Universidade Federal de Mato Grosso
Instituto de Ciências Exatas e da Terra
Departamento de Matemática

Bruno Henrique Barbosa Duarte

Geradores de números pseudoaleatórios no ensino médio.

Cuiabá/MT
2025

Bruno Henrique Barbosa Duarte

Geradores de números pseudoaleatórios no ensino médio.

Dissertação apresentada ao curso de Mestrado Profissional em Matemática – Profmat, da Universidade Federal de Mato Grosso, como requisito parcial para obtenção do título **de Mestre em Matemática**

Área de concentração: Matemática na Educação Básica. Linha de Pesquisa: Divulgação e Popularização de matemática da Educação Básica.

Prof. Dr. Aldi Nestor de Souza
Orientador

Cuiabá/MT
2025

Dados Internacionais de Catalogação na Fonte.

D812g Duarte, Bruno Henrique Barbosa.
Geradores de números pseudoaleatórios no ensino médio [recurso eletrônico] / Bruno Henrique Barbosa Duarte. -- Dados eletrônicos (1 arquivo : 32 f., il. color., pdf). -- 2025.

Orientador: Aldi Nestor de Souza.
Dissertação (mestrado profissional) – Universidade Federal de Mato Grosso, Instituto de Ciências Exatas e da Terra, Programa de Pós-Graduação Profissional em Matemática, Cuiabá, 2025.
Modo de acesso: World Wide Web: https://ri.ufmt.br.
Inclui bibliografia.

1. Ensino de matemática. 2. Proposta pedagógica. 3. Congruências lineares. 4. Geradores congruênciais lineares. 5. Mersenne Twister. I. Souza, Aldi Nestor de, *orientador*. II. Título.

Ficha catalográfica elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).

MINISTÉRIO DA EDUCAÇÃO

UNIVERSIDADE FEDERAL DE MATO GROSSO

PRÓ-REITORIA DE ENSINO DE PÓS-GRADUAÇÃO

PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

AV. FERNANDO CORRÊA DA COSTA, 2367 - BOA ESPERANÇA - 78.060-900 - CUIABÁ/MT

FONE: (65) 3615-8576 – E-MAIL: PROFMAT.ICET@UFMT.BR

FOLHA DE APROVAÇÃO

TÍTULO**: GERADORES DE NÚMEROS PSEUDOALEATÓRIOS NO ENSINO MÉDIO**

AUTOR: **MESTRANDO BRUNO HENRIQUE BARBOSA DUARTE**

Dissertação defendida e aprovada em 31 de março de 2025.

COMPOSIÇÃO DA BANCA EXAMINADORA

1. **Prof. Dr. Aldi Nestor de Souza** (Presidente Banca/orientador)

Instituição: Universidade Federal de Mato Grosso

2. **Prof. Dr. Reinaldo de Marchi** (Membro Interno)

Instituição: Universidade Federal de Mato Grosso

3. **Prof. Dr. Jorge Mauricio Jaramillo Monsalve** (Membro externo)

Instituição: Instituto Federal de Mato Grosso

Cuiabá, 10/04/2025.

Documento assinado eletronicamente por **JORGE MAURICIO JARAMILLO MONSALVE**, **Usuário Externo**, em 10/04/2025, às 15:53, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **ALDI NESTOR DE SOUZA**, **Docente da Universidade Federal de Mato Grosso**, em 10/04/2025, às 15:57, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **REINALDO DE MARCHI**, **Docente da Universidade Federal de Mato Grosso**, em 10/04/2025, às 20:22, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

A autenticidade deste documento pode ser conferida no site http://sei.ufmt.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **7808302** e o código CRC **AAB56C19**.

À minha mãe, pelo seu amor incondicional.
À minha amada, pela paciência, apoio e luz que trouxe a cada etapa deste caminho.

Agradecimentos

Agradeço à minha amada, por sempre me fortalecer e não deixar que desistir fosse uma opção. Agradeço à minha mãe, que em todo tempo mostrou-se atenta e crente de que conseguiria chegar até aqui. Deixo aqui o meu agradecimento aos colegas de turma e todo o corpo docente do programa, que não mediram esforços para que este objetivo fosse alcançado. Agradeço a escola e a universidade públicas, através das quais consegui estudar e garantir minha formação. Agradeço aos trabalhadores que defendem esses espaços, em particular aos trabalhadores da segurança e da limpeza que asseguram, com seu valioso trabalho, condições de funcionamento desses espaços de formação.

Muito obrigado a todos.

Àqueles que, como eu,
foram cativados pela Matemática
deixo estas palavras do poeta:

Você vai encher os vazios
com as suas peraltagens,
e algumas pessoas vão te amar
por seus despropósitos!

Manoel de Barros.

Resumo

Este trabalho tem como objetivo investigar alguns casos conhecidos de geradores de números pseudoaleatórios, buscando esclarecer as questões fundamentais que envolvem esse tema. Além disso, propomos levar essa discussão para o contexto da educação básica, promovendo debates com estudantes e educadores, em projetos interdisciplinares e mesmo durante aulas de matemática.

Palavras chave: Ensino de matemática; Proposta pedagógica; Congruências lineares; Geradores congruênciais lineares; Mersenne Twister.

Abstract

This paper aims to investigate some known cases of pseudorandom number generators, seeking to clarify the fundamental questions surrounding this topic. In addition, we propose to take this discussion to the context of basic education, promoting debates with students and educators, in interdisciplinary projects and even during mathematics classes.

Keywords: Mathematics teaching; Pedagogical proposal; Linear congruences; Linear congruential generators; Mersenne Twister.

Lista de Figuras

Lista de Tabelas

Lista de siglas

A seguir, segue-se as siglas utilizadas nesta dissertação.

Profmat	Mestrado Profissional em Matemática em Rede Nacional;
UFMT	Universidade Federal de Mato Grosso;
ICET	Instituto de Ciências Exatas e da Terra;
DMAT	Departamento de Matemática;
MIT	Instituto de Tecnologia de Massachussets.
IMPA	O Instituto de Matemática Pura e Aplicada

Sumário

Introdução

A motivação para desenvolver esse trabalho surgiu durante a disciplina Matemática e Atualidades, ofertada no segundo semestre de 2024 pelo PROFMAT. Em particular, geradores de números pseudoaleatórios foram discutidos na disciplina. Mas também foram discutidas muitas implicações que esses números tem com o cotidiano das pessoas. Durante a disciplina, circulavam notícias sobre a regulação de casas de apostas esportivas, a popularidade do 'jogo do tigrinho', e investigações contra *influenciadores* envolvidos com apostas ilegais..

Com o advento da era digital, muitas informações circulam nas redes, em particular na internet, a cada dia mais informações pessoais estão nas redes, quer seja para login em alguma plataforma ou rede social, como também em conversas mais privativas, entre amigos. Assim sendo, faz-se extremamente necessário assegurar que estas informações permaneçam em segurança. A geração de senhas cada vez mais fortes e menos previsíveis faz-se necessária, um exemplo disso, é o fato de que a maioria das plataformas hoje pedem senhas com caracteres alfanuméricos e especiais, os navegadores já sugerem senhas fortes, haja visto que, é muito difícil para nós elaborarmos uma senha totalmente aleatória, quero dizer, sem que haja algum elemento óbvio, que nos auxilie a recordá-las, pois a cada dia mais precisamos de mais senhas, afinal estamos sendo apresentados a novas plataformas educacionais a todo instante.

Além de senhas como foi apresentado, são cada vez mais frequentes os sorteios virtuais, o uso de algoritmos para jogos eletrônicos, além de muitoas plataformas que utilizam autenticação em dois fatores, que significa a necessidade, além da senha, de um código temporário para o acesso. Esse é o caso, por exemplo, da plataforma gov.br. Em síntese, estruturas matemáticas se fazem cada vez mais presentes no cotidiano das pessoas, das mais variadas formas, mesmo que elas não se deem conta disso.

Os geradores de números aleatórios é um mecanismo com qual é possível gerar

uma sequência de números com as funções acima citadas. Existem dois tipos de geradores: os pseudoaleatórios e os verdadeiramente aleatórios. Segundo [7] "um número verdadeiramente aleatório é aquele em que, através de condições iniciais idênticas, é impossível chegar a um mesmo resultado - o número gerado - ...". Em contrapartida, um número pseudoaleatório é aquele que, embora pareça aleatório, se usarmos as mesmas condições iniciais que lhe deram origem, tornaremos a gerar o mesmo número.

Ainda segundo [7], o que caracteriza os geradores de números verdadeiramente aleatórios é o fato de estes recorrerem a elementos ocasionais, portanto sujeitos a mutações imprevisíveis, tais como, amplificação de ruído, baseados em osciadores, com circuítos caóticos e partículas quânticas. Geradores de números pseudoaleatórios, por sua vez, são determinísticos, isto é, ainda que possuam chaves complexas, ainda é possível determiná-los, uma vez que se conheça o algoritmo que lhes deram origem.

Esse trabalho se propões a investigar alguns casos conhecidos de geradores de números pseudoaleatórios e com isso lançar luz sobre a problemática geral que envolve tais números. Além disso, pretendemos levar essa temática para os espaços educativos da educação básica, discutir com estudantes e educadores, em projetos interdisciplinares e mesmo durante as aulas de matemática.

Resumidamente, o trabalho encontra-se dividido em 4 capítulo: no primeiro fazemos um apanhado de temas de Aritmética, que são fundamentos matemáticos dos geradores que apresentaremos; no segundo capítulo apresentaremos os geradores de números pseudoaleatórios congruentes lineares e o Mersenne Twister, que são gerados a partir de um primo de Mersenne; no terceiro capítulo apresentaremos uma abordagem dos números aleatórios para o ensino médio e no último capítulo faremos algumas considerações finais com propostas de trabalhos futuros.

Capítulo

1

Fundamentos de Aritmética Básica

Nesse capítulo apresentamos alguns dos fundamentos teóricos da aritmética básica, ou aritmética dos números inteiros, que são a base dos geradores de números pseudoaleatórios que apresentaremos no trabalho. Embora sejam fundamentos amplamente conhecidos e presentes em vasta literatura, achamos prudente, por completude do trabalho, apresentá-los aqui em forma de capítulo. A referência bibliográfica para o que apresentaremos neste capítulo é [2], onde podem ser encontrados, além de mais exemplos, as demonstrações dos teoremas aqui apenas enunciados.

Teorema 1.1. *Dados $a, b \in \mathbb{Z}$, com b não nulo, existem, únicos q e m, tais que*

$$a = bq + r, \text{com } 0 \leq |r| \leq b - 1.$$

Esse resultado é fundamental devido a existência e unicidade do resto. O conjunto dos restos, no caso em que b>0, cumpre um papel crucial na teoria dos números por permitir construir novos conjuntos, o conjunto das classes dos restos, que se tornaram fundamentais para a teoria.

Exemplo 1.1. *Considere $a = 200$ e $b = 32$. Nesse caso, $q = 6, r = 8$ e $200 = 32 \cdot 6 + 8$. Além disso, pelo Teorema da Divisão Euclidiana, para qualquer número inteiro positivo b, existem únicos q e r tais que*

$$200 = b \cdot q + r, \text{com } 0 \leq r \leq b - 1.$$

No caso específico em que $b = 32$, os valores são $q = 6$ e $r = 8$, como já mostrado.

Exploraremos uma das noções mais fecundas da aritmética introduzida por Gauss no

seu livro *Disquisitiones Arithmeticae*, de 1801. Trata-se da realização de uma aritmética com os restos da divisão euclidiana por um número fixado.

1.1 Aritmética dos Restos

Seja m um número natural. Diremos que dois números inteiros a e b são congruentes módulo m se os restos de sua divisão euclidiana por m são iguais. Quando os inteiros a e b são congruentes módulo m, escreve-se

$$a \equiv b \mod m$$

Por exemplo $17 \equiv 5 \mod 2$ já que os restos da divisão de 17 e de 5 por 2 são iguais a 1.

Quando a relação $a \equiv b \mod m$ for falsa, diremos que a e b não são *congruentes*, ou que são *incongruentes*, módulo m. Nestes casos, escreveremos, $a \not\equiv b \mod m$.

Como o resto da divisão de um número inteiro qualquer por 1 é sempre nulo, tempos que $a \equiv b \mod 1$, quaisquer que sejam a, $b \in \mathbb{Z}$. Isso torna desinteressante a aritmética dos restos módulo 1. Portanto, doravante, consideraremos sempre $m > 1$.

Decorre, imediatamente, da definição que a congruência, módulo um inteiro fixado m, é uma relação de equivalência. Vamos enunciar isso explicitamente abaixo.

Proposição 1.2. *Seja $m \in \mathbb{N}$. Para todos $a, b, c \in \mathbb{Z}$, tem-se que*

i. $a \equiv a \mod m$ *Se*

ii. se $a \equiv b \mod m$, *então* $b \equiv a \mod m$,

iii. se $a \equiv b \mod m$ *e* $b \equiv c \mod m$, *então* $a \equiv c \mod m$.

Para verificar se dois números são congruentes módulo m, é suficiente aplicar o resultado abaixo.

Proposição 1.3. *Suponha que $a, b, m \in \mathbb{Z}$ com $m>1$. Tem-se que $a \equiv b \mod m$ se, e somente se, $m|b-a$, isto é, m divide $b-a$.*

O fato da noção de congruência ter equivalência compatível com as operações de adição e multiplicação nos inteiros a torna muito poderosa, vejamos a seguir.

Proposição 1.4. *Sejam $a, b, c, d, m \in \mathbb{Z}$, com $m>1$.*

i. Se $a \equiv b \mod m$ *e* $c \equiv d \mod m$, *então* $a + c \equiv b + d \mod m$.

ii. Se $a \equiv b \mod m$ *e* $c \equiv d \mod m$*, então* $ac \equiv bd \mod m$*.*

Corolário 1.5. *Para todos* $n \in \mathbb{N}$*,* $a, b \in \mathbb{Z}$*, se* $a \equiv b \mod m$*, então tem-se que* $a^n \equiv b^n \mod m$*.*

Com a notação de congruências, o Pequeno Teorema de Fermat enuncia-se como se segue:

Teorema 1.6. *Se* p *é um número primo e* $a \in \mathbb{Z}$*, então* $a^p \equiv a \mod p$*. Além disso, se* p *não divide* a*, então* $a^{p-1} \equiv 1 \mod p$*.*

Exemplo 1.2. *Sejam* p *um número primo e* $a, b \in \mathbb{Z}$*. Temos que*

$$(a \pm b)^p \equiv a^p \pm b^p \mod p.$$

O resultado decorre da formulação acima do Pequeno Teorema de Fermat, pois

$$(a \pm b)^p \equiv a \pm b \equiv a^p \pm b^p \mod p.$$

1.2 Funçao φ de Euler

Esta função é um conceito fundamental na teoria dos números, particulamente neste trabalho, a fim de auxiliar em algumas informações quanto às raízes primitivas, que serão abordadas na próxima seção.

Definição 1.7. *Designaremos por* $\varphi(m)$ *o número de elementos de um sistema reduzido de resíduos módulo* $m > 1$*, que corresponde à quantidade de números naturais entre* 0 *e* $m - 1$ *que são primos com* m*. Pondo* $\varphi(1) = 1$*, isso define uma importante função*

$$\varphi : \mathbb{N} \longrightarrow \mathbb{N},$$

chamada função φ *de Euler.*

Da definição, seque que

$$\varphi(m) \leq m - 1, \text{para todo } m \geq 2.$$

Além disso, se $m \geq 2$, então $\varphi(m) = m - 1$ se, e somente se, m é um número primo.

Exemplo 1.3. *Note que, os restos possíveis na congruência módulo* 10 *são* $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$*, destes os que são coprimos com o* 10*, ou seja,* $mdc(10, 1) =$

$mdc(10,3) = mdc(10,7) = mdc(10,9) = 1$, são $\{1,3,7,9\}$, isto é, um total de quatro elementos, logo, $\varphi(10) = 4$.

Para $m = 20$, temos sabemos que os possíveis restos na congruência módulo 20 são $\{0,1,2,...,17,18,19\}$, destes os que são coprimos com o 20, são $\{1,3,7,9,11,13,17,19\}$, temos então que $\varphi(20) = 8$.

Teorema 1.8. *Sejam $m, \in \mathbb{Z}$, com $m>1$ e $mdc(a,m) = 1$. Então,*

$$a^{\varphi(m)} \equiv 1 \mod m$$

A seguir veremos como calcular $\varphi(m)$, quando m não é primo.

Proposição 1.9. *Sejam $m, m' \in \mathbb{N}$, tais que $mdc(m,m') = 1$. Então*

$$\varphi(mm') = \varphi(m) \cdot \varphi(m').$$

Uma outra proposição que é válida enunciarmos, pois será de grande valia neste trabalho, é a seguinte:

Proposição 1.10. *Se p é um número primo e r, um número natural, então tem-se que*

$$\varphi(p^r) = p^r - p^{r-1}.$$

Outro elemento teórico que será bastante explorado neste trabalho é o de raízes primitivas de um corpo finito, por isso, abordaremos neste capítulo sua definição e teoremas.

1.3 Corpo finito: raízes primitivas

Um corpo é uma coleção de elementos na qual é possível definir duas operações, denominadas 'adição' e 'multiplicação', que devem satisfazer propriedades análogas às dos números racionais e reais. Essas propriedades incluem a associatividade, a comutatividade, a distributividade da multiplicação em relação à adição, a existência de um elemento neutro para a adição e para a multiplicação, além da garantia da existência do inverso aditivo e do inverso multiplicativo para todos os elementos não nulos.

O corpo $\mathbb{Z}_p$ dos inteiros módulo p (p primo), é evidentemente o exemplo mais familiar de corpo finito e a compreensão dele e de suas raízes primitivas compõem a base do nosso

estudo. Note que $\mathbb{Z}_7$ é um corpo finito.

$\oplus$	0	**1**	**2**	**3**	**4**	**5**	**6**
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Tabela 1.1: Tabela Aditiva, módulo 7.

$\otimes$	0	**1**	**2**	**3**	**4**	**5**	**6**
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Tabela 1.2: Tabela Multiplicativa, módulo 7.

Na tabela 1.1 é possível visualizar o inverso aditivo de cada elemento pertencente a $\mathbb{Z}_7$, já na tabela 1.2 é possível verificar o inverso multiplicativo de cada elemento pertencente a $\mathbb{Z}_7$.

Definição 1.11. *Um elemento não nulo cujas potências enumeram todos os outros elementos não nulos de um corpo é chamado primitivo ou uma raiz primitiva.*

Sabe-se que o conjunto que representa os não-nulos de $\mathbb{Z}_p = \{1, 2, 3, ..., p-1\}$, onde p é um número primo, é um grupo multiplicativo.

Por exemplo temos que o conjunto dos não-nulos de $\mathbb{Z}_7$, isto é, $\mathbb{Z}_7 - \{0\} = \{1, 2, 3, 4, 5, 6\}$ e que o conjunto dos não nulos de $\mathbb{Z}_{11}$, ou seja, $\mathbb{Z}_{11} - \{0\} = \{1, 2, 3, ..., 9, 10\}$ são grupos multiplicativos..

Teorema 1.12. *Se n é primo, então o conjunto $E = \{1, 2, ..., n-1\}$ é um grupo cíclico com respeito à multiplicação módulo n. Se $g \in E$ é tal que $E = \{g, g^2, g^3, ..., g^{n-1}\}$, g é chamado uma raiz primitiva de E.*

Demonstração.
Comecemos observando que $E = \{1, 2, 3, ..., n-1\}$ é um grupo com respeito à multiplicação módulo n. Com efeito, como n é primo, todo $a \in E$ é relativamente primo com n. A conclusão segue de um corolário muito conhecido e útil que afirma que: Sejam a e b dois inteiros com $a < b$. Se $mdc(a, b) = 1$, existe um único $x \in \{1, ..., n-1\}$ tal que $ax \equiv 1 \mod b$.

Pelo Pequeno Teorema de Fermat, para todo $a \in E$, temos $a^{p-1} = 1$. (Note que a igualdade $a^{p-1} = 1$ é dentro do grupo G. Seu significado é $a^{n-1} \equiv 1 \mod n$. Seja r o menor inteiro tal que $a^r = 1$. Estamos certos de que tal r existe, já que $a^{n-1} = 1$. Este r é o chamado a *ordem* do elemento a. Considere o conjunto $F = \{a, a^2, ..., a^r = 1\}$. É fácil verificar que F é de fato um subgrupo de E contendo r elementos. Logo, pelo Teorema de Lagrange, segue que $r|n-1$.

Devemos mostrar que existe um $a \in E$ com ordem $n-1$. Seja d um divisor próprio de $n-1$. Mostraremos que existem exatamente d elementos de G cujas ordens dividem d. De fato, todos os elementos a cujas ordens dividem d são soluções da congruência $x^d - 1 \equiv 0 \mod n$. O resultado desejado segue do seguinte lema:

Seja n um primo, $S = \{0, 1, 2, ..., n-1\}$ e $P_d(x) = x^d - 1$, em que $d|n-1$, a congruência $P_d(x) \equiv 0 \mod n$ tem exatamente d soluções distintas no conjunto $E = S - \{0\}$

Decomponha $n-1$ em fatores primos, $n-1 = p_1^{k_1} \cdots p_s^{k_s}$ e considere os polinômios $Q_{p_i^{k_i}}(x) = x^{{p_i}^{k_i}} - 1$. Pelo citado no parágrafo anterior, cada congruência $Q_{p_i^{k_i}}(x) \equiv 0 \mod n$ tem exatamente $p_i^{k_i}$ soluções em E: todas as soluções são elementos de E cuja ordem divide $p_i^{k_i}$. Se todas as soluções de $Q_{p_i^{k_i}}(x) \equiv 0 \mod n$ correspondem a elementos do grupo com ordem menor que $p_i^{k_i}$, então suas ordem dividiriam $p_i^{k_i - 1}$. Estes elementos seriam então soluções da congruência $Q_{p_i^{k_i}}(x) = x^{{p_i}^{k_i - 1}} - 1 \equiv 0 \mod n$. Isto é uma contradição, já que $Q_{p_i^{k_i}}(x) \equiv 0 \mod n$ tem exatamente $p_i^{k_i - 1}$ soluções em E. Logo, seja $g_i \in E$ uma solução de $Q_{p_i^{k_i}}(x) \equiv 0 \mod n$ correspondendo a um elemento $p_i^{k_i}$. Podemos verificar facilmente que

$$g = g_1 \cdots g_s$$

tem ordem $p_1^{k_1} \cdots p_s^{k_s} = n - 1$. □

Exemplo 1.4. *Raízes Primitivas em* $\mathbb{Z}_7 - \{0\}$.

O conjunto dos não-nulos de $\mathbb{Z}_7 = \{1, 2, 3, 4, 5, 6\}$. *Tomando,* $g = 3$, *temos que:*

$$\begin{aligned}
3^1 &\equiv 3 \mod 7,\\
3^2 &\equiv 9 \equiv 2 \mod 7,\\
3^3 &\equiv 6 \mod 7,\\
3^4 &\equiv 18 \equiv 4 \mod 7,\\
3^5 &\equiv 12 \equiv 5 \mod 7,\\
3^6 &\equiv 15 \equiv 1 \mod 7.
\end{aligned}$$

Note que, para $g = 3$, *obtivemos exatamente,* $\{3, 2, 6, 4, 5, 1\} = \mathbb{Z}_7 - \{0\}$.
Observe que, quando tomamos $g = 2$, *temos:*

$$\begin{aligned}
2^1 &\equiv 2 \mod 7,\\
2^2 &\equiv 4 \mod 7,\\
2^3 &\equiv 8 \equiv 1 \mod 7.
\end{aligned}$$

Concluimos que $g = 2$ *não é raiz primitiva de* $\mathbb{Z}_7 - \{0\}$, *pois só gera* $\{2, 4, 1\}$.

Exemplo 1.5. *Raízes Primitivas em* $\mathbb{Z}_{11} - \{0\}$.

O conjunto dos não-nulos de $\mathbb{Z}_{11} = \{1, 2, \ldots, 10\}$.

Raiz Primitiva: $g = 2$

$$\begin{aligned}
2^1 &\equiv 2 \mod 11,\\
2^2 &\equiv 4 \mod 11,\\
2^3 &\equiv 8 \mod 11,\\
2^4 &\equiv 16 \equiv 5 \mod 11,\\
2^5 &\equiv 10 \mod 11,\\
2^6 &\equiv 20 \equiv 9 \mod 11,\\
2^7 &\equiv 18 \equiv 7 \mod 11,\\
2^8 &\equiv 14 \equiv 3 \mod 11,\\
2^9 &\equiv 6 \mod 11,\\
2^{10} &\equiv 12 \equiv 1 \mod 11.
\end{aligned}$$

Note que, para $g = 2$, obtivemos exatamente, $\{2, 4, 8, 5, 10, 9, 7, 3, 6, 1\} = \mathbb{Z}_{11} - \{0\}$. Observque que, quando tomamos $g = 3$, temos:

$$\begin{aligned}
3^1 &\equiv 3 \mod 11,\\
3^2 &\equiv 9 \mod 11,\\
3^3 &\equiv 27 \equiv 5 \mod 11,\\
3^4 &\equiv 15 \equiv 4 \mod 11,\\
3^5 &\equiv 12 \equiv 1 \mod 11.
\end{aligned}$$

Conclui-se que $g = 3$ não é raiz primitiva de $\mathbb{Z}_{11} - \{0\}$, pois gera apenas $3, 9, 5, 4, 1$.

Agora enuciaremos um teorema que nos auxilia a mensurar quantas raízes primitivas existem módulo p, com p primo.

Teorema 1.13. *Seja p um primo. Para cada $d|p\text{-}1$, existem exatamente $\varphi(d)$ elementos em $\mathbb{Z}_p$ com ordem d. Em particular, p possui exatamente $\varphi(p-1)$ raízes primitivas.*

Embora até aqui consigamos garantir a existência de raízes primitivas para um dado primo p e pelo Teorema 1.13 seja possível obter a quantidade de raízes primitivas para este p, segundo [10] encontrar uma raiz primitiva, geralmente precisamos prosseguir pela força bruta, recorrer a computadores ou a tabelas extensas que foram construídas. Em [10] é possível encontrar a seguinte tabela que lista a menor raiz primitiva positiva para cada primo abaixo de 200:

Número primo (p)	Menor raiz primitiva	Número primo (p)	Menor raiz primitiva
2	1	89	3
3	2	97	5
5	2	101	2
7	3	103	5
11	2	107	2
13	2	109	6
17	3	113	3
19	2	127	3
23	5	131	2
29	2	137	3
31	3	139	2
37	2	149	2
41	6	151	6
43	3	157	5
47	5	163	2
53	2	167	5
59	2	173	2
61	2	179	2
67	2	181	2
71	7	191	19
73	5	193	5
79	3	197	2
83	2	199	3

Tabela 1.3: Raízes Primitivas Mínimas de Números Primos

Segundo [10] na maioria dos casos esta raiz é um número bem pequeno. Entre os 78498 primos ímpares até 10^6, uma raíz primitiva menor ou igual a 6 é valida para 80% desses primos; onde 2 é uma raiz primitiva para 29841 primos ou aproximadamente 37% das vezes; enquanto 3 é raiz primitiva para 17814 primos, isto é, em 22% das vezes.

O seguinte teorema auxília a verificar se $a \in \mathbb{Z}_p$ é uma raiz primitiva.

Teorema 1.14. *Um inteiro a é raiz primitiva p se $a^{\frac{\varphi(p-1)}{d}} \not\equiv 1 \mod p$ para todos os primos d divisores de $p-1$.*

Exemplo 1.6. *Pelo Teorema 1.13, temos que em $\mathbb{Z}_{31}$, fazendo*

$$\varphi(31-1) = \varphi(30) = \varphi(2) \cdot \varphi(3) \cdot \varphi(5) = 1 \cdot 2 \cdot 4 = 8$$

Portanto $\mathbb{Z}_p$ tem exatamente 8 raizes primitivas, para verificar se 2 é uma delas, usaremos o teorema 1.14.

Note que:

$$2^{\frac{30}{2}} \equiv 2^5 \cdot 2^5 \cdot 2^5 \equiv 32 \cdot 32 \cdot 32 \equiv 1 \mod 31$$

Pelo Teorema 1.14, concluímos que 2 não é raiz primitiva de 31. Vejamos agora, se 3 é raiz primitiva de 61, observe:

$$3^{15} \equiv 27^5 \equiv (-4)^5 \equiv (-64) \cdot (16) \equiv -2(16) \equiv -1 \equiv 30 \not\equiv 1 \mod 31 \tag{1.1}$$

$$3^{10} \equiv 3^4 \cdot 3^4 \cdot 3^2 \equiv 19 \cdot 19 \cdot 9 \equiv 20 \cdot 9 \equiv 25 \not\equiv 1 \mod 31 \tag{1.2}$$

$$3^5 \equiv 81 \cdot 3 \equiv 19 \cdot 3 \equiv 26 \not\equiv 1 \mod 31 \tag{1.3}$$

Assim pelo Teorema 1.14, concluímos que 3 é uma das raízes primitivas de 31.

No próximo capítulo é perceptível a relevância dos números primos na geração de números pseudoaleatórios, portanto é de suma importância abordagem dos números primos de Mersenne. O resultado que se segue apresentará uma proposição e um racíocinio sobre eles.

Proposição 1.15. *Sejam a e n números naturaris maiores do que 1. Se $a^n - 1$ é primo, então $a = 2$ e n é primo.*

Demonstração.
Admitamos que $a^n - 1$ seja primo, com $a > 1$ e $n > 1$.
Suponhamos, por absurdo, que $a > 2$. Logo, $a - 1 > 1$ e $a - 1 | a^n - 1$.
É um fato conhecido que $a - b$ divide $a^n - b^n$, para todo $a, b, n \in \mathbb{N}$.
Portanto, $a^n - 1$ não é primo, o que é uma contradição. Consequentemente, $a = 2.n = rs$ com $r > 1$ e $s > 1$. Como $2^r - 1$ divide $(2^r)^s - 1 = 2^n - 1$ (novamente, pela proposição 1.14.), segue que $2^n - 1$ não é primo, contradição. Logo, n é primo. □

Os números de Mersenne são os números da forma

$$M_p = 2^p - 1,$$

onde p é um número primo.

No intervalo $2 \leq p \leq 5000$ os números de Mersenne que são primos, chamados primos de Mersenne, correspondem aos seguintes valores: 2, 3, 5, 7, 13, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253 e 4423. Atualmente, no segundo semestre de 2024, um ex-funcionário da Nvidia chamado Luke Durante entrou para história, pois no dia 12 de outrubro, através do projeto colaborativo global de computação chamado de Grande Busca pela Internet de Primos de Mersenne (GIMPS, sigla em inglês),pois conseguiu obter o número $M_{136279841} = 2^{136279841} - 1$ um primo de Mersenne, que adiante perceberá a importância destes números em geradores de números pseudoaleatórios.

Estes são extremamente relevante,pois são a base do sistema de criptografia RSA, um dos mais importantes da história. Desenvolvido em 1978 pelo matemático Ron Rivest, o criptógrafo Adi Shamir e o cientista da computação Leonard Adleman, ele foi criado para proteger a transmissão de informações online.

Capítulo

2

Geradores Congruenciais Lineares

Nesse capítulo trataremos dos geradores de números pseudoaleatórios. Como dito na introdução, trata-se de geradores que são determinísticos, isto é, que funcionam à base de um algoritmo bem definido e que não sofrem influência de eventos extras.

A principal vantagem desses geradores está em sua eficiência computacional, uma vez que não exigem hardware especializado para capturar entropia externa. Por outro lado, sua natureza determinística exige cuidados na escolha do algoritmo, pois uma implementação fraca pode levar a padrões previsíveis, comprometendo aplicações críticas, como criptografia e simulações estatísticas.

Contudo, ela é muito útil em simulações rápidas e menos críticas, como em jogos eletrônicos antigos (e.g., geradores de mapas aleatórios) ou algoritmos para embaralhar pequenas listas. Já o Mersenne Twister, segundo [1] o fato de ter sido aprovado pelos principais testes de aleatoriedade existentes o torna apto a se tornar padrão em diversas aplicações, por ser mais robusto e ter um período incomparavelmente longo, que será detalhado neste capítulo, é amplamente adotado em aplicações que exigem alta qualidade de aleatoriedade, como em métodos de Monte Carlo (física, finanças) e jogos modernos (ex.: Minecraft, que utiliza variantes desse algoritmo em seu sistema de recompensas aleatórias)

Iniciaremos o capítulo apresentando o caso do gerador congruencial linear.

Definição 2.1. *Um gerador congruencial linear é um tipo muito comumente usado de gerador de números aleatórios. Ele gera uma sequência sobre o conjunto* $E = \{1, ..., p-1\}$ *usando a regra*

$$x_{n+1} \equiv ax_n \mod p,$$

onde p é primo e a é uma raiz primitiva de $\mathbb{Z}_p$. Isto é, a é um elemento de E tal que

$$\begin{cases} a^k \not\equiv 1 \mod p \\ a^{p-1} \equiv 1 \mod p \end{cases}$$

Lembremos que $\mathbb{Z}_p$, é um conjunto de inteiros $\{0, ..., p-1\}$ com adição e multiplicação módulo p. Definido desta forma, $\mathbb{Z}_p$ é um corpo quando p é primo. Isto implica que: adição e multiplicação são, ambas, comutativas e associativas, cada operação tem um elemento neutro, multiplicação é distributiva sobre a adição, todos os elementos têm inversos aditivos e, finalmente, todos os elementos não nulos têm inversos multiplicativos. Usaremos estas propriedades sem prova nas discussões a seguir. Tome como exemplo simples o caso $p = 7$. Vemos que 2 não é uma raiz primitiva, já que $2^3 = 8 \equiv 1 \mod 7$. No entanto, observamos que 3 é uma raiz primitiva, uma vez que

$$\begin{cases} 3^2 \equiv 2 \mod 7 \\ 3^3 \equiv 6 \mod 7 \\ 3^4 \equiv 18 \equiv 4 \mod 7 \\ 3^5 \equiv 12 \equiv 5 \mod 7 \\ 3^6 \equiv 15 \equiv 1 \mod 7 \end{cases}$$

A prova de que sempre existe uma raiz primitiva $a \in \mathbb{Z}_p$, está capítulo 1 deste trabalho, teorema 1.12.

O motivo para a escolha de a como sendo uma raíz primitiva de $\mathbb{Z}_p$ é que com isso a congruência $x_{n+1} \equiv ax_n \mod p$, dado um valor inicial x_0, percorre todos os elementos de $\mathbb{Z}_p$. Para se verificar isso, basta notar que, como vimos no teorema 1.12, as potências de a geram todos os elementos de $\mathbb{Z}_p$. Assim, escolhido um elemento inicial x_0 qualquer de $\mathbb{Z}_p$, estamos escolhendo uma potência de a, que ao ser multiplicado por a gera um outro elemento de $\mathbb{Z}_p$ e prosseguindo, encontramos todos os demais.

Exemplo 2.1. *Gerando bolões da Mega-Sena*

A mega sena sorteia 6 dezenas dentre as dezenas de 1 a 60. Uma prática que se tornou corriqueira foi a de grupos de amigos ou empresas realizarem bolões da mega-sena. A ideia do bolão é fazer um número alto de apostas e com isso aproximar de "cercar"o máximo de resultados possíveis.

O gerador congruencial linear fornece um modo de elaborar bolões, ou um modo de gerar sequências de números dentre as dezenas 01 a 60. Basta escolher uma raiz primitiva de $\mathbb{Z}_{61}$, um valor inicial e o número de jogos contendo seis números que se pretende.

Para resolver o problema proposta acima, escreveremos o seguinte gerador $x_{n+1} \equiv ax_n \mod 61$, se a for uma raiz primitiva de 61, temos que a congruência acima geraria todos os elementos de $\mathbb{Z}_p$. Note que pelo Teorema 1.14, verificaremos se 2 é uma raiz primitiva de 61.

$$\begin{aligned}
2^{30} \equiv (2^6)^5 \equiv 64^5 \equiv 3^5 \equiv 60 \not\equiv 1 \mod 61 \\
2^{20} \equiv (2^6)^3 \cdot 4 \equiv 3^3 \cdot 4 \equiv 108 \equiv 47 \not\equiv 1 \mod 61 \\
2^{15} \equiv 8^5 \equiv 8^2 \cdot 8^2 \cdot 8 \equiv 9 \cdot 8 \equiv 72 \equiv 11 \not\equiv 1 \mod 61 \\
2^{12} \equiv (2^6)^2 \equiv 3^2 \equiv 9 \not\equiv 1 \mod 61 \\
2^{10} \equiv 2^6 \cdot 2^4 \equiv 3 \cdot 16 \equiv 48 \not\equiv 1 \mod 61 \\
2^6 \equiv 3 \not\equiv 1 \mod 61 \\
2^5 \equiv 32 \not\equiv 1 \mod 61 \\
2^4 \equiv 16 \not\equiv 1 \mod 61 \\
2^3 \equiv 8 \not\equiv 1 \mod 61 \\
2^2 \equiv 4 \not\equiv 1 \mod 61
\end{aligned}$$

Como verificamos que 2 é raiz primitiva de $\mathbb{Z}_{61}$, escreveremos nosso gerador da seguinte maneira

$$x_{n+1} \equiv 2x_n \mod 61$$

Fizemos os cálculos em planilhas e fica visível que ao mudarmos o valor inicial x_0, gera-se outras 6 dezenas.

Observe, na sequência de tabelas abaixo:

n	Xn	Cálculo (2*xn)	Resto (2*Xn) módulo 61 [X(n+1)]
0	15	30	30
1	30	60	60
2	60	120	59
3	59	118	57
4	57	114	53
5	53	106	45

Dezenas para um jogo:	30	60	59	57	53	45

Tabela 2.1: Valor inicial = 15

n	Xn	Cálculo (2*xn)	Resto (2*Xn) módulo 61 [X(n+1)]
0	21	42	42
1	42	84	23
2	23	46	46
3	46	92	31
4	31	62	1
5	1	2	2

Dezenas para um jogo:	42	23	46	31	1	2

Tabela 2.2: Valor inicial = 21

n	Xn	Cálculo (2*xn)	Resto (2*Xn) módulo 61 [X(n+1)]
0	3	6	6
1	6	12	12
2	12	24	24
3	24	48	48
4	48	96	35
5	35	70	9

Dezenas para um jogo:	6	12	24	48	35	9

Tabela 2.3: Valor inicial = 3

n	Xn	Cálculo (2*xn)	Resto (2*Xn) módulo 61 [X(n+1)]
0	4135	8270	35
1	35	70	9
2	9	18	18
3	18	36	36
4	36	72	11
5	11	22	22

Dezenas para um jogo:	35	9	18	36	11	22

Tabela 2.4: Valor inicial = 4135

n	Xn	Cálculo (2*xn)	Resto (2*Xn) módulo 61 [X(n+1)]
0	52	104	43
1	43	86	25
2	25	50	50
3	50	100	39
4	39	78	17
5	17	34	34

Dezenas para um jogo:	43	25	50	39	17	34

Tabela 2.5: Valor inicial = 52

n	Xn	Cálculo (2*xn)	Resto (2*Xn) módulo 61 [X(n+1)]
0	9	18	18
1	18	36	36
2	36	72	11
3	11	22	22
4	22	44	44
5	44	88	27

Dezenas para um jogo:	18	36	11	22	44	27

Tabela 2.6: Valor inicial = 9

Na próxima seção veremos alguns outros tipos de geradores de números pseudoaleatórios.

2.1 Gerador Congruente Linear Misto

O Gerador Congruente Linear Misto remete à recorrência abaixo:

$$x_{n+1} \equiv ax_n + c \mod m$$

Geradores congruenciais lineares mistos são usadas comumente em muitos **softwares**, onde os valores $m = 2^{31}$, $a = 1.103.515.245$ e $c = 12.345$ são frequentemente tomados, este citado é o gerador utilizado na linguagem de programação ANSI-C. Esta recursão produz uma sequência de números inteiros no conjunto $\{0, 1, 2, ..., 2^{31} - 1\}$.

No entanto, um gerador por congruência linear pode não ser visto com bons olhos por especialistas, é possível notar que um ponto positivo para ele é a economia, pois minimiza o tempo computacional e uso de memória, ou seja, do ponto de vista estatístico é mais fraco, porém é suficiente para tarefas à mão, como é possível observar nos exemplos abaixo.

Exemplo 2.2. *Gerando senhas aleatórias de* 5 *dígitos.*

Vamos considerar os seguintes 17 *símbolos e a congruência módulo* 17*. Adotaremos também a seguinte identificação* $@ = 10, \# = 11, ..., + = 16$*. Ou seja, quando o resto for* 10 *usaremos o símbolo* @ *e assim sucessivamente. Para os símbolos que são números menores que 10, usaremos os próprios símbolos, portanto, se o resto for* 7 *usamos o próprio algarismo que já conhecemos. Temos aqui então definida a lista dos símbolos que usaremos:*

$$(0, 1, 2, 3, 4, 5, 6, 7, 8, 9, @, \#, \$, \%, \&, *, +)$$

Consideraremos a seguinte congruência

$$x_{n+1} \equiv 7x_n + 6 \mod 17, \textit{ com o valor inicial, sendo } x_1 = 10 = @$$

Logo,

$$\begin{aligned} x_2 &\equiv 70 + 6 \equiv 8 \mod 17 \\ x_3 &\equiv 56 + 6 \equiv 11 \mod 17 \\ x_4 &\equiv 77 + 6 \equiv 15 \mod 17 \\ x_5 &\equiv 105 + 6 \equiv 9 \mod 17 \end{aligned}$$

Por fim, temos uma senha com cinco dígitos, esta é: @ 8 # + 9

Um Gerador Congruente Linear Misto bastante utilizado é $m = 2^M$ e $c > 0$. O período completo $p = 2^M$ é obtido se, e somente, se $a \equiv 1 \mod 4$, isto é, se $a - 1$ é múltiplo de 4 e c é ímpar, sendo $c = 1$ frequentemente escolhido. Os bits de mais baixa ordem (menos significativos) possuem um padrão cíclico, decorrente da utilização de uma potencia de 2 para m. Por Exemplo, a sequência alterna entre números pares e ímpares. Apesar disto, o módulo com potência de 2 é frequentemente utilizado, pois torna o processo de realização da operação módulo eficiente. Além do mais, os números reais obtidos da sequência inteira não possuem um padrão muito regular nos bits de mais alta ordem (mais significativos) e ainda são utilizados em muitas aplicações.

Exemplo 2.3.

$$x_{n+1} \equiv 5x_n + 1 \mod 2^4$$

Sejam $a = 5, c = 1, m = 16$ e $x_0 = 1$ A sequência de inteiros aleatórios geradas por essa recorrrência é: $1, 6, 15, 12, 13, 2, 11, 8, 9, 14, 7, 4, 5, 10, 3, 0, 1, 6, 15, 12, 13, 2, 11, 8, 9, 14, ...$

Observa-se que o período p é igual a 16 ($p = 2^M = 2^4 = 16$). Esta sequência possui o período mais longo possível e é uniforme, isto é, preenche completamente o espaço de inteiros entre 0 e 15. Exibe através do seu período o padrão de alternar inteiros ímpares e pares; assim, o dígito binário mais à direita exibe o padrão regular 1, 0, 1, 0,... Também ao selecionar qualquer valor inicial entre 0 e 15, desloca-se ciclicamente a sequência acima.

Existem outros tantos geradores de números aleatórios, traremos a apresentação de outros dois, sendo o último deles o gerador de uma das principais linguagens de programação atualmente, o Python.

Exemplo 2.4. *Segundo [1], os geradores Lagged Fibonacci foram criado para serem uma melhoria aos geradores congruentes lineares. Esses geradores são baseados na sequência de Fibonacci, que pode ser descrita pela seguinte relação de recorrência:*

$$S_n = S_{n-1} + S_{n-2}$$

A fórmula da sequência Fibonacci nos mostra que cada termo da sequência é igual à soma dos seus dois termos anteriores. Contudo, é possível generalizar essa fórmula da seguinte forma:

$$S_n = S_{n-j} \star S_{n-k} \mod m, 0 < j < k$$

Nessa fórmula, o novo termo é uma combinação de quaisquer dois termos anteriores. O termo m é normalmente uma potencia de 2 ($m = 2^M$) onde M frequentemente é 32 ou 64. O operador $\star$ pode ser uma operação de adição, subtração, multiplicação e pode ser também uma operação binária.

Exemplo 2.5. *A seguir, temos um exemplo de um Gerador Lagged Fibonacci, gerando uma sequência de 6 números, a partir da seguinte congruência:*

$$x_{n+2} \equiv x_n + x_{n+1} \mod 2^4, \text{ com } x_0 = 4135 \text{ e } x_1 = 2.$$

Com os valores iniciais citados acima, obtivemos a tabela abaixo:

Gerador Lagged Fibonacci												
n	X(n)	X(n+1)	X(n) + X(n+1)	Resto X(n) + X(n+1) módulo 2^4 [X(n+2)]								
0	4135	2	4137	9								
1	2	9	11	11								
2	9	11	20	4								
3	11	4	15	15								
4	4	15	19	3								
5	15	3	18	2	Numeros Gerados	9	11	4	15	3	2	

Tabela 2.7: Gerador Lagged Fibonacci

Um exemplo de gerador Lagged Fibonacci muito utilizado é o Mersenne Twister, como foi citado anteriormente, é o gerador utilizado na linguagem Python.

2.1.1 Mersenne Twister

O Mersenne Twister é um gerador de números pseudoaleatórios desenvolvido em 1997 por Makoto Marsumoto e Takuji Nishimura. Trata-se de uma variação aprimorada de um gerador do tipo Lagged Fibonacci, capaz de produzir números aleatórios de alta qualidade. Seu desenvolvimento surgiu para corrigir diversas limitações presentes em algoritmos mais antigos.

O nome Mersenne Twister está relacionado ao período de repetição, que é definico como um número primo de Mersenne, outrora apresentado no capítulo 1. Esse gerador utiliza uma matriz de recorrência linear e possui uma fórmula de recorrência bastante sofisticada.

Existem duas versões amplamente utilizadas do Mersenne Twister, que diferem principalmente no tamanho do primo de Mersenne aplicado:

- MT19937 (32 bits
- MT19937-64 (64 bits)

Ambas são reconhecidas por sua eficiência e robustez na geração de números pseudoaleatórios. Para diversas aplicações, o Mersenne Twister tem se consolidado como o gerador de números aleatórios padrão. Um exemplo notável de sua utilização é na linguagem de programação Python, onde ele é implementado como o algoritmo principal para geração de valores pseudoaleatórios.

Abaixo temos dois exemplos de números sendo gerados pelo Mersenne Twister, para gerá-los foi utilizado a plataforma gratuita Google Colab.

Neste primeiro, temos o gerador em questão, gerando uma lista de 5 sequências, com números variando de 0 a 100.

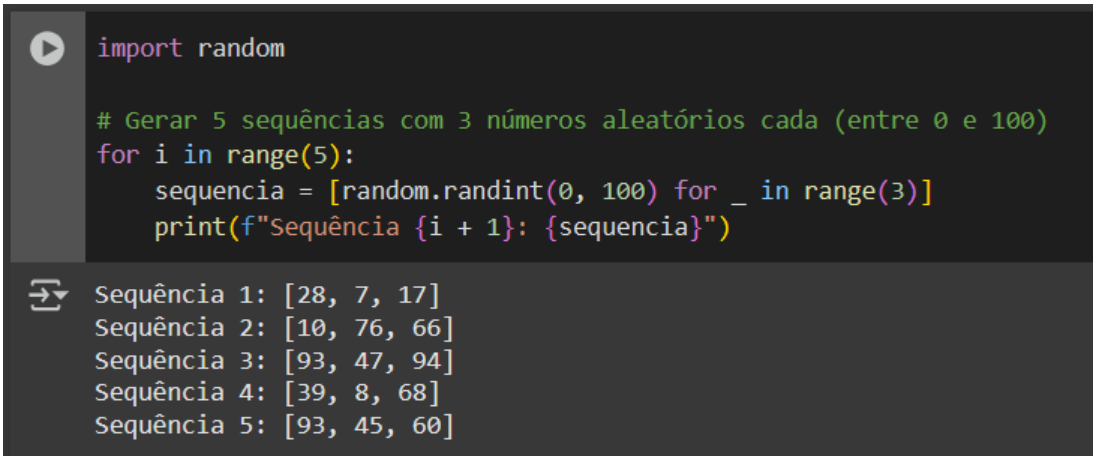

Figura 2.1: Números aleatórios no Python

Já no segundo a proposta foi retornar ao problema da Mega-Sena e pedir pra ele gerar 5 sequências de números inteiros entre 1 e 60. Observe

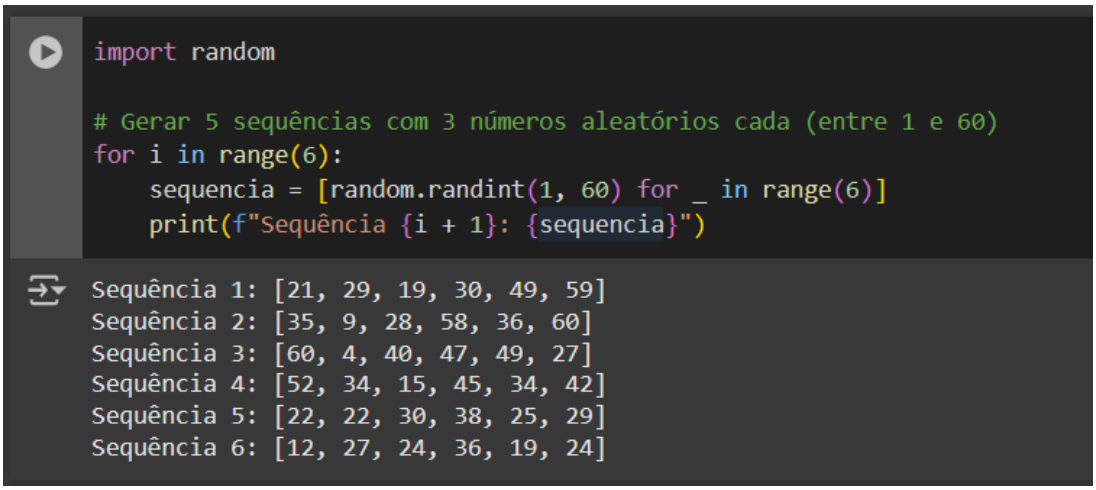

Figura 2.2: Números aleatórios no Python - Sena

Entre as principais características do Mersenne Twister, destacam-se:

- Período extremamente longo: O algoritmo possui um período de repetição de $2^{19937} - 1$, o que o torna adequado para simulações complexas e de longa duração.
- Robustez estatística: O gerador foi amplamente testado e aprovado nos principais testes de aleatoriedade, garantindo alta qualidade na distribuição dos números produzidos.

Essas propriedades fazem do Mersenne Twister uma escolha confiável para métodos estatísticos avançados, que demandam alta precisão e ausência de padrões previsíveis.

Capítulo

3

Geradores de números pseudoaleatórios: uma abordagem para o ensino médio

Este capítulo tem como objetivo abordar a temática dos geradores de números aleatórios e sua aplicação no cotidiano, adaptada para o ensino médio, com a intenção de que os estudantes e professores possam conhecer, fazer uso e debater mais essa ferramenta matemática em sala de aula e verificar como, independente de termos consciência disso ou não, como a matemática atravessa de maneira avassaladora nosso cotidiano.

Devido aos estudantes dessa faixa do ensino médio não conhecerem a noção de congruência, adaptaremos o tema utilizando a divisão com restos, tema que eles conhecem desde o ensino fundamental. Pontuamos que nada muda, dado que congruência é aritmética dos restos. Com relação às raízes primitivas, não faremos uso desse conceito nessa adaptação, apenas indicaremos que estudos futuros são necessários para se compreender mais profundamente o tema dos geradores de números pseudoaleatórios.

A proposta esta alinhada às competências gerais da Base Nacional Comum Curricular (BNCC) (BRASIL, 2018), especialmente no que diz respeito ao desenvolvimento do pensamento científico, crítico e criativo (Competência 2) e à cultura digital (Competência 5). Além disso, a Lei de Diretrizes e Bases da Educação Nacional (LDB 9.394/96) (BRASIL, 1996) reforça a importância de uma formação que associe teoria e prática, preparando os estudantes para compreender e intervir na realidade.

A intenção é despertar o interesse do aluno por meio de ferramentas acessíveis, como planilhas eletrônicas, que auxiliam na compreensão de conceitos como algoritmos e aleatoriedade. Sabe-se que a utilização de tecnologias digitais na educação matemática favorece a experimentação e a construção ativa do conhecimento.

Além disso, busca-se demonstrar que os geradores de números aleatórios estão presentes em diversas situações cotidianas, como:

- Sistemas de autenticação em dois fatores (2FA);
- Mecânicas de jogos (sorteio de cartas, abertura de baús com recompensas);
- Cassinos virtuais e seus impactos sociais (discutindo questões como probabilidade e vício em jogos de azar).

Por fim, esperamos que o estudante não apenas compreenda os fundamentos matemáticos por trás desses sistemas, mas também reflita sobre suas implicações éticas e sociais, desenvolvendo um pensamento crítico — conforme preconiza a BNCC no eixo da cidadania e responsabilidade social.

3.1 Apresentando o tema em sala de aula

3.1.1 Atividades envolvendo aleatoriedade vs pseudoaleatoriedade

Dinâmica Inicial:

- Orientar os estudantes que pesquisem e listem situações cotidianas que dependem de sorte/aleatoriedade (ex.: sorteio de amigo secreto, resultados de jogos de dados).
- No segundo momento questionar junto aos estudantes, "Como um computador, que segue regras fixas, simula sorte?"

3.2 Geradores congruenciais lineares adaptados para o ensino médio.

Nesta seção, será desenvolvida uma proposta pedagógica voltada para o Ensino Médio, com o objetivo de facilitar a compreensão dos geradores congruenciais lineares. A metodologia adotada priorizará atividades interativas, exemplos concretos e ferramentas computacionais, visando despertar o interesse dos alunos e consolidar o aprendizado por meio da experimentação e resolução de problemas.

3.2.1 Algoritmo da Divisão Eucliana como Base

Conceito-Chave:
A divisão euclidiana ($a = b \cdot q + r$) gera um resto r, com $0 \leq r < q$, com $a, b, q, r \in \mathbb{Z}$, podendo ser usado para criar sequências aparentemente aleatórias.

Atividade 1: Gerando Números, utilizando os restos

1. Escolher um número "valor inicial"($X_0 = 15$).
2. Aplicar repetidamente:

$$X_{n+1} = \text{resto da divisão de } (5 \cdot X_n + 3) \text{ por } 16.$$

- Passo a passo:
  - $15 \times 5 = 75$
  - $75 + 3 = 78$
  - $78 \div 16 = 4$ com resto 14, temos então que $X_1 = 14$.
  - Repita o passo a passo para $X_1 = 14$, assim obterá $X_2 = 9$, e assim por diante.

Tabela de Resultados

n	X_n	**Cálculo**	**Resto** X_{n+1}
0	15	$(5 \times 15 + 3) \div 16$	14
1	14	$(5 \times 14 + 3) \div 16$	9
2	9	$(5 \times 9 + 3) \div 16$	0
3	0	$(5 \times 0 + 3) \div 16$	3
4	3	$(5 \times 3 + 3) \div 16$	2
5	2	$(5 \times 2 + 3) \div 16$	13
6	13	$(5 \times 13 + 3) \div 16$	4
7	4	$(5 \times 4 + 3) \div 16$	7

Tabela 3.1: Tabela com alguns números gerados da recorrência citada acima.

Crie seu próprio gerador

- Opção A: Lápis e papel
- Opção B: Planilha/Scratch/Python

Havendo a possibilidade e recurso para trabalhar com planilhas, segue a captura de telas e uma sugestão de elaboração passo a passo no Google Sheets, após ter enunciado as colunas e colocado o valor inicial (X_n), faremos:

- 1º Passo: Na terceira célula ao lado do valor inicial escolhido, $X_0 = 15$, escrevemos o Cálculo definido pela recorrência.

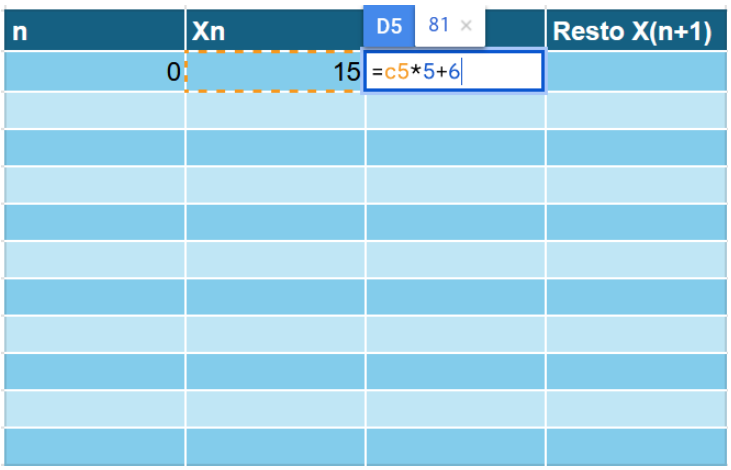

Figura 3.1: Inserindo lei de recorrência

- 2º Passo: Pedir para calcular o resto do cálculo da celula anterior, módulo 32.

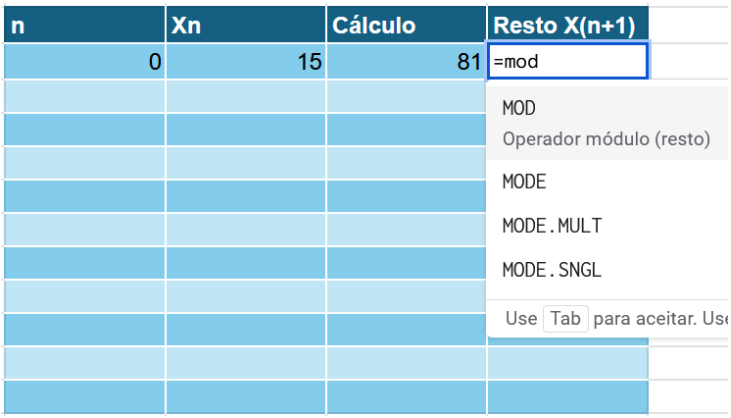

Figura 3.2: Incluindo operador módulo

- 3º Passo: Definir que as para calcular o resto, usaremos a célula anterior, isto é, do cálculo e aplicaremos módulo 32, observe na figura abaixo.

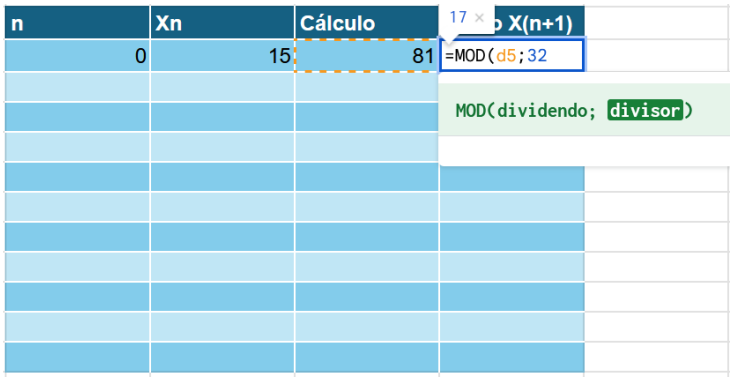

Figura 3.3: Definindo o módulo

- 4º Passo: Por fim, arrastando para baixo 9 células em cada coluna, a fim de que se repita o que ocorreu nas primeiras linhas, conseguiremos gerar 9 números pseudoaleatórios, localizados na segunda coluna da tabela, como é possível observar.

n	Xn	Cálculo	Resto X(n+1)
0	15	81	17
1	17	91	27
2	27	141	13
3	13	71	7
4	7	41	9
5	9	51	19
6	19	101	5
7	5	31	31
8	31	161	1
9	1	11	11

Figura 3.4: Geração de nove números pseudo aleatórios

Reflexão Final:

- Por que bancos não utilizam formas simples como a que testamos?
- Se um jogo usasse uma regra previsível, como um jogador poderia trapacear.

O intuito desta reflexão é levar os estudantes a analisarem a fragilidade inerente aos geradores por congruência linear, compreendendo, assim, a necessidade de métodos mais robustos para a geração de números aleatórios. Essa discussão pode incentivá-los a explorar geradores mais "fortes"e suas aplicações práticas, inclusive no cotidiano.

Além disso, por se tratar de um método previsível, esse tipo de gerador torna-se particularmente vulnerável a manipulações. Isso levanta questionamentos relevantes:

será que casas de apostas, mesmo as voltadas para o esporte, que frequentemente disponibilizam cassinos virtuais em suas plataformas, utilizam geradores de números pseudoaleatórios? E, se sim, como essa escolha influencia diretamente a sociedade atual?

Considerações Finais

Neste trabalho, foi possível verificar a aplicação da matemática em um dos temas mais importantes da humanidade: a segurança de dados. Demonstrou-se como ela possibilita a criação de senhas mais seguras e a geração de códigos para autenticação em dois fatores. Um dos resultados alcançados foi despertar no professor e no estudante uma visão crítica sobre o papel da matemática, pois, ao compreender as ferramentas matemáticas que fundamentam a segurança de dados e a criptografia, o leitor deste trabalho não mais interpretará notícias como as citadas em [4] e [8] como meros caprichos matemáticos ou algo totalmente alheio à sua realidade.

Embora, conforme relatado em [4], o cofundador do projeto colaborativo GIMPS (Great Internet Mersenne Prime Search) tenha afirmado ao The Washington Post que a busca por números primos gigantes "é entretenimento para nerds da matemática"e "uma boa maneira de passar o tempo", a relevância desses estudos vai muito além. Em [9], Teixeira, pesquisador do IMPA, alerta para um futuro incerto, já que acredita que a computação quântica poderá, um dia, fatorar até mesmo os maiores números primos com facilidade. Isso pode exigir a adoção de métodos mais eficazes para proteger dados, como a criptografia baseada em curvas elípticas, citada por Teixeira como uma alternativa promissora.

Esse trabalho ilustrou como a sociedade em que vivemos é dependente de matemática. Para assuntos tão comuns como a geração de senhas e sorteios, estão lá conteúdos matemáticos, alguns muito simples, outros mais sofisticados, presentes. Ilustrou também que, independente de as pessoas saberem matemática, a vida delas depende e é regulada por conteúdos matemáticos que geram algoritmos e ajudam na organização e funcionamento da sociedade.

Como sugestões para desenvolvimentos futuros, propõe-se o estudo de números verdadeiramente aleatórios, o que exigirá o domínio de outras competências na área de comunicação e segurança de dados. Além disso, sugere-se uma investigação

sobre a Lei dos Grandes Números, que permite determinar matematicamente diversos resultados em jogos de azar, trazendo clareza sobre como a soma de múltiplas variáveis aleatórias independentes (ou não correlacionadas) tende a se aproximar de sua esperança matemática.

Por fim, espera-se que esta pesquisa sirva como ferramenta para ampliar a compreensão dos estudantes sobre a presença da matemática em seu cotidiano, reforçando a importância dos geradores de números pseudoaleatórios no contexto da educação matemática e da segurança digital.

Referências Bibliográficas

[1] Souza, G. S; Alves JR, N. *Geradores de Números Aleatórios*. CBPF, 6 páginas, Rio de Janeiro, 2011.

[2] Hefez, Abramo. *Aritmética*. 2ª ed., SBM, Coleção PROFMAT 08, 298 páginas, Rio de Janeiro, 2016.

[3] Bertolossi, H. J. *Números (Pseudo) Aleatórios, Probabilidade Geométrica, Métodos de Monte Carlo e Estereologia*. IME/UFF, 5 páginas, Rio de Janeiro.

[4] IMPA. *Descoberto número primo com quase 25 milhões de dígitos*. Publicado no site do IMPA. Disponível em: https://impa.br/noticias/descoberto-numero-primo-com-quase-25-milhoes-de-digitos/. Acessado em 10 de Março de 2025.

[5] Brasil. *BNCC: Base Nacional Comum Curricular*. Ministério da Educação. Brasília, DF: MEC, 2017. Disponível em: https://www.gov.br/mec/pt-br/cne/bncc_ensino_medio.pdf. Acessado em 11 de janeiro de 2025.

[6] Brasil. *LDB: Lei de Diretrizes e Bases da Educação Nacional - Lei nº 9.394/1996*. 7. ed. Brasília, DF: Senado Federal, 2023. 64 p. Disponível em: https://www2.senado.leg.br/bdsf/bitstream/handle/id/642419/LDB_7ed.pdf. Acessado em 11 de janeiro de 2025.

[7] Monteiro, P.A.,G. *Gerador de Números Aleatórios Integrado em Tecnologia CMOS*. Dissertação (Metrado em Engenharia Eletrotécnica e de Computadores) - Departamento de Engenharia Eletrotécnica e de Computadores, Universidade Nova de Lisboa. 66 páginas, Lisboa, 2022.

[8] Marin, J. *Número primo de 41 milhões de dígitos é descoberto por matemático*. Publicado

no site da CNN. Disponível em: https://www.cnnbrasil.com.br/tecnologia/numero-primo-de-41-milhoes-de-digitos-e-descoberto-por-matematico/#goog_rewarded. Acessado em 23 de Março de 2025.

[9] IMPA. *Por que a descoberta do maior número primo importa?*. Publicado no site da IMPA. Disponível em: https://impa.br/notices/por-que-a-descoberta-do-maior-numero-primo-importa/. Acessado em 27 de Março de 2025.

[10] Burton, D.M. *Elementary Number Theory* 7ªed. Connect Learn Suceed, 440 páginas, Nova Iorque, 2007.