## Aritmética modular, parte II

Ejemplo 1. Encuentre (si existe) la solución de la congruencia lineal  $9x \equiv 3 \pmod{15}$ 

Primero calculamos el mcd(15,9) usando el algoritmo de Euclides:

$$15 = 1.9 + 6$$
  
 $9 = 1.6 + 3$   
 $6 = 2.3$ 

 $\therefore$  mcd(15,9) = 3 y como mcd(15,9) = 3 | b = 3, entonces la congruencia lineal sí tiene solución.

De la definición de congruencia modular tenemos:

$$9x \equiv 3 \pmod{15} \leftrightarrow 15 \mid (9x - 3) \leftrightarrow 9x - 3 = 15k \leftrightarrow 9x + 15(-k) = 3 \text{ [ec. diofántica]}$$

Para encontrar x usamos la identidad de Bézout:

$$3 = 9 - 1.6 = 9 - 1.(15 - 1.9) = 9 - 15 + 9 = 9(2) + 15(-1) \rightarrow x = 2$$

La solución general para la variable  $x = 2 + \lambda \cdot (15/3) = 2 + 5\lambda$ 

Estamos buscando todas las soluciones de la congruencia lineal en  $\mathbb{Z}_1$  5, es decir,  $0 \le x \le 14$ :

$$\lambda = -1 \longrightarrow x = 2 - 5 = -3 \notin \mathbb{Z}_1$$
 5

$$\lambda = 0 \longrightarrow x = 2 \in \mathbb{Z}_1$$
 5

$$\lambda = 1 \longrightarrow x = 2 + 5 = 7 \in \mathbb{Z}_1$$
 5

$$\lambda = 2 \rightarrow x = 2 + 10 = 12 \in \mathbb{Z}_{1.5}$$

$$\lambda = 3 \rightarrow x = 2 + 15 = 17 \notin \mathbb{Z}_{15}$$

En conclusión, las tres soluciones de la congruencia lineal  $9x \equiv 3 \pmod{15}$  son  $x \equiv 2, 7 \& 12 \pmod{15}$ .

Ejemplo 2. Encuentre (si existe) la solución de la congruencia lineal  $8x \equiv 12 \pmod{20}$ .

Primero calculamos el mcd(20,8):

$$20 = 2 \cdot 8 + 4$$

$$8 = 2.4$$

 $\therefore$  mcd(20,8) = 4 y como mcd(20,8) = 4 | b = 12, la congruencia lineal sí tiene solución

$$8x \equiv 12 \pmod{20} \rightarrow 8x + 20(-k) = 12$$
 [ec. diofántica]

Por la identidad de Bézout sabemos que existen v y w tales que 8v + 20w = 4.

$$4 = 20 + 8(-2) \rightarrow v = -2 \& w = 1$$

Luego multiplicamos ambos lados de la ecuación por 3:

$$12 = 20(3) + 8(-6) \rightarrow x = -6$$

L	a so	luc	ión	ge	ner	al 1	para	ı la	var	iab	le x	es	x	= -(	5 +	· \(\lambda(2	20/4	1) =	-6	+ 5	λ												
				U		,											1	,															
4	!\R	ecc	ord	eme	os c	que	bus	scar	nos	s so	luc	ion	es (	en Z	Z 2	ο, e	s de	ecir	; 0	$\leq x$	≤ 1	9:											
		2 -	2			- 1																											$\perp$
		λ = λ =																															$\dashv$
		λ =					-																										_
		λ=	= 5	<b>→</b> ,	x =	19																											+
		1		,	1				1			1 - 1	1				_ 1		1.0		10	(	_ 1	20)									
E	n cc	ne	usı	on,	ias	s ci	iatro	o sc	Huc	1011						enc 19				x =	12	(m	oa	20)	SO	n							$\top$
											<i>,</i> ,		, , ,				(111)	<i>J</i> u 2	-0)														
																																	_
E	n re	sun	ner	ı, da	ada	un	a co	ong	rue	ncı	a li	nea	ıl <i>a</i> :	$x \equiv$	b (	mo	d n	) te	nen	10S:													_
•	si 1	nco	l(a.	n)	= 1	$\rightarrow$	· la	con	gru	enc	ia	line	eal 1	ien	e s	solu	ciói	n úi	nica	ì													$\dashv$
	S1 1								D- v				1002			7010	10.																_
																						a,n)	) sc	luc	ion	es							+
		° 1	ncc	l(a,	n)	∤ <i>b</i>	$\rightarrow$	la c	on	gru	enc	ıa I	ine	al t	ien	e n	) ti	ene	sol	ucı	ón												+
																																	$\top$
S	istei	nas	s de	co	ng	rue	enci	as i	line	ale	S																						
n	<b>Nofi</b> z	iai	án	Co	10	1101	<b></b>	gig4	0.222	a d	0.0			om o	• • •	, lin	امما	00.4	0 111			nto	do	do	2.0	má	0.00	200	<b>6</b> 110	nai	20		
	efir neal		UII.	36	16	Hai	IIIa	515t	em	a u	e c	กแล	gru	enc	ıas	5 1111	eai	ies a	a ui	CO	nju	ши	ae	uo	8 0	Ша	s cc	лıg	rue	HCI	as		$\perp$
																																	_
-	jem	nlo	3	End	nie	ntr	e (s	i ex	iste	) la	9 SO	luc	ión	de	l si	igni	ente	e si	ster	ทล (	de d	con	gri	ienc	ias	lin	eale	-S.					
٦,	jeni		J.		Juc	1101	(5	. 0/1	150	, 10	1 50	Tuc	,1011	uc		541		U DI	5001	iiu (		0011	5.0	CIIC	145	1111	Cui						
		<i>x</i> =		`		1																											
		<i>x</i> =	≣ 3	(mo	od :	5)																											
		-										-																					_
					_	_	ir la	i so	luc	ıón	de	la s	sigi	ııer	ite	ma	nera	a x	=x	+;	$x_2$	en (	lon	de .	$x_1$ e	s u	n m	ıúlt	ıplo	de	5 y	$X_2$	_
es	s un	mı	ıltıj	olo	ae	3:							r	= 5	k .	& x	=	3 k															_
													Λ <sub>1</sub>	J.	Λ <sub>1</sub> '	αλ	2	$J_{\kappa_2}$															$\dashv$
d	e ma	ane	ra (	jue	al	eva	ılua	r er	ı la	pri	me	ra e	cua	acić	n.	$x \equiv$	2 (1	noc	13)	ten	em	ios:											$\dashv$
		<i>E</i> 1_	,	2 1-	_ /	) (-		2)		<i>-</i> 1_		) <u> </u> _	2		1_		1_	24	(1_	1-)	_ ^	) Га.		l: _ C		7							$\dashv$
		SK.	_	$\mathcal{K}_2$	= 4	4 (ľ	1100	3)	$\rightarrow$	$\mathcal{SK}_1$	+ -	$K_2$	- 2	_ 3	κ -	<del>)</del> )	κ <sub>1</sub> -	7 3(	$\kappa_2^{-}$	κ)	_ 2	Lec	ن. C	liofa	ıntı	caj							
		5 =	= 1 -	3 +	2																												
		3 =			1																												_
		2 =	= 2	1																													_
		1 =	= 3	_ 2	= 3	3 _ 4	(5 -	3) =	= 3	(2)	+ 5	<b>(_1</b>	) —	<del>)</del> 2	= 1	3(4)	+ 4	5(-2	2) _	→ k	= .	2											$\dashv$
		1	,			' '	(5 =	J)		(2)	. 3	( 1	,		-	J( <u>-</u> T)	<u> </u>	7(-2	<i>'</i>	<sup>1</sup> 1													$\dashv$
S	imil	arn	nen	te a	ıl e	val	uar	x e	n la	se	gun	ıda	ecı	iaci	ión	x =	3 (	(mc	od 5	) te	ner	nos	3:										+
		<i>-</i> 1		2.1		, ,				<i>E</i> 1		1			. 1		(1	1		2 1		Г	ļ ,	1: 0		_ ¬							$\dashv$
		ЭK.	1	$3K_2$	= .	5 (I	nod	3)	$\rightarrow$	$\Im K_1$	+ -	$K_2$	- 3	= 5	K -	<del>)</del> 5	$(k_1)$	- <i>K</i>	) + .	$5K_2$	= 3	Lec	e. c	liofa	ıntı	caj							
		1 =	= 3	- 2	= 3	3 - (	(5 -	3)=	= 3	(2)	+ 5	(-1	) —	→ 3	= 3	3(6)	+ 5	5(-3	3) –	$\rightarrow k$	=	6											
							1	´		ľ		`	1		1			`	ľ	2													

En	co	ncl	usi	ón,	<i>x</i> =	= 5 <i>l</i>	k <sub>1</sub> +	3k	=	<b>5(-</b> 2	2) +	- 3(	6) =	= 8	y la	ı so	luc	ión	de	S15	ster	na (	de (	con	gru	enc	as	lın	eal	es e	S:	
								Í		5(-2			$x \equiv$	8 (	mo	d 1	5)															
$\top$																																
Te	ore	ma	ı. (İ	Тео	ren	ıa e	chir	10 α	lel	resi	duc	)																				
												,																				
Un	sis	ster	na	de	con	ıgrı	uen	cias	s lir	neal	es o	de 1	a fo	orm	ıa <i>a</i>	$_{i}\equiv$	bi (	mo	d n	) ti	ene	so	luc	ión	ún	ica	si:					
				mc	d(n	i, N	j) =	1 (	con	$i \neq$	<i>j</i> , e	s d	ecii	, lo	s n	ıód	ulo	s sc	n p	rin	10S	rel	ativ	/OS	a p	are	S					
Eje	erci	cio	4.	En	cue	ntr	e (s	si e	s po	sib	le)	la s	solu	ıcić	n d	el s	iste	ema	de	co	ngı	uei	ncia	ıs li	nea	iles	:					
3																																
		$x \equiv$																														
		$x \equiv$																														
	-	x =	9 (	mc	od 1	11)																										
	1					7	1 1 \		(5	111			- 7																			
Ayı	иаа	<i>!</i> :-1	om	e x	= (	/ ·	I I );	r +	(5	11)	$x_2$	+ (3	)•/)	$x_3$																		
+																																
+		$\dashv$																														
+																																
+		-																														
		$\dashv$																														
		-																														
							1																									
							1																									
+		-																														
+		-																														
		_																														
_		-																														
		_																														
_		_																														
							1	4	4																							- 1