# Lista 2

# Grupo MV:

Marcos Gabriel Leão Muñoz - 11611BCC026

Vitor Martins Basso - 11611BCC034

**OBS.: Todos os códigos usados nas questões estão em anexo**

**Exercise 2.1.1 - For the tiny Lehmer generator defined by g(x) = ax mod 127, find all the full-period multipliers.**

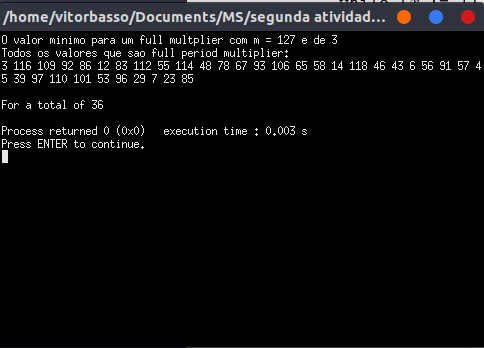
**a) How many are there?**

**b) What is the smallest multiplier?**

**Resposta:**

**A)** Para um m = 127, existem 36 full period multipliers.

**B)** Para um m = 127, o menor valor para um full period multipliers é 3.



**Exercise 2.1.6 - In ANSI C an int is guaranteed to hold all integer values between −(2^15 −1) and 2^15 −1 inclusive.**

**(a) What is the largest prime modulus in this range?**

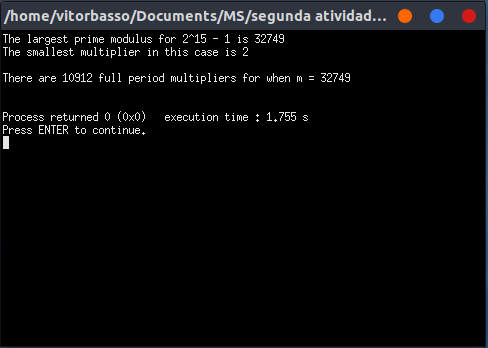
**(b) How many corresponding full-period multipliers are there and what is the smallest one?**

**Resposta:**

**(A) :** O maior módulo primo é 32749

**(B) :** Usando os fatores de (32749 – 1) :

(((2-1)\*(3-1)\*(2729-1))/9)\*(32749-1) = 10912 full-period multipliers. Detalhes no código.



**Exercise 2.1.8**

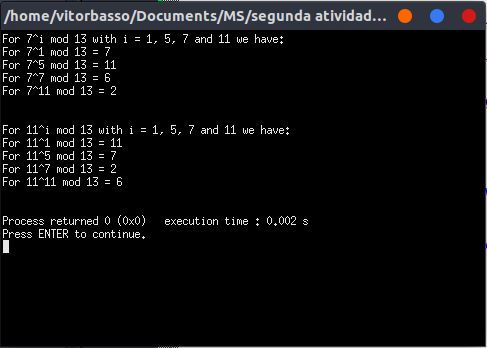
**(a) Evaluate 7^i mod 13 and 11^i mod 13 for i = 1, 5, 7, 11.**

**(b) How does this relate to Example 2.1.5?**

**Resposta:**

**(A):** Resultados na foto.

**(B):** O exemplo 2.1.5 contém os mesmos *a* full-period desta questão, porque o mesmo *m* é usado. O teorema 2.1.4 diz que dado um *a* full-period com modulo *m* primo, pode-se encontrar o resto dos full-period com a fórmula



**Exercise 2.1.9 –**

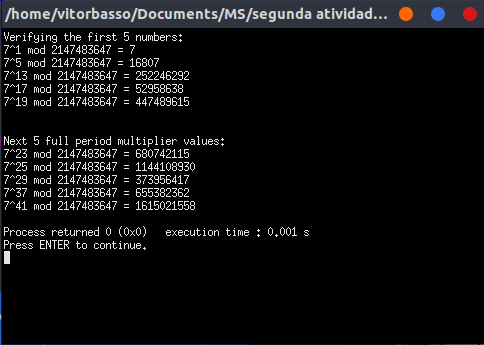
**(a) Verify that the list of five full-period multipliers in Example 2.1.6 is correct.**

**(b) What are the next five elements in this list?**

**Resposta:**

**(A):** Verificação demonstrada na foto.

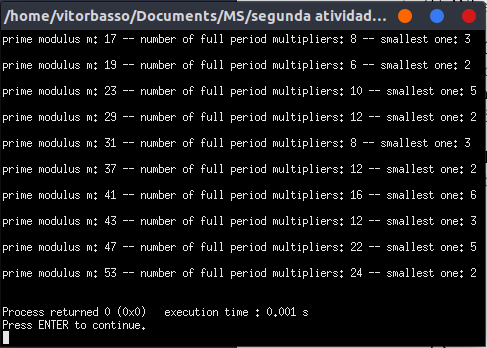
**(B):** Utilizando os próximos índices com o teorema 2.1.4 obtêm-se o resultado na foto.



**Exercise 2.1.11- For the first few prime moduli, this table lists the number of full-period multipliers and the smallest full-period multiplier. Add the next 10 rows to this table.**

**Resposta:**

Detalhes no código em anexo correspondente



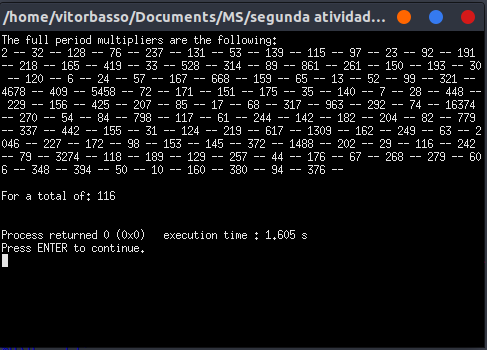
**Exercise 2.2.11 - Let m be the largest prime modulus less than or equal to 2 15 − 1 (see Exercise 2.1.6).**

**(a) Compute all the corresponding modulus-compatible full-period multipliers.**

**(b) Comment on how this result relates to random number generation on systems that support 16-bit integer arithmetic only.**

**Resposta:**

**A)** Os full period multipliers que também são module compatible para esse caso são os seguintes, com um total de 116:

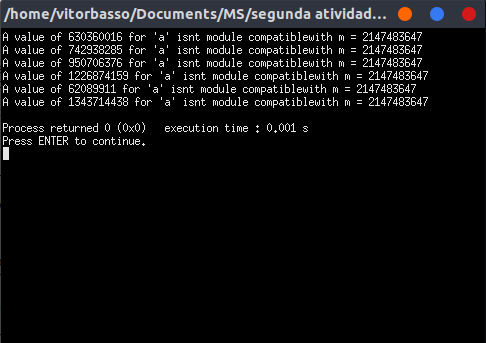


**B)** Esse resultado possibilita o uso da fórmula x = a \* (x % q), o que garante um melhor desempenho a sistemas de 16-bit integer, pois evita o overflow realizando a multiplicação do multiplicador com um número menor (x mod q em vez de a \* x). Portanto, é possível calcular uma faixa maior de números aleatórios utilizando dessa fórmula no lugar de xi+1 = (xi \* a) mod m, especialmente em sistemas que suportam apenas aritméticas de 16-bit integer.

**Exercise 2.2.15 - Determine whether the multipliers associated with  
m = 2^31 −1 given by Fishman (2001): a = 630 360 016, a = 742 938 285,  
a = 950 706 376, a = 1 226 874 159, a = 62 089 911, and a = 1 343 714 438 are modulus-compatible.**

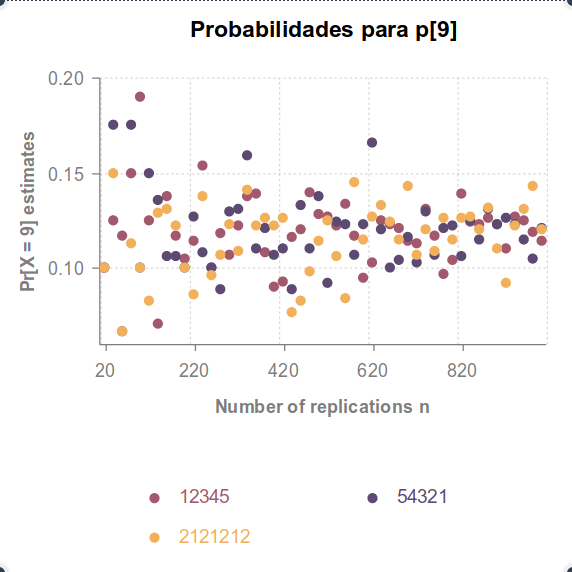
**Resposta:**

Detalhes no código em anexo correspondente



**Exercise 2.3.6 - According to slides number seven and eight  from section 2.3, example 2.3.6, construct a graph similar to slide eight but Pr(X=9).**

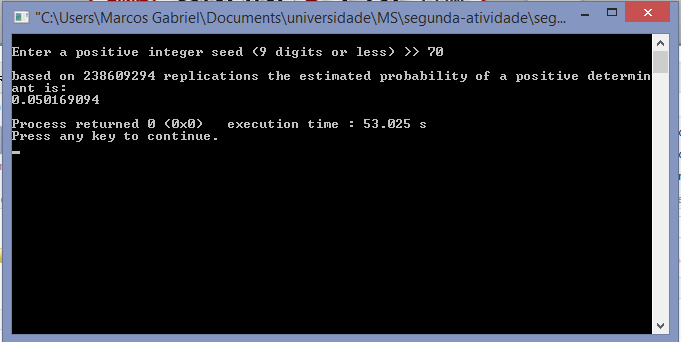
**Resposta:**



**Exercise 2.4.1 - Modify program det so that all 2^31 −1 possible matrices associated with the random number generator with  
 (a, m) = (48271, 2^31 −1)   
are generated.**

**Resposta:**

Apenas modifica-se o N, que determina o número de replicações do programa, para ((2^31) - 1) / 9

****