Universidad de la República
Facultad de Ingeniería
IMERL: Matemática Discreta 2, semipresencial

Primer parcial (segunda prueba)
24 de setiembre de 2018.
Duración: 3 horas

Ejercicio 1. (9 puntos)
El número de la cédula uruguaya tiene la forma $x_1x_2 \dots x_7 - x_8$ donde cada $x_i, i = 1, 2 \dots 8$ es un dígito de 0 a 9. El dígito verificador x_8 se calcula de la siguiente manera. Sea

$$c = \sum_{i=1}^{7} a_i \cdot x_i,$$

donde $(a_1, a_2, a_3, a_4, a_5, a_6, a_7) = (2, 9, 8, 7, 6, 3, 4)$. Entonces x_8 es: $r \equiv -c \pmod{10},\ 0 \leq r < 10$.

a. Verificar cuál o cuáles de las siguientes cédulas son falsas:

- Cédula (A): 5806386-7. *FALSA*
- Cédula (B): 418160-6. *CORRECTA*

b. Investigar si el dígito verificador detecta el error de copiar mal el segundo dígito.

Solución:
Asumamos que calculamos el código con $x_1, y_2, x_3, x_4, x_5, x_6, x_7$ con $y_2 \neq x_2$, y probemos que el dígito verificador que surge es diferente de x_8.

Calculamos $\sum_{i=1}^{7} a_i \cdot x_i$ y comparamos con $a_1 \cdot x_1 + a_2 \cdot y_2 + \sum_{i=3}^{7} a_i \cdot x_i$, donde $(a_1, a_2, ..., a_7) = (2, 9, 8, 7, 6, 3, 4)$, como arriba.

Asumamos por absurdo que los códigos verificadores coinciden:

$$\sum_{i=1}^{7} a_i \cdot x_i \equiv a_1 \cdot x_1 + a_2 \cdot y_2 + \sum_{i=3}^{7} a_i \cdot x_i \pmod{10},$$

entonces, $a_2 \cdot x_2 \equiv a_2 \cdot y_2 \pmod{10}$. Como $a_2 = 9$ tenemos que $9x_2 \equiv 9y_2 \pmod{10}$, y como 9 es invertible módulo 10, de hecho $9 \cdot 9 \equiv 1 \pmod{10}$, se obtiene que $x_2 \equiv y_2 \pmod{10}$. O sea x_2 es el mismo dígito que y_2, contradiciendo la hipótesis. Por lo tanto lo asumido es falso, con lo cual los dígitos verificadores que surgen son diferentes.

c. Probar que el dígito verificador detecta el error de intercambiar los dos primeros dígitos x_1, x_2.

Solución:

Asumamos que $x_2 \neq x_1$ (sin falta de generalidad podemos asumir que $x_2 > x_1$), pues si son iguales no surge ningún problema en intercambiar los dígitos.
Supongamos que:

$$\sum_{i=1}^{7} a_i \cdot x_i \equiv a_1 \cdot x_2 + a_2 \cdot x_1 + \sum_{i=3}^{7} a_i \cdot x_i \pmod{10}$$

Eso implica que:

$$a_1 \cdot x_2 + a_2 \cdot x_1 \equiv a_1 \cdot x_1 + a_2 \cdot x_2 \pmod{10}.$$

Luego:

$$x_1 \cdot (a_2 - a_1) \equiv x_2 \cdot (a_2 - a_1) \pmod{10}.$$

Como $a_2 = 9$ y $a_1 = 2$ tenemos que $a_2 - a_1 = 7$. Luego, como $\text{mcd}(7, 10) = 1$, se tiene que 7 es invertible módulo 10. De hecho $7 \cdot 3 \equiv 1$ (mód 10).

Habíamos obtenido que: $7 \cdot x_1 \equiv 7 \cdot x_2$ (mód 10), con lo cual, multiplicando por 3 obtenemos que: $x_1 \equiv x_2$ (mód 10). Como x_1 y x_2 son dígitos (entre 0 y 9) congruentes módulo 10, entonces $x_1 = x_2$, absurdo.
Por lo tanto:

$$\sum_{i=1}^{7} a_i \cdot x_i \not\equiv a_1 \cdot x_2 + a_2 \cdot x_1 + \sum_{i=3}^{7} a_i \cdot x_i \text{ (mód 10)}$$

Ésto es lo que se quería demostrar.

Ejercicio 2. (9 puntos)

a. Demostrar el Teorema de Euler.
Sean $a, n \in \mathbb{Z}$ tales que $\text{mcd}(a, n) = 1$, entonces: $a^{\varphi(n)} \equiv 1 (\text{mód } n)$.

Solución:

Ver la demostración en las notas de teórico (Teorema 2.6.5, página 41).

b. Calcular $22^{232} \equiv x$ (mód 9).

Solución:

Vamos a utilizar el Teorema de Euler con $n = 9$ y $a = 22$ (obsérvese que $\text{mcd}(a, n) = 1$, como pide la hipótesis del teorema citado). Como $\varphi(9) = 6$, tenemos que $22^{\varphi(9)} \equiv 1$ (mód 9), o sea $22^6 \equiv 1$ (mód 9). Luego $22^{232} = 22^{6 \cdot 38 + 4} = (22^6)^{38} \cdot 22^4 \equiv 22^4$ (mód 9). Por otro lado $22 \equiv 4$ (mód 9), lo que implica que $22^4 (\text{mód } 9) \equiv 4^4$ (mód 9). Como $4^2 = 16 \equiv 7$ (mód 9) concluimos que $22^{232} \equiv 7^2$ (mód 9) $\equiv 4$ (mód 9).

c. Calcular $22^{232} \equiv y$ (mód 36).

Solución:

Vimos que $22^{232} \equiv 4$ (mód 9). Por otro lado $22^{232} \equiv 0$ (mód 4) $\equiv 4$ (mód 4). O sea que $22^{232} - 4$ es múltiplo de 9 y es múltiplo de 4. Pero 4 y 9 son primos entre sí, por lo que $22^{232} - 4$ es múltiplo de 36. O sea, $22^{232} \equiv 4$ (mód 36).

Ejercicio 3. (12 puntos)

a. Hallar el mcd $(7^4 - 1, 11^4 - 1)$.

Solución:

Tenemos que $7^4 - 1 = 49 \cdot 49 - 1 = (50 - 1) \cdot (50 - 1) - 1 = 2500 - 100 + 1 - 1 = 2400$.

A su vez $11^4 - 1 = 121 \cdot 121 - 1 = 14641 - 1 = 14640$.

Como $14640 = 2400 \cdot 6 + 240$, tenemos que $\text{mcd}(14640, 2400) = \text{mcd}(2400, 240) = 240$.

b. Demostrar que si $p \geq 7$ es primo entonces $240 | (p^4 - 1)$.

Solución:

Obsérvese que $240 = 24 \cdot 10 = 3 \cdot 8 \cdot 2 \cdot 5$, o sea, $240 = 16 \cdot 3 \cdot 5 = 2^4 \cdot 3 \cdot 5$.
Debemos probar que 2^4 divide a $p^4 - 1$, que 3 divide a $p^4 - 1$ y que 5 divide a $p^4 - 1$, para todo primo $p \geq 7$. Eso es necesario pero también suficiente para probar que 240 divide a $p^4 - 1$ para todo primo $p \geq 7$, pues 2^4, 3 y 5 son primos entre sí.

Probemos primero que 3 divide a $p^4 - 1$: como todos los primos, excepto el 3, son de la forma $3k + 1$ o $3k + 2$, tenemos que $p \equiv 1$ (mód 3) o $p \equiv 2$ (mód 3), para todo primo $p \geq 7$. Luego

$p^2 \equiv 1$ (mód 3), para todo primo $p \geq 7$. Por lo tanto $p^4 \equiv 1$ (mód 3), para todo primo $p \geq 7$. O sea que 3 divide a $p^4 - 1$, para todo primo $p \geq 7$.

Probemos ahora que 5 divide a $p^4 - 1$ para todo primo $p \geq 7$, o equivalentemente, probemos que $p^4 \equiv 1$ (mód 5), para todo primo $p \geq 7$. Sabemos que por ser $p \geq 7$ primo, tenemos que $p \equiv 1$ (mód 5), o $p \equiv 2$ (mód 5), o $p \equiv 3$ (mód 5) $\equiv -2$ (mód 5), o $p \equiv 4$ (mód 5) $\equiv -1$ (mód 5).

En el primer y cuarto caso tenemos que $p^2 \equiv 1$ (mód 5), y en el segundo y tercer caso tenemos que $p^2 \equiv 4$ (mód 5) $\equiv -1$ (mód 5). Luego, elevando nuevamente al cuadrado tenemos que en todos los casos $p^4 \equiv 1$ (mód 5), para todo primo $p \geq 7$, lo que queríamos probar.

Por último queremos probar que $p^4 \equiv 1$ (mód 16), para todo primo $p \geq 7$. Todos los primos, excepto el 2, son de la forma $16k+1$, o $16k+3$, o $16k+5$, o $16k+7$, o $16k+9$, o $16k+11$, o $16k+13$, o $16k+15$. Analizando los 8 casos, como en las discusiones anteriores, vemos que $p^4 \equiv 1$ (mód 16), para todo primo $p \geq 7$.

Luego 2^4, 3 y 5 dividen a $p^4 - 1$ para todo primo $p \geq 7$, lqqd.

c. Sea $A \subset \mathbb{Z}^*$ un subjconjunto no vacío de números enteros diferentes de cero. Definimos $\text{mcd}(A) = \text{máx}\{d \in \mathbb{Z}^+ \ / \ d|a, \text{ para todo } a \in A\}$.
Probar, a partir de las partes anteriores, que: $\text{mcd}\{p^4 - 1 \ / \ p \geq 7, \ p \text{ primo}\} = 240$.

Solución:

Hemos probado que 240 divide a $p^4 - 1$ para todo primo $p \geq 7$, luego $240 = \text{mcd}\{p^4 - 1 \ / \ p \geq 7, \ p \text{ primo}\}$, pues no puede haber un divisor común a todos los números de la forma $p^4 - 1$, con p primo, mayor que 240, porque en la primer parte vimos que el mcd $(7^4 - 1, 11^4 - 1) = 240$.