UNIVERSIDADE FEDERAL DO AMAZONAS
PRÓ-REITORIA DE PESQUISA E PÓS GRADUAÇÃO
DEPARTAMENTO DE APOIO A PESQUISA
PROGRAMA INSTITUCIONAL DE INICIAÇÃO CIENTÍFICA

RIGOR CIENTÍFICO EM TEORIA DOS NÚMEROS - APLICAÇÕES À CRIPTOGRAFIA RSA

Bolsista: Carla Almeida Rodrigues, CNPq

Manaus
2010

UNIVERSIDADE FEDERAL DO AMAZONAS
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
DEPARTAMENTO DE APOIO À PESQUISA
PROGRAMA INSTITUCIONAL DE INICIAÇÃO CIENTÍFICA

RELATÓRIO PARCIAL
PIB-E/0010/2009

Bolsista: Carla Almeida Rodrigues

Orientador: Prof. Dr. Nilomar Vieira de Oliveira

Manaus
2010

Sumário

Introdução **4**

1 Resultados **7**

1.1 Uma Introdução a Criptografia 7

1.2 Teoria dos Números Básica 10

2 Criptografia RSA **21**

2.1 Pré-codificação 21

2.2 Codificação 22

2.3 Decodificação 23

2.4 Por que o RSA é seguro? 25

Conclusão **26**

Cronograma **27**

Referências **28**

Introdução

Neste relatório encontram-se estudos feitos em Teoria dos Números, e alguns resultados em relação ao estudo principal do projeto, a Criptografia RSA.

A *Criptografia* é a arte ou a ciência de escrever em cifra ou em códigos mensagens, de forma a permitir que somente o destinatário a decifre e a compreenda, ou seja, a Criptografia transforma textos originais em textos cifrados e ilegíveis. De uma forma mais estrita, a criptografia obtém métodos matemáticos de codificar e decodificar uma mensagem de modo que apenas seu destinatário, através do uso de uma chave de decodificação, possa interpretá-la.

Na década de 70 surgiu um novo método criptográfico, o chamado algoritmo assimétrico. A idéia foi criada por Diffe e Hellman e, colocada em prática com o desenvolvimento do RSA criado por Ronald L. Rivest, Adi Shamir e Leonard Adleman, recebendo assim suas iniciais. O método tem base teórica na álgebra abstrata e na teoria dos números. Devido ao apelo matemático deste método, no decorrer deste projeto nos aprofundaremos mais nas técnicas da criptografia RSA.

Encontra-se também neste relatório o cronograma das atividades realizadas e as referências bibliográficas utilizadas.

Objetivos

Objetivo Geral:

Incentivar a participação dos estudantes de graduação em projetos de pesquisas, para que desenvolvam a prática e o pensamento científico com a orientação de grandes pesquisadores. Qualificar os profissionais desta área expandindo seus conhecimentos de forma rigorosa, tanto no projeto como em sua graduação ajudando os mesmos a terem um aprendizado e progresso de conhecimentos matemáticos. Capacitar os participantes para entrarem no mercado de trabalho ou na área de pesquisa.

Objetivo Específico:

Enriquecer o conteúdo com relação a Teoria dos Números, com ênfase em Criptografia, ilustrando de maneira simples os estudos e relatando a importância do projeto no desenvolvimento da matemática, ampliando os conhecimentos e dando ao bolsista maturidade em sua formação acadêmica, dando-lhe um maior grau de abstração, preparando-o para um nível mais avançado de estudo, por exemplo, curso de pós-graduação *Lato Sensu* e *Stricto Sensu* em Matemática.

Metodologia

O projeto tem ênfase em uma grande área da matemática que é a Teoria dos Números. A metodologia utilizada está de acordo com as normas científicas. Nesse contexto, tivemos como fontes de pesquisa livros específicos da área já referida, além de outros de áreas da Matemática que nos deram suporte ao estudo que estamos realizando, e serviram para o enriquecimento de conteúdos e exposição do projeto. O conhecimento adquirido foi assimilado através de seminários propostos pelo orientador e estudo individual.

Capítulo 1

Resultados

1.1 Uma Introdução a Criptografia

Antes de comersarmos a falar do RSA é importante uma pequena revisão sobre alguns aspectos históricos da Criptografia e em seguida apontaremos seus aspectos teóricos, fundamentados através da Teoria dos Números. O termo *Criptografia* surgiu da fusão das palavras gregas *Kriptós* e *gráphein* que significam *oculto* e *escrever*, ou seja, é uma *escrita escondida*. A Criptografia estuda os métodos de codificar uma mensagem de forma que só o destinatário possa interpretá-la. É a arte dos *códigos secretos*, o mais simples destes códigos é a técnica de trocar as letras do alfabeto. Uma técnica semelhante foi o usado pelo imperador *César* para comunicar-se com suas tropas em combate pela Europa. Todo código vem acompanhado de duas receitas, uma para codificar e outra decodificar uma mensagem. Decodificar é o que o usuário legítimo faz quando recebe uma mensagem e quer lê-la, já decifrar é ler uma mensagem sem ser o usuário legítimo, ou seja, para decifrar uma mensagem é necessário quebrar o código. Os códigos como o de César são muito fáceis de decifrar, devido a frequência de cada letra em uma palavra, por exemplo: na língua portuguesa as vogais são mais frequentes que as consoantes e a vogal mais frequente é o A, tornando-se assim um método não muito confiável.

Assim, foi necessário inventar novos códigos, que fossem difíceis de decifrar, mesmo com a ajuda de um computador. Estes códigos foram criados para o uso em aplicações comerciais, e não na comunicação entre espiões, por isso os códigos são todos de *chave pública*. Esta foi uma idéia introduzida em 1976 por *Diffie* e *Hellman* da Universidade de Stanford. No código usado por César, se você sabe codificar então sabe decodificar,

já em um código de *chave pública* saber codificar não significa saber decodificar. Isto parece impossível, pois se sei codificar para decodificar é só desfazer o que fiz, mas nesse método desfazer o processo de codificação pode não ser tão fácil quanto parece.

O método de criptografia de chave pública mais conhecido é o RSA. Este foi um código inventado em 1978 por R.L.Rivest, A.Shamir e L. Adleman. As letras RSA correspondem às iniciais dos inventores do código, esse é atualmente o método mais usado nas aplicações comerciais.

O RSA é um grande exemplo de criptografia de chave assimétrica. Isto é, há uma chave pública, que todos conhecem e serve para codificar a mensagem. Porém, há uma chave privada, que é usada para decodificar a mensagem.

Exemplo: Para codificar uma mensagem utiliza-se um número $n = pq$, produto de dois primos. Essa é a chave pública. A chave privada é constituida pelos primos p e q.

A segurança do método vem do fato de que é difícil fatorar n para descobrir p e q, já que são números muito grandes (de 150 algarismos ou mais). Mas:

Como fatorar um número inteiro de maneira eficiente?

Como determinar se um dado inteiro é primo?

E a parte da matemática que estuda as propriedades dos números inteiros é a teoria de números, a qual enfocaremos sucitamente na seção seguinte.

Como Surgiu o RSA?

O algoritmo RSA surgiu por intermédio de três amigos, *Ron Rivest*, *Adi Shamir*, *Leonard Adleman*.

Ron Rivest, um jovem cientista da computação, dono de uma curiosidade científica insaciável e de uma imensa capacidade de absorver e aplicar novas idéias. Assim que leu o trabalho publicado por Diffie e Hellman, ficou obcecado pelo assunto e passou a procurar sem descanso uma função matemática que pudesse transformar a idéia dos dois criptólogos num sistema real e viável, pois até então, não existia um algoritmo que podesse colocar em prática o sistema de chave pública idealizado pelos dois. Além disso, Rivest acabou contagiando um colega, *Adi Shamir*, também cientista da computação. Os dois conjecturaram e produziram teorias mirabolantes que, uma após a

outra, eram contestadas pelo terceiro colega, *Leonard Adleman*, o único matemático do trio. Depois de quase um ano tentando não obtiveram sucesso, pois todas as sugestões de Rivest e Shamir tinham falhas imperdoáveis.

A esperança estava quase se esgotando quando Rivest em uma noite de insônia, lembrou-se de uma particularidade da matemática muito simples e que provavelmente havia tomado conhecimento do assunto quando ainda estava na escola primária: a fatoração. Multiplicar dois números primos é uma questão de segundos mas, se temos apenas o resultado e quisermos encontrar os números primos *(fatores)* deste resultado, o processo é bem mais demorado. À medida que multiplicamos números primos cada vez maiores, o tempo gasto para fatorar o resultado aumenta exponencialmente. Talvez esta função fosse a resposta tão procurada.

Rivest escreveu até o romper do dia e, logo de manhã, foi procurar Adleman que acostumado com as explosões intelectuais do amigo, começou a ler o texto preparando-se para encontrar defeitos. Leu, releu e, para o espanto dos dois, não havia nada para ser contestado. Nasceu assim o primeiro algoritmo de chave pública, a primeira cifra assimétrica perfeitamente acabada.

Rivest havia batizado o algoritmo de ARS, colocando as iniciais do sobrenome do trio pesquisador em ordem alfabética. Adleman protestou porque achava que tinha contribuído pouco e porque não via futuro algum na publicação do trabalho, pediu inclusive que seu nome fosse retirado, mas Rivest, ciente da importância do papel desempenhado por cada um, pediu que Adleman pensasse melhor no assunto. Não querendo contrariar os amigos, Adleman concordou que seu nome fosse citado em último lugar, motivo pelo qual a cifra foi rebatizada e passou a ser chamada de RSA.

1.2 Teoria dos Números Básica

Definição 1 *Sejam $a, b \in \mathbb{Z}$, dizemos que $a \mid b$ se existir um $k \in \mathbb{Z}$ tal que $b = ak$. Se a não divide b denotamos $a \nmid b$.*

Proposição 1 *Seja a, b e $k \in \mathbb{Z}, a \mid b$ e $b \mid c$, então $a \mid c$.*

Demonstração Se $a \mid b$ e $b \mid c$ então existem k_1 e $k_2 \in \mathbb{Z}$ que $b = k_1 a$ e $c = k_2 b$, substituindo b na equação $c = k_2 b$ temos $c = k_1 k_2 a$ logo $a \mid c$.

Proposição 2 *Se a, b, c, m e $n \in \mathbb{Z}$, $c \mid a$ e $c \mid b$ então $c \mid (ma + nb)$.*

Demonstração Se $c \mid a$ e $c \mid b$ então $a = k_1 c$ e $b = k_2 c$, multiplicando por m e n respectivamente temos $ma = mk_1 c$ e $nb = nk_2 c$, somando-se temos $ma + nb = (mk_1 + nk_2)c$ logo $c \mid (ma + nb)$.

Propriedades da Divisibilidade

(i) $n \mid n$

(ii) $d \mid n \Rightarrow ad \mid an$

(iii) $ad \mid an$ e $a \neq 0 \Rightarrow d \mid n$

(iv) $1 \mid n$

(v) $n \mid 0$

(vi) $d \mid n$ e $n \neq 0 \Rightarrow |d| \leq |n|$

(vii) $d \mid n$ e $n \mid d \Rightarrow |d| = |n|$

(viii) $d \mid n$ e $d \neq 0 \Rightarrow (n/d)|n$.

Teorema 1 (Eudoxius) *Dados a, b inteiros com $b \neq 0$ então a é multiplo de b ou se encontra entre dois multiplos consecutivos de b, isto é, para cada par de inteiros a e $b \neq 0$ existe um inteiro q tal que, para $b > 0$,*

$$qb \leq a < (q + 1)b$$

e para $b < 0$,

$$qb \leq a < (q-1)b.$$

Teorema 2 (Algoritmo da Divisão) *Sejam* $a, b \in \mathbb{Z}, b > 0$*, existe um único par de inteiros* q *e* r *tais que*

$$a = qb + r, \ \ com\ 0 \leq r < b \qquad (r = 0 \Leftrightarrow b \,|\, a).$$

Demonstração (*Existência*) Pelo teorema de Eudoxius, como $b > 0$, existe q que satisfaz a seguinte desigualdade

$$qb \leq a < (q+1)b,$$

e isso nos diz que $a - qb \geq 0$ e $a - qb < b$. Assim, se chamarmos $r = a - qb$, então teremos garantido a existência de q e r.

(*Unicidade*) Suponhamos que existam r e r_1, q e q_1 tais que:

$$a = qb + r \qquad \text{com} \qquad 0 \leq r < b$$

e

$$a = q_1 b + r_1 \qquad \text{com} \qquad 0 \leq r_1 < b.$$

Assim, das duas desigualdades acima, podemos deduzir que

$$(qb + r) - (q_1 b + r_1) = 0 \Rightarrow b(q - q_1) = r_1 - r,$$

donde $b|(r_1 - r)$. Agora, como $r_1 < b$ e $r < b$, devemos ter $|r_1 - r| < b$ e, conseqüentemente, como $b|(r_1 - r)$ devemos ter $r_1 - r = 0$, o que implica que $r = r_1$. E, deste fato, concluímos que $q_1 b = qb \Rightarrow q_1 = q$, pois $b \neq 0$.

Definição 2 *O Maximo Divisor Comum de* $a, b \in \mathbb{Z}$ *(a ou b diferente de zero), denotado por* (a, b)*, é o maior inteiro que divide* a *e* b*.*

Teorema 3 *Seja* d *o máximo divisor comum de* a *e* b*, então existem* n_0 *e* $m_0 \in \mathbb{Z}$ *tais que* $d = n_0 a + m_0 b$*.*

Demonstração Seja B o conjunto de todas as combinações lineares $\{na + mb\}$ e d o menor entre todos os elementos estritamente positivos de B. Portanto, $d = n_0 a + m_0 b$.

Mostraremos que d é o máximo divisor comum de a e b. Assim temos $d \geq 0$. Aplicando o algoritmo da divisão em a e d, o que é possível, pois $d > 0$: $a = qd + r$ $(0 \leq r < d)$, ou $a - qd = r$, e substituindo o valor de d temos: $r = a - q(n_0 a + m_0 b) = (1 - qn_0)a + (-qm_0)b$. Isto mostra que $r \in B$. Então, r não pode ser estritamente positivo, pois é menor que d(= mínimo de B).Logo, $r = 0$ e, portanto, $a = dq$. Ou seja $d|a$ e de forma análoga se prova que $d|b$. Como c é um divisor comum de a e b $(c|a \ e \ c|b, \ c > o)$, existem inteiros k_1 e k_2 tais que $a = k_1 c$ e $b = k_2 c$ e, portanto, $d = n_0 a + m_0 b = n_0 k_1 c + m_0 k_2 c = c(n_0 k_1 + m_0 k_2)$, o que implica que $c|d$. Pela propriedade da divisibilidade (vi), temos que $d \geq c$ isto é, d é o divisor comum positivo de a e b, concluímos que $d = n_0 a + m_0 b$.

Teorema 4 *O máximo divisor comum d de a e b é o divisor positivo de a e b o qual é divisível por todo divisor comum.*

Demonstração Do teorema anterior e pela Proposição 2 da divisão concluímos que se d_1 é divisor comum de a e b, então $d_1|d$. Portanto não podem existir dois números tendo cada um a propriedade de ser divisível por todo divisor comum. Isto por causa da Propriedade (vii) que, no caso de números positivos d_1 e d, nos diz que d_1 deve ser igual a d.

Definição 3 *Sejam $a, b \in \mathbb{Z}$ são relativamente primos quando $(a, b) = 1$.*

Teorema 5 *Se $a|bc$ e $(a, b) = 1$, então $a|c$.*

Demonstração Como $(a, b) = 1$ pelo teorema 1 existem inteiros n em tais que $na + mb = 1$. Multiplicando - se os dois lados desta igualdade por c temos: $n(ac)+m(bc) = c$. Como $a|ac$ e, por hipótese, $a|bc$ então, pela Proposição 2 da divisão, $a|c$.

Teorema 6 *Se a e b são inteiros e $a = qb + r$ onde q e r são inteiros, então $(a, b) = (b, r)$.*

Demonstração Da relação $a = qb + r$ podemos concluir que todo divisor de b e r é um divisor de a. Esta mesma relação, escrita na forma $r = a - qb$, nos diz que todo divisor de a e b é um divisor de r. Logo o conjunto dos divisores comuns de a e b é igual ao conjunto dos divisores comuns de b e r, o que nos garante o resultado $(a, b) = (b, r)$.

Teorema 7 (Algoritmo Euclidiano) *Sejam $r_0 = a$ e $r_1 = b$ inteiros não - negativos com $b \neq 0$. Se o algoritmo da divisão for aplicado sucessivamente para se obter*

$$r_j = q_{j+1}r_{j+1} + r_{j+2}, \qquad 0 \leq r_{j+2} < r_{j+1}$$

para $j = 0, 1, 2, ..., n-1$ e $r_{n+1} = 0$ então $mdc(a, b) = r_n$, o último resto não - nulo.

Demonstração Aplicando o algoritmo da divisão para dividir $r_0 = a$ por $r_1 = b$ obtendo assim $r_0 = q_1r_1 + r_2$, em seguida podemos dividir r_1 por r_2 temos, $r_1 = q_2r_2 + r_3$ e assim, sucessivamente, até a obtenção do resto $r_{n+1} = 0$. Como, a cada passo o resto é sempre menor do que o anterior, e estamos trabalhando com números inteiros positivos, após um número finito de aplicações do algoritmo da divisão, teremos um resto nulo.

Temos, pois, a seguinte sequência de equações:

$r_0 = q_1r_1 + r_2, \qquad 0 \leq r_2 < r_1$

$r_1 = q_2r_2 + r_3, \qquad 0 \leq r_3 < r_2$

$r_2 = q_3r_3 + r_4, \qquad 0 \leq r_4 < r_3$

$\vdots$

$r_{n-2} = q_{n-1}r_{n-1} + r_n, \qquad 0 \leq r_n < r_{n-1}$

$r_{n-1} = q_nr_n + 0$

A última destas equações nos diz, pelo teorema 6, que o $mdc(r_n, r_{n-1}) = r_n$. A penúltima, que este número é igual a (r_{n-1}, r_{n-2})e seguindo desta maneira teremos, por repetidas aplicações do teorema 6, a sequência:

$$r_n = (r_{n-1}, r_n) = (r_{n-2}, r_{n-1}) = ... = (r_1, r_2) = (r_0, r_1) = (a, b)$$

Portanto o $mdc(a, b)$ é o último resto não-nulo da sequência de divisões descrita.

Teorema 8 (Algoritmo Euclidiano Estendido) *Sejam a e b inteiros positivos e seja d o máximo divisor comum entre a e b. Existem inteiros α e β tais que*

$$\alpha.a \ + \ \beta.b \ = \ d$$

Definição 4 (Números Primos) *Diz - se que um inteiro positivo $p > 1$ é um número primo ou apenas um primo, se e somente se 1 e p são os seus únicos divisores positivos. Um inteiro positivo maior que 1 e que não é primo diz - se composto.*

Teorema 9 (Teorema Fundamental da Aritmética) *Todo inteiro maior do que 1 pode ser representado de maneira única (a menos da ordem) como um produto de fatores primos.*

Demonstração Se n é primo não há nada a ser demonstrado. Suponhamos que n é composto. Seja $p_1(p_1 > 1)$ o menor dos divisores positivos de n. Afirmamos que p_1 é primo, o que é verdade, pois, caso contrário existiria p, $1 < p < p_1$ com $p|n$, contradizendo a escolha de p_1. Logo, $n = p_1 n_1$.

Se n_1 for primo a prova está completa. Caso contrário, tomamos p_2 como o menor fator de n_1. pelo argumento p_2 é primo e temos que $n = p_1 p_2 n_2$.

Fazendo este procedimento repetidas vezes obtemos uma sequência decrescente de inteiros positivos $n_1, n_2, ..., n_r$. Como todos eles são inteiros $p_1, p_2, ..., p_k$ não são, necessariamente, distintos, n terá, em geral, a forma:

$$n = p_1^{a_1} p_2^{a_2} ... p_k^{a_k}$$

.

Para mostrar a unicidade podemos usar indução em n. Para $n = 2$ a afirmação é verdadeira. Assumimos, então, que ela se verifica para todos os inteiros maiores do que 1 e menores do que n. Vamos provar que ela também é verdadeira para n. Se n é primo, não há nada a provar, portanto vamos supor que n seja composto e que tenha duas fatorações, isto é,

$$n = p_1 p_2 ... p_s = q_1 q_2 ... q_r$$

.

Vamos provar que $s = r$ e que cada p_i é igual a algum q_j. Como p_1 divide o produto $q_1 q_2 ... q_r$ ele divide pelo menos um dos fatores q_j. Sem perda de generalidade podemos supor que $p_1 | q_1$. Como são ambos primos, isto implica $p_1 = q_1$. Logo $n/p_1 = p_2 ... p_s = q_2 ... q_r$. Como $1 < n/p_1 < n$, a hipótese de indução nos diz que as duas fatorações são idênticas, isto é, $s = r$ e, a menos da ordem, as fatorações $p_1 p_2 ... p_s$ e $q_1 q_2 ... q_r$ são iguais.

Teorema 10 *A sequência dos números primos é infinita.*

Demonstração Vamos supor que a sequência dos primos seja finita. Seja pois, $p_1, p_2, ..., p_n$ a lista de todos os primos. Consideramos o número $R = p_1 p_2 ... p_n + 1$. É claro que R não é divisível por nenhum dos p_i de nossa lista e que R é maior do que qualquer p_i. Mas, pelo teorema 9, ou R é primo ou possui algum fator primo e isto implica na existência de um primo que não pertence à nossa lista. Portanto a sequência dos números primos não pode ser finita.

Definição 5 (Congruência) *Se a e b são inteiros dizemos que a é congruente a b módulo m ($m > 0$) se $m \mid (a - b)$. Denotamos isto por $a \equiv b \mod m$.*
Se $m \nmid (a - b)$ dizemos que a é incongruente a b módulo m.

Exemplo: $11 \equiv 3 \mod 2$, pois $2 \mid (11 - 3)$.

Proposição 3 *Se a e b são inteiros, temos que $a \equiv b \mod m$ se, e somente se, existir um inteiro k tal que $a = b + km$.*

Demonstração Se $a \equiv b \mod m$, então m divide $(a - b)$ e, então existe um $k \in \mathbb{Z}$ tal que $a - b = km$, logo $a = b + km$. A recíproca também é verdade.

Proposição 4 *Se a, b, m e d são inteiros, $m > 0$, as seguintes sentenças:*

1. $a \equiv a \mod m$
2. *Se* $a \equiv b \mod m$, *então* $b \equiv a \mod m$

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

Demonstrações

1. Esta propriedade é imediata, pois $a - a = 0 = m \times 0$

2. Se $a \equiv b \mod m$ então m divide $(a - b)$ e, consequentemente, $a - b = km$ para algum $k \in \mathbb{Z}$. Mas, $b - a = -mk = m \times (-k)$, de forma que m divide $(b - a)$, isto é, $b \equiv a \mod m$

3. Se $a \equiv b \mod m$, então existe algum $k_1 \in \mathbb{Z}$ tal que $a - b = k_1 m$. Semelhantemente, como $b \equiv c \mod m$, então existe algum $k_2 \in \mathbb{Z}$ tal que $b - c = k_2 m$ e, consequentemente, $(a - c) = (a - b) + (b - c) = (k_1 + k_2)m$. Assim, $(a - c)$ é múltiplo de m e, portanto, $a \equiv c \mod m$.

Teorema 11 *Se* a, b, c *e* m *são inteiros tais que* $a \equiv b \mod m$*, então*

1. $a + c \equiv b + c \mod m$

2. $a - c \equiv b - c \mod m$

3. $ac \equiv bc \mod m$

Demonstrações

1. Como $a \equiv b \mod m$ então $a - b = km$ para algum $k \in \mathbb{Z}$, e $(a - b) = (a + c) - (b + c) = km$, de onde $a + c \equiv b + c \mod m$.

2. Como $a \equiv b \mod m$ então $a - b = km$ para algum $k \in \mathbb{Z}$, e $(a - b) = (a - c) - (b - c) = km$, de onde $a - c \equiv b - c \mod m$.

3. Como $a \equiv b \mod m$ então $a - b = km$ para algum $k \in \mathbb{Z}$, implicando que $(a - b)c = (km)c = (kc)m$, isto é, $(a - b)c$ é múltiplo de m, pois $kc \in \mathbb{Z}$, e então $ac \equiv bc \mod m$.

Teorema 12 (Teorema do Resto Chinês) *Sejam* $m_1, m_2, ..., m_k$ *números inteiros, relativamente primos dois a dois (isto é, tais que o* $mdc(m_i, m_j) = 1$*, se* $i \neq j$*). Então, o sistema de congruências*

$$\begin{cases} x & \equiv & a_1 & \text{mod } m_1 \\ x & \equiv & a_2 & \text{mod } m_2 \\ & \vdots & & \\ x & \equiv & a_k & \text{mod } m_k \end{cases}$$

admite única solução côngruas módulo $m_1 m_2 ... m_k$.

Demonstração Consideremos o número $m = m_1.m_2...m_k$.
Para cada índice i definimos $y_i = \frac{m}{m_i}$. Sendo que y_i é o produto de todos os inteiros $m_1, m_2, ..., m_k$, y_i é relativamente primos com m_i, ou seja, o $mdc(y_i, m_i) = 1$. Assim podemos determinar inteiros b_i e c_i tais que: $y_i b_i + m_i c_i = 1$, $1 \leq i \leq k$. Mostraremos então que o número $X = a_1 y_1 b_1 + a_2 y_2 b_2 + ... + a_k y_k b_k$ é uma solução do sistema $X = a_1 y_1 b_1 + a_2 y_2 b_2 + ... a_k y_k b_k \equiv a_i y_i b_i \mod m_i$ temos que $x_i m_i \equiv 1 \mod m_i$, logo $X \equiv a_i y_i b_i \equiv a_i \mod m_i$, isto é X é uma solução da equação $X \equiv a_i \mod m_i$, para cada i, que também é uma solução do sistema.

(*Unicidade*) Suponhamos que X_1 é outra solução, temos que $X_1 \equiv a_i \mod m_i$, $1 \leq i \leq k$, mas também $X \equiv a_i \mod m_i$ pela transitividade da relação de congruência vem que $X_1 \equiv X \mod m_i$, isto é, $m_i \mid (X_1 - X)$, para cada i, $1 \leq i \leq k$. Ainda como os inteiros m_i são relativamente primos, temos que $m_1.m_2...m_k \mid (X_1 - X)$, logo $X_1 \equiv X \mod m$.

Aplicação

1. Três satélites passarão sobre o Rio de Janeiro esta noite. O primeiro à 1 hora da madrugada, o segundo às 4 horas e o terceiro às 8 horas da manhã. Cada satélite tem um período diferente. O primeiro leva 13 horas para completar uma volta em torno da Terra, o segundo 15 horas e o terceiro 19 horas. Determine quantas horas decorrerão, a partir da meia - noite, até que os três satélites passem ao mesmo tempo sobre o Rio.

   Resolução

   $x = 1 + 13k_1$
   $x = 4 + 15k_2$
   $x = 8 + 19k_3$

Colocando na forma de congruência.

$x \equiv 1 \mod 13$
$x \equiv 4 \mod 15$
$x \equiv 8 \mod 19$

Aplicando o Teorema do Resto Chinês no sistema, temos:

$m = 13.15.19 = 3705$

$y_1 = \frac{3705}{13} = 285$
$y_2 = \frac{3705}{15} = 247$
$y_3 = \frac{3705}{19} = 195$

Colocando na forma de congruência linear

$285x_1 \equiv 1 \mod 13$, $247x_2 \equiv 1 \mod 15$ e $195x_3 \equiv 1 \mod 19$

mas $x_1 = 12$, $x_2 = 13$ e $x_3 = 4$

Logo $x = a_1.y_1.x_1 + a_2.y_2.x_2 + a_3.y_3.x_3$
x = 1.285.12 + 4.247.13 + 8.195.4
x = 3420 + 12844 + 6240
x = 22504

Como $22504 \equiv 274 \mod 3705$, então $x \equiv 274 \mod 3705$.
$x = 274 + 3705k$

Os satélites passarão juntos sobre o céu do Rio pela primeira vez 274 horas depois da meia noite e só voltarão a passar juntos novamente a cada 3705 horas.

Teorema 13 (Pequeno Teorema de Fermat) *Seja p um número primo e a um*

número inteiro, então.
$a^p \equiv a \mod p$

Demonstração Por Indução:
Como podemos observar que para $P(1)$ vale, pois $1^p = 1$. Suponhamos então que $k^p \equiv k \mod p$. Mas para fazer uma relação entre $P(k)$ e $P(k+1)$, $k \in \mathbb{Z}$ usaremos ouma versão do*binômio de Newton* para congruências que diz:

$$(a+b)^p = a^p + b^p + \sum_{i=1}^{p-1} \binom{p}{i} a^{p-i} b^i.$$

Portanto, mostrando que o termo
$\sum_{i=1}^{p-1} \binom{p}{i} a^{p-i} b^i$
é congruente a zero módulo p chegaremos ao resultado desejado. Considerando o número

$$\binom{p}{i} = \frac{p(p-1)...(p-i+1)}{i!}$$

Para que a fração acima dê lugar a um número inteiro é peciso que o numerador seja completamente cancelado por termos no denominador, suponhamos que $1 \leq i \leq p-1$ então o denominador não p como um de seus fatores, portanto p não pode ser cancelado com nenhum termo do denominador, o que é verdade já que p é primo, logo o número inteiro é multiplo de p quando $1 \leq i \leq p-1$. Consequentemente
$\sum_{i=1}^{p-1} \binom{p}{i} a^{p-i} b^i \equiv 0 \mod p$

Portanto

$$(a+b)^p \equiv a^p + b^p \mod p$$

Voltando a demonstração por indução em supomos que $k^p \equiv k \mod p$, vamos mostrar que $(k+1)^p \equiv k+1 \mod p$. Usando o binômio de Newton que acabamos e mostrar, temos que

$$(k+1)^p \equiv k^p + 1^p \equiv k^p + 1 \mod p$$

Como por hipótese temos

$k^p \equiv k \mod p$, então

$(k+1)^p \equiv k^p + 1 \equiv k + 1 \mod p$

Definição 6 (Função ϕ de Euler) *Chama - se função de Euler a função aritmética ϕ(fi) assim definida para todo inteiro positivo n:*

$\phi\,(n)$ = *número de inteiros positivos que não superam n e que são primos com n.*

Teorema 14 ($\phi\,(n)$) *Se o inteiro n>1, então $\phi\,(n) = n - 1$ se e somente se n é primo.*

Demonstração Se n>1 é primo, então os inteiros positivos menores que n é primo com n e, portanto,

$$\phi\,(n) = n - 1$$

Reciprocamente, se $\phi\,(n) = n - 1$, 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, d e n, isto é, $\phi\,(n) \leq n - 2$. Logo, n é primo.

Capítulo 2

Criptografia RSA

2.1 Pré-codificação

A mensagem a ser criptografada será *eu gosto de matemática*.
O primeiro passo é, converter as letras em números usando a seguinte tabela.

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

Obs: Os espaços entre as palavras será substituido pelo numero 99, mas neste caso especifico não utilizaremos.

A pré-codificação ficará assim:

1430991624282924991314992210291422102918121 0

Agora, os numeros acima devem ser quebrados em blocos, a forma de escolher os blocos não é única, mas cada bloco deve ser menor que n. Não pode começar um bloco por *0* e também deve-se tomar o cuidado para que eles não correspondam a nenhuma unidade linguística, para impossibilitar a decifração por contagem de frequência.

Assim tomemos $p = 17$ e $q = 23$ dois primos quaisquer, logo $n = p \times q = 17 \times 23 = 391$. Os blocos ficarão assim:

14 - 309 - 9 - 162 - 42 - 82 - 92 - 49 - 91 - 3 - 149 - 92 - 210 - 291 - 42 - 210 - 291 - 81 - 210.

2.2 Codificação

A chave de codificação é o par *(n,e)* sendo e um inteiro positivo que é inversível $\phi(n)$ ou seja o $mdc(e, \phi(n)) = 1$, na verdade e é o menor primo que não divide $\phi(n)$, neste caso escolhemos *e=3*. Para codificar um bloco b, sendo que b é um inteiro positivo menor que n. Denotaremos o bloco codificado por *C(b)*.

C(b)= resto da divisão de b^e por n.

Codificando cada bloco separadamente:
$14^3 \equiv 7 \mod 391$
$309^3 \equiv 333 \mod 391$
$9^3 \equiv 338 \mod 391$
$162^3 \equiv 185 \mod 391$
$42^3 \equiv 189 \mod 391$
$82^3 \equiv 58 \mod 391$
$92^3 \equiv 207 \mod 391$
$49^3 \equiv 349 \mod 391$
$91^3 \equiv 114 \mod 391$
$3^3 \equiv 27 \mod 391$
$149^3 \equiv 89 \mod 391$
$92^3 \equiv 207 \mod 391$
$210^3 \equiv 165 \mod 391$
$291^3 \equiv 178 \mod 391$
$42^3 \equiv 189 \mod 391$
$210^3 \equiv 165 \mod 391$

$291^3 \equiv 178 \mod 391$
$81^3 \equiv 72 \mod 391$
$210^3 \equiv 165 \mod 391$

Logo a mensagem codificada fica assim:

7 - 333 - 338 - 185 - 189 - 58 - 207 - 349 - 114 - 27 - 89 - 207 - 165 - 178 - 189 - 165 - 178 - 72 - 165

2.3 Decodificação

Para decodificar um bloco da mensagem codificada. Precisamos de n e o inverso de e em $\phi(n)$, que chamaremos de d, ou seja, a chave de decodificação é o par *(n,d)*.

$D(a) =$ resto da divisão de a^d por n.

Sendo que a é o bloco codificado e que $\phi(n) = (p-1) \times (q-1)$, então
$\phi(n) = 16 \times 22 = 352$
Para calcular d iremos aplicar o algoritmo euclidiano estendido.
Dividindo $\phi\ (391) = 352$ por 3.

$$352 = 117 \times 3 + 1$$

onde

$$1 = 352 + (-117) \times 3$$

Logo o inverso de 3 módulo 352 é -117, como iremos usar d como expoente de potências é necessário que d seja positivo. Portanto $d = 352 - 117 = 235$, que é o menor inteiro positivo congruente a $-117 \mod 352$. Para decodificar dividiremos cada bloco a pelos primos 17 e 23, que são os primos em que n se fatora.

Como:

$$333 \equiv 10 \mod 17$$

$$333 \equiv 11 \mod 23$$

Assim

$$333^{235} \equiv 10^{235} \mod 17$$

$$333^{235} \equiv 11^{235} \mod 23$$

Aplicando o teorema de Fermat, temos:

$$10^{235} \equiv (10^{16})^{14} 10^{11} \equiv 10^{11} \equiv 3 \mod 17$$

$$11^{235} \equiv (11^{22})^{10} 11^{15} \equiv 11^{15} \equiv \mathit{9.9.20} \equiv 10 \mod 23$$

$$x \equiv 3 \mod 17$$

$$x \equiv 10 \mod 23$$

Aplicando o Teorema do Resto Chinês no sistema acima, temos:

$M = 17.23 = 391$

$$m_1 = \frac{391}{17} = 23$$
$$m_2 = \frac{391}{23} = 17$$

Colocando na forma de congruência

$23x \equiv 1 \mod 17$ e $17x \equiv 1 \mod 23$
mas $x_1 = 3$ e $x_2 = 19$

Logo $x = 3 \times 23 \times 3 \ + \ 10 \times 17 \times 19 = 207 \ + \ 3230 = 3437$

Como $3437 \equiv 309 \mod 391$, então $x \equiv 309 \mod 391$.

309 corresponde ao segundo bloco. E procedendo da mesma forma com os outros blocos voltaremos a mensagem original.

2.4 Por que o RSA é seguro?

O RSA é um método de chave pública. Sendo p e q os parâmetros desse sistema e $n = pq$. A chave de codificação é a chave pública, portanto o par n,e é conhecido por qualquer usuário, sendo que o RSA só será considerado seguro se for difícil calcular d quando apenas n e e são conhecidas, mas só sabemos calcular d aplicando o algoritmo euclidiano estendido a $\phi(n)$ e e, por outro lado para calcular $\phi(n)$ sem fatorar n de forma a obter p e q é muito difícil. Portanto só é possível quebrar o código se coseguirmos fatorar n, mas se n for muito grande isso será quase impossível.

Conclusão

A álgebra tem como objetivo dotar o aluno dos conceitos fundamentais das teorias de grupos. No entanto, apenas conceitos não são suficientes para dar ao aluno uma visão da disciplina, para isto são necessários alguns resultados estruturais, que justificam o trabalho desprendido no estudo de teorias básicas, como por exemplo: A Teoria dos Números. Alguns desses estudos relacionados a teoria dos números são essenciais para o estudo da criptografia RSA.

O sistema RSA é um dos métodos de criptografia mais seguro, pois sua chave pública possui primos com valores muito altos, cerca de 150 algarismos, em que os cálculos só possam ser feitos por meio de um computador, mesmo pra um computador muito eficiente é praticamente impossível quebrar o código, assim o RSA é um sistema muito seguro.

A Criptografia, por sua vez, é uma técnica muito interessante em toda a sua forma prática. Através dela podemos nos comunicar livremente e com segurança. Este é um método usado particularmente pelos bancos para a proteção dos dados de seus clientes.

Cronograma

O desenvolvimento do projeto obedece o seguinte cronograma:

Atividades	Ago	Set	Out	Nov	Dez	Jan	Fev	Mar	Abr	Mai	Jun	Jul
Noções Sucintas de Teoria dos Números		X	X	X	X	X	X					
Divisibilidade		X	X									
Números Primos			X									
Teorema do Resto Chinês				X								
Elaboração do Relatório Parcial				X	X	X						
Apresentação Oral Parcial				X								
Congruências					X	X	X					
Pequeno Teorema de Fermat									X			
Criptografia RSA										X	X	
Elaboração do Relatório Final										X	X	
Apresentação Final												X

Referências Bibliográficas

[1] Santos, José Plinio de Oliveira. Introdução à Teoria dos Números. Segunda Edição. Rio de Janeiro: IMPA, CNPq, 2000.

[2] Coutinho, S. C. Números Inteiros e Criptografia RSA. Segunda Edição. Rio de Janeiro: IMPA/SBM, 2000.

[3] Alencar Filho, Edgar de. Teoria Elementar dos Números. Segunda edição. São Paulo: Nobel, 1985.

[4] Milis, Francisco César Polcino. Coelho, Sônia Pitta. Números: Uma Introdução à Matemática. São Paulo: Editora da universidade de São Paulo, 2000.

[5] Domingues, Hygino H. Iezzi, Gelson. Álgebra Moderna. Quarta edição reform. São Paulo: Atual, 2003.

[6] Coutinho, S. C. Criptografia. Programa de Iniciação Científica da OBMEP 2007.