PRUEBAS DE CONOCIMIENTO CERO Y SUS APLICACIONES

JOSÉ LUIS CÁNOVAS SÁNCHEZ

Tutores
LEANDRO MARÍN MUÑOZ
ANTONIO JOSÉ PALLARÉS RUIZ

Facultad de Matemáticas
Universidad de Murcia

José Luis Cánovas Sánchez: *Pruebas de Conocimiento Cero y sus Aplicaciones,* Junio 2017

RESUMEN

TODO

Short summary of the contents in -English- Spanish. . . a great guide by Kent Beck how to write good abstracts can be found here:

`https://plg.uwaterloo.ca/~migod/research/beckOOPSLA.html`

ABSTRACT

1500 words of Introduction in English. . .

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

LISTINGS

ACRONYMS

1 INTRODUCCIÓN

2 PRELIMINARES

Para poder comprender los resultados de los siguientes capítulos necesitaremos recordar ciertas definiciones y propiedades de álgebra que se cursan durante el grado, e introducir otros preliminares de algoritmia que formalizan el estudio. No incluiremos demostraciones, pues son los conceptos básicos de donde partiremos para desarrollar el resto del trabajo, pero el lector que quiera conocerlas puede consultar las referencias en **TODO: cite**.

2.1 PRELIMINARES DE ÁLGEBRA

ARITMÉTICA ELEMENTAL

Definición 2.1. Un entero d se dice que es el **máximo común divisor** de dos enteros a y b si es el mayor entero que divide a ambos. Lo denotaremos $d = \mathrm{mcd}(a, b)$.

Euclides describió en su obra *Los Elementos* un método para calcular el mcd de dos enteros, que hoy en día se conoce como *Algoritmo de Euclides*. La propiedad que utiliza el algoritmo para calcular el mcd es la siguiente:

Proposición 2.2. *Sean $a, b \in \mathbb{Z}$. Entonces, para todo $\alpha \in \mathbb{Z}$ se tiene:*

$$\mathrm{mcd}(a, b) = \mathrm{mcd}(a, b - \alpha a) = \mathrm{mcd}(a - \alpha b, b).$$

En particular, cuando $b \neq 0$ y la división entera de a entre b es $a = bq + r$, tenemos que $\mathrm{mcd}(a, b) = \mathrm{mcd}(b, r)$.

Algoritmo 2.3 (Euclides)**.** Encuentra el mcd de $a, b \in \mathbb{Z}$:

1. Inicializa $r_0 = a$ y $r_1 = b$.
2. Calcula las siguientes divisiones euclídeas

$$\begin{aligned} r_0 &= q_1 r_1 + r_2 \\ r_1 &= q_2 r_2 + r_3 \\ &\dots \\ r_{n-3} &= q_{n-2} r_{n-2} + r_{n-1} \\ r_{n-2} &= q_{n-1} r_{n-1} + r_n \end{aligned}$$

   hasta que se obtenga un $r_n = 0$, con $r_{n-1} \neq 0$.

3. Como $b = r_1 > r_2 > ... \geqslant 0$ y cada r_i es entero, para $i = 1, 2, ...$, se obtiene $r_n = 0$ en un número finito de pasos y acaba el algoritmo con $\mathrm{mcd}(a, b) = r_{n-1}$.

A partir del *Algoritmo de Euclides* se puede expresar d como una "combinación $\mathbb{Z}$-lineal" de a y b:

$$d = as + bt$$

conocida como la *Identidad de Bézout*.

El algoritmo se conoce como *Algoritmo de Euclides extendido*:

Algoritmo 2.4 (Euclides extendido)**.** Encuentra el $d = \mathrm{mcd}$ de a, $b \in \mathbb{Z}$ y valores s, $t \in \mathbb{Z}$ tal que $d = as + bt$.

1. Inicializa $r_0 \leftarrow a, r_1 \leftarrow b, s_0 \leftarrow 1, t_0 \leftarrow 0, s_1 \leftarrow 0, t_1 \leftarrow 1$
   $i \leftarrow 1$
2. Mientras $r_i \neq 0$:
   Calcule la división euclídea $r_{i-1} = q_i r_i + r_{i+1}$
   $s_{i+1} \leftarrow s_{i-1} - q_i s_i$
   $t_{i+1} \leftarrow t_{i-1} - q_i t_i$
   $i \leftarrow i + 1$
3. $d = r_{i-1} \quad s = s_{i-1} \quad t = t_{i-1}$

Observación. Los valores de s y t no tienen por qué ser únicos:
$a(s - kb) + b(t + ka) = as - kba + bt + kba = as + bt = d$

Utilizaremos la Identidad de Bézout para calcular los inversos en aritmética modular.

GRUPOS Y ANILLOS

CONGRUENCIAS

Definición 2.5. Sean a, b, $n \in \mathbb{Z}$, $n \neq 0$, diremos que a y b son **congruentes módulo** n, y lo escribiremos $a \equiv b \bmod n$, si la diferencia $a - b$ es múltiplo de n.

Cuando $a \equiv b \bmod n$ decimos que b es un ***residuo*** *de* a *módulo* n.

Proposición 2.6. *La relación de* ***congruencia módulo*** n *es una relación de equivalencia, es decir, es reflexiva, simétrica y transitiva.*

Esto establece una relación de equivalencia en $\mathbb{Z}$, en la que la **clase** de un entero a módulo n es $\overline{a} = \{a + kn\}_{k \in \mathbb{Z}}$. Cuando no exista confusión, escribiremos la clase de equivalencia $\overline{a}$ como a. El correspondiente conjunto cociente, de las *clases de resto módulo* n, es $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots \overline{n-1}\}$, y hereda la suma y producto de $\mathbb{Z}$ convirtiéndose en un anillo conmutativo con neutros $\overline{0}$ para la suma y $\overline{1}$ para el producto.

Teorema 2.7. *El anillo* $\mathbb{Z}_n$ *es un cuerpo cuando* n *es un número primo.*

Teorema 2.8 (Euler)**.** *Si* x *es coprimo con*

Si tenemos ahora dos enteros a y b coprimos, es decir, $\mathrm{mcd}(a, b) = 1$, usando el *algoritmo de Euclides extendido* podemos encontrar r y s de la *Identidad de Bézout* tales que:

$$as + bt = 1$$

Si a esta igualdad le aplicamos módulo b, obtenemos el inverso de a en $\mathbb{Z}_b$:

$$\begin{array}{ccccc} (as + bt) \bmod b & \equiv & as \bmod b & \equiv & 1 \bmod b \\ \overline{as + bt} & = & \overline{as} & = & \overline{1} \end{array}$$

Así hemos demostrado el siguiente resultado:

Proposición 2.9. *Si* $\mathrm{mcd}(a, n) = 1$*, entonces el elemento inverso* a^{-1}*,* $0 < a^{-1} < n$*, existe y* $aa^{-1} \equiv 1 \bmod n$*.*

2.2 PRELIMINARES DE CRIPTOGRAFÍA

Teoría de complejidad algorítmica, problema de P NP, problema RSA de factorizar N, problemas de decisión, estadística usada en el estudio de los ZKP (*ensembles*), *probabilistic computations*, ...

La mayor parte está en los primeros capítulos de Fundamentals of Computer Security, y de sus referencias se podrá sacar más detallado.

3 RESIDUOS CUADRÁTICOS

TODO : Párrafo de introducción al capítulo y referencias

Teoría de símbolos de Lebesgue, ..., residuos cuadráticos, cálculo de raíz discreta?

Definición 3.1. Sea $a \in \mathbb{Z}_n^*$. Se dice que a es un *residuo cuadrático* módulo n, o un *cuadrado* módulo n, si existe un $x \in \mathbb{Z}_n^*$ tal que $x^2 \equiv a \bmod n$. Si no existe dicho x, entonces a se llama un *no-residuo cuadrático* módulo n.

El conjunto de todos los residuos cuadráticos módulo n de $\mathbb{Z}_n^*$ los denotaremos como Q_n o bien como $\mathbb{Z}_n^{Q+}$. Al conjunto de los no-residuos cuadráticos lo denotamos como $\overline{Q_n}$.

Observación. Por definición $0 \notin \mathbb{Z}_n^*$, y por tanto $0 \notin Q_n$ y $0 \notin \overline{Q_n}$.

Proposición 3.2. *Sea p un primo impar. Se cumple que $|Q_p| = \frac{p-1}{2}$ y $|\overline{Q_p}| = \frac{p-1}{2}$, es decir, la mitad de los elementos de $\mathbb{Z}_p^*$ son residuos cuadráticos, y la otra mitad no-residuos cuadráticos.*

Demostración. Sea $\alpha \in \mathbb{Z}_p^*$ un generador de $\mathbb{Z}_p^*$. Un elemento $a \in \mathbb{Z}_p^*$ es un residuo cuadrático módulo p sii $a \equiv \alpha^i \bmod p$ donde i es un entero par. Como p es primo, $\phi(p) = p - 1 = |\mathbb{Z}_p^*|$, que es un entero par, y de ahí se sigue el enunciado. □

3.1 SÍMBOLOS DE LEGENDRE-JACOBI-KRONECKER

4 PRUEBAS DE CONOCIMIENTO CERO

4.1 DEFINICIÓN

4.2 ESTUDIO DE ZKPS

Una subsección por cada ZKP analizado.

5 APLICACIONES DE ZKP

?

Aplicación de ZKP en los certificados de Idemix. Analizar cómo realizan pruebas de Y, O, etc.

6

IMPLEMENTACIONES

?

Implementaciones de símbolos, raíz discreta, ZKPs, ...

APPENDIX

A CÓDIGO FUENTE

Listing 1: A floating example (`listings` manual)

```
for i:=maxint downto 0 do
begin
{ do nothing }
end;
```

DECLARACIÓN DE ORIGINALIDAD

Yo, José Luis Cánovas Sánchez, autor del TFG PRUEBAS DE CONOCIMIENTO CERO Y SUS APLICACIONES, bajo la tutela de los profesores Leandro Marín Muñoz y Antonio José Pallarés Ruiz, declaro que el trabajo que presento es original, en el sentido de que ha puesto el mayor empeño en citar debidamente todas las fuentes utilizadas.

Murcia, Junio 2017

José Luis Cánovas Sánchez