# 19 Reunião 19: 02/JUL/2021


Figure 1: Mafalda por Quino

## 19.1 Reuniões passadas

Nas reunião passada conversamos bastante sobre como encontrar o mdc de dois inteiros, em particular, discutimos o

- Teorema (*pequeno*) de Euler
- Teorema *pequeno* de Fermat
- Aritmética modular
- Equações diofatinas
- Algoritmo de Euclides e
- Algoritmo de Euclides estendido
- Divisibilidade

Hoje traremos todas essas ferramentas para nos ajudar e talvez mais algumas.

## 19.2 Hoje

> Às vezes, são as pessoas que ninguém pode imaginar
> que fazem as coisas que ninguém pode imaginar.
>
> Alan Turing

Hoje utilizaremos tudo que estivemos treinando nas *últimas várias* reuniões para entendermos o sistema criptográfico de chave pública RSA.

A sigla RSA é devida aos sobrenomes de Ronald Linn Rivest, Adi Shamir e Leonard Adleman, que publicaram o algoritmo em 1977

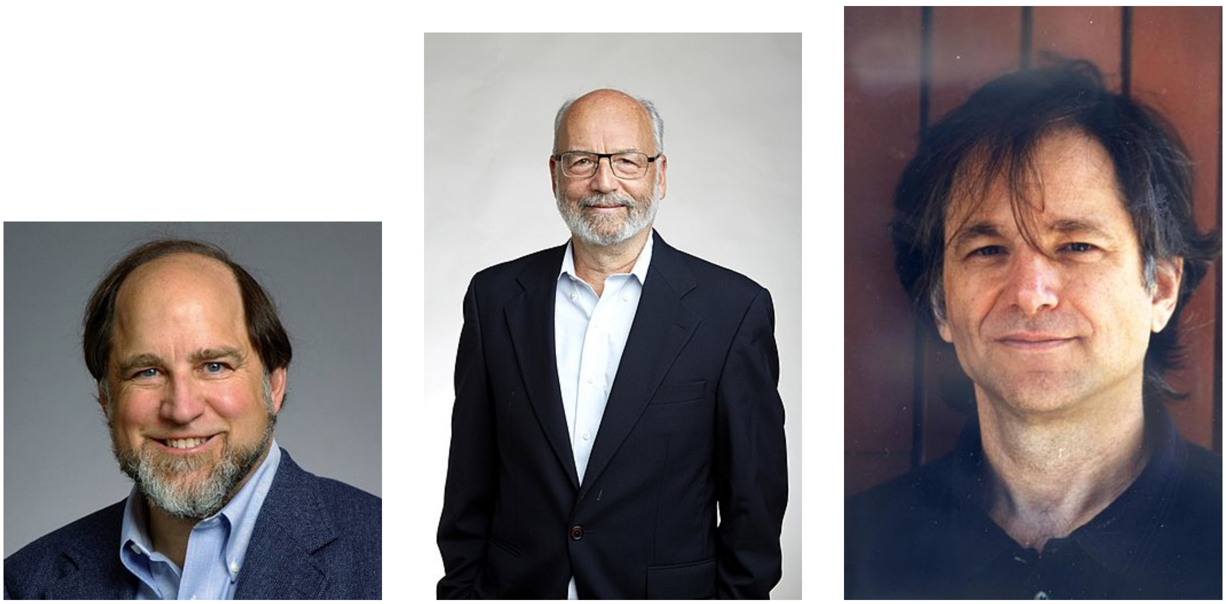

Figure 2: Ron Rivest, Adi Shamir e Leonad Adleman.(Fonte: Wikepidia)

O sistema se apoia em ideias atribuídas a Alan Turing.

Começamos com um verdadeiro catálogo das ferramentas que utilizaremos. Estas ferramentas são um resumão do que o Sinai apresentou nas últimas reuniões e que vamos precisar para grudar os pedaços do RSA. *Pule esse resumo e volte para ler os pontos você não lembrar e forem necessários quando forem necessários.* Em seguida está a descrição do sistema e a demonstração da sua correção.

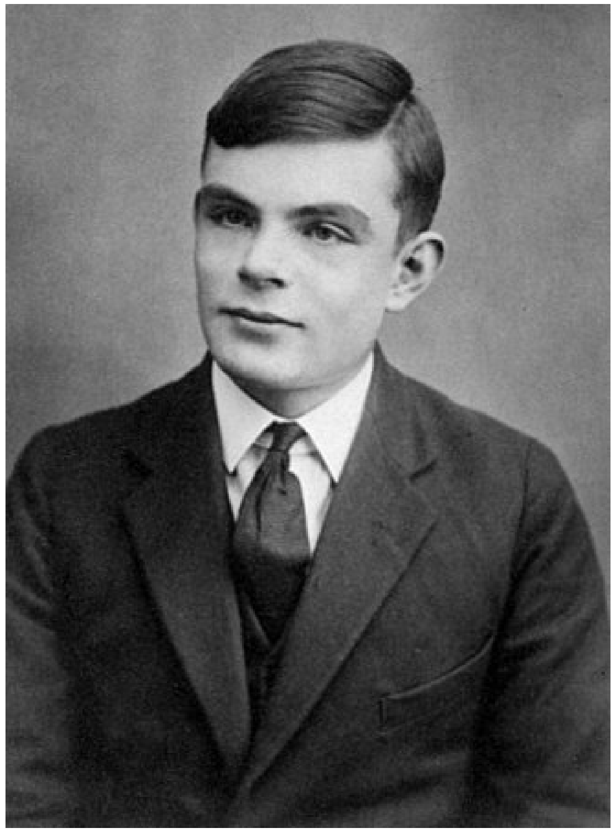

Figure 3: Alan Turing (1912-1954). (Fonte: Wikipedia)

## 19.3 Reuniões passadas: versão estendida

Hmm, em tudo que faremos $n$ será um inteiro positivo.

### Euclides e o mdc

Um **divisor comum** de $a$ e $b$ é um número que divide ambos. O **máximo divisor comum** de $a$ e $b$, denotado por $\mathrm{mdc}(a, b)$, é o maior inteiro positivo que é divisor comum de $a$ e $b$.

Para calcular o $\mathrm{mdc}(a, b)$ o algoritmo de Euclides se apoia na recorrência:

$$\mathrm{mdc}(a,b) = \begin{cases} a & \text{se } b = 0 \\ \mathrm{mdc}(b, a\%b) & \text{para } b > 0. \end{cases}$$

**Teorema 1** (Algoritmo de Euclides estendido)**.** *Sejam $a$ e $b$ inteiros, $a > b \geq 0$. Existem inteiros $r$ e $s$ tais que*

$$\mathrm{mdc}(a, b) = r \times a + s \times b.$$

Uma aplicação do algoritmo de Euclides estendido é encontrar soluções inteiras de sistemas lineares da forma $ax + by = c$, onde $a, b$ e $c$ são valores em $\mathbb{N}$ dados.

## Equações diofantinas

Essas equações são chamadas **diofantinas**.

**Teorema 2** (Equações diofantinas)**.** *Sejam $a, b$ e $c$ números inteiros tais que $a$ e $b$ não são ambos nulos. Existem inteiros $x$ e $y$ tais que $ax + by = c$ se e somente se* $\mathrm{mdc}(a, b) \mid c$.

**Teorema 3** (Soluções de equações diofantina)**.** *Sejam $a, b$ e $c$ números inteiros tais que $a$ e $b$ não são ambos nulos. Se $x$ e $y$ são solução inteira de $ax + by = c$, então, para todo $k$ em $\mathbb{Z}$*

$$x + \frac{b}{\mathrm{mdc}(a, b)}k, \quad y - \frac{a}{\mathrm{mdc}(a, b)}k$$

*é uma solução. Além disso, todas as soluções inteiras são desta forma.*

## Aritmética modular

Dizemos que $a$ é congruente a $b$ módulo $n$ se $n \mid (a - b)$, em símbolos

$$a \equiv b \mod n.$$

**Lema 4** (módulo e resto)**.** $a \equiv b \mod n \iff a\%n = b\%n.$

Por exemplo, $29 \equiv 15 \mod 7$ pois $29\%7 = 1 = 15\%7$.

O lemma a seguir mostra a razão de $\equiv$ ter comportamento similar com igualdade. Esse fenômeno recebe o nome técnico de relação de equivalência.

**Lema 5** (Equivalência entre $\equiv$ e $=$)**.**

$$\begin{aligned} a \equiv a &\mod n \quad \textit{(reflexividade)} \\ a \equiv b \iff b \equiv a &\mod n \quad \textit{(simetria)} \\ (a \equiv b \wedge b \equiv c) \implies a \equiv c &\mod n \quad \textit{(transitividade)} \end{aligned}$$

Logo, $a \equiv a\%n \mod n$. Isto faz a ponte entre $\equiv$ e os nossos programas com seus restos operadores $\%$ de resto de divisão.

**Lema 6** (Aritmética do mod)**.** *Se* $a \equiv b \mod n$ *e* $c \equiv d \mod n$*, então:*

*(a)* $a + b \equiv c + d \mod n$ *e*

*(b)* $a \times b \equiv c + d \mod n$*.*

Por exemplo, $64 \equiv 4 \mod 5$ e $27 \equiv 2 \mod 5$, portanto

- $64 + 27 \equiv 4 + 2 \equiv 1 \mod 5$, de fato $(64 + 27)\%5 = 91\%5 = 1$
- $64 \times 27 \equiv 4 \times 2 \equiv 8 \equiv 3 \mod 5$, mais uma vez, $(64 \times 27)\% = 1728\%5 = 3$

## Inversos

O inverso (multiplicativo) de um número $x \mod n$ é um número $x^{-1} \in \{0, 1, \ldots, n-1\}$ tal que

$$x \times x^{-1} = 1 \mod n.$$

Para $n = 15$ temos que 8 é o inverso multiplicativo de 2 pois

$$8 \times 2 \equiv 16 \equiv 1 \mod 15.$$

Já, para $n = 15$, 3 não possui inverso múltiplicativo

$$\begin{aligned}
3 \times 0 = 0 &\mod 15 \\
3 \times 1 = 3 &\mod 15 \\
3 \times 2 = 6 &\mod 15 \\
3 \times 3 = 9 &\mod 15 \\
3 \times 4 = 12 &\mod 15 \\
3 \times 5 = 0 &\mod 15 \\
3 \times 6 = 3 &\mod 15 \\
3 \times 7 = 6 &\mod 15 \\
\vdots \quad &\quad \vdots
\end{aligned}$$

De fato, suponha por contradição que exista $x$ inverso multipicativo de $3 \mod 15$, ou seja, $3 \times x \equiv 1 \mod 15$. Nesse caso teríamos que

$$
\begin{aligned}
5 \times 1 \equiv 5 \times (3 \times x) &\mod 15 \text{ (pelo lema da aritmética do mod)} \\
(5 \times 3) \times x &\mod 15 \text{ (associatividade do mod)} \\
15 \times x &\mod 15 \\
0 \times x &\mod 15 \\
0 &\mod 15.
\end{aligned}
$$

Assim $5 \equiv 0 \mod 15$ o que é uma contradição pois 15 não divide $5 - 0 = 5$.

Dois inteiros $a$ e $b$ são **relativamente primos** ou **coprimos** se $a$ e $b$ não têm fatores primos comuns. Em outras palavras, $a$ e $b$ são coprimos se $\text{mdc}(a, b) = 1$.

**Lema 7** (do inverso)**.** *Se $k \in \{0, 1, \ldots, n-1\}$ e $n$ são coprimos, então $k$ tem um inverso $\mod n$.*

**Lema 8** (da unicidade do inverso)**.** *Se $a \in \{0, 1, \ldots, n-1\}$ e $b \in \{0, 1, \ldots, n-1\}$ de são inversos de $k \mod n$, então $a = b$.*

*Prova.*

$$
\begin{aligned}
a &\equiv a \times 1 \mod n \\
&\equiv a \times (b \times k) \mod n \\
&\equiv (a \times k) \times b \mod n \\
&\equiv 1 \times b \mod n \\
&\equiv b \mod n.
\end{aligned}
$$

□

**Cancelamento**

Para números reais é comum cancelamos valores para simplificar expressões. Por exemplo, se $t \neq 0$ escrevemos que $t \times a = t \times b \implies a = b$.

Para aritmética modular ($\equiv$) ou aritmética do resto de divisão (%), temos que ser mais cuidadosos pois não é verdade que

$$3 \times 10 = 3 \mod 15 \implies 10 = 5 \mod 15.$$

Um inteiro $k \in \{0, 1, \ldots, k\}$ é **cancelável** $\mod n$ se

$$k \times a \equiv k \times b \mod n,$$

para todos os inteiros $a$ e $b$.

Um situação em que podemos cacelar é a descrita a seguir

**Lema 9** (do cancelamento)**.** *Se* $k \in \{0, 1, \ldots, n-1\}$ *então são equivalentes:*

- $\mathrm{mdc}(k, n) = 1$,
- $k$ *tem um inverso* $\mod n$, *e*
- $k$ *é cancelável.*

$\square$

**Teorema de Euler**

Agora sim, chegou a cereja do bolo...

Para $n > 0$, que é nosso caso em toda a reunião de hoje, defimos $\phi(n)$ como sendo o número de inteiros em $\{0, 1, 2, \ldots, n-1\}$ coprimos com $n$.

Por exemplos, para $n = 12$ temos que entre 0 e 11 os inteiros coprimos com 12 são $1, 5, 7, 11$ e portanto $\phi(12) = 5$.

Na última reunião o Sinai provou o seguinte teorema.

**Teorema 10** (Teorema de Euler)**.** *Se $n$ e $k$ são coprimos então*

$$k^{\phi(n)} \equiv 1 \mod n.$$

□

Por exemplo, para $n = 12$ e $k = 5$ temos que

$$\begin{aligned} 5^{\phi(12)} &\equiv 5^2 \times 5^2 \mod 12 \\ &\equiv 1 \times 1 \mod 12 \text{ (pois, } 25 = 2 \times 12 + 1) \\ &\equiv 1 \mod 12. \end{aligned}$$

O Sinai ainda apresentou a seguinte consequência ilustre desse teorema

**Teorema 11** (Pequeno Teorema de Fermat)**.** *Se $p$ é primo e $k$ não é múltiplo de $p$, então*

$$k^{p-1} \equiv 1 \mod p.$$

□

Por exemplo, para $p = 7$ e $k = 6$ temos que

$$\begin{aligned} 6^{7-1} &\equiv 6^6 \mod 7 \\ &\equiv (6^2)^3 \mod 7 \\ &\equiv 36^3 \mod 7 \\ &\equiv 1^3 \mod 7 \text{ (pois } 36\%7 = 1) \\ &\equiv 1 \mod 7. \end{aligned} \tag{1}$$

A última peça do quebra-cabeças que utilizaremos é

**Lema 12.** *Se $p$ e $q$ são primos, $p \neq q$ então,*

$$\phi(p \times q) = (p-1) \times (q-1).$$

$\square$

Por exemplo, se $p$ é primo, então $1, 2, \ldots, p-1$ são coprimos com $p$.
Como $\phi(7) = 6$ e $\phi(3) = 2$, então $\phi(21) = \phi(7 \times 3) = \phi(7) \times \phi(3) = 12$.

## 19.4 Sistema criptográfico RSA

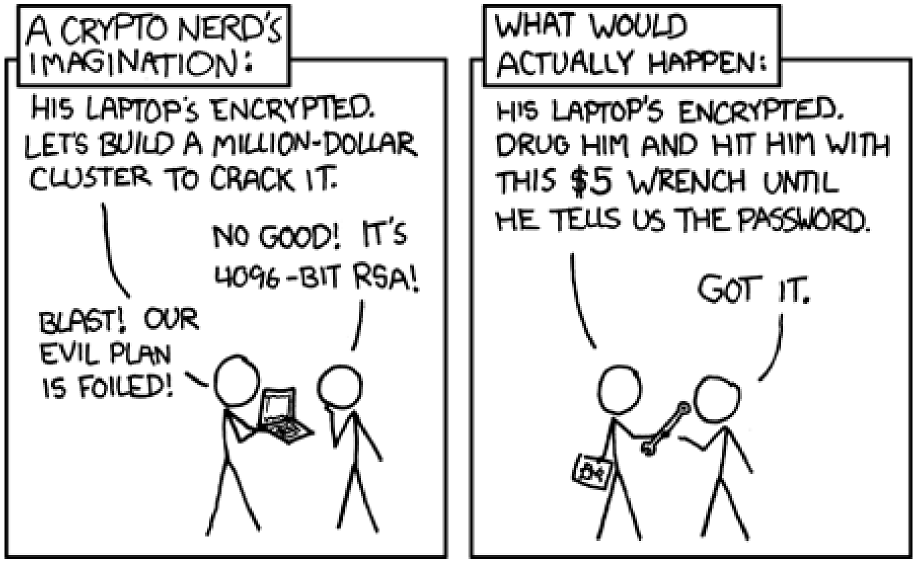


Figure 4: Fonte: xkcd

Passamos agora a descrever o sistema criptográfico de chave pública RSA. Depois da descrição veremos a prova de que ele funciona corretamente.

Digimos que Alice deseja receber mensagens criptografadas se suas/seus colegas de MAC0105. Suporemos que essas mensagens são números inteiros em $\{0, 1, \ldots, n-1\}$. Bem, isso não é problema pois sabemos que qualquer texto pode ser visto como um número inteiro, certo?

Para isso Alice criará uma **chave pública**, que será amplamente divulgada nas redes sociais, e uma **chave secreta** que será guardada a sete chaves.

Qualquer pessoa com a chave pública de Alice pode lhe enviar mensagens criptografada, qualquer pessoa mesmo. Pode até ser alguém que Alice não conhece, nunca viu e vai lhe enviar spam.

Os passos para que Alice **prepare o ambiente** para receber mensagens criptografadas é o seguinte.

## Preparação

**Passo 1.** ($p$ e $q$) Inicialmente, Alice **gera dois primos** $p$ e $q$. Se não quiser ter trabalho Alice pode ir no site Big Primes e pegar uns primos por lá. Na prática é bom que Alice escolha primos $p$ e $q$ relativamente grandes.

**Passo 2.** (valor de $n$) Em seguida Alice produz o inteiro $n = p \times q$.

**Passo 3.** ($e$ e a chave pública) No próximo passo, Alice seleciona um inteiro $e \in \{0, 1, 2, \ldots, n-1\}$ que é coprimo com $\phi(n) = (p-1) \times (q-1)$. Em outras palavras, $e$ deve ser um inteiro tal que

$$\mathrm{mdc}(e, (p-1) \times (q-1)) = 1.$$

Alice sabe como fazer isso pois cursou MAC0105.

Com isso Alice já tem a chave pública que será divulgada a todas e todos nas suas redes sociais. Essa **chave pública** é o par de inteiros $(e, n)$. Pronto, Alice já pode receber mensagens criptografadas.

**Passo 4.** ($d$ e a chave privada) Bem, depois de receber as mensagens é desejável que ela consiga ler e entender as mensagens. Agora é chegado o momento de Alice gerar sua chave privada que como o nome diz, deverá ser guardada a 7 chaves. Mais uma vez, Alice usa seus conhecimentos de MAC0105 para determinar $d \in \{0, 1, \ldots, n-1\}$ que seja inverso de $e \mod (p-1)(q-1)$, ou seja,

$$d \times e \equiv 1 \mod \phi(n).$$

## Codificação

Para transmitir uma mensagem $m \in \{0, 1, \ldots, n-1\}$ para Alice, devemos usar a chave pública que temos e calcular $\hat{m} \in \{0, 1, \ldots, n-1\}$ tal que

$$\hat{m} = m^e \,\%\, n \quad (\implies \hat{m} \equiv m^e \mod n).$$

A mensagem enviada a Alice será $\hat{m}$

## Decodicação

Para obter a mensagem original $m$, Alice usa a chave privada e calcula

$$m = \hat{m}^d \,\%\, n \quad (\implies m \equiv \hat{m}^d \mod n).$$

Bem, no momento não está nada claro que $m$ é de fato a mensagem original. Trataremos disto mais adiante. Antes é bom verificarmos se a *mágica está no ar*.

## 19.5 Análise do RSA

Figure 5: Fonte: portablepress.com

Vamos primeiro abrir a caixa de ferramentas e verificar que os passos da preparação fazem sentido e podem ser realizados.

**Passo 1.** Para obter os primos $p$ e $q$ podemos utilizar amostragem e testar primalidade rapidamente utilizando um algoritmo probabilístico como o de Miller e Rabin.

**Passo 3.** O inteiro $e$ pode ser qualquer primo maior que $\max(p, q)$, mas tipicamente é um primo pequeno. Isso deve fazer com que $d$ seja grande. Para verificar que $\text{mdc}(e, \phi(n)) = 1$ usamos o algoritmo de Euclides.

**Passo 4.** O invervo de $e \mod \phi(n)$ existe pois $\text{mdc}(e, \phi(n)) = 1$ e portanto $e$ e $\phi(n)$ são coprimos; veja o lema 7 do inverso.

Para determinar o inverso de $e$ aplicamos o algoritmo estendido de Euclides. Pelo teorema 1 existem inteiros $r$ e $s$ tais que

$$1 = r \times e + s \times \phi(n) \implies r \times e \equiv 1 \mod \phi(n).$$

Devido ao teorema 3 das soluções de equações diofantinas temos que

$$(r + k \times \phi(n)) \times e \equiv 1 \mod \phi(n)$$

para todo inteiro $k$. Portanto, podemos determinar $k$ tal que $d = r + k \times \phi(n)$ é um inteiro em $\{0, 1, \ldots, n\}$ e

$$d \times e \equiv 1 \mod \phi(n).$$

Vejamos agora que a decodificação recupera a mensagem original.

Pela codificação sabemos que

$$\hat{m} = m^e \,\%\, n \;\equiv\; m^e \mod n.$$

Pelo lema 6 da aritmética do mod, elevando a $d$ ambos os lados da equivalência acima obtemos que

$$\hat{m}^d \equiv m^{ed} \mod n. \tag{2}$$

Como $d$ é inverso de $e \mod \phi(n)$ e pela definição de congruência temos que existe um inteiro $s$ tal que

$$ed = 1 + s\phi(n) = 1 + s(p-1)(q-1).$$

Substituindo essa igualdade em (2) chegamos a

$$\hat{m}^d \equiv m^{ed} \equiv m^{1+s(p-1)(q-1)} \equiv m \times m^{s(p-1)(q-1)} \mod n.$$

Como $n = pq$, dessa equivalência e da definição de congruência concluímos que

$$\hat{m}^d \equiv m \times m^{s(p-1)(q-1)} \mod p, \text{ e que} \tag{3}$$
$$\hat{m}^d \equiv m \times m^{s(p-1)(q-1)} \mod q. \tag{4}$$

Se $m$ é multiplo de $p$ então $m \equiv 0 \mod p$ e $\hat{m}^d \equiv m \mod p$. Se $m$ não é múltiplo de $p$, então pelo Teorema Pequeno de Fermat temos que $m^{p-1} \equiv 1 \mod p$ e de (3) derivamos que

$$\hat{m}^d \equiv m \times m^{s(p-1)(q-1)} \equiv m \times (m^{p-1})^{s(q-1)} \equiv m \mod p$$

Assim, vale que

$$\hat{m}^d \equiv m \mod p. \tag{5}$$

De maneira semelhante, trocando $p$ por $q$, obtemos que

$$\hat{m}^d \equiv m \mod q. \tag{6}$$

Das equivalências (5) e (6) concluímos que

$$p \,|\, (\hat{m}^d - m) \quad \text{e } q \,|\, (\hat{m}^d - m)$$

e como $p$ e $q$ são primos

$$pq \,|\, (\hat{m}^d - m)$$

Como $n = pq$ então

$$\hat{m}^d \equiv m \mod n$$

e como $m$ é um inteiro entre 0 e $n-1$, então

$$m = \hat{m}^d \ \% \ n$$

que é justamente a operação feira pela decodificação.

## 19.6 Conversa de bar

Figure 6: Fonte: therichest.com