Teoría de Códigos y criptografía
Curso 2009-2010

Hoja 5 (Complejidad. Factorización.)

1. Una de las claves para que RSA funcione es el siguiente resultado: si $n = pq$, con p, q primos distintos, y $ed \equiv 1 \mod \phi(n)$, entonces $(m^e)^d \equiv m \mod n$ para cualquier entero m.

a) Sea ahora $N = mcm(p-1, q-1)$ [mcm=mínimo común múltiplo]. Demuestra que si $ed' \equiv 1 \mod N$, entonces $(m^e)^{d'} \equiv m \mod n$ para cualquier entero m.

b) Dados dos enteros cualesquiera a, b, describe un algoritmo rápido para calcular $mcm(a, b)$, y explica por qué es rápido. [SUGERENCIA: ¿Cuál es la relación entre $mcm(a, b), mcd(a, b)$ y ab?]

2. La siguiente fórmula es bién conocida:

$$\sum_{j=1}^{n} j^2 = \frac{n(n+1)(2n+1)}{6}.$$

Estima en función de n el número de bit-operaciones necesarias para calcular tanto el término de la izquierda como el de la derecha.

3. Se trata de estimar en función de n el número de bit-operaciones necesarias para calcular el producto de todos los números primos menores que n. Suponemos que hemos calculado con anterioridad una lista muy larga que contiene todos los primos menores que n

a) Si definimos $\pi(n) = Card\{p \in \mathbf{N} \mid p < n, p \text{ es primo}\}$, el Teorema del Número Primo nos dice que $\lim_{n\to\infty} \frac{\pi(n)}{n/\log n} = 1$. Utiliza este resultado para estimar el número de dígitos en el producto de todos los números primos menores que n.

b) Da una cota para el número de bit-operaciones necesarias para hacer una de las multiplicaciones que intervienen en dicho producto.

c) Estima el número total de bit-operaciones necesarias para calcular el producto de todos los números primos menores que n.

4. Probar que 15 es un pseudo-primo en base 4, que 28 es un pseudo-primo en base 9 y que 91 es un pseudo-primo en base 3.

5. Sea n un número impar compuesto y sea $(b, n) = 1$.

a) Sea p un divisor primo de n y escribamos $n' = n/p$. Probar que si n es un pseudo-primo en base b entonces $b^{n'-1} \equiv 1 \mod p$.

b) Demostrar que ningún entero de la forma $n = 3p$, con $p > 3$ primo, puede ser un pseudo-primo en bases 2, 5 ni 7.

c) Demostrar que ningún entero de la forma $n = 5p$, con $p > 5$ primo, puede ser un pseudo-primo en bases 2, 3 ni 7.

d) Probar que 91 es el menor pseudo-primo (impar) en base 3.

6. a) Probar que si $2^n - 1$ es primo entonces n es primo, y que si $2^n + 1$ es primo entonces $n = 2^k$. Los números $M_p := 2^p - 1$, con p primo, se llaman "números de Mersenne" y "primos de Mersenne" en caso de ser primos. Los de la forma $F_k := 2^{2^k} + 1$ se llaman "números de Fermat" y "primos de Fermat" si son primos. Los primeros primos de Mersenne son 3,7, 31, 127, y todos los primos de Fermat conocidos son 3, 5, 17, 257 y 65537.

b) Probar que todos los números de Fermat y todos los números de Mersenne son pseudo-primos en base 2. (SUGERENCIA: Para los números de Fermat, estudiar primero $2^{2^k} \mod F_k$, y comprobar que podemos calcular 2^{F_k} a partir de este valor por iteración de cuadrados. Para los de Mersenne, empezar por ver que $p|M_p - 1$ y deducir de ello que $M_p = 2^p - 1|2^{M_p - 1} - 1$.)

c) A pesar de lo anterior, comprobar que uno puede ver que $M_{11} = 2047$ no es primo utilizando un sencillo test de primalidad.

7. Sea n un número de Carmichael. Demostrar que

a) n no es divisible por m^2 para ningun $m > 1$;

b) $n - 1$ es divisible por $p - 1$ para cualquier divisor primo p de n;

c) n es divisible por lo menos por 3 primos.

8. a) Prueba que los siguientes son números de Carmichael: 561, 1105, 1729, 2465, 2821, 6601, 41041, 825265.

b) Demuestra que 561 es el menor número de Carmichael.

9. Supongamos que m es un entero positivo tal que $6m + 1$, $12m + 1$ y $18m + 1$ son todos primos. Demostrar que $n = (6m + 1)(12m + 1)(18m + 1)$ es un número de Carmichael. (Esta idea es una de las que han sido utilizadas para intentar demostrar que hay infinitos números de Carmichael, y durante mucho tiempo fue el método utilizado para encontrar números de Carmichael muy grandes.)

10. Dado que es muy facil saber si un número par es primo o no (el único par primo es el 2), no tiene demasiado sentido aplicar tests de primalidad a los números pares. Sin embargo, y por aquello de tener una teoría completa, se pide: demostrar que no existen números de Carmichael pares, o sea, que para todo n par existe b tal que $(b, n) = 1$ y $b^{n-1} \not\equiv 1 \mod n$.

11. Recordemos que la existencia de infinitos números de Carmichael es un resultado reciente (Alford, Granville, Pomerance 1992). Sin embargo, la existencia de infinitos pseudo-primos (verdaderos, o sea, no primos) en base 2 era bien conocida. Posiblemente la demostración más simple es la siguiente (Malo 1903): probar que si n es un pseudo-primo en base 2 compuesto, entonces $n' := 2^n - 1$ también es un pseudo-primo en base 2 compuesto. (SUGERENCIA: Tanto la composición como la pseudo primalidad se basan en el hecho de que si $a|b$ entonces $2^a - 1|2^b - 1$, y en observar que si n es pseudo-primo en base 2 entonces $n|n' - 1$.)

12. 1. Encontrar los valores de b para cuales 21 es pseudoprimo fuerte en base b.

2. Encontrar los valores de b para cuales 35 es pseudoprimo fuerte en base b.

Los dos ejercicios siguientes muestran que la condición de p seudo-primalidad fuerte es mucho más restrictiva que la de pseudo-primalidad, y cómo esto se puede aprovechar para factorizar.

13. Demuestra que 561, que es incluso un número de Carmichael, no es un pseudo-primo fuerte en base 2. (De hecho, 561 solo es pseudo-primo fuerte en 8 de las 318 bases no triviales posibles. Los otros dos pseudo-primos en base 2 menores que 1000, o sea, 341 y 645, tampoco son pseudo-primos fuertes en base 2.)

14. Prueba que si encontramos un b tal que n es pseudo-primo en base b, pero no pseudo-primo fuerte en base b, entonces no es difícil encontrar un factor no trivial de n.

Algunos problemas relacionados con lo que se utiliza en R.S.A.

15. Encontrar el menor primo mayor que 7674. (La idea es entender cómo se buscan primos "grandes", aunque he limitado el tamaño para que podamos trabajar en la calculadora. Si tienes acceso a un ordenador puedes buscar primos mayores (por ejemplo, de 6 cifras). Las

dos pistas son: buscar siempre los factores "muy pequeños" y recordar que el menor número que es pseudoprimo fuerte en bases 2 y 3 es $1{,}373{,}653 = 829 \cdot 1657$.)

16. Los números 85026517 y 85026567 son producto de dos primos. Factorizarlos.

17. El número 12871 es el producto de dos primos. Utiliza el método de Kraitchick-Dixon para factorizarlo. (Nota: al cribar los $Q(x)$ no hace falta que te preocupes de los primos $p \geq 17$.)

18. Sea n un número natural impar.

1. Demostrar que n es divisible por un sólo primo si y sólo si la ecuación $x^2 = \bar{1}$ tiene sólo 2 soluciones $(\pm\bar{1})$ en $\mathbb{Z}_n$.

2. Suponemos que $a^m = \bar{1}$ para todos $a \in U(\mathbb{Z}_n)$. Demostrar que m es un número par.

3. Suponemos que $a^m = \bar{1}$ para todos $a \in U(\mathbb{Z}_n)$ pero existe $b \in U(\mathbb{Z}_n)$ tal que $b^{\frac{m}{2}} \neq \bar{1}$. Demostrar que $a^{\frac{m}{2}} \neq \bar{1}$ por lo menos para la mitad de los elementos en $U(\mathbb{Z}_n)$.

4. Suponemos que n es producto de 2 primos impares p y q y m cumple que $a^m = \bar{1}$ para todos $a \in U(\mathbb{Z}_n)$ pero existe $b \in U(\mathbb{Z}_n)$ tal que $b^{\frac{m}{2}} \neq \bar{1}$. Sea A el subconjunto de $U(\mathbb{Z}_n)$ tal que $a^{\frac{m}{2}} - \bar{1}$ es divisible sólo por uno de los primos p or q. Demostrar que A tiene la mitad de los elementos de $U(\mathbb{Z}_n)$.

5. Suponemos que n es producto de 2 primos impares p y q. Usando los apartados anteriores construir un algoritmo probabilístico que dado un algoritmo que rompe RSA (es decir, busca la clave d a partir de la clave e) descompone n con una probabilidad alta.

19. Suponemos que N es producto de dos primos distintos. Demostrar que si conocemos $x \in \mathbb{Z}/N\mathbb{Z}$ distinto de $\bar{0}$ y $\bar{1}$ tal que $x^2 = x$, entonces podemos factorizar N de forma eficiente.

20. Al cifrar los mensajes mediante el criptosistema RSA el primer número n de la clave (n, e) de un usario se coge igual al producto de 2 primos distintos.

1) ¿Porqué no se usan claves con n igual a un número primo?

2) ¿Qué ventajas o desventajas tendrías si usaras una clave con n igual al producto de 3 primos distintos?