UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO - UFES

PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL – PROFMAT

DISSERTAÇÃO DE MESTRADO

Um Jogo que Estimula o Aprendizado da Criptografia RSA

Karina Marchetti Bonno Escobar

Vitória, Espírito Santo
2019

Karina Marchetti Bonno Escobar

Um Jogo que Estimula o Aprendizado da Criptografia RSA

Trabalho de conclusão apresentado ao Corpo Docente do Programa de Pós-Graduação em Matemática em Rede Nacional PROFMAT CCE - UFES, como requisito parcial para obtenção do título de Mestre em Matemática.

Universidade Federal do Espírito Santo

Orientador: Prof Dr. Florêncio Ferreira Guimarães Filho

Vitória, Espírito Santo
2019

Ficha catalográfica disponibilizada pelo Sistema Integrado de Bibliotecas - SIBI/UFES e elaborada pelo autor

---

Escobar, Karina Marchetti Bonno, 1972-
E74j Um jogo que estimula o aprendizado da criptografia RSA / Karina Marchetti Bonno Escobar. - 2019.
47 f. : il.

Orientador: Florêncio Ferreira Guimarães Filho.
Dissertação (Mestrado Profissional em Matemática em Rede Nacional) - Universidade Federal do Espírito Santo, Centro de Ciências Exatas.

1. Criptografia RSA. 2. Pequeno teorema de Fermat. 3. RPG Maker. I. Guimarães Filho, Florêncio Ferreira. II. Universidade Federal do Espírito Santo. Centro de Ciências Exatas. III. Título.

CDU: 51

UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO

Centro de Ciências Exatas

Programa de Pós-Graduação em Matemática em Rede Nacional - PROFMAT

"Um Jogo que Estimula o Aprendizado da Criptografia RSA"

Karina Marchetti Bonno Escobar

Defesa de Dissertação de Mestrado Profissional submetida ao Programa de Pós-Graduação em Matemática em Rede Nacional da Universidade Federal do Espírito Santo como requisito parcial para a obtenção do título de Mestre em Matemática.

Aprovada em 26/04/2019 por:

Prof. Dr. Florêncio Ferreira Guimarães Filho
Orientador – UFES

Prof. Dr. Moacir Rosado Filho
Membro Interno – UFES

Prof. Dr. José de Arimatéia Fernandes
Membro Externo – UFCG

Este trabalho é dedicado à minha querida mãe, Maria Marchetti e ao meu amado marido, Francisco Emilio Grijó Escobar, que sempre me incentivaram e me deram força para seguir em frente.

Agradecimentos

Aos meus colegas de curso, pela parceria e aprendizado estabelecidos;
Aos Profs. Drs. Moacir Rosado, Júlia Wrobel, Rosa Elvira, Domingos Sávio e Alancardek de Araújo, todos do Departamento de Matemática da UFES, pela dedicação ao longo do curso;
Finalmente, ao meu orientador Prof. Dr. Florêncio Ferreira Guimarães Filho, um dos meus idólos, pela sua orientação e paciência.

Resumo

Neste trabalho, apresentamos os principais resultados matemáticos que justificam o funcionamento da criptografia RSA e sua segurança, tais como pequeno teorema de Fermat, equações diofantinas e teorema do resto chinês. Apresentamos ainda a importância dos jogos games, em especial o RPG *Maker*, nas aulas de matemática. Com o intuito de aplicar a criptogria RSA foi criado um jogo eletrônico, no estilo RPG (Role Playing Game).

Palavras-chave: Criptografia RSA; Pequeno teorema de Fermat; RPG *Maker*.

Abstract

In this work, we present the main mathematical results that justify the operation of RSA encryption and its security, such as Fermat's small theorem, Diophantine equations and Chinese remainder theorem. We also present the importance of games, especially RPG textit Maker, in math classes. In order to apply RSA cryptogria, an electronic RPG (Role Playing Game) game was created.

Keywords:RSA Encryption;Fermat's Little Theorem;RPG *Maker*.

Lista de ilustrações

Sumário

1 Introdução

A criptografia estuda os métodos de como codificar uma mensagem de tal forma que apenas o destinatário consiga decodificá-la.

Com o avanço da computação e um maior uso da internet, aumentou-se a necessidade de melhorar os métodos de criptografia. Em 1976, Diffie e Hellman criaram a criptografia com chave pública a qual é composta por duas chaves, uma pública e outra privada (mantida em segredo).

A partir da criação da criptografia com chave pública, Rivest, Shamir e Adleman, criram em 1978, o método de criptografia chamado *Criptografia RSA*, que leva as iniciais de seus nomes, utilizando a teoria da aritmética modular.

No capítulo 2, encontra-se conceitos básicos de aritmética que são importantes para o entendimento da criptografia RSA, são eles: divisão dos números inteiros, algorítmo de Euclides, equações diofantinas e números primos.

No capítulo 3, ainda trabalhando conceitos para o entendimento da criptografia RSA, encontra-se congruência módulo m, o pequeno teorema de Fermat e o teorema Chinês do Resto.

O capítulo 4, explica o funcionamento do método RSA.

O intuito do presente trabalho é despertar o interesse do corpo discente pela aula, diminuindo as faltas e atrasos, incentivar a pesquisa individual, desenvolver o trabalho em equipe, estimular a criatividade e o autoconhecimento, utilizando o jogo eletrônico de RPG como material didático para o ensino da criptografia RSA.

A metodologia utilizada pelo professor, ao repassar os conteúdos, quase sempre é a principal causa de desmotivação e desinteresse pelo ensino em geral MATTAR (2010).

Como afirma MATTAR (2010):

> "A retenção do conhecimento é naturalmente baixa quando os alunos setam para passivamente assistir a aulas sobre algo que não faz sentido para eles."

Muitos autores destacam a importância dos jogos como elementos motivadores e facilitadores no processo de aprendizagem.

No livro *Serious games*, publicado originalmente em 1970, Clark Abt explora as maneiras pelas quais os jogos em geral, podem ser utilizados na educação.

Para Abt

> "Jogos são dispositivos de ensino e treinamento efetivos para alunos de qualquer idade, e em muitas situações, porque são altamente motivadores e comunicam muito eficientemente conceitos e fatos em muitas áreas.Eles criam representações dramáticas do problema real estudado. Os jogadores assumem papéis realistas, encaram problemas, formulam estratégias, tomam decisões e recebem *feedback* rápido da consequência de suas ações."

No Capítulo 5, encontra-se um jogo de RPG eletrônico, construído por mim, na tentativa de motivar a aprendezagem da criptografia RSA na sala de aula das turmas de ensino médio.

2 Aritmética Básica

Neste capítulo será feito uma breve revisão dos pontos mais importantes de aritmética para o entedimento do funcionamento do método RSA de criptografia.

2.1 Divisão nos Números Inteiros

Dados dois números $a,b \in \mathbb{Z}$ dizemos que a divide b, ou que b é múltiplo de a, ou ainda que a é divisor de b se existir um número $q \in \mathbb{Z}$ tal que $b{=}a{\cdot}q$. Neste caso, usa-se a notação $a|b$.
Se isso não acontecer, ou seja, a não dividir b escreve-se $a\nmid b$.

Lema 1. *Sejam a, b,c, $d \in \mathbb{Z}$. Tem-se:*

(1) Se $d \mid a$ e $d \mid b$, então $d \mid (ax + by)$ para qualquer combinação linear de a e b com coeficientes x,$y \in \mathbb{Z}$;
(2) (Limitação) Se $d \mid a$, então $a = 0$ ou $|d| \leqslant |a|$;
(3) (Transitividade) Se $a \mid b$ e $b \mid c$, então $a \mid c$;

Demonstração. Se $d \mid a$ e $d \mid b$, então existem q_1 e $q_2 \in \mathbb{Z}$ tais que $a = dq_1$ e $b = dq_2$, $ax+by = d(q_1x+q_2y)$. Como $q_1x+q_2y \in \mathbb{Z}$, tem-se que $d \mid (ax+by)$, donde conclui-se (1).

Para mostrar (2), suponha que $d \mid a$ e $a \neq 0$. Neste caso, $a = dq$ com $q \neq 0$, assim $|q| \geq 1$ e $|a| = |d||q| \geq d$.

Finalmente provaremos (3). Se $a \mid b$ e $b \mid c$, então existem q_1 e $q_2 \in$ Z tais que $b = aq_1$ e $c = bq_2$, logo $c = aq_1q_2$ e portanto $a \mid c$.

□

Teorema 1. *(Divisão Euclidiana) Dados a e $b \in \mathbb{Z}$ com $b \neq 0$, então existem únicos q,* e *$r \in Z$ tais que*

$$a = bq + r \quad e \quad 0 \leq r \leq |b|.$$

Neste caso, q é chamado de quociente e r de resto.

Demonstração. Considere o conjunto

$$S = \{x = a - by; y \in \mathbb{Z}\} \cap (\mathbb{N} \cup \{0\})$$

Como o conjunto dos números Naturais não permite cota superior, existe um $n \in \mathbb{Z}$ tal que $n(-b) > -a$, logo $a - nb > 0$, mostrando que S não é vazio.

O conjunto S é limitado inferiormente por 0, logo, pelo Pricípio da Boa Ordenação, tem-se que S possui um menor elemento r.

Suponhamos então que $r = a - bq$. Sabendo que $r \geqslant 0$ é preciso mostrar que $r < |b|$.

Suponha, por absurdo, $r > |b|$. Daí, existe $s \in \mathbb{N} \cup \{0\}$ tal que $r = |b| + s$, com $0 \leq s < r$. Mas isso contradiz o fato de r ser o menor elemento de S, pois $s = a-(q\pm1)b \in$ Z, com $s < r$.

Para provarmos a unicidade, suponha que $a = bq + r = bq' + r'$, onde $q, q', r, r' \in \mathbb{Z}$, $0 \leq r < |b|$ e $0 \leq r' < |b|$. Assim tem-se que $-|b| < -r \leq r' - r \leq r' < |b|$. Logo, $|r' - r| < b$. Por outro lado, $b(q - q') = r' - r$, o que implica $|b||q - q'| = |r' - r| < |b|$, o que só é possível se $q = q'$, e consequentemente, $r = r'$ □

2.2 Algoritmo de Euclides

Definição 1. *Dizemos que um número inteiro $d \geq 0$ é um máximo divisor comum(mdc) de a e b, se possuir as seguintes propriedades:*
(1) d é um divisor comum de a e b, e
(2) d é divisível por todo divisor comum de a e b.

Notação 1. *Se d é o máximo divisor comum de a e b escrevemos $d = (a, b)$.*

Definição 2. *Sejam a e b dois inteiros tais que $a \neq 0$ ou $b \neq 0$. Dizemos que $m > 0$ é um mínimo múltiplo comum de a e b se:*
(1) m é um múltiplo comum de a e b,
(2) se c é um múltiplo comum de a e b, então $m|c$.

Notação 2. *Se m é o mínimo múltiplo comum de a e b escrevemos $m = [a, b]$.*

Lema 2. *(Euclides). Se $a = bq + r$, então $(a, b) = (a, r)$.*

Demonstração. Basta mostrar que $D_a \cap D_b = D_b \cap D_r$, já que se estes conjuntos forem iguais, em particular, seus máximos também serão iguais. Se $d \in D_a \cap D_b$ temos $d \mid a$ e $d \mid b$, logo $d \mid a - bq \Leftrightarrow d \mid r$ e portanto $d \in D_b \cap D_r$. Da mesma forma, se $d \in D_b \cap D_r$, temos $d \mid b$ e $d \mid r$, logo $d \mid bq + r \Leftrightarrow d \mid a$ e assim $d \in D_a \cap D_b$.

□

Vamos aplicar o Lema 2 para calcular o (a, b).

Demonstração. Vamos supor que $1 < b < a$. Se $b \mid a$, então $(a, b) = b$. Se $b \nmid a$, pela divisão euclidiana, pode-se escrever $a = bq_1 + r_1$, com $0 < r_1 < b$, e pelo Lema 2, tem-se duas possibilidades:

(1) $r_1 \mid b \Leftrightarrow (a, b) = (r_1, b) = r_1$

(2) $r_1 \nmid b$, então pode-se efetuar a divisão euclidiana de b por r_1, obtendo $b = r_1q_2 + r_2$, com $0 < r_2 < r_1$. Novamente há duas possibilidades r_2 dividir ou não r_1, podendo ser aplicado o algoritmo sucessivas vezes, gerando uma sequência decrescente finita de $r_j, j = 1, 2, 3, ...$(o que sempre ocorre, pois o conjuntos dos números Naturais tem sempre um menor elemento. □

O algoritmo acima pode ser sintetizado e realizado na prática da seguinte maneira: Inicialmente, efetuamos a divisão $a = bq_1 + r_1$ e colocamos os número envolvidos no seguinte diagrama:

	q_1
a	b
r_1	

A seguir, continuamos efetuando a divisão $b = r_1q_2 + r_2$ e colocamos os números envolvidos no diagrama a seguir.

	q_1	q_2
a	b	r_1
r_1	r_2	

Prosseguindo, enquanto for possível, teremos:

	q_1	q_2	q_3	...	q_{n-1}	q_n	q_{n+1}
a	b	r_1	r_2	...	r_{n-2}	r_{n-1}	$r_n = (a, b)$
r_1	r_2	r_3	r_4	...	r_n		

Teorema 2. *Relação de Bézout: Sejam a e b dois números inteiros não nulos simultaneamente e seja $d = (a, b)$; nestas condições, existem inteiros m e n tais que;*

$$d = ma + nb$$

Demonstração. Consideremos o conjunto $A = \{(ra + sb) > 0; r, s \in\}\mathbb{Z}$. Note que $A \neq \varnothing$, logo pelo Príncípio da Boa Ordenação existe $d_1 = minA > 0$. Como $d_1 \in A$, então existem m e $n \in \mathbb{Z}$, tais que;

$$d_1 = ma + nb$$

E observando que $d \mid a$ e $d \mid b$ resulta que $d \mid d_1$, daí temos $d \leq d_1$. Com essas afirmações, obtemos $d_1 \mid a$ e $d_1 \mid d$. Suponha que d_1 não divida nem a nem b. Assim existiriam números inteiros q, q', t, t' tais que:

$$a = d_1 q + t, \quad com \quad 0 < t < d$$

$$b = d_1 q' + t', \quad com \quad 0 < t' < d$$

Segue-se;

$$t = a - qd_1 = a - q(ma + nb)$$

$$t = a - qma - qnb$$

$$t = (1 - qm)a - (qn)b$$

e

$$t' = b - q'd_1 = b - q'(ma + nb)$$

$$t' = b - q'ma - q'nb$$

$$t = (-q'm)a + (1 - q'n)b$$

Como $0 < t$, $t' < d_1$ temos que t e $t' \in$A. Absurdo! Uma vez que $0 < t < d_1 = minA$. Portanto, d_1 é divisor comum positivo de a e b, logo $d_1 \leq d$ e então $d_1 = d$

□

Teorema 3. *(Lema de Gauss): Sejam a, b e c números inteiros. Se $a \mid bc$ e $(a, b) = 1$, então $a \mid c$*

Demonstração. Como $a \mid bc$, existe um número inteiro e tal que $bc = ae$.
Como $(a, b) = 1$, pela Proposição 1, existem números naturais m , n tais que

$$ma + nb = 1.$$

Multiplicando por c ambos os lados da igualdade acima, temos que

$$c = nac + mbc.$$

Substituindo bc por ae nesta última igualdade, temos que

$$c = mac + nae = a(mc + ne)$$

e, portando $a \mid c$. □

2.3 Equações Diofantinas Lineares

Equações da forma

$$aX + bY = c$$

com a, b, $c \in \mathbb{Z}$ são chamadas *equações diofantinas lineares.*

Nem sempre estas equações possuem soluções inteiras. As condições necessárias para uma equação diofantina ter solução serão dadas nas duas proposições a seguir.

Proposição 1. *Sejam a, b, $c \in \mathbb{Z}$. A equação $aX + bY = c$ admite solução em números inteiros se, e somente se, $(a, b) \mid c$*

Demonstração. ($\Rightarrow$) Suponhamos que (x_0, y_0 seja solução da equação, isto é:

$$ax_0 + by_0 = c.$$

Seja $(a, b) = d$, por definção de *máximo divisor comum*, temos que $d \mid a$ e $d \mid b$, então, d divide qualquer combinação linear formada pelos inteiros a e b. Portanto $d \mid (ax_0 + by_0)$
($\Leftarrow$) Seja $(a, b) = d$. Se $d \mid c$, então $c = dm$ para algum $m \in \mathbb{Z}$. Além disso existem inteiros x_0, y_0 tais que $ax_0 + by_0 = d$ (relação de Bézout). Logo, $a(x_0m) + b(y_0m) = dm = c$ e, portanto, (mx_0, my_0 é solução da equação.

□

Proposição 2. *Seja x_0, y_0 uma solução da equação $aX + bY = c$, onde $(a, b) = 1$. Então, as soluções x, y em $\mathbb{Z}$ da equação são*

$$x = x_0 + tb, \quad y = y_0 - ta; \quad t \in \mathbb{Z}.$$

Demonstração. Seja x, y uma solução de $aX + bY = c$, logo,

$$ax_0 + by_0 = ax + by = c$$

Consequentemente,

$$a(x - x_0) = b(y_0 - y) \tag{2.1}$$

Como $(a, b) = 1$, segue-se que $b \mid (x - x_0)$. Logo,

$$x - x_0 = tb, \quad t \in \mathbb{Z}$$

Substituindo a expressão de $x - x_0$ acima em (2.1), segue-se que

$$y_0 - y = ta,$$

o que prova que as soluções são do tipo exibido. Por outro lado, x, y, como no enunciado, é solução, pois

$$ax + by = a(x_0 + tb) + b(y_0 - ta) = ax_0 + by_0 = c$$

□

Observação 1. *Segue da Proposição 2 que a equação diofantina $aX + bY = c$, com $(a, b) = 1$, admite infinitas soluções inteiras.*

2.4 Números Primos

Nesta seção apresentaremos alguns resultado sobre números primos que formarão uma das bases para teoria de criptografia método RSA.

Definição 3. *Um número natural maior do que 1 e que só é divisível por 1 e por si próprio é chamado de número primo.*

Proposição 3. *Dados dois números primos p e q e um número inteiro a qualquer. Temos:*
(1) Se $p \mid q$, então $p = q$.
(2) Se $p \nmid q$, então $(p, q) = 1$.

Demonstração. (1) Como $p \mid q$ e sendo q primo, temos $p = 1$ ou $p = q$. Sendo p primo, tem-se $p > 1$, o que acarreta $p = q$.
(2) Seja $(p, a) = d$, temos que $d \mid p$ e $d \mid a$. Portanto, $d = p$ ou $d = 1$. Mas $d \neq p$, pois $p \nmid a$ e, consequentemente, $d = 1$.

□

Proposição 4. *Sejam $a, b, p \in \mathbb{Z}$, com p primo. Se $p \mid ab$, então $p \mid a$ ou $p \mid b$.*

Demonstração. Basta provar que, se $p \mid ab$ e $p \nmid a$, então $p \mid b$. Mas, se $p \nmid a$, temos que $(p, a) = 1$, e o resultado segue-se do Lema de Gauss (Teorema 3).

□

Teorema 4. *(Teorema Fundamental da Aritmética).Seja $n \geq 2$ um número natural, pode-se escrever n de uma única forma como um produto*

$$n = p_1.p_2...p_n$$

onde $m \geq 1$ é um número natural e $p_1 \leq p_2 \leq ... \leq p_m$ são primos.

Demonstração. Se n é um número primo não há o que demonstrar, pois basta que se faça $m = 1 \Rightarrow p_1 = n$. Se n é composto, seja $p_1 > 1$ o menor dos divisores positivos de n.

Pode-se provar que p_1 é primo. De fato, caso contrário existiria um p, com $1 < p < p_1$ tal que $p \mid p_1$, donde $p \mid n$, o que iria contradizer a escolha de p_1 como menor divisor. Assim n pode ser escrito $n = p_1 n_1$.

Se n_1 for primo a prova está finalizada, mas se n_1 for composto, seja $p_2 > 1$ o menor dos divisores positivos de n_1. Pode-se provar que p_2 é primo, logo $n = p_1 p_2 n_2$. Repete-se o processo até encontrar um n_r que seja primo.

Como $n_1, n_2, ...n_r$ é uma sequência decrescente, onde todos os termos pertencem aos naturais, então será finita.

Os primos da sequência $p_1, p_2, ..., p_m$ não são necessariamente distintos, a forma de n será:

$$n = p_1^{\alpha_1}.p_2^{\alpha_2}.p_3^{\alpha_3}...p_m^{\alpha_m}.$$

Sendo $\alpha_1, \alpha_1, ..., \alpha_m \in \mathbb{N}$

Precisa-se provar a unicidade da fatoração. Para n for primo não há o que provar. Para isso suponha que n seja composto e tenha duas fatorações:

$$n = p_1.p_2...p_r \quad e \quad n = q_1.q_2...q_s.$$

É preciso mostrar que $r = s$ e que cada p_i é igual a algum dos q_j. Como $p_1 \mid q_1.q_2...q_s$, e como ambos são primos, logo p_1 divide um dos fatores q_j, donde a menos de ordem, podemos supor $p_1 = q_1$. Da mesma forma $p_2 \mid q_1.q_2...q_s$, como ambos são primos, implica que $p_2 = q_2$, repetindo o processo, tem-se que $r = s$, logo as fatorações $p_1.p_2...p_r$ e $q_1.q_2...q_s$ são idênticas.

□

Teorema 5. *Existem infinitos números primos.*

Demonstração. Suponha, por absurdo, que a sucessão de números primos seja finita e dada por $p_1, p_2, ..., p_n$. Seja $P = p_1.p_2...p_n + 1$. Seja p um número primo que divide P. Esse primo não pode ser igual a nenhum dos p_i pois, senão, dividiria P e dividiria $p_1.p_2...p_n$. Logo dividiria $P - p_1.p_2...p_n = 1$, o que é absurdo. Portanto, p é um número primo que não pertence à sucessão e, portanto, existe um primo diferente de $p_1.p_2...p_n$. Portanto, existem infinitos primos. □

Definição 4. *O número $\phi(m)$ é o número de inteiros positivos menores que, ou iguais a m, que são relativamente primos com m.*

Um fato importante de se notar, a partir da definição, é que $\phi(p) = p - 1$ se p é um número primo, já que ele é coprimo com todos os menores que ele. A definição da função ϕ de Euler será importante no sistema de cifragem da RSA.

3 Congruência

Seja m um número narural. Diremos que dois números interios 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

$$a \equiv b \bmod m$$

Proposição 5. *Suponha que $a, b, m \in \mathbb{Z}$, com $m > 1$. Tem-se $a \equiv b \bmod m$ se, e somente se, $m \mid b - a$.*

Demonstração. Sejam $a = mq + r$, com $0 \leqslant r < m$ e $b = mq' + r'$, com $0 \leqslant r' < m$, as divisões euclidianas de a e b por m, respectivamente. Logo,

$$b - a = (q' - q) + (r' - r).$$

Portanto, $a \equiv b \bmod m$ se, e somente se, $r = r'$, o que, em vista da igualdade acima, é equivalente a dizer que $m \mid b - a$, já que $|r - r'| < m$. □

3.1 Algumas Propriedades

Proposição 6. *Seja $n \in \mathbb{N}$ e $n > 1$, para todos $a, b, c \in \mathbb{Z}$, tem-se:*

(1) (Reflexividade) $a \equiv a \bmod m$;

(2) (Simetria) Se $a \equiv b \bmod m$, então $b \equiv a \bmod m$;

(3) (Transitividade) Se $a \equiv b \bmod m$ e $b \equiv c \bmod m$, então $a \equiv c \bmod m$;

(4) (Compatibilidade com a soma e a diferença) Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $a + c \equiv b + d \bmod m$ e $a - c \equiv b - d \bmod m$;

Desta pode ser concluída uma propriedade em particular: se $a \equiv b \bmod m$, *então* $ka \equiv kb \bmod m$ para todo k inteiro*;*

*(5) (Compatibilidade com produto) Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $ac \equiv bd \bmod m$.*Em particular*, se $a \equiv b \bmod m$, então $a^n \equiv b^n \bmod m$ para todo n natural;*

(6) (Cancelamento) Se $(c, m) = 1$, então $ac \equiv bc \bmod m \Leftrightarrow a \equiv b \bmod m$

Demonstração. (1): Se $a \equiv a \bmod m$, pela proposição 5, concluímos que $m \mid a - a$, isto é, $m \mid 0$.

(2): Como $a \equiv b \bmod m$, segue-se que $m \mid b - a$, isto é, existe um k inteiro tal que $mk + (a - b) = 0$, multiplicando a última equação por (-1) temos, $m(-k) + (a - b) = 0$, isto é, $m \mid a - b$.

(3): Suponha que $a \equiv b \bmod m$ e $b \equiv c \bmod m$. Desde modo, $m \mid b - a$ e $m \mid c - b$, isto é, existem k e k' inteiros tais que $mk + (b - a) = 0$ e $mk' + c - b = 0$, segue-se que $m(k + k') + c - a = 0$, isto é, $m \mid c - a$.

(4): Suponha que $a \equiv b \bmod m$ e $c \equiv d \bmod m$. Logo, temos que $m \mid b - a$ e $m \mid d - c$. Observe que $m \mid (b - a) + (d - c)$ e portanto, $m \mid (b + d) - (a + c)$.

(5): Como $m \mid b - a$ e $m \mid d - c$ segue que $m \mid d(b - a)$ e $m \mid a(d - c)$. Desta forma pode-se concluir que $m \mid d(b - a) + a(d - c)$, ou seja, $m \mid db - ac$.

(6): Se $a \equiv b \bmod m$, segue-se imediatamente da propriedade 4 que $a + c \equiv b + c \bmod m$, pois $c \equiv c \bmod m$.

Reciprocamente, se $a + c \equiv b + c \bmod m$, então $m \mid b + c - (a + c)$, o que implica que $m \mid b - a$ e, consequentemente, $a \equiv b \bmod m$.

□

Algumas propriedades adicionais que serão utilizadas

Proposição 7. *Sejam $a, b \in Z$ e $m, n, m_1, ..., m_r$ inteiros maiores que 1. Tem-se:*

(1) *Se $a \equiv b \bmod m$ e $n \mid m$, então $a \equiv b \bmod n$;*

(2) *Se $a \equiv b \bmod m_i$, $\forall i = 1, 2, ..., r \Leftrightarrow a \equiv b \bmod [m_1, ..., m_r]$;onde $[m_1, ..., m_r] = mmc(m_1, ..., m_r)$*

(3) *Se $a \equiv b \bmod m$, então $(a, m) = (b, m)$;*

Demonstração. (1) Se $a \equiv b \bmod m$, então $m \mid b - a$. Como $n \mid m$, segue que $n \mid b - a$. Logo, $a \equiv b \bmod n$

(2) Se $a \equiv b \bmod m_i$, $i = 1, ..., r$, então $m_i \mid b - a$, para todo i. Sendo $b - a$ um múltiplo de cada m_i, segue-se que $[m_1, ..., m_r] \mid b - a$, o que prova que $a \equiv b \bmod [m_1, ..., m_r]$. A

recíproca decorre o item (1).

(3) Se $a \equiv b \bmod m$, então $m \mid b - a$ e, portanto, $b = a + tm$, sendo $t \in \mathbb{Z}$. Logo, pelo Lema 2, tem-se que

$$(a, m) = (a + tm, m) = (b, m)$$

□

3.2 Inverso Módulo m

Dizemos que um inteiro a é o inverso módulo m de outro inteiro b e vice-versa quando

$$ab \equiv 1 \bmod m.$$

O teorema seguinte estabelece a condição para que um inteiro qualquer k possua inverso módulo m.

Teorema 6. *Dados k e m inteiros, $m > 1$. O inteiro k possui inverso módulo m se, e somente se, k e m forem co-primos, ou seja, $(k, m) = 1$.*

Demonstração. ($\Rightarrow$) Se k e m forem co-primos então, $(k, m) = 1$ e, pela relação de Bézout, existem inteiros a e b tais que $ak + bm = 1 \Rightarrow ak \bmod m + bm \bmod m = 1 \Rightarrow ak \bmod m = 1$ (pois $bm \bmod m = 0$)$\Rightarrow ak \equiv 1 \bmod m \Rightarrow a$ é o inverso de $k \bmod m$.
($\Leftarrow$) Se a for o inverso de k módulo m, ou seja $ak \equiv 1 \bmod m$, então $m \mid 1 - ak$, isto é, existe um b inteiro tal que $1 - ak + mb = 0$, multiplicando essa última equação por (-1), temos, $ak - mb = 1$, ou ainda, $ak + m(-b) = 1$ e isso implica que $(k, m) = 1$ □

3.3 Função φ de Euler

Definição 5. *Se $n = 1$, então $\varphi(n) = 1$; se $n > 1$, então $\varphi(n)$ é o número de inteiros k tais que $1 \leqslant k < n$ e $(k, n) = 1$.*

Teorema 7. *Sejam r e s números inteiros positivos com $r > 1$ e $s > 1$ e $(r, s) = 1$. Então $\varphi(r.s) = \varphi(r).\varphi(s)$.*

Demonstração. A preposição é verdadeira se r ou s é igual a 1, pois, temos:

$$(1.s) = \varphi(s) = 1.\varphi(s) = \varphi(1).\varphi(s)$$
$$(r.1) = \varphi(r) = \varphi(r).1 = \varphi(r).\varphi(1)$$

Suponhamos, pois, $r > 1$ e $s > 1$. Neste caso os inteiros de 1 a rs podem ser dispostos em r colunas com s inteiros em cada uma delas, do seguinte modo:

$$\begin{array}{ccccccc} 1 & & 2 & ... & h & ... & r \\ r+1 & & r+2 & & r+h & & 2r \\ 2r+1 & & 2r+2 & & 2r+h & & 3r \\ \vdots & & \vdots & & \vdots & & \vdots \\ (s-1)r+1 & & (s-1)r+2 & & (s-1)r+h & & sr \end{array}$$

Por ser $(qr+h, r) = (h, r)$, os inteiros da h-ésima coluna são primos com r se e somente se h é primo com r. E como na primeira linha o número de inteiros que são primos com r é igual a $\varphi(r)$, segue-se que existem somente $\varphi(r)$ colunas formadas com inteiros que são todos primos com r. Por outro lado, em cada uma destas $\varphi(r)$ colunas existem $\varphi(s)$ inteiros que são primos com s, porque na progressão aritmética:

$$h, r+h, 2r+h, ..., (s-1)r+h$$

onde $(h, r) = 1$, o número de termos que são primos com s é igual a $\varphi(s)$. Assim sendo, o número total de inteiros que são primos com r e com s, isto é, que são primos com rs, é igual a $\varphi(r).\varphi(s)$, e isto significa que $\varphi(r.s) = \varphi(r).\varphi(s)$.

□

Teorema 8. *Se o inteiro $n > 1$, então $\varphi(n) = n$ - 1 se e somente se n é primo.*

Demonstração. Se $n > 1$ é primo, então cada um dos inteiros positivos menores que n é primo com n e, portanto, $\varphi(n) = n-1$. Se, por outro lado $\varphi(n) = n-1$, com $n > 1$, então n é primo, pois, se n fosse composto, teria pelo menos um divisor d tal que $1 < d < n$, de modo que pelo menos dois dos inteiros $1, 2, 3, ..., n$ não seriam primos com n, isto é, $\varphi(n) = n - 2$. Logo, n é primo. □

3.4 Pequeno Teorema de Fermat

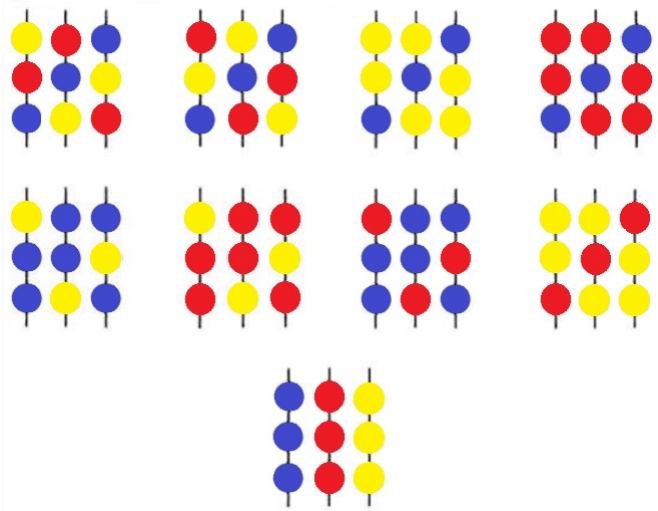
Teorema 9. *Seja p um número primo, então que p divide o número $a^p - a$, para todo número inteiro a.*

Demonstração. Suponhas que desejamos formar conrrentes com p pérolas coloridas e que possuímos, em mãos, pérolas suficientes que nos permitem o uso ilimitado de cada uma das n cores. Desse modo, pelo Princípio Fundamental da Contagem, o número de correntes que podemos formar é n^p, pois cada pérola pode ser escolhido de n maneiras e são p escolhas para cada corrente. A Figura 1 ilustra o caso em que $n = 3$ e $p = 3$.

Das n^p possibilidades, exatamente n correntes possuem pérolas de exatamente uma cor. Colocando estas à parte e, de maneira ilustrada da Figura 2, juntando as duas extremindades de cada uma das $n^p - n$ correntes formando $n^p - n$ pulseiras.

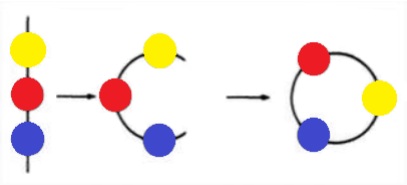
Nós podemos alterar qualquer corrente de pérolas, removendo um pérola da parte de cima e colocando-a na parte de baixo. Tal operação produz uma corrente diferente sem

Figura 1 – As vinte e sete correntes de três pérolas com três cores possíveis.



Fonte: Elaborada pelo autor.

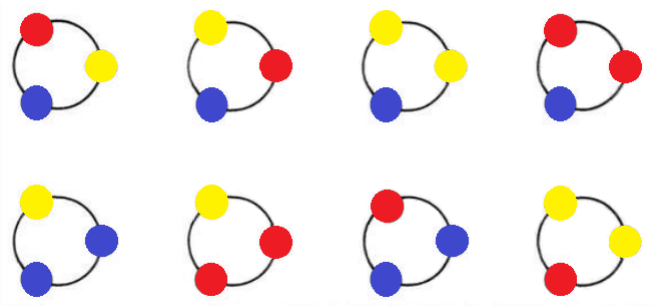
Figura 2 – A formação de uma pulseira a partir de uma corrente.



Fonte: Elaborada pelo autor.

alterar a pulseira resultante. Quando $n = 3$ e $p = 3$, as 24 correntes multicoloridas podem ser reunidas em 8 grupos de 3 correntes que podem ser obtidas, uma das outras, por uma ou mais repetições da alteração que descrevemos. Veja os oito primeiros grupos da Figura 1. Observamos que, para cada um destes oito diferentes grupos corresponde uma pulseira distinta (veja Figura 3).

Figura 3 – As oito pulseiras de três pérolas com três cores possíveis (pulseiras de uma cor excluídas).



Fonte: Elaborada pelo autor.

Agora, seja k o menor número de vezes que esta alteração pode ser repetida até que a

corrente principal seja reproduzida. Assim, temos $k > 1$, pois excluímos as correntes em que todas as pérolas são de uma mesma cor. Observe que após $2k$ alterações a pulseira original será reproduzida novamente e, de forma semelhante, após 3k, 4k, etc. Pelo algorítmo da divisão de Euclides existem h e r tais que $p = hk + r$, com $0 \leqslant r < k$.

Como uma corrente é produzida após a hk alterções e é também produzida após p alterações, serão necessárias r alterações, após a $hk^{\underline{a}}$ alteração para se obter a reprodução da coloração inicial. Como $r < k$ e k é menor número inteiro positivo de alterações necessárias para a obtenção de uma reprodução, então $r = 0$. Daí, $p = hk$, ou seja, $k \mid p$ e, portanto, $k = p$, já que $k > 1$ e p é um número primo. Consequentemente, as $n^p - n$ correntes podem ser agrupadas em grupos de p correntes cada, e é claro que cada grupo gera uma pulseira diferente.

Portanto, o número de pulseiras N multiplicado por p fornece o número de correntes que não são formadas de uma única cor, que é $n^p - n$. Logo $pN = n^p - n$, isto é, $p \mid n^p - n$. □

Corolário 1. *Se p é um número primo e se a é um número natural não divisível por p, então p divide $a^{p-1} - 1$.*

Demonstração. Como, pelo Pequeno Teorema de Fermat, $p \mid a(a^{p-1}-1)$ e como $(a, p) = 1$, segue-se, imediatamente, que p divide $a^{p-1} - 1$. □

3.5 Teorema Chinês dos Restos

Considere o sistema de congruência da forma:

$$X \equiv c_i \bmod m_i, i = 1, ..., r \tag{3.1}$$

Teorema 10. *(Teorema Chinês dos Restos). Sejam $m_1, ..., m_r$, inteiros postivos primos entre si dois a dois, isto é, $(m_i, m_j) = 1, \forall i \neq j$. Então o sistema de congruências*

$$\begin{cases} x \equiv a_1 \bmod m_1 \\ x \equiv a_2 \bmod m_2 \\ \quad\quad \vdots \\ x \equiv a_r \bmod m_r \end{cases}$$

tem solução inteira x onde $a_1, ..., a_r$ são inteiros dados e o conjunto de todas as soluções é $\{y \in \mathbb{Z} \mid y \equiv x \bmod m_1, ..., m_r\}$.

Demonstração. Seja $M = m_1...m_r$. Temos que $\frac{M}{m_j} \equiv 0 \bmod m_i, \forall i \neq j$ e $\left(\frac{M}{m_j}, m_j\right) = 1$, logo existe $x \in \mathbb{Z}$ tal que $\frac{M}{m_j}x_j \equiv 1 \bmod m_j$, pelo Teorema 6.
Considere $x = a_1\frac{M}{m_1}x_1 + a_2\frac{M}{m_2}x_2 + ... + a_r\frac{M}{m_r}x_r$. Temos que $x \equiv a_i\frac{M}{m_i}x_i \bmod m_i$, mas $\frac{M}{m_i}x_i \equiv 1 \bmod m_i \Rightarrow x \equiv a_i.1 = a_i \bmod m_i, \forall i \leqslant r$, isto é, x é solução do sistema. Suponha que exista um $y \in \mathbb{Z}$ tal que $y \equiv a_1 \bmod m_i, \forall i \leq r \Leftrightarrow y \equiv x \bmod m_i \forall i \leq r \Leftrightarrow m_i \mid y - x, \forall i \leq r \Leftrightarrow m_1...m_r \mid y - x \Leftrightarrow y \equiv x \bmod m_1...m_r$. □

3.6 Maneiras de Calcular Potências Módulo m

(1) Escrevendo o expoente na base 2.
Lembre-se que:

$$a^b \bmod m = (a \mod m)^b \mod m.$$

Onde: a notação $(a \mod m)^b$ representa o resto da divisão de $a^b \bmod m$ elevado a potência b.

Exemplo 1. *Calcule* $43^{11} \bmod 5$.

Solução

$43^{11} \bmod 5 = (43 \bmod 5)^{11} \bmod 5 = 3^{11} \bmod 5$

$11 = 1011_2 = 8 + 2 + 1 \Rightarrow 3^{11}\text{mod}5 = 3^{8+2+1}\text{mod}5 =$

$(3^8 \times 3^2 \times 3^1)\text{mod } 5 = (3^8 \bmod 5 \times 3^2 \bmod 5 \times 3^1 \bmod 5)\text{mod } 5$

$3^1\text{mod } 5 = 3\text{mod } 5 = 3$

$3^2\text{mod } 5 = 9\text{mod } 5 = 4$

$3^4\text{mod } 5 = 81\text{mod } 5 = 1$

$3^8\text{mod } 5 = (3^4)^2\text{mod } 5 = 1^2\text{mod } 5 = 1$

$43^{11}\text{mod } 5 = (1 \times 4 \times 3)\text{mod } 5 = 12\text{mod } 5 = 2$

Portanto, $43^{11}\text{mod } 5 = 2$.

(2) Usando o Pequeno Teorema de Fermat.

Exemplo 2. *Calcular o resto da divisão de* 7^{213} *por* 17.
Pelo Pequeno Teorema de Fermat, temos:

$$7^{16} \equiv 1 \bmod 17$$

Por outro lado $7^{213} = (7^{16})^{13} \times 7^5 \equiv 1 \times 7^5 \equiv 7^5 \bmod 17$
e como $7^2 = 49 \equiv 15 \equiv -2 \bmod 17$*, segue-se que*

$$7^5 \equiv (-2)^2 \times 7 \equiv 11 \bmod 17$$

Logo, $7^{213} = (7^{16})^{13} \times 7^5 \equiv 1 \times 7^5 \equiv 7^5 \equiv 11 \bmod 17$

(3) Usando Teorema Chinês dos restos.

Exemplo 3. *Calcular o resto da divisão de* 2^{693} *por* 1387.
Observe que $1387 = 19 \times 73$ *Pelo Pequeno Teorema de Fermat, temos:*

$$2^{693} \equiv 2^9 \equiv 18 \equiv -1 \bmod 19$$

$$2^{693} \equiv 2^{45} \equiv (2^9)^5 \equiv 1 \bmod 73$$

Isto nos dá o seguinte sistema de congruências

$$\begin{cases} x \equiv -1 \bmod 19 \\ x \equiv 1 \bmod 73 \end{cases}$$

Pelo Teorema do Resto Chinês, temos $M = m_1.m_2 = 19.73 = 1387$*,* $M_1 = \dfrac{M}{m_1} = m_2 = 73$*,* $M_2 = \dfrac{M}{m_2} = 19$*, temos que:*

$$y_1.73 \equiv 1 \bmod 19\text{, } \textit{que resulta em } y_1 = 6$$
$$e$$
$$y_2.19 \equiv 1 \bmod 73\text{, } \textit{que resulta em } y_2 = 50$$

A solução geral do sistema será da forma $x = M_1y_1a + M_2y_2b + Mt$*, ou seja,*

$$x = 73.6.(-1) + 19.50.1 + 1387t$$

$$x = 512 + 1387.t$$

Logo, o resto da divisão de 2^{693} *por* 1387 *é* 512.

4 Criptografia RSA

A criptografia estuda os métodos para codificar uma mensagem de modo que só seu destinatário legítimo consiga interpretá-la. Todo processo de codificação é composto de duas etapas básicas: a codificaçãoo da mensagem e a decodificação da mensagem. Decodificar é o que um destinatário legítimo do código faz para ler a mensagem.

A base teórica do processo de implantação da criptografia moderna é a aritmética modular, já estudada séculos antes por Euler, Gauss, Fermat entre outros.

A grande característica da internet é o seu caráter democrático. As informações fluem de maneira pública e o acesso a elas é aberto a todos. Surge então a necessidade, para manter a privacidade de certas informações, do uso da criptografia.

A criptografia RSA é um sistema de criptografia onde a chave de codificação é pública, permitindo então que qualquer pessoa codifique mensagens, e a chave de decodificação é privada. Este tipo de criptografia é extremamente adequado para, por exemplo, comércio eletrônico na Internet.

A impossibilidade de se quebrar o sistema de criptografia RSA ocorre em razão da não existência de algoritmos eficientes para o processo de divisão de inteiros. Atualmente são utilizados números com 150 algarismos, para os quais com a capacidade de computação atual o processo de fatoração levaria milhares de anos.

O métpdp RSA foi inventado em 1978 por R. L. Rivest, A. Shamir e L. Adleman. Eles trabalhavam no Massachussets Institute of Technology (M.I.T). As letras RSA correspondem às iniciais dos nomes inventores do código. Há vários outros códigos de chave pública, mas o RSA é, atualmente, o mais usado em aplicações comerciais.

Vamos precisar de dois número primos: p e q. Para codificar a mensagem basta utilizar $n = p.q$. A chave pública de codificação é o número n.

A chave de decodificação é constituída pelos primos e deve ser mantida em segredo pois a segurança do RSA depende disto. O fato de n ser conhecido para os casos em que n (150 algarismos) torna praticamente impossível se conhecer os primos p e q.

4.1 Etapas da criptografia RSA

Primeira etapa: pré-codificação

A primeira coisa que temos que fazer para utilizar o RSA é transformar a mensagem em uma sequência de números. Vamos utilizar o código ASCII para converter cada caracter da mensagem em seu respectivo valor numérico na tabela ASCII transformando o texto então em um número gigantesco. Este número é quebrado em blocos de números menores do que o valor da chave pública n.

Cada bloco pré-codificado será chamado de b.

Segunda etapa: codificação

- n (chave pública, $n = p.q$, p,q são números primos);
- $\varphi(n) = (p-1)(q-1)$;
- e(número inteiro e positivo) tal que $mdc(e, \varphi(n)) = 1$;
- chave de codificação par (n, e);

Agora com a mensagem dividida em blocos, codificaremos cada um dos blocos separadamente.

Vamos chamar de $C(b)$ cada bloco codificado.

$$C(b) = \text{resto da divisão de } b^e \text{ por } n.$$

Terceira etapa: decodificação

- o inverso de e em $\varphi(n)$ que denotaremos por d.

$$e \cdot d \equiv 1 \bmod \varphi(n)$$

- O par (n,d) é a chave de decodificação do sistema RSA.

Seja $C(b)$ o bloco codificado e $D(C(b))$ o processo de decodificação:

$$D(C(b)) = \text{resto da divisão de } C(b)^d \text{ por } n.$$

Exemplo: Codificar a palavra GIZ

Etapa 1: pré-codificação

Figura 4 – tabela ASCII

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35
0	1	2	3	4	5	6	7	8	9	espaço		
36	37	38	39	40	41	42	43	44	45	46		

Fonte: Elaborada pelo autor.

GIZ (16 18 35) que será representado por (161835)

Vamos adotar $p = 11$ e $q = 23$. Assim $n = 253$ (Chave Pública).

Quebrando em blocos de números menores do que n obtemos: 16 18 35

Etapa 2: codificação

Agora precisamos encontrar um inteiro positivo e tal que mdc$(e, \varphi(n))$=1.

Lembrando: $\varphi(n) = (p-1)(q-1)$, como adotamos p=11 e $q = 23$, temos $\varphi(n) = 10.22 = 220$.

Como 3 é primo e não divide 220, podemos adotar $e = 3$.

Chamamos o par (n,e) de chave de codificação. Para este caso a chave de codificação é (253,3).

A ideia é pegar todos os blocos, elevar a e (neste caso $e = 3$) e obter o resto da divisão por n (neste caso 253). Assim obtemos:

Calcular o resto da divisão de 16^3 por 253.

Observe que $253 = 11 \times 23$. Pelo Pequeno Teorema de Fermat, temos:

$$16^3 \equiv 5^3 \equiv 4 \bmod 11$$

$$16^3 \equiv 16 \times 16^2 \equiv 16 \times 3 \equiv 2 \bmod 23$$

Isto nos dá o seguinte sistema de congruências

$$\begin{cases} x \equiv 4 \bmod 11 \\ x \equiv 2 \bmod 23 \end{cases}$$

Pelo Teorema do Resto Chinês, temos $M = m_1.m_2 = 11.23 = 253$, $M_1 = \dfrac{M}{m_1} = m_2 = 23$, $M_2 = \dfrac{M}{m_2} = 11$, temos que:

$$y_1.23 \equiv 1 \bmod 11, \text{ que resulta em } y_1 = 1$$

e

$$y_2.11 \equiv 1 \bmod 23, \text{ que resulta em } y_2 = 21$$

A solução geral do sistema será da forma $x = M_1 y_1 a + M_2 y_2 b + Mt$, ou seja,

$$x = 23.1.4 + 11.21.2 + 253t$$

$$x = 554 + 253t$$

Lembrando que

$$554 \equiv 48 \bmod 253$$

Logo, o resto da divisão de 16^3 por 253 é 48.

Calcular o resto da divisão de 18^3 por 253.

Pelo Pequeno Teorema de Fermat, temos:

$$18^3 \equiv 18 \times 18^2 \equiv 18 \times 5 \equiv 2 \bmod 11$$

$$18^3 \equiv 18 \times 18^2 \equiv 18 \times 2 \equiv 13 \bmod 23$$

Isto nos dá o seguinte sistema de congruências

$$\begin{cases} x \equiv 2 \bmod 11 \\ x \equiv 13 \bmod 23 \end{cases}$$

Pelo Teorema do Resto Chinês, temos $M = m_1.m_2 = 11.23 = 253$, $M_1 = \dfrac{M}{m_1} = m_2 = 23$, $M_2 = \dfrac{M}{m_2} = 11$, temos que:

$$y_1.23 \equiv 1 \bmod 11, \text{ que resulta em } y_1 = 1$$

e

$$y_2.11 \equiv 1 \bmod 23, \text{ que resulta em } y_2 = 21$$

A solução geral do sistema será da forma $x = M_1 y_1 a + M_2 y_2 b + Mt$, ou seja,

$$x = 23.1.2 + 11.21.13 + 253t$$

$$x = 3049 + 253t$$

Lembrando que

$$3049 \equiv 13 \bmod 253$$

Logo, o resto da divisão de 18^3 por 253 é 13.

Calcular o resto da divisão de 35^3 por 253.
Pelo Pequeno Teorema de Fermat, temos:

$$35^3 \equiv 2^3 \equiv 8 \bmod 11$$

$$35^3 \equiv 12^3 \equiv 3 \bmod 23$$

Isto nos dá o seguinte sistema de congruências

$$\begin{cases} x \equiv 8 \bmod 11 \\ x \equiv 3 \bmod 23 \end{cases}$$

Pelo Teorema do Resto Chinês, temos $M = m_1.m_2 = 11.23 = 253$, $M_1 = \dfrac{M}{m_1} = m_2 = 23$, $M_2 = \dfrac{M}{m_2} = 11$, temos que:

$$y_1.23 \equiv 1 \bmod 11, \text{ que resulta em } y_1 = 1$$

e

$$y_2.11 \equiv 1 \bmod 23, \text{ que resulta em } y_2 = 21$$

A solução geral do sistema será da forma $x = M_1 y_1 a + M_2 y_2 b + Mt$, ou seja,

$$x = 23.1.8 + 11.21.3 + 253t$$

$$x = 877 + 253t$$

Lembrando que

$$877 \equiv 118 \bmod 253$$

Logo, o resto da divisão de 35^3 por 253 é 118.

Desta forma, a mensagem codificada é: **48 13 118**

Etapa 3: decodificação

Agora, nossa tarefa é encontrar o inverso multiplicativo de e em $\varphi(n)$ que chamaremos de d.

Para este caso, devemos encontrar o inverso multiplicativo de 3 em 220, isto é, o número d tal que a divisão do produto $3d$ por $\varphi(n)$ deixe resto 1 ($3d = 220q + 1$).

Resolvendo essa equação obtemos d = -73. Como o expoente não pode ser negativo, então $d = 220 - 73 = 147$.

Chamamos o par (253,147) de chave de decodificação.

Agora, a ideia é elevar cada *C(b)* ao expoente d (neste caso 147) e encontrar o resto da divisão desta potência por n (neste caso 253).

Pelo Pequeno Teorema de Fermat, temos:

$$48^{147} \equiv 4^2 \equiv 5 \bmod 11$$

$$48^{147} \equiv 2 \times 13^2 \equiv 16 \bmod 23$$

Isto nos dá o seguinte sistema de congruências

$$\begin{cases} x \equiv 7 \bmod 11 \\ x \equiv 0 \bmod 23 \end{cases}$$

Pelo Teorema do Resto Chinês, temos $M = m_1.m_2 = 11.23 = 253$, $M_1 = \dfrac{M}{m_1} = m_2 = 23$, $M_2 = \dfrac{M}{m_2} = 11$, temos que:

$$y_1.23 \equiv 1 \bmod 11, \text{ que resulta em } y_1 = 1$$

e

$$y_2.11 \equiv 1 \bmod 23, \text{ que resulta em } y_2 = 21$$

A solução geral do sistema será da forma $x = M_1 y_1 a + M_2 y_2 b + Mt$, ou seja,

$$x = 23.1.5 + 11.21.16 + 253t$$

$$x = 3811 + 253t$$

Lembrando que

$$3811 \equiv 16 \bmod 253$$

Logo, o resto da divisão de 48^{147} por 253 é 16.

Pelo Pequeno Teorema de Fermat, temos:

$$13^{147} \equiv 13^{7} \equiv 7 \bmod 11$$

$$13^{147} \equiv 13^{15} \equiv 18 \bmod 23$$

Isto nos dá o seguinte sistema de congruências

$$\begin{cases} x \equiv 7 \bmod 11 \\ x \equiv 18 \bmod 23 \end{cases}$$

Pelo Teorema do Resto Chinês, temos $M = m_1.m_2 = 11.23 = 253$, $M_1 = \dfrac{M}{m_1} = m_2 = 23$, $M_2 = \dfrac{M}{m_2} = 11$, temos que:

$$y_1.23 \equiv 1 \bmod 11, \text{ que resulta em } y_1 = 1$$

e

$$y_2.11 \equiv 1 \bmod 23, \text{ que resulta em } y_2 = 21$$

A solução geral do sistema será da forma $x = M_1 y_1 a + M_2 y_2 b + Mt$, ou seja,

$$x = 23.1.7 + 11.21.18 + 253t$$

$$x = 4319 + 253t$$

Lembrando que

$$4319 \equiv 18 \bmod 253$$

Logo, o resto da divisão de 13^{147} por 253 é 18.

Pelo Pequeno Teorema de Fermat, temos:

$$118^{147} \equiv 118^{7} \equiv 2 \bmod 11$$

$$118^{147} \equiv 118^{15} \equiv 12 \bmod 23$$

Isto nos dá o seguinte sistema de congruências

$$\begin{cases} x \equiv 2 \bmod 11 \\ x \equiv 12 \bmod 23 \end{cases}$$

Pelo Teorema do Resto Chinês, temos $M = m_1.m_2 = 11.23 = 253$, $M_1 = \frac{M}{m_1} = m_2 = 23$, $M_2 = \frac{M}{m_2} = 11$, temos que:

$$y_1.23 \equiv 1 \bmod 11, \text{ que resulta em } y_1 = 1$$
$$\text{e}$$
$$y_2.11 \equiv 1 \bmod 23, \text{ que resulta em } y_2 = 21$$

A solução geral do sistema será da forma $x = M_1 y_1 a + M_2 y_2 b + Mt$, ou seja,

$$x = 23.1.2 + 11.21.12 + 253t$$

$$x = 2818 + 253t$$

Lembrando que

$$2818 \equiv 35 \bmod 253$$

Logo, o resto da divisão de 118^{147} por 253 é 35.

4.2 Por que funciona?

Relembrando:
Pré-codificação: 16-18-35 cada bloco desse conjunto foi chamado de b.
Codificação: 48-13-118 cada bloco desse conjunto foi chamado de $C(b)$ (resto da divisão de b^e por n.
Decodificação: 16-18-35 cada bloco desse conjunto foi chamada de $D(C(b))$ (resto da divisão $C(b)^d$ por n.
Quero provar que $D(C(b)) = b$
Sabemos que:

$$(C(b))^d \equiv D(C(b)) \bmod n \ (1)$$
$$\text{e}$$
$$b^e \equiv C(b) \bmod n \ (2)$$

Substituindo (2) em (1), temos:
$(b^e)^d \equiv D(C(b)) \bmod n$
Porém, d é o inverso de e módulo $\varphi(n)$, ou seja, $ed \equiv 1 \bmod \varphi(n)$ que é igual a:

$$ed = 1 + k\varphi(n) \text{ para algum k inteiro}$$
$$ed = 1 + k(p-1)(q-1)$$
$$b^{ed} = b^{1+k(p-1)(q-1)} = b.b^{k(p-1)(q-1)}$$

Lembrando que o objetivo e provar que $(b^e)^d \equiv b \bmod p$. Observemos dois casos:
Caso 1: mdc(b,p)$\neq 1$
Daí, $b = \lambda p \Rightarrow b \equiv 0 \bmod p \Rightarrow (b^e)^d \equiv b \bmod p$.
Logo, $(b^e)^d \equiv b \bmod p$.
Caso 2: mdc(b,p) $= 1$

$$ed = 1 + k\varphi(n) \text{ para algum k inteiro.}$$
$$ed = 1 + k(p-1)(q-1)$$
$$b^{ed} = b^{1+k(p-1)(q-1)} = b.b^{(p-1)k(q-1)}$$

Como mdc(b,p) $= 1$, pelo teorema de Fermat, $b^{(p-1)} \equiv 1 \; mod \, p$.
Assim, $b^{ed} \equiv b.1^{k(q-1)} \bmod p$
Logo,$(b^e)^d \equiv b \bmod p$.
De forma análoga, prova-se que $(b^e)^d \equiv b \bmod q$.
Temos então o sistema:

$$\begin{cases} b^{ed} \equiv b \bmod p \\ b^{ed} \equiv b \bmod q \end{cases}$$

Segue que:
$b^{ed} = b + \lambda p \Rightarrow b^{ed} - b = \lambda p$, para algum λ inteiro
e
$b^{ed} = b + \mu q \Rightarrow b^{ed} - b = \mu q$, para algum μ inteiro
Como mdc(p,q) $= 1$, temos $b^{ed} - b = \rho pq \Rightarrow b^{ed} \equiv b$, mod pq, para algum ρ inteiro
e consequentemente,
$b^{ed} \equiv b \bmod n$, já que $n = pq$.
Fica provado que:
$b^{ed} \equiv (b^e)^d \equiv b \equiv D(C(b)) \bmod n$.
Observe que $0 \leq D(C(b)) < n$, $1 \leq b < n$ e $b \equiv D(C(b)) \bmod n$.
Logo, concluímos que $D(C(b)) = b$.

5 O uso de games na sala de aula: uma visão geral

O vídeo animação intitulado de *Vídeo games and learning*[1]
Como afirma MATTAR (2010):

> "aprendizado tangencial, não é o que você aprende ao ser ensinado, mas o que aprende por ser exposto a coisas, em um contexto no qual você está envolvido."

Ainda sobre o vídeo, fica clara a ideia de que o aprendizado com jogos será facilitado e permitido. Em outras palavras, se não somos forçados a aprender e estando envolvido com o game, a chance de aprendizado é grande.
Como afirmar MATTAR (2010):

> "a ideia de aprendizado tangencial considera que um a parte da sua audiência se autoeducará, caso você facilite sua introdução a assuntos que possam lhe interessar, em um contexto que ela considere excitante e envolvente."

Vale a pena ressaltar uma outra diferença entre os games e o aprendizado tradicional: a forma de lidar com o erro. Como cita MATTAR (2010):

> "O papel do fracasso em videogames é muito diferente do que na escola, que não integra a colaboração e a competição como nos games. Nos games, o custo do fracasso é normalmente diminuído - quando os jogadores fracassam, eles podem recomeçar de seu último jogo salvo. Além disso, o fracasso ao matar um mestre, por exemplo, é em geral encarado com uma maneira de aprender e, numa próxima oportunidade, tentar vencer."

Gwen Solomon e Lynne Schrum são escritores do livro *Web 2.0: new tolls, new schools*[2]. No capítulo 2 os autores escrevem sobre nossos alunos e de sua relação com a

[1] PORTNOW, James;FLOYD, Daniel. *vídeo games learning.* Edge, set.2008. Disponível em:<http://https://www.youtube.com/watch?v=rN0qRKjfX3s>. O vídeo é baseado no post de Portnow, "The power of tangential learning", 10 set.2008, disponível em:<http://www.edge-online.com/blogs/the-power-tangencial-learning?page=0%2C0>.

[2] SOLOMON, Gwen; SCHRUM, Lynne. *Web 2.0> new tools, new schools.* Washington: ISTE, 2007.

tecnologia, de como lidam com a informação e o que esperam da escola.
Deixar os alunos escolherem seus métodos de apresentação, aonde querrem ir para achar a informação, com que estilo desejam aprender, salas personalizadas (em que os alunos possam encontrar e utilizar as ferramentas que desejam) e professores que possam oferecer a cada aluno aquilo de que ele precisa para ter sucesso são algumas sugestões dadas pelos autores para aproveitar as características dos nossos novos alunos.

5.1 RPG Maker : uma ferramenta para o ensino da matemática

RPG denomina-se também *Role Playing Game* que significa "jogo de representação"ou "jogo do faz-de-conta", modalidade de jogo que se utiliza da representatividade como fator determinante.

O RPG *Maker* é um software que viabiliza a construção de RPGs eletrônicos, criado pela empresa ASCII e, atualmente desenvolvida pela Enterbrain. No editor você pode criar mapas, programar acontecimentos no jogo através de eventos pré programados. Todas as versões do programa incluem o RTP, um pacote de gráficos e sons comuns entre todos que usam o RPG Maker (o RPG Maker não irá rodar a não ser que você instale antes o seu respectivo RTP) prontos para serem utilizados nos jogos. A versão em inglês do RPG *Maker MV* está disponível em https://rpg-maker-mv.jaleco.com.

O RPG *Maker MV* é um software de fácil programação. Não requer domínio de uma linguagem específica. Basta ter noção de como trabalhar com condições (se, então) e variáveis. Assistindo a alguns videos do *You Tube* você consegue aprender tranquilamente.

ELEMENTOS BÁSICOS NA CONSTRUÇÃO DE UM JOGO USANDO RPG Maker	
Temas e Objetivos	O tema de um jogo é o assunto abordado pela história (ex.: uma guerra, uma fuga, um desastre, ...) e o objetivo é que se desejar alcançar após percorrer a aventura. No caso educacional pode ser o aprendizado, a revisão, a introdução de um determinado conteúdo, entre outros).
Conteúdo a ser trabalhado	É um recorte de determinado conteúdo para cada membro do jogo (protagonista, antagonista, coadjuvantes, aliados, informantes e figurantes).
Descrição de Ambientes	É a construção dos cenários que estão inseridos na aventura (casas, castelos, florestas, ilhas, etc...).
Chamado a Aventura	É algo inusitado que acontece para que as protagonistas se sintam convidadas a sair da rotina e ir se aventurar.
Enredo	É o desenvolvimento da história em si, a sequência de acontecimentos (início, meio e fim do jogo), onde ocorrem as ações, as situações desafiantes, as informações, entre outras ações.
Meta-enredo	É como se chamam as ações em paralelo, ou seja, as alternativas, decisões das personagens no contexto da história.
Distribuição de Pistas	É o que o criador faz quando seleciona os lugares onde são reveladas as pistas, que indicam ara onde a personagem dever seguir, o que fazer e os próximos acontecimentos.
Desafios	São situações geradas durante a história que fazem a personagem pensar, refletir, conjecturar, objetivando prosseguir no jogo.
Recompensa	É a finalização do jogo, de forma que haja a possibilidade de encontrar, resolver, desvendar, alcançar o que havia sido o chamado do jogo.

5.2 Cripto: o jogo

Jogo desenvolvido no RPG *Maker MV* pela professora Karina Marchetti Bonno Escobar para estimular o aprendizado da Criptografia RSA pelos alunos do ensino médio.

Tela de início do jogo

A Figura 1 mostra a tela inicial do jogo onde permite o jogador iniciar um novo jogo ou carregar um jogo que ele estava jogando.

A tela de introdução é formada por um fundo, disponível na plataforma do RPG

Figura 5 – Tela inicial do jogo.

Fonte: Elaborada pelo autor.

Maker. Nesta primeira etapa ocorre o carregamento das funções do jogo, entre elas o histórico, observado na Figura 6, que controla a vida do personagem, bem como troca de equipamentos e ataque dos inimigos. O nome escolhido para o personagem foi Haroldo, A qualquer momento do jogo o aluno pode acessar seu histórico e saber que tipo de itens ou equipamentos ele possui. Para isto basta pressionar a tecla "Esc" do computador, nesta tela o aluno tem o poder de salvar o jogo, para isso basta selecionar a opção salvar e continuar jogando do ponto em que parou em outro momento. Todas as funcionalidades utilizadas no jogo são defendidas por vários autores que falam sobre RPG no ensino, tais como MORATORI, 2003 e SILVA, 2009.

A missão do jogo

No segundo cenário ocorre, logo em seguida a entrada nesta fase, Haroldo, seguido por Patrícia, são teletransportados para um mundo medieval. É feita uma pequena introdução, dizendo que para que os dois personagens voltem ao seu mundo será necessário descobrir a senha do portal, que está critptografada pelo método RSA, e que os moradores darão dicas para a decodificação da senha(fornecimento dos blocos de codificação, chave pública e a chave privada). Foram utilizadas figuras da própria plataforma para montar o cenário, bem como figuras de uso irrestrito capturadas da internet, conforme observado na Figura 7.

Caminhando pela vila

Figura 6 – Histórico do personagem.

Fonte: Elaborada pelo autor.

Figura 7 – Apresentação do jogo.

Fonte: Elaborada pelo autor.

Com o objetivo de obter as dicas para decodificar a senha do portal, Haroldo e Patrícia, irão percorrer as casas dos moradores da vila, em troca, eles deverão fazer algumas tarefas, por exemplo: enfrentar um batalha para matar um rato, capturar cristais entre outros.

Depois de cumpridas todas as tarefas dadas pelos moradores e com os blocos de decodificação, chaves públicas e a chave privada é hora do jogador fazer os cálculos para descobrir a senha do portal.

As telas seguintes mostram uma tentativa de senha equivocada e uma tentativa de senha correta. Se o jogador errar a senha três vezes o jogo acaba. Se acertar, Haroldo e Patrícia voltam para o seu mundo.

Figura 8 – Apresentação do jogo.

Fonte: Elaborada pelo autor.

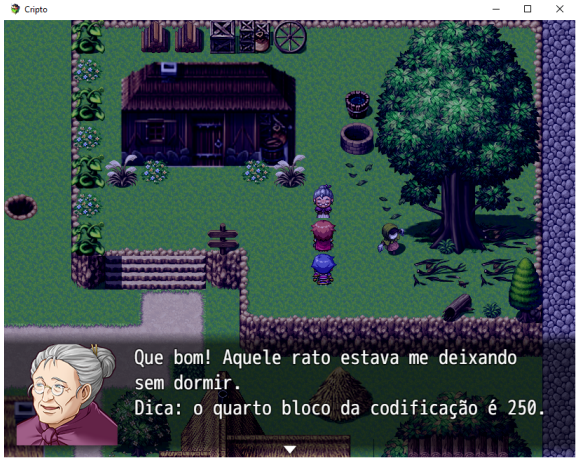
Figura 9 – Tarefa dada pela moradora da vila.

Fonte: Elaborada pelo autor.

Figura 10 – Batalha para matar o rato

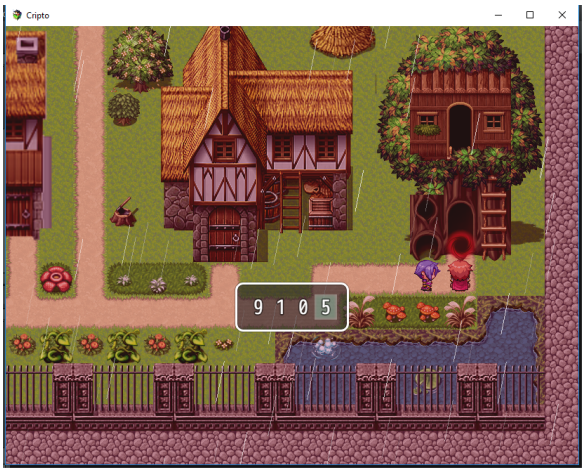
Fonte: Elaborada pelo autor.

Figura 11 – Dica dada após a morte do rato.



Fonte: Elaborada pelo autor.

Figura 12 – Senha errada.



Fonte: Elaborada pelo autor.

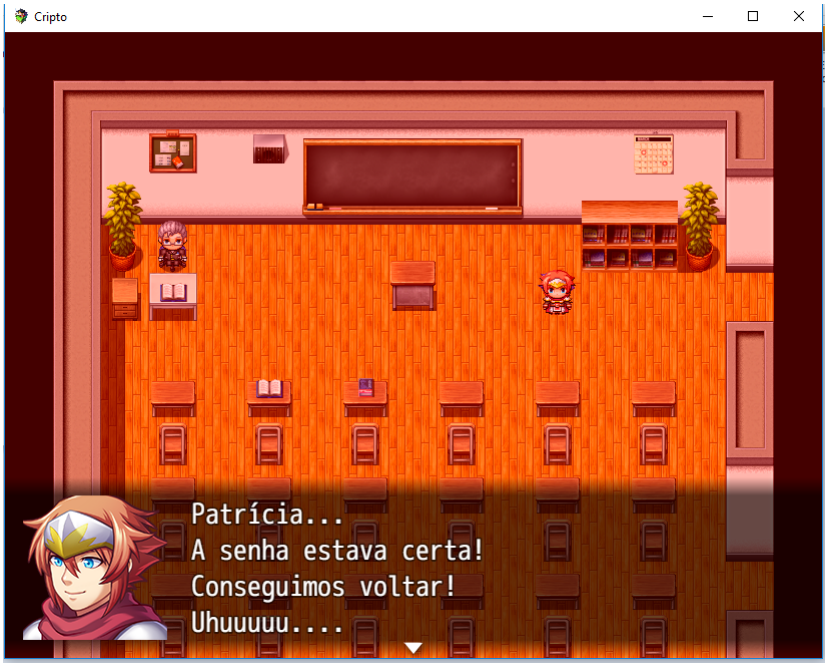
Figura 13 – Mensagem de senha errada.

Fonte: Elaborada pelo autor.

Figura 14 – Senha correta.

Fonte: Elaborada pelo autor.

Figura 15 – Mensagem de senha correta.



Fonte: Elaborada pelo autor.

6 Considerações finais

Será que pode existir algum jeito de fatorar números primos enormes, com certa de 150 algarismos? Se a resposta for sim, a Criptografia RSA está com os seus dias contados, já que o segredo dessa criptografia é trabalhar com um número n que representa o produto de números primos grandes. Há algum anos físicos observaram que é possível usar propriedades quânticas da matéria na construção de computadores que teriam várias características diferenes dos atuais, os chamados computadores quânticos. Veja o que diz ROUSSEAU (2015) sobre computadores quânticos:

> "Computadores quânticos não são ainda uma séria ameaça para o sistema de criptografia RSA. No momento, computadores quânticos do mundo real são capazes de fatorar apenas inteiros muito pequenos: em 2002, o número 15 foi fatorado com a ajuda de um computador quântico de sete qubits por Isaac Chuang e seu time de pesquisadores."

O jogo cripto foi desenvolvido pensando no aluno de ensino médio que convive diretamente com a tecnologia e faz dos jogos eletrônicos parte de sua vida. Daí a ideia de aliar a tecnologia como atividades lúdica para o ensino e aprendizagem da criptografia RSA. O RPG *Maker* foi o escolhido por possuir plataformas que possibilitam criar o cenário, o enredo da história, colocar personagens, batalhas e desafios de acordo com sua ideia e orientação do professor. Para criar um jogo é necessário ter uma noção de programação, lembrando que o ensino da programação é uma das competências específicas de matmática e suas tecnologias para o ensino médio da BNCC (Base Nacional Comum Curricular)

> "Compreender e utilizar, com flexibilidade e precisão, diferentes registros de representação matemáticos (algébrico, geométrico, estatístico, computacional etc.), na busca de solução e comunicação de resultados de problemas."

Esse jogo pode ser utilizado em qualquer lugar desde que tenha um computador e o programa instalado na máquina. O jogo motiva a discurssão entre os alunos sobre a resolução de estratégias, construção da história e claro, sobre o assunto abordado: Criptografia RSA. Sugere-se que o jogo seja aplicado aos alunos de ensino médio e alunos do cuso de licenciatura em matemática com o objetivo de mostrar que jogos podem servir como ferramenta de ensino e aprendrizagem.

Referências

[1] ABT, Clark. *Serious games*. Lanham: University Press of America, 1987.

[2] MARTINEZ, F. E. Brochero, MOREIRA, C. G. , SALDANHA, N. C., TENGAN E. *Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro*, 2010,Projeto Euclides, IMPA.

[3] OLIVEIRA, José Plinio. *Introdução à Teoria dos Números*,1998, Matemática Universitária.

[4] FONSECA, Rubens V., *Teoria dos Números*, 2011, Universidade do Estado do Pará.

[5] ANDREWS, G. E. *Number Theory*, 1994, DOVER.

[6] COUTINHO, S.C *Números inteiros e Criptografia RSA*, 2014, IMPA.

[7] MATTAR, João. *Games em educação: como os nativos digitais aprendem*, 2010, Pearson Prentice Hall.

[8] MORATORI Patrick Barbosa., *Por Que Utilizar Jogos Educativos no Processo de Ensino Aprendizagem?*, UFRJ. Rio de Janeiro, 2003. Disponível em http://www.nce.ufrj.br/ginape/publicacoes/trabalhos/PatrickMaterial/TrabfinalPatrick2003.pdf. Acesso em 10 de janeiro de 2019.

[9] SILVA, M. V.. O jogo de papéis (RPG) como tecnologia educacional e o processo de aprendizagem no ensino médio. Curitiba/PR, 2009.

[10] ALENCAR FILHO.E., *Teoria Elementar dos Números*, Editora Nobel, São Paulo, 1985.

[11] ROUSSEAU, Christiane, SAINT-AUBIN, Yvan, *Matemática e Atualidade*, 2015, Coleção PROFMAT.