Máster de Formación de profesorado de Secundaria Obligatoria y Bachillerato.
Curso 2012-2013
COMPLEMENTOS PARA LA FORMACIÓN DISCIPLINAR EN MATEMÁTICAS

HOJA DE PROBLEMAS: Aritmética II.
(Para entregar **a Eugenio** el 26 de febrero.)

Es obvio, pero os recuerdo que, aunque no os salga un problema o un apartado, podéis usarlo para otros. Lo único que hay que evitar son los argumentos circulares.

(1) a) Encuentra el dígito de control c de este código EAN: $5 - 449000 - 00099c$.
b) En este código EAN se ha borrado un número, ¿cuál era?: $5 - 449000 - 03?895$

(2) La letra del NIF es un "dígito" de control que sirve para evitar errores. Cada letra se asigna dependiendo del resto que resulta de dividir el número del DNI entre 23 de acuerdo con la siguiente tabla:

Resto:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
Letra:	T	R	W	A	G	M	Y	F	P	D	X	B	N	J	Z	S	Q	V	H	L	C	K	E

a) Comprueba lo anterior en tu NIF.
b) Calcula la letra que corresponde a estos DNI: 54126620, 02516341, 00001234.
c) Observa que si escribimos las 8 cifras del DNI como $a_7a_6a_5a_5a_3a_2a_1a_0$, y llamamos L a la letra, el NIF satisface la ecuación $\sum_{i=0}^{7} a_i \cdot 10^i - L \equiv 0 \mod 23$
d) Demuestra que si se introduce un error en un dígito del NIF (número o letra) nos daremos siempre cuenta.
e) ¿Nos daremos siempre cuenta si se intercambian dos dígitos (número o letra) del NIF, incluso si no son consecutivos?
f) ¿Cuál es el dígito borrado en el NIF $00230?34 - Z$? ¿Podemos siempre recuperar un dígito (número o letra) que se haya borrado de un NIF si sabemos qué posición ocupaba?
g) Para que todo esto funcione es muy importante escribir **siempre**, como hemos hecho en el apartado b), las 8 cifras del NIF, incluso si son ceros. Para ver por qué es así, encuentra un ejemplo de un NIF con 8 cifras en el que si nos olvidamos de escribir una (nos quedan entonces 7 cifras) la letra no detecte que se ha cometido un error. Por tanto para poder detectar erroresdebemos **insistir** en que nos tienen que dar las 8 cifras.

(3) Un usuario del criptosistema RSA ha publicado la clave $(n, e) = (629, 419)$ y recibe el mensaje cifrado **251**. ¿Cuál era el mensaje original? [NOTA: para simplificar, los mensajes son números. De hecho la respuesta es **208** y se trata de que justifiques cómo se llega a él. Mira el final de la clase.]

(4) Recordemos que $\mathbb{Z}/N$ denota las clases de resto módulo N. Sea $n \in \mathbb{Z}$. Que exista $\frac{1}{n} \in \mathbb{Z}/N$ significa que existe un $x \in \mathbb{Z}$ tal que $x \cdot n \equiv 1 \mod N$. Entonces $x = \frac{1}{n} \in \mathbb{Z}/N$.
El objetivo es demostrar: existe $\frac{1}{n} \in \mathbb{Z}/N \iff (n, N) = 1$.
a) Observa que $x = \frac{1}{n} \in \mathbb{Z}/N \iff$ existe $b \in \mathbb{Z}$ tal que $1 - x \cdot n = b \cdot N$, o lo que es lo mismo, $1 = x \cdot n + b \cdot N$.
b) Demuestra que la existencia de $\frac{1}{n} \in \mathbb{Z}/N \Rightarrow (n, N) = 1$.
c) Utiliza la Identidad de Bezout para demostrar que $(n, N) = 1 \Rightarrow$ existe $\frac{1}{n} \in \mathbb{Z}/N$.

(5) a) Observa que el apartado c) del problema anterior nos da un método para calcular $\frac{1}{n} \in \mathbb{Z}/N$ (cuando existe), y utilízalo para encontrar la (única) solución de $133x \equiv 1000 \mod 2010$.
b) Demuestra que si $N = p$ es primo y $A \not\equiv 0 \mod p$, la ecuación $A \cdot X \equiv B \mod p$ tiene siempre solución y es única.
c) Da un ejemplo de una ecuación de la forma $A \cdot X \equiv B \mod N$, con $A \not\equiv 0 \mod N$, que **no** tenga solución.
d) Da un ejemplo de una ecuación de la forma $A \cdot X \equiv B \mod N$, con $A \not\equiv 0 \mod N$, que tenga **más de una** solución.