Francisco Javier Romero Yesares

Manual de usuario

Aritmética modular

Para ejecutar el programa abrimos una ventana del terminal de Linux.
Navegamos hasta el directorio donde se encuentra el programa.
Ejecutamos la orden **./aritmetica_modular**.

Al abrirse el programa se mostrará un menú en que podemos elegir varias opciones:

1. **Potencia**. En esta opción podremos calcular la potencia de **a** elevado a **b** con modulo **p**. P debe ser un número primo. Se utilizará el teorema de Fermat.
2. **Logaritmo v1**. En esta opción podremos calcular el logaritmo en base **a** de **b** en modulo **p.** P debe ser un número primo. En este algoritmo se crearán las dos tablas para el algoritmo de Shanks.
3. **Logaritmo v2**. En esta opción podremos calcular el logaritmo en base **a** de **b** en modulo **p**. P debe ser un número primo. En este algoritmo se creará únicamente una tabla para el algoritmo de Shanks.
4. **Todos**. En esta opción podremos resolver los tres apartados anteriores de una vez.
5. **Salir**. En esta opción podremos abandonar el programa.

Al elegir alguna de las opciones, se nos pedirán tres números: **a, b** y **p**. Estos números serán los utilizados para los cálculos de la siguiente manera.

Potencia: $\mathbf{a^b \pmod p}$

Logartimo v1 y v2: $\mathbf{\log_a b \pmod p}$

Cuando ejecutamos alguna de estas opciones se nos mostrará el resultado, en caso de que exista y el tiempo de cálculo.

Ejemplo:

Calculando la potencia.
Para a=7, b=111, p=53.

Resultado potencia: 29
Tiempo potencia: 1.1e-05 segundos