

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 $g(x) = ax \bmod 127$, 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.

```
/home/vitorbasso/Documents/MS/segunda atividade...
0 valor minimo para um full multplier com m = 127 e de 3
Todos os valores que sao full period multiplier:
3 116 109 92 86 12 83 112 55 114 48 78 67 93 106 65 58 14 118 46 43 6 56 91 57 4
5 39 97 110 101 53 96 29 7 23 85

For a total of 36

Process returned 0 (0x0)   execution time : 0.003 s
Press ENTER to continue.

```

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?

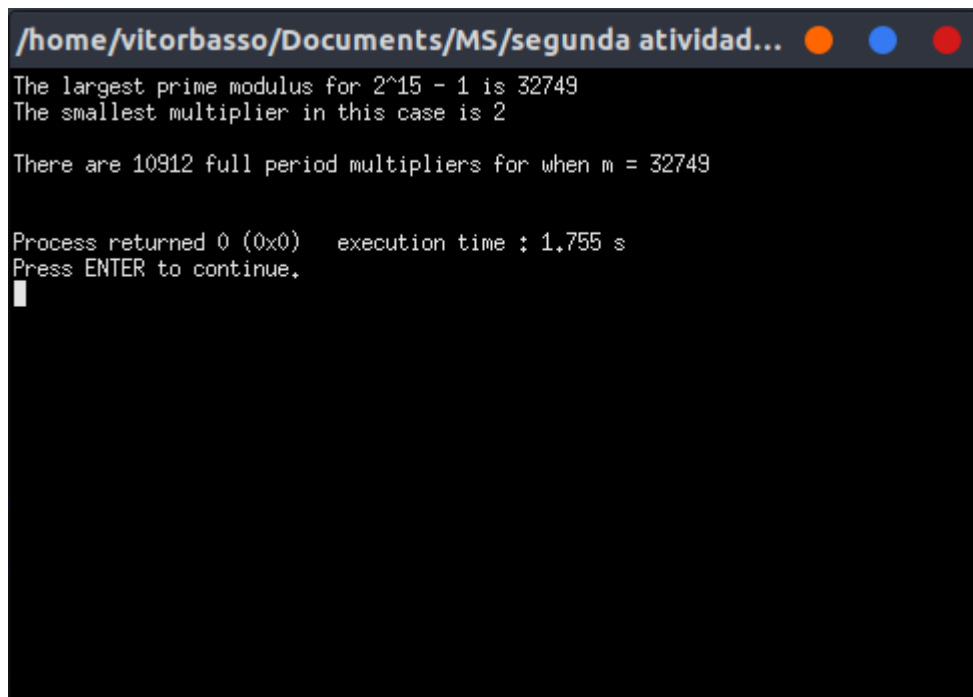
(b) How many corresponding full-period multipliers are there and what is the smallest one?

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.

A terminal window with a dark background and light-colored text. The window title is "/home/vitorbasso/Documents/MS/segunda atividade...". The output text reads: "The largest prime modulus for 2^15 - 1 is 32749", "The smallest multiplier in this case is 2", "There are 10912 full period multipliers for when m = 32749", "Process returned 0 (0x0) execution time : 1.755 s", and "Press ENTER to continue." followed by a cursor.

```
/home/vitorbasso/Documents/MS/segunda atividade...
The largest prime modulus for 2^15 - 1 is 32749
The smallest multiplier in this case is 2

There are 10912 full period multipliers for when m = 32749

Process returned 0 (0x0) execution time : 1.755 s
Press ENTER to continue.
█
```

Exercise 2.1.8

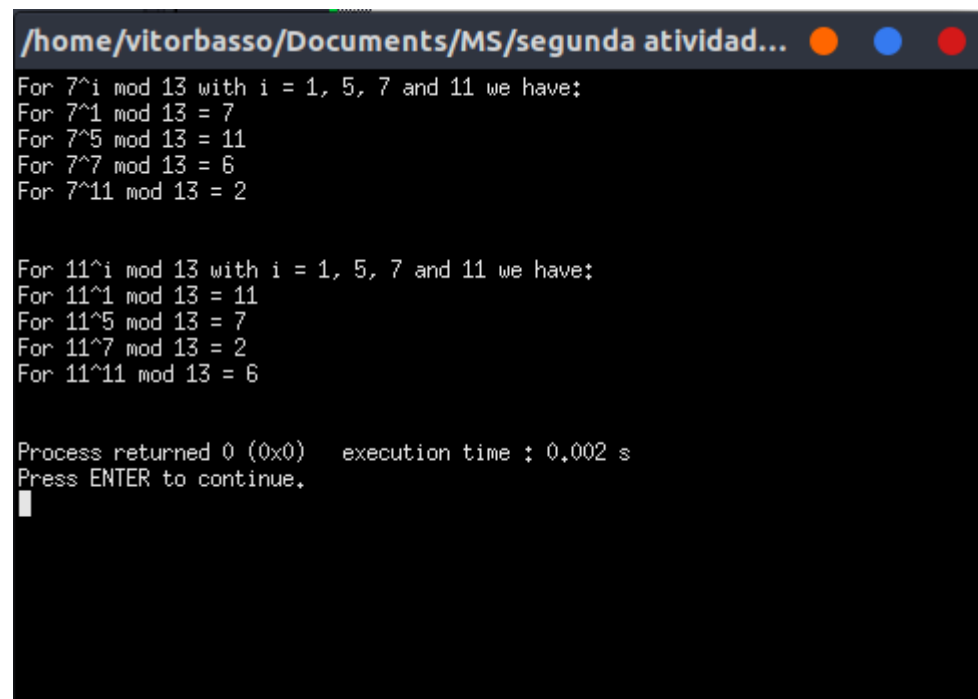
(a) Evaluate $7^i \bmod 13$ and $11^i \bmod 13$ for $i = 1, 5, 7, 11$.

(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



```
/home/vitorbasso/Documents/MS/segunda actividad...
For 7^i mod 13 with i = 1, 5, 7 and 11 we have:
For 7^1 mod 13 = 7
For 7^5 mod 13 = 11
For 7^7 mod 13 = 6
For 7^11 mod 13 = 2

For 11^i mod 13 with i = 1, 5, 7 and 11 we have:
For 11^1 mod 13 = 11
For 11^5 mod 13 = 7
For 11^7 mod 13 = 2
For 11^11 mod 13 = 6

Process returned 0 (0x0)   execution time : 0.002 s
Press ENTER to continue.
█
```

Exercise 2.1.9 –

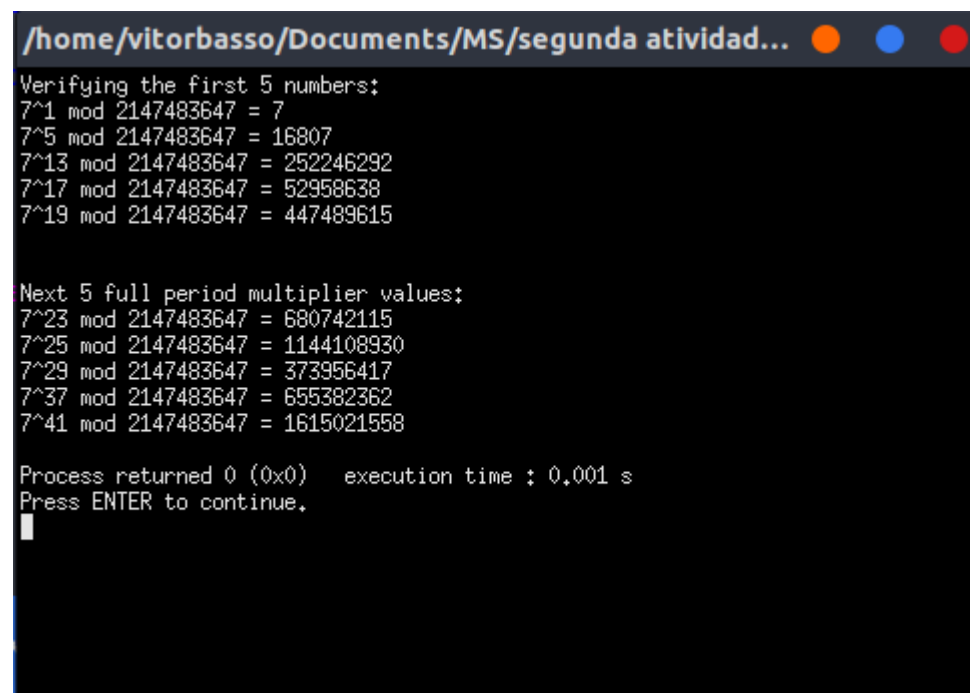
(a) Verify that the list of five full-period multipliers in Example 2.1.6 is correct.

(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.



```
/home/vitorbasso/Documents/MS/segunda actividad...
Verifying the first 5 numbers:
7^1 mod 2147483647 = 7
7^5 mod 2147483647 = 16807
7^13 mod 2147483647 = 252246292
7^17 mod 2147483647 = 52958638
7^19 mod 2147483647 = 447489615

Next 5 full period multiplier values:
7^23 mod 2147483647 = 680742115
7^25 mod 2147483647 = 1144108930
7^29 mod 2147483647 = 373956417
7^37 mod 2147483647 = 655382362
7^41 mod 2147483647 = 1615021558

Process returned 0 (0x0)   execution time : 0.001 s
Press ENTER to continue.
█
```

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

```
/home/vitorbasso/Documents/MS/segunda atividade...
prime modulus m: 17 -- number of full period multipliers: 8 -- smallest one: 3
prime modulus m: 19 -- number of full period multipliers: 6 -- smallest one: 2
prime modulus m: 23 -- number of full period multipliers: 10 -- smallest one: 5
prime modulus m: 29 -- number of full period multipliers: 12 -- smallest one: 2
prime modulus m: 31 -- number of full period multipliers: 8 -- smallest one: 3
prime modulus m: 37 -- number of full period multipliers: 12 -- smallest one: 2
prime modulus m: 41 -- number of full period multipliers: 16 -- smallest one: 6
prime modulus m: 43 -- number of full period multipliers: 12 -- smallest one: 3
prime modulus m: 47 -- number of full period multipliers: 22 -- smallest one: 5
prime modulus m: 53 -- number of full period multipliers: 24 -- smallest one: 2

Process returned 0 (0x0)   execution time : 0,001 s
Press ENTER to continue.
█
```

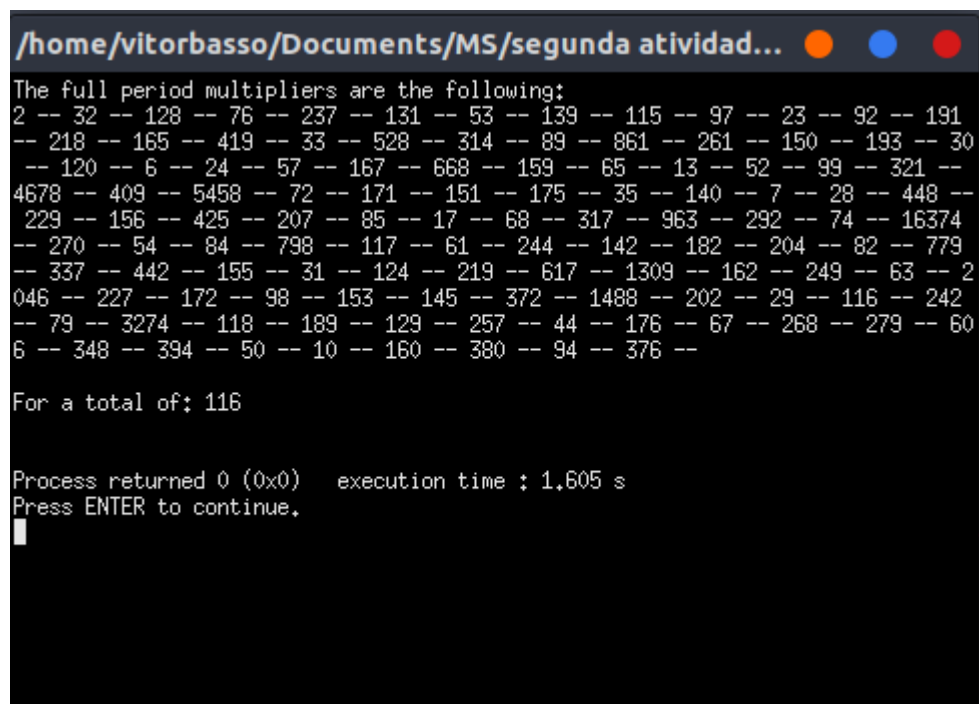
Exercise 2.2.11 - Let m be the largest prime modulus less than or equal to $2^{15} - 1$ (see Exercise 2.1.6).

(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:



```
/home/vitorbasso/Documents/MS/segunda atividade...
The full period multipliers are the following:
2 -- 32 -- 128 -- 76 -- 237 -- 131 -- 53 -- 139 -- 115 -- 97 -- 23 -- 92 -- 191
-- 218 -- 165 -- 419 -- 33 -- 528 -- 314 -- 89 -- 861 -- 261 -- 150 -- 193 -- 30
-- 120 -- 6 -- 24 -- 57 -- 167 -- 668 -- 159 -- 65 -- 13 -- 52 -- 99 -- 321 --
4678 -- 409 -- 5458 -- 72 -- 171 -- 151 -- 175 -- 35 -- 140 -- 7 -- 28 -- 448 --
229 -- 156 -- 425 -- 207 -- 85 -- 17 -- 68 -- 317 -- 963 -- 292 -- 74 -- 16374
-- 270 -- 54 -- 84 -- 798 -- 117 -- 61 -- 244 -- 142 -- 182 -- 204 -- 82 -- 779
-- 337 -- 442 -- 155 -- 31 -- 124 -- 219 -- 617 -- 1309 -- 162 -- 249 -- 63 -- 2
046 -- 227 -- 172 -- 98 -- 153 -- 145 -- 372 -- 1488 -- 202 -- 29 -- 116 -- 242
-- 79 -- 3274 -- 118 -- 189 -- 129 -- 257 -- 44 -- 176 -- 67 -- 268 -- 279 -- 60
6 -- 348 -- 394 -- 50 -- 10 -- 160 -- 380 -- 94 -- 376 --

For a total of: 116

Process returned 0 (0x0)   execution time : 1.605 s
Press ENTER to continue.
```

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 ($x \bmod q$ em vez de $a * x$). Portanto, é possível calcular uma faixa maior de números aleatórios utilizando dessa fórmula no lugar de $x_{i+1} = (x_i * a) \bmod m$, 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:

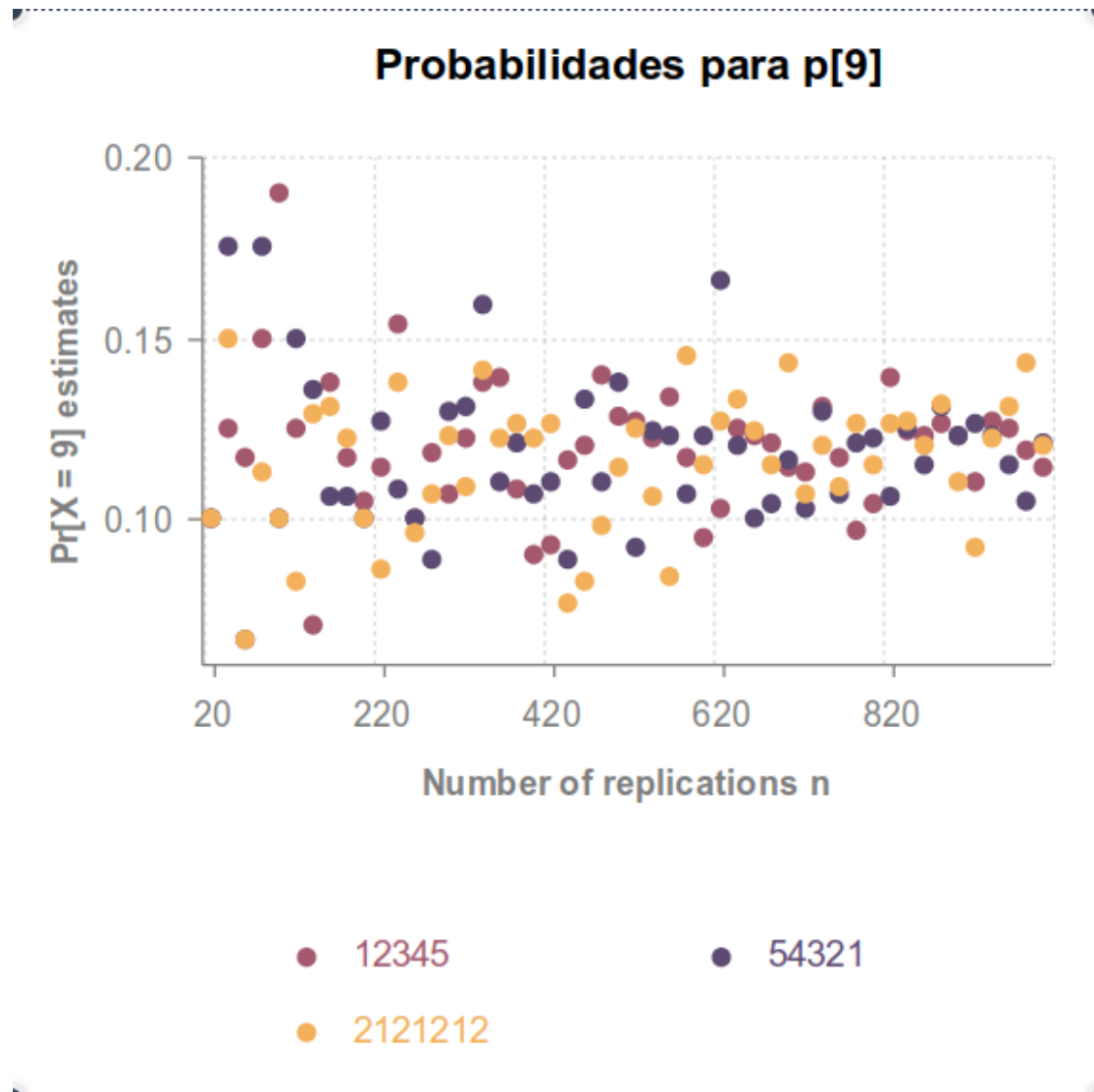
Detalhes no código em anexo correspondente

```
/home/vitorbasso/Documents/MS/segunda actividad...
A value of 630360016 for 'a' isnt module compatiblewith m = 2147483647
A value of 742938285 for 'a' isnt module compatiblewith m = 2147483647
A value of 950706376 for 'a' isnt module compatiblewith m = 2147483647
A value of 1226874159 for 'a' isnt module compatiblewith m = 2147483647
A value of 62089911 for 'a' isnt module compatiblewith m = 2147483647
A value of 1343714438 for 'a' isnt module compatiblewith m = 2147483647

Process returned 0 (0x0)   execution time : 0.001 s
Press ENTER to continue.
█
```

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:



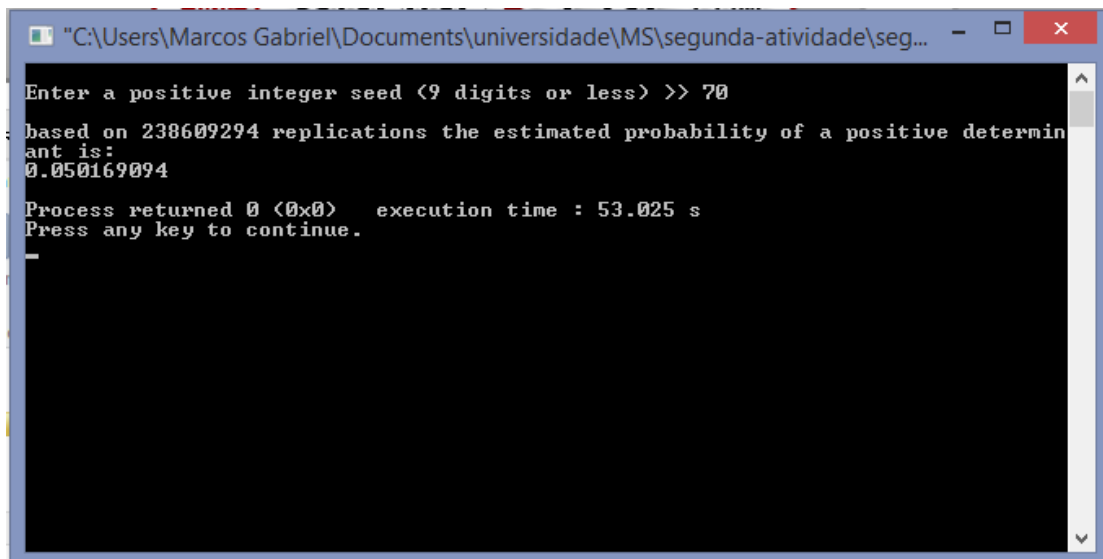
Exercise 2.4.1 - Modify program det so that all $2^{31} - 1$ possible matrices associated with the random number generator with

$$(a, m) = (48271, 2^{31} - 1)$$

are generated.

Resposta:

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



```
"C:\Users\Marcos Gabriel\Documents\universidade\MS\segunda-atividade\seg... - [X]
Enter a positive integer seed <9 digits or less> >> 70
based on 238609294 replications the estimated probability of a positive determin
ant is:
0.050169094
Process returned 0 (0x0)   execution time : 53.025 s
Press any key to continue.
-
```