La herramienta ArtEM: aritmética entera y modular

Alfonso Gutiérrez, Violeta Migallón, José Penadés
Dpto. de Ciencia de la Computación e Inteligencia Artificial
Universidad de Alicante
03080 Alicante
e-mail: algutlan@hotmail.com
violeta@dccia.ua.es
jpenades@dccia.ua.es

Héctor Migallón
Dpto. de Física y Arquitectura de Computadores
Universidad Miguel Hernández
03202 Elche (Alicante)
e-mail: hmigallon@umh.es

Resumen

Los contenidos de matemática discreta en las titulaciones de informática incluyen una parte relativa a aritmética entera y modular. En este artículo presentamos una herramienta que ha sido diseñada para la realización de las prácticas de dicha parte y que actualmente se está utilizando en la asignatura Matemática Discreta de la Universidad de Alicante.

1. Introducción

La herramienta ArtEM (*Arit*mética *E*ntera y *M*odular) [3], es una aplicación informática programada en Visual Basic [5] y desarrollada con el fin de ser utilizada en las prácticas de cualquier asignatura que incluya como tópicos los relacionados con la aritmética entera y modular [1], [2], [4]. Está estructurada en 5 menús básicos:

- Euclides.
- Ecuaciones diofánticas.
- Números primos.
- Aritmética modular.
- Aplicación a la criptografía.

Los tres primeros menús están dedicados a la aritmética entera, el cuarto menú proporciona cálculos básicos en la aritmética modular como los cálculos del representante de clase, inverso de un elemento, función de Euler y potencias. El quinto menú constituye una aplicación a la criptografía centrándose en dos criptosistemas, uno de clave privada y otro de clave pública.

Todos los algoritmos disponibles en ArtEM se desarrollan de tal forma que el usuario es capaz de reconocer los pasos que se han seguido para su ejecución, de manera que se obtiene un importante valor pedagógico.

En las siguientes secciones describiremos el contenido de ArtEM, estudiando cada uno de sus menús por separado.

2. Menú Euclides

En este menú se desarrolla el algoritmo de Euclides para el cálculo del máximo común divisor de dos enteros. Además de describir el algoritmo de forma genérica se tiene la opción de mostrar todos los cálculos del propio algoritmo, tal y como se muestra en la Figura 1.

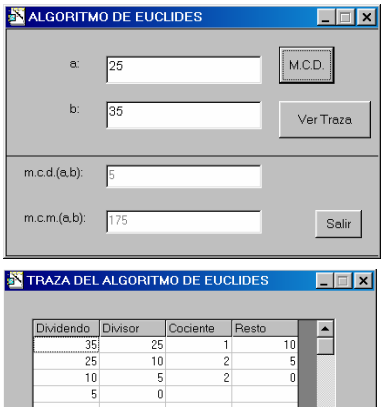

Figura 1. Algoritmo de Euclides

3. Menú ecuaciones diofánticas

En este menú se ofrece la posibilidad de resolver ecuaciones diofánticas, es decir, ecuaciones de la forma $ax+by=c$, donde a, b, c son enteros y x, y son las incógnitas que también son números enteros. Además de mostrar una descripción de los resultados teóricos necesarios para la correcta resolución de estas ecuaciones, se muestra el algoritmo necesario para el cálculo de una solución particular de una ecuación diofántica. En la ejecución del algoritmo, el usuario debe introducir los valores de a, b y c, obteniendo una solución particular de la ecuación diofántica correspondiente -cuya traza puede ser consultada- y la solución general. Como muestra presentamos la solución de la ecuación $2700x + 1500y = 234000$ en la Figura 2.

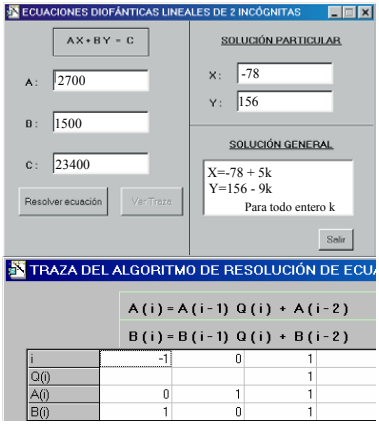

Figura 2. Ecuaciones diofánticas

4. Menú números primos

Se desarrollan en este menú procedimientos para crear una lista de números primos, averiguar si un número entero es primo y factorizar un entero en producto de sus primos. Estos algoritmos vienen acompañados de su descripción formal. La complejidad de estos algoritmos limita su uso a enteros pequeños. Las opciones que presenta este menú vienen indicadas en la Figura 3.

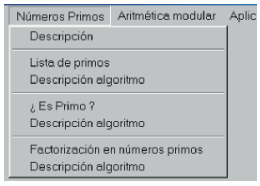

Figura 3. Opciones del menú números primos

5. Menú aritmética modular

Presentamos en este menú diversos cálculos básicos relacionados con la aritmética modular. Éstos son el cálculo del representante de clase en el conjunto de los enteros congruentes módulo n, que representamos por Z_n, el cálculo del inverso en Z_n, el cálculo de la función de Euler y el cálculo de potencias en Z_n. Como muestra presentamos el cálculo de la potencia $[5]^{75}$ en Z_{23}. El programa identifica que el $mcd(5,23)=1$ y por tanto, como el valor de la función de Euler en 23 es 22, se tiene que $[5]^{22}=[1]$. Así, como $[5]^{75}=([5]^{22})^3\ [5]^9$ sólo será necesario calcular $[5]^9 = [5]^8\ [5]$, que en este caso es $[11]$. Mostramos, en la Figura 4, la salida que se obtiene de la ejecución correspondiente a la traza del algoritmo.

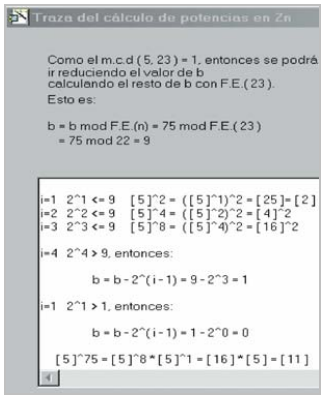

Figura 4. Cálculo de potencias en Z_n

6. Menú aplicación a la criptografía

En este menú pretendemos familiarizarnos con ciertas aplicaciones de la aritmética modular a la criptografía. Tiene dos partes claramente diferenciadas: la elección del alfabeto a utilizar y la elección del sistema criptográfico. En lo que se refiere a la elección del alfabeto, la aplicación tiene preestablecidos una serie de alfabetos que pueden ser seleccionados con el correspondiente menú, como muestra la Figura 5.

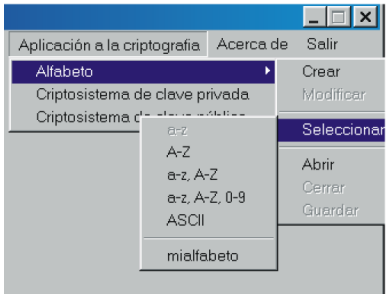

Figura 5. Elección del alfabeto

También se permite crear un alfabeto propio e incluso leerlo de disco si previamente se había creado. Para crear un alfabeto lo único que se debe hacer es ir asignando valores numéricos a cada uno de los caracteres que queremos que formen parte de nuestro alfabeto. El módulo con el que se trabajará en la codificación y descodificación vendrá dado en función del valor numérico asignado mayor. Como ejemplo, en la Figura 6, mostramos el alfabeto *{A,B,C,D,E,F,G}* al que se le han asociado las equivalencias numéricas *{11,16,1,23,20,17,24}* respectivamente y que en la Figura 5 viene definido con el nombre de *mialfabeto*.

Ya sea con un alfabeto creado por el usuario o con un alfabeto predefinido por la aplicación se dispone de dos tipos de criptosistemas: uno de clave privada y otro de clave pública. El criptosistema de clave privada corresponde con un criptosistema clásico cuyas funciones de cifrado y descifrado calculadas sobre Z_n son respectivamente:

$C_{r,s}([m]) = [r][m] + [s], \ / \ mcd(r,n)=1.$
$D_{r,s}([m^*]) = [r]^{-1}([m^*]-[s]).$

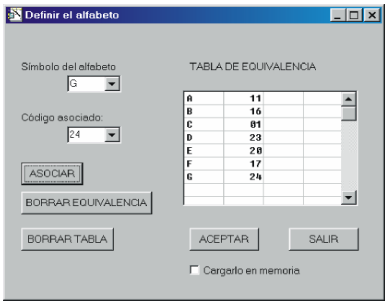

Figura 6. Definición de un nuevo alfabeto

Por su parte, el criptosistema de clave pública corresponde con el código RSA.

Como ejemplo de utilización de la aplicación ArtEM para este tipo de problemas, vamos a suponer que se ha seleccionado el alfabeto predefinido formado por los caracteres de la *A* a la *Z*, de la *a* a la *z*, y el espacio en blanco. Esto hace un total de *55* caracteres por lo que trabajaremos en Z_{55}. Vamos a realizar una codificación utilizando el criptosistema de clave privada. En primer lugar el programa nos pedirá *r* y *s*. Como *mcd(r,55)* debe ser *1*, el programa nos indica posibles valores de *r* a partir de un valor mínimo que el usuario introduce.

Si por ejemplo seleccionamos *s=8* y *r=6*, podremos, a través del botón *continuar*, iniciar una codificación con estas claves. La Figura 7 muestra la codificación de la frase "Esto es una prueba" usando este sistema criptográfico de clave privada y las claves anteriores. La primera ventana contiene la frase en cuestión que queremos codificar, la segunda ventana contiene la transcripción inmediata según el alfabeto que hayamos elegido y que se encuentra en la tabla de conversión, la tercera ventana contiene los valores numéricos de la codificación y la última ventana ya reproduce los caracteres codificados.

Así, con este sistema criptográfico la frase "Esto es una prueba" ha quedado codificada como "fJOñCcJCUhFCsDUcLF". La aplicación también permite invertir el proceso para descodificar un texto determinado. El proceso se realiza paso por paso pinchando en la correspondiente pestaña y en cada paso la aplicación nos da información de qué es lo que está haciendo.

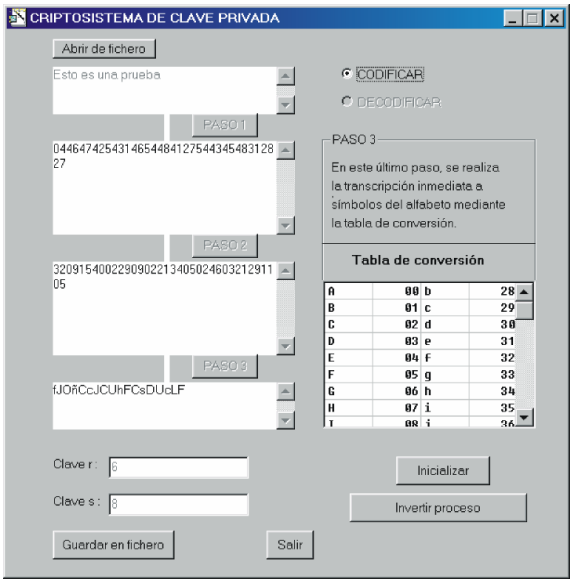

Figura 7. Ejemplo de codificación

7. Conclusión

El objetivo que nos marcamos con el diseño de la herramienta ArtEM fue el intentar impulsar el aprendizaje, experimentación, asimilación y ampliación de algunos de los contenidos de la matemática discreta, por parte del alumnado, con el uso del ordenador. No se trata de aprender a programar, pues para ello ya existen otras asignaturas, sino de aprovechar las capacidades pedagógicas del ordenador en beneficio de la calidad de nuestra docencia. La experiencia ha mostrado que el interés por parte del alumnado es muy aceptable y que además dichas prácticas facilitan la asimilación y comprensión de los contenidos de la aritmética entera y modular.

Tengamos en cuenta que, para el alumnado de informática en particular, esta materia tiene un grado de dificultad bastante considerable.

Referencias

[1] Biggs, N.L. *Matemática discreta.* Vicens Vives, 1994.

[2] Dierker, P.F., Voxman, W.L. *Discrete mathematics*. HBJ, 1986.

[3] Gutiérrez, A., Migallón, H., Migallón V., Penadés, J. *ArtEM*. Disponible en http://www.dccia.ua.es/~jpenades/ArtEM.html.

[4] Grimaldi, R.P. *Matemáticas discretas y combinatoria. Una introducción con aplicaciones*. Addison-Wesley, 1998.

[5] Petroutsos E., *Visual Basic 6*. Ediciones Anaya Multimedia S. A., 1999.