ô î 9	ó õ 9

Wo • Œš Z}Á •šŒ}vPoÇÇ}µ PŒ }Œ ]• PŒ Á]šZšZ o ΥZ]‰ ]vÇ}µŒ Œ X

îìíï îìíð

]o]vPµ o	V	ñ ò 9
íñX]•šŒ]šo,Œ•v}μŒͺΡ} <sup>^</sup> ‰]ομΫ}ν	ó ì 9	ï ô 9
‰ Œšu vš•š}Á Œ ]u‰Œ}À]vP ]zĕjŒ[]š}‰]ŒFvÄke}s∛z <sup>X</sup> Œ	v	ó í 9
Z]( u]•vK&oo	ó ì 9	òï9
]o]vPµ o	v	ô ì 9
íòX]•šŒ]šο Œ•šI•š‰•š;-;υπ∞ω;υu-n		

Wo • CE š Z}Á •šCE}vPoÇÇ}μ PCE }CE ]• PCE Á]šZ šZ ‰CE} μCE •X

	îìíï	îìíð
]o]vPµ o	V	ô î 9
îìΧ/Iv}ÁšZ‰Œ}µŒ•(}ŒŒC <sup>*</sup> ‰]οµŸ}v	õ í 9	íìì9
Z Œ ••u všX Z] ( u] • vKK8šZ Œ	v	ôï9
Z]( u]•VK&bo	ô ï 9	ô ó 9
]o]vPµ o	V	ô ì 9
îíX / Iv}ÁšZ ‰Œ} μŒ • (}Œ.o	õ ì 9	õ ñ 9
Z] ( u] • vKH8šZ Œ	V	ó ô 9
Z]( u]•VK&bo	ó õ 9	ô î 9
]o]vPµ o	V	î ó 9
îîΧ / Ζ À Ɖ Œ] v ]•Œ]u]v ^‰ ] ο μ ϔ}v	ñ ñ 9	ïò9
š /^ X Z] ( u] • vKH8š Z Œ	V	ï í 9
Z](u]•√K⊗bo	îï9	ïí9

Wo • Œš Z}Á •šŒ}vPoÇÇ}µ PŒ }Œ ]• PŒ Á]šZ šZ Ɖ šŸ}v• (}ŒÇ}µŒ PŒ}µ‰X

			îìíï	îìíð
	]o]vPµ (	)	v	òð9
	^‰ ] 0		õ í 9	ó ï 9
îïX/uP]Àv o]v∙šZšOE	Z] (	^ u]•vKk8šZ Œ	v	ó ò 9
	Z] (	u]•vK&so	ó ô 9	óð9
	]o]vPµ (	)	V	òð9
îðXDÇ ‰ ŒssuvsilÁ}ŒEIPŒ}µ‰	^‰]0	μ Ÿ}v	ô î 9	ò î 9
CE CE •}v o X	Z] (	u]•vKk-8šZ0E	v	óð9
	Z] (	u] ∙vK&so	ò ô 9	ó í 9
] 0		)	v	ó ï 9
îñX/u•Ÿ∙. Á]šZšZu}µvš}		μ Ϋ}v	ó ï 9	ô ò 9
}všCE}o / ZÀ }À CE uÇ }Áv Á}CE	IX <sub>Z</sub> ] (	u]•VKK-8šZOE	v	ô õ 9
	Z] (	u] ∙vK&so	ô ó 9	ô ó 9
	]o]vPµ (	)	v	ð ñ 9
îòXDÇÁ}CEIvÀ]CE}vuvš]•š}}	^‰ ] 0	μ Ϋ}v	î ó 9	ðí9
	Z] (	u] • vKk-8šZ OE	V	î ñ 9
	Z] (	u]•vK&bo	ïð9	ïì9

îìíï

î	ì	í	ï	î	ì	í	ð	

] o ] v P µ	0	v	õ 9
^ ‰ ] O	μ Ÿ}v	õ 9	ñ 9
Z] (	u] • vKk-8šZ OE	v	ñ 9
Z] (	u]•K8		

Z ] o š v•]}v