Pontificia Universidad Católica de Chile
Escuela de Ingeniería
Departamento de Ciencias de la Computación

Ayudante: Nicholas Mc-Donnell
Email: namcdonnell@uc.cl

Ayudantía 09

Euler-Fermat y Teorema Fundamental de la Aritmética

IIC3253 – Criptografía

Fecha: 2021-05-26

1. Euler-Fermat

1.1. Recordatorio

Teorema 1.1 (Inverso Modular)**.** *Dado $a \in \mathbb{Z}$, existe $a^{-1} \in \mathbb{Z}$ tal que $a \cdot a^{-1} \equiv 1 \mod n$ si y solo si* $\gcd(a, n) = 1$.

Definición 1.1 ($\mathbb{Z}_n^*$)**.** Se define $\mathbb{Z}_n^*$ como el conjunto $\{a \in \mathbb{Z} \mid 1 \leq a < n \wedge \gcd(a, n) = 1\}$.

Definición 1.2 (Función φ)**.** La función $\varphi : \mathbb{N} \to \mathbb{N}$ se define como

$$\varphi(n) = |\mathbb{Z}_n^*| .$$

1.2. Teorema Euler-Fermat

Teorema 1.2 (Euler-Fermat)**.** *Dado $a \in \mathbb{Z}$ tal que* $\gcd(a, n) = 1$*, se tiene que*

$$a^{\varphi(n)} \equiv 1 \mod n$$

Demostración. Se toma la función

$$\begin{aligned} f_a : &\mathbb{Z}_n^* \to \mathbb{Z}_n^* \\ &x \mapsto (ax) \mod n \end{aligned}$$

y se nota que es una biyección, por lo que se tiene la siguiente congruencia:

$$\begin{aligned} x_1 \cdot \ldots \cdot x_{\varphi(n)} &\equiv (ax_1) \cdot \ldots \cdot (ax_{\varphi(n)}) \mod n \\ &\equiv a^{\varphi(n)} x_1 \cdot \ldots \cdot x_{\varphi(n)} \mod n \end{aligned}$$

Multiplicando por los inversos de cada x_i a cada lado se llega a lo pedido. □

Problema 1:
Demuestre que f_a es una biyección. (*Hint: demuestre que $f_{a^{-1}}$ es su inversa.*)

Teorema 1.3. *Dado p, q primos distintos se tiene que $\varphi(p) = p-1$ y $\varphi(pq) = (p-1)(q-1)$.*

Demostración. El primer resultado es inmediato ya que para todo $1 \leq a < p$ se tiene que $\gcd(a, p) = 1$ por definición de primo. Para el segundo resultado, se nota que se pueden contar los a tal que $\gcd(a, pq) > 1$, estos son los números que son divisibles por p o por q que son menores a pq, como el menor entero positivo divisible por p y por q es pq se tiene que solo hay que contar enteros divisibles por p y después enteros divisibles por q. Se nota que los enteros divisible por p son $p, 2p, \ldots, (q-1)p$, que son $q-1$, y similarmente hay $p-1$ divisibles por q. Por lo que $\varphi(pq) = (pq-1) - (q-1) - (p-1) = pq - p - q + 1 = (p-1)(q-1)$. □

Problema 2:
Demuestre que $\varphi(p^n) = p^{n-1}(p-1)$ para p primo.(*Hint: cuente los que no son coprimos.*)

2. Teorema Fundamental de la Aritmética

Teorema 2.1. *Dado $a, b, c \in \mathbb{Z}$ tales que $\gcd(a, b) = 1$ y $a \mid bc$, entonces $a \mid c$.*

Demostración. Como $a \mid bc$ se tiene que $ak = bc$ para algún $k \in \mathbb{Z}$. Usando Bezout se tiene que $ax + by = 1$ para algunos $x, y \in \mathbb{Z}$, multiplicando todo por c se tiene que $acx + bcy = c$ y reemplazando se tiene $a(cx + ky) = c$, con lo que se concluye que $a \mid c$. □

Lema 2.2. *Dado p primo y $a, b \in \mathbb{Z}$, se tiene que si $p \mid ab$ entonces $p \mid a$ o $p \mid b$.*

Demostración. Si $p \mid a$, se tiene el resultado. En otro caso, se tiene que $\gcd(a, p) = 1$, por lo que por el teorema anterior se tiene que $p \mid b$. □

Teorema 2.3 (Teorema Fundamental de la Aritmética)**.** *Todo entero descomposición en producto de primos, y es única salvo reordenamientos.*

Demostración. Para la existencia se usará inducción fuerte. El paso base es $n = 2$, se sabe que 2 es primo, por lo que se tiene el caso base. Dado n si es primo, se tiene lo pedido, si no, existen $1 < a, b < n$ tales que $n = ab$, y por hipótesis inductiva se tiene que $a = p_1 \cdot \ldots \cdot p_k$ y $b = q_1 \cdot \ldots \cdot q_l$, por lo que $ab = p_1 \cdot \ldots \cdot p_k \cdot q_1 \cdot \ldots \cdot q_l$, con lo que se tiene lo pedido.

Para la unicidad dado n se toman dos descomposiciones primas, $n = p_1 \cdot \ldots \cdot p_k = q_1 \cdot \ldots \cdot q_l$. Dado p_1, como $p_1 \mid n$ por el lema anterior se tiene que $p_1 \mid q_i$ para algún i, y por definición de primo se tiene que $p_1 = q_i$, dividiendo ambos lados por p_1 se tiene el mismo caso, pero con menos primos, por lo tanto se tiene lo pedido. □

Nota. *Dado que los primos tienen un orden natural, hay una descomposición canónica de cada entero n, donde $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, $\alpha_i \geq 0$ y p_i es el i-ésimo primo..*

2.1. Aplicaciones y Problemas

Problema 1:

Demuestre que dado $a, b \in \mathbb{Z}$, donde $a = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ y $b = p_1^{\beta} \cdot \ldots \cdot p_k^{\beta}$, se tiene que $\gcd(a, b) = p_1^{\min(\alpha_1, \beta_1)} \cdot \ldots \cdot p_k^{\min(\alpha_k, \beta_k)}$.

Ejemplo: 2.1. Se tienen $a = 24$ y $b = 60$, se nota que $\gcd(a, b) = 12 = 2^2 \cdot 3$, y que $a = 2^3 \cdot 3$ y $b = 2^2 \cdot 3 \cdot 5$.

Problema 2:

Dados $a, b \in \mathbb{Z}$ tales que $\gcd(a, b) = 1$ y $ax = by$ demuestre que $a \mid y$ y $b \mid x$ usando TFA.

Demostración. Demostración sin TFA: Se nota que $a \mid by$ por lo que por teorema demostrado anteriormente se tiene que $a \mid y$, similarmente se tiene que $b \mid x$. □

Problema 3:

Demuestre usando TFA que si $a^2 \mid b^2$ entonces $a \mid b$.

Problema 4:

Demuestre lo anterior sin TFA.

Problema Bonus:

Demuestre que existe una función f de $\mathbb{N}$ a las secuencias de naturales con finitos términos no ceros[1] tal que $f(a \cdot b) = f(a) + f(b)$, si y solo si se tiene TFA y existen infinitos primos.

[1] De forma más precisa, al conjunto $\{\{a_n\}_{n \in \mathbb{N}} \mid \forall n \in \mathbb{N}\, a_n \in \mathbb{N}$ y para finitos n se tiene que $a_n \neq 0\}$.