Ejercicios de CTC):
(Hoja no. 1 Octubre 2018).

1. Encontrar un número de cinco cifras que de restos 3, 5, y 9, cuando se divide por 7, 11 y 17 respectivamente

2. (i) Calcular el órden multiplicativo de 7 mod 601. (Indic. Si $7^a = 1 mod 601$ entonces a divide a 600/2 ó 600/3 ó 600/5.

   (ii) Idem de 3 mod 65537.

3. Sea $m = 2^4.3^3.5^2.7.11.13.19.31.37.41.61.73.181$.

   (a) Calcular $8993^{1082}(\bmod m)$.

   (b) Si a es un entero positivo primo con m y menor que m, encontrar la menor potencia con exponente positivo de a que nos da a^{-1}.

4. Enunciar y demostrar un criterio de divisibilidad entre 4. Idem entre 11. Idem entre 7.

5. Sea $m, e \in \mathbb{N}$ dados, y supongamos que m no divide a e. Probar que el siguiente algoritmo encuentra un α tal que $\alpha \mid m$ y $\mathrm{mcd}(\alpha, e) = 1$. ¿Es la solución encontrada con el algoritmo dado la mayor posible?. Calcular la complejidad del algoritmo.

   Algoritmo: $g_0 := m; h_0 := mcd(m, e)$. Para todo $i \geq 1 : g_i := g_{i-1}/h_{i-1}; h_i := (g_i, h_{i-1})$, hasta $h_l = 1$. Entonces $\alpha := g_l$. (Indicación. Probar que en cada etapa: $\prod_{j=0}^{i-1} h_j g_i = m$))

6. Dar un algoritmo de complejidad $O((\log n)^4)$ para averiguar si un entero $n \in Z^+$ es potencia pura , y si lo es escribirlo como tal: $n = r^k$, para ciertos $r, k \in \mathbb{Z}^+$. (Indicación: Utilícese la misma idea que para calcular la parte entera de la raíz cuadrada de n.)

7. Sea n un entero positivo. Demostrar que si $2^n - 1$ es primo, entonces n es primo, y que si $2^n + 1$ es primo, entonces n es una potencia de 2. Un primo del primer tipo se lama " primo de Mersenne", y uno del segundo "primo de Fermat". Escribir cuatro ejemplos de cada tipo.

8. Utilizando TCR,

   i) Calcular las raíces cuadradas de 1, $mod\, 35$, $mod\, 55$, $mod\, 30$.

   ii) Calcular si existen las raíces cuadradas de : $16 mod\, 21$, $53 mod\, 77$.

9. Sea p un número primo impar y $p - 1 = 2^s t'$ donde t' es impar, y sean $s, t \in \mathbb{N}$ y t también número impar . Demostrar que el número de soluciones en $\mathbb{Z}/ < p >^*$ de la ecuación : $x^{2^r t} = -1 \mathrm{mod} p$ (x es la incógnita) es: 0 si $r \geq s$, y es igual a $2^r \gcd(t, t')$ si $r < s$.

10. Utilizando el ejercicio anterior , encontrar las soluciones de :

$$x^6 \equiv -1 mod\, 25 \times 13$$

    (Indic. Calcular separadamente $x^6 \equiv -1 mod\, 25$ (resp. $mod\, 13$) , aplicando el ejercicio mencionado, y luego usar TCR)

11. Usar el algoritmo de Euclides para encontrar $mcd(f, g)$ y los coeficientes de una identidad de Bezout para f, $gF_p[X]$ en cada uno de los ejemplos siguientes:

    (a) $f = X^3 + X + 1, g = X^2 + X + 1, p = 2$

    (b) $f = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1, g = X^4 + X^2 + X + 1, p = 2$

    (c) $f = X^3 X + 1, g = X^2 + 1, p = 3.(d) f = X^5 + X^4 + X^3 X^2 X + 1, g = X^3 + X^2 + X + 1, p = 3$

12. El cuerpo $\mathbb{F}_{32}$ puede describirse como $\mathbb{Z}/<2>[X]/<X^5+X^2+1>$, $x := X$ m$od.X^5+X^2+$. (i) Calcular $(x^3+x^2)^{-1}$. (ii) Calcular x^{25} en $\mathbb{F}_{32}$ escribiéndolo en función de la base como $\mathbb{Z}/<2>$ espacio vectorial $1, x, x^2, x^3, x^4$. (iii) ¿Es X^5+X^2+1 primitivo? Expresar $(x^{20}+x^{10})$ como potencia de x.

13. Sea un LFSR con $m = 5$ y polinomio asociado $f = X^5 + X^2 + 1 \in \mathbb{F}_2$. Considérese el estado inicial $1, 1, 0, 1, 0$. Se pide: (i) Calcular un polinomio $u(X)$ con $\deg(u) \leq 4$ t.q. denotando $S(X)$ a la función generatriz de la sucesión obtenida por el LFSR se tenga, $S(X) = u/f^*$ (ii) Calcular el periodo de dicha sucesión. ¿Es una sucesión PN?

14. Para cada uno de los cuerpos enumerados abajo, $\mathbb{F}_q$, donde $q = p^r$, p primo, representarlo utilizando un polinomio irreducible con coeficientes en $\mathbb{F}_p$ cuya raíz α sea generador del grupo cíclico $\mathbb{F}_q^*$. Escribir todas las potencias de α como polinomios en α de grado menor que r: (a) $\mathbb{F}_4$, (b) $\mathbb{F}_8$, (c) $\mathbb{F}_{27}$, (d) $\mathbb{F}_{25}$.

15. Sea el cuerpo $K = \mathbb{F}_2[x]/<f(x)>$, donde $f(x) = x^6 + x + 1$. Sea $\alpha = x \,\mathrm{m}od.\, f$. (i) Calcular los órdenes multiplicativos de α y $\beta := \alpha^3$ en K^*. (ii) Demostrar que el polinomio mínimo de β sobre $\mathbb{F}_2$ es $m(x) := x^6 + x^4 + x^2 + x + 1$.

16. i) En los siguientes polinomios irreducibles sobre $\mathbb{F}_2[x]$, cual es el menor n tal que el polinomio $f(x)$ es divisor de $x^n - 1$: (a) $f(x) = x^6 + x^3 + 1$; (b) $f(x) = x^6 + x^5 + 1$

    ii) Calcular, para cada uno de los dos valores de $f(x)$ anteriores (a) y (b)), una raíz del polinomio $f(T) = x^3 + x^2 + 1$ en el cuerpo $\mathbb{F}_2^6 = \mathbb{F}_2[x]/<f(x)>$ en función de la base $\{1, x, ..., x^5\}$ (en cada caso).

    iii) Calcular, para cada uno de los dos valores de $f(x)$ anteriores (a) y (b) (si las hay), las raíces primitivas novenas de la unidad en el cuerpo $\mathbb{F}_2[x]/<f(x)>$ en función de la base $\{1, x, ..., x^5\}$

17. Si $f \in \mathbb{F}_2[x]$ es un polinomio primitivo ¿Lo es tambien su recíproco f^*?

18. Dados $f = x^6 + x + 1, g = x^6 + x^3 + 1 \in \mathbb{F}_2[x]$, ¿Son primitivos? ¿Son irreducibles?

    (ii) Consideremos una secuencia cifrante producida por un LFSR que tiene polinomio característico f, ¿que periodo tendrá esa secuencia en función del valor inicial $(z_0, \ldots, z_5) \in \mathbb{F}_2^6$ que tomemos. Misma pregunta para g.

    (iii) Considérese un sistema de cifrado en flujo que utiliza éste LFSR con distintos valores iniciales para producir secuencias cifrantes de bits, y un criptoanalísta que intenta atacarlo, es decir desconoce el polinomio y el valor inicial usado.¿ Cuántos bits consecutivos del texto original tendrá que descifrar para esperar romper completamente el sistema; es decir, encontrar el polinomio, respectivamente en los dos casos f y g anteriores?

19. Ayudándose del Maple, probar si son primitivos los siguiente polinomios de $\mathbb{F}_2[x]$ que son usados en la actualidad en el algoritmo A5 de cifrado de voz en algunos sistemas de teléfonía móvil : $x^{22} + x + 1$, $x^{23} + x^{15} + x^2 + x + 1$, $x^{17} + x^5 + 1$. En cada caso estudiar, según los valores iniciales cuál será el periodo de una sucesión binaria generada por el LFSR que tiene como polinomio característico cada uno de ellos .