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

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

Ayudantía 04

Aritmética Modular

IIC3253 – Criptografía

Fecha: 2021-04-14

1. Inverso Modular

Teorema 1.1 (Algoritmo Extendido de Euclides)**.** *Dado* $a, b \in \mathbb{Z}$ *el algoritmo devuelve* $x, y, g \in \mathbb{Z}$ *tales que* $ax + by = g$ *y* $g = \gcd(a, b)$*, en* $O(\log(\text{mín}(a, b)))$ *pasos.*

Corolario (Bezout)**.** *Dado* $a, b \in \mathbb{Z}$ *existen* $x, y, g \in \mathbb{Z}$ *tales que* $ax + by = g$ *y* $g = \gcd(a, b)$*.*

Definición 1.1 (Inverso Modular)**.** Dado $a, b \in \mathbb{Z}$, se dice que b es el inverso modular de a si y solo si $ab \equiv 1 \mod n$. En general b se denota como a^{-1}.

Problema 1:
Demuestre que el inverso modular es único modulo n.

Teorema 1.2 (Inverso Modular)**.** *Dado* $a \in \mathbb{Z}$*, a tiene inverso modular si y solo si* $\gcd(a, n) = 1$*.*

Para demostrar el teorema se demostrará un lema, respecto al siguiente concepto.

Definición 1.2 (Divisor de Cero)**.** Sea $a \in \mathbb{Z}$ tal que $a \not\equiv 0 \mod n$, se dice que a es divisor de cero, si y solo si existe un $b \in \mathbb{Z}$ tal que $b \not\equiv 0 \mod n$ y $ab \equiv 0 \mod n$.

Lema 1.3. *Sea* $a \in \mathbb{Z}$ *un divisor de cero, entonces a no tiene inverso modular.*

Demostración. Se asume por contradicción que a tiene inverso modular, sea $b \in \mathbb{Z}$ tal que $b \not\equiv 0 \mod n$ y $ab \equiv 0 \mod n$. Entonces se tiene que

$$\begin{aligned} a \cdot a^{-1} &\equiv 1 \mod n \\ b(a \cdot a^{-1}) &\equiv b \mod n \\ (ba)a^{-1} &\equiv b \mod n \\ 0 \cdot a^{-1} &\equiv b \mod n \\ 0 &\equiv b \mod n \end{aligned}$$

lo cual es una contradicción. □

Volviendo al teorema de Inverso Modular:

Demostración. $\underline{\Longleftarrow}$ Por Bezout se tiene que existen $x, y \in \mathbb{Z}$ tales que $ax + ny = 1$, por lo que $n \mid 1 - ax$, o sea, $ax \equiv= 1 \mod n$, lo que nos dice que a tiene inverso modular.

$\underline{\Longrightarrow}$ Usando contrapositiva se tiene que $\gcd(a, b) = g > 1$, como $g \mid n$ y $g \mid a$, entonces $\frac{n}{g} \in \mathbb{Z}$ y $\frac{a}{g} \in \mathbb{Z}$. Por lo que $n \mid \frac{an}{g}$, pero $n \nmid \frac{n}{g}$, con lo que se tiene que $a \cdot \frac{n}{g} \equiv 0 \mod n$, por lo que a es divisor de cero, y usando el lema anterior se tiene que a no tiene inverso modular. □

2. Congruencias Lineales

Definición 2.1 (Congruencia Lineal)**.** Dado $a, b, c \in \mathbb{Z}$, se dice que $ax + b \equiv c \mod n$ es una congruencia lineal.

Nota. *Es claro que toda congruencia lineal se puede reducir a la forma* $ax \equiv b \mod n$.

Teorema 2.1. *Las congruencias lineales de la forma* $ax \equiv b \mod n$ *tienen solución si y solo si* $\gcd(a, n) \mid b$ *o* $b \equiv 0 \mod n$.

Demostración. $\underline{\Longleftarrow}$ Sea $g = \gcd(a, n)$, si $g = 1$, entonces la congruencia tiene como solución $x \equiv a^{-1}b \mod n$. Si $g \mid b$ y $g > 1$, entonces se toma $a' = a/g$, $b' = b/g$ y $n' = n/g$, se nota que $a'x \equiv b' \mod n'$ tiene solución, ya que $\gcd(a', n') = 1$, por lo que $ax \equiv b \mod n$ tiene solución. Si $b \equiv 0 \mod n$, entonces $x \equiv 0 \mod n$ es solución.

$\underline{\Longrightarrow}$ Usando contrapositiva y contradicción se tiene que g no divide a b y $b \not\equiv 0 \mod n$. Se ve lo siguiente

$$\begin{aligned} ax \equiv b \mod n &\iff n \mid ax - b \\ &\iff ny = ax - b \\ &\iff b = ax - ny, \end{aligned}$$

más aún $g \mid a$ y $g \mid n$, por lo que $g \mid ax - ny$, pero eso es lo mismo que $g \mid b$, lo que es una contradicción. $\square$