FACULDADE DE TECNOLOGIA DE AMERICANA – FATEC
CURSO DE ANALISE E DESENVOLVIMENTO DE SISTEMAS

RAMON LACAVA GUTIERREZ GONÇALES

ALGORITMO DE SHOR

AMERICANA
2017

SUMÁRIO

1 INTRODUÇÃO

A necessidade de enviar e receber mensagens sem que outras pessoas possuam conhecimento do conteúdo, com exceção do destinatário e o remetente sempre existiu. A este método se dá o nome de criptografia. Uma mensagem pode ser decodificada de várias formas, como por exemplo, atribuir a cada letra do alfabeto um número, embora este método não seja recomendado pela necessidade de que ambos (destinatário e remetente) devem conhecer a tabela de códigos utilizados para a tradução da mensagem. Também existem métodos utilizados para o descobrimento do conteúdo de uma mensagem chamados ataques frequencistas que analisam a frequência de letras utilizadas para descobrir o conteúdo da frase, o que torna o método ineficiente. A criptografia na qual apenas o destinatário e o remetente sabem os códigos de codificar é chamado de criptografia de chave privada, porem na mesma ocorre um problema da distribuição de chaves. Já na criptografia de chave pública, todos sabem codificar uma mensagem, mas apenas o destinatário sabe como decodifica-la.

Um dos métodos de chave pública mais utilizados é a criptografia RSA, criado no Instituto de Tecnologia de Massachussets (MIT). É um ótimo método, e sua segurança é baseada pois ainda não existe um algoritmo rápido para fatorar números compostos grandes na computação convencional. Com o surgimento da computação quântica, foi possível descobrir algoritmos rápidos para resolver diversos problemas. Um dos algoritmos foi o de Shor, criado em 1994, que se trata de um algoritmo poderoso na fatoração de inteiros. Esse algoritmo fatora números pequenos até 15, mas caso este modelo evolua e trabalhe com números tão grandes quanto o computador clássico, a criptografia RSA se tornará obsoleta.

2 VISÃO GERAL DO ALGORITMO

Até 1990, computação quântica era apenas uma curiosidade. Porem isso mudou em 1994, quando Shor publicou seu algoritmo quântico que resolve o problema de fatoração de números. Utilizando esse algoritmo, um número seria fatorado muito mais rapidamente do que com máquinas clássicas e por isso ficou conhecido como “killer application”. A fatoração de números grandes é a base de alguns sistemas de criptografia, como o RSA. Assim, o algoritmo de Shor passou a despertar interesse na comunidade cientifica.

Shor provou que um computador quântico pode fatorar números grandes em um curto tempo. Um computador convencional precisaria rodar por bilhões de anos para fatorar um número de 400 dígitos. Uma máquina quântica pode fazer isso em cerca de 1 ano. Códigos antes que eram indecifráveis agora poderiam ser decifrados.

Tamanho do Número a Ser Fatorado (em bits)	Tempo de Fatoração por Algoritmo Clássico	Tempo de Fatoração por Algoritmo Quântico
512	4 dias	34 segundos
1024	100 mil anos	4,5 minutos
2048	100 mil bilhões de anos	36 minutos
4096	100 bilhões de quadrilhões de anos	4,8 horas

Tabela 1: Comparação entre os tempos estimados para fatoração de números de tamanhos diferentes com o algoritmo clássico e com o de Shor. Fonte: Revista Ciência Hoje, Vol. 33, n. 193, Maio de 2003.

O algoritmo de Shor (também conhecido como Sho97) é um algoritmo quântico que dado um inteiro n composto impar que não é potência de primo, devolve um fator de n com probabilidade limitada de erro.

As restrições impostas para o valor de n não representam problema. Encontrar um fator de um número par é trivial, e também é fácil desenvolver um algoritmo que decide $n = a^k$ para inteiros a e $k > 1$, e que devolve a e k nesse caso. O algoritmo de Shor pode ser usado para resolver problemas de fatoração em tempo polinomial no tamanho de entrada.

O algoritmo é baseado em uma redução do problema da busca de um fator de n ao problema da busca do período de uma sequência. Como a redução utiliza aleatorização, é possível que ela falhe, isto é, que nenhum fator de n seja encontrado, porem a probabilidade deste evento é limitada. O algoritmo resolve o seguinte problema: dado um inteiro positivo N, achar os fatores primos de N. Na computação clássica não existe algoritmo que resolva esse problema em tempo polinomial.

3 ALGORITMO DE SHOR

O algoritmo explora o argumento de que dois fatores primos, p e q de um número positivo $n = p.q$ podem ser encontrados determinando o período de uma função $f(a) = x^a \ mod \ N$, para qualquer $x < n$ que não tenha fatores comuns com n. Abaixo é apresentado o pseudocódigo do algoritmo Shor.

Algoritmo $Shor(n)$

1. escolha um inteiro $1 < x < n$ aleatoriamente
2. se $mdc(x, n) > 1$
3. então devolva $mdc(x, n)$
4. **seja r o período da função** $f(a) := x^a \ mod \ n$
5. se r for ímpar ou $x^{\frac{r}{2}} \equiv -1 \ (mod \ n)$
6. então o procedimento falhou (deve-se escolher outro x e recomeçar o procedimento)
7. devolva $mdc(x^{\frac{r}{2}} + 1, n)$

O algoritmo de Shor utiliza um único passo quântico, o cálculo do período da função na linha 4. Caso o algoritmo execute a linha 3, o valor devolvido é um fator de n. Caso $mdc(x,n) = 1$, então x está em $\mathbb{Z}_n^*$. O período r é o tamanho do subgrupo de $\mathbb{Z}_n^*$ gerado por x. De acordo com o teorema, r é o menor inteiro positivo tal que $x^r \equiv 1 \ (mod \ n)$. O valor da linha 7 é de fato um fator de n.

Vamos realizar uma simulação do algoritmo. Digamos que queremos encontrar os fatores primos de $n = 15$. Pegamos um número aleatório $x < n$. Supomos que o número sorteado seja $x = 7$ (note que x não tem fatores comuns a não ser 1) e definimos a função $f(a) = 7^a \ mod \ 15$. O período de f é $r = 4$ ($f(a)$ assume os valores 1, 7, 4, 13, 1, 7, 4,... quando $a = 0, 1, 2, 3, 4, 5, 6 \ldots$ respectivamente). Logo, o cálculo do máximo divisor entre 15 e $50 = 7^{4/2} + 1$ devolve o valor 5, que é um dos fatores primos de 15.

Definir o período de uma função não é simples mas encontrar o período de uma função relacionada com o número 15 pode ser descrita dessa maneira:

1. Encontrar um número que não tem fatores em comum com 15, diferente de 1, como 11.
2. Dividir 11 por 15, se obtém 0 com resto 11.
3. Eleve o resto ao quadrado, assim se encontra 121.

4. Dividir 121 por 15 para se obter 8 com resto 1.
5. Eleve ao cubo 11 para obter 1331.
6. Divida 1331 por 15 para obter 88 com resto 11.

Ao continuar a elevar 11 a potencias superiores, vamos notar que o resto de 15 será alternadamente 11 e 1. Assim, dizemos que o período de 11 em relação a ser dividido por 15 é 2. Isso é útil para fatorar 15, pois:

1. Eleve 11 a potência dada pelo seu período, 2, e o resultado é 121.
2. Tire a raiz quadrada para se obter 11.
3. Subtraia e some 1 a 11 para se obter um par de números, 10 e 12.
4. Encontre o maior denominador comum de 10 e 15, e 12 e 15. O primeiro é 5 e o último é 3, que também são fatores de 15.

O algoritmo de Shor utiliza a propriedade de sobreposição quântica para conseguir reduzir através de funções quânticas especificas a complexidade do tempo de solução de problema de fatoração de exponencial para polinomial. A fatoração de um número em primos está em NP^{10}(classe de problemas de decisão para os quais não existem soluções polinomiais).

APENDICE A – TEORIAS PARA COMPREENSÃO DO ALGORITMO

O apêndice a seguir apresenta algumas teorias necessárias para a melhor compreensão do algoritmo de Shor. É explicado um pouco sobre a divisibilidade e primalidade, aritmética modular e grupos.

A.1 DIVISIBILIDADE E PRIMALIDADE

A divisão de um número inteiro por outro permeia toda a teoria dos números.

1ª Definição. Dados os números n e d inteiros, é dito que d divide n se existe um inteiro k tal que $n = k\,.d$, e isso é denotado por $d \mid n$. Neste caso, dizemos também que n é divisível por d e que n é múltiplo de d. Se $d \mid n$ e $d \geq 0$, então d é um divisor de n. Se d não divide n, isso é denotado por $d \nmid n$.

2ª Preposição. Dados os números d, a, b inteiros, se d divide a e b, então d divide $a.x + b.y$ para quaisquer $x, y \in \mathbb{Z}$.

3ª Definição. Dados um número $n > 1$, dizemos que n é primo se os únicos divisores de n são 1 e n. Vale observar que 1 não é nem primo nem composto.

4º Teorema. Existem infinitos números primos.

5º Teorema. Dados $m \geq 0$ e $n > 0$ inteiros, então existem inteiros q e r satisfazendo $m = q.n + r$ e $0 <= r < n$ e tais inteiros são únicos. O q é o quociente da divisão de m por n e o r é o resto da divisão de m por n, chamado de $m \bmod n$. A variável n divide m somente se $m \bmod n = 0$.

6ª Definição. Dados os números inteiros a, b, d, dizemos que d é divisor comum de a e b se d é divisor de a e de b. Se a ou b forem diferentes de 0 então o maior divisor comum de a e b é chamado de máximo divisor comum de a e b, e é denotado por $mdc(a,b)$. Se o $mdc(a,b)$ for igual a 1, dizemos que a e b são relativamente primos ou primos entre si.

7º Teorema. Sejam a, b inteiros não nulos, o $mdc(a,b)$ é o menor elemento positivo do conjunto $\{a.x + b.y : x, y \in \mathbb{Z}\}$ de combinações lineares inteiras de a e b.

8º Corolário. Dados os números inteiros a e b, ambos não nulos, caso d seja um divisor comum de a e b, então $d \mid mdc(a,b)$.

9º Teorema (recursão de Euclides). Dados os inteiros $a >= 0$ e $b > 0$, então $mdc(a,b) = mdc(b, a \bmod b)$.

10ª Preposição. Dados os inteiros positivos d, a, b e supondo que $d \mid a.b$, se $mdc(d,a) = 1$, então $d \mid b$.

11º Teorema. Seja p um número primo e a, b inteiros, se $p \mid a.b$, então $p \mid a$ ou $p \mid b$.

12º Teorema (fatoração única). Dado $n > 1$ sendo que n é um inteiro, então existe um único modo de escrever n na forma

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},$$

Onde $k >= 1$, os inteiros $p1 < p2 < \ldots < pk$ são primos e $ei > 0$ para todo i.

A.2 ARITMETICA MODULAR

Dado um número a pertencendo aos $\mathbb{Z}$ e dividi-lo por 2 temos duas possibilidades de resto, 0 se o número for par, 1 se o número for ímpar. Assim, é possível definir o conjunto $\mathbb{Z}2$, para ser formado pelos restos da divisão do número por 2.

$$\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$$

O símbolo − acima dos números, por exemplo de 0, indica que não é apenas o número 0 mas sim o conjunto de todos os números pares, semelhante ao 1 que representa todos os números impares.

Também é possível definir $\mathbb{Z}n$.

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}^1.$$

É interessante o uso de operações matemáticas nestes conjuntos. A regra de soma diz que a soma de dois pares resulta em um par. A soma de dois impares resulta em um par e se for um par e um impar o resultado será um ímpar.

$$\begin{aligned}\overline{0}+\overline{0} &= \overline{0},\\ \overline{1}+\overline{1} &= \overline{0},\\ \overline{1}+\overline{0} &= \overline{1},\\ \overline{0}+\overline{1} &= \overline{1}.\end{aligned}$$

Também é possível demonstrar a multiplicação, como por exemplo ao utilizar o conjunto $\mathbb{Z}4$ com o elemento $\overline{2}$.

$$\begin{aligned}\overline{2}\cdot\overline{0} &= \overline{0}\\ \overline{2}\cdot\overline{1} &= \overline{2}\\ \overline{2}\cdot\overline{2} &= \overline{4}=\overline{0}\\ \overline{2}\cdot\overline{3} &= \overline{6}=\overline{2},\end{aligned}$$

Conjunto possui 0, 1, 2, 3, ou seja, vai até n - 1 o conjunto Z4

Também é possível analisar o elemento $\overline{2}$ no conjunto $\mathbb{Z}5$.

$$\begin{aligned}\overline{2}\cdot\overline{0} &= \overline{0}\\ \overline{2}\cdot\overline{1} &= \overline{2}\\ \overline{2}\cdot\overline{2} &= \overline{4}\\ \overline{2}\cdot\overline{3} &= \overline{6}=\overline{1}\\ \overline{2}\cdot\overline{4} &= \overline{8}=\overline{3},\end{aligned}$$

A.3 GRUPOS

Um conjunto G com uma operação (*) é um grupo se (*) possui as seguintes propriedades.

1. Fechado: Dados a e b pertencentes a G, se a * b = c, então c pertence a G.
2. Elemento neutro: Existe um elemento e pertencente a G tal que para todo a pertencente a G temos a * e = e * a = a.
3. Associatividade: Dados a, b, c pertencentes a G temos a * (b * c) = (a * b) * c.

4. Elemento inverso: Dado um elemento a pertencente a G qualquer, existe um elemento a’ pertencente a G tal que a * a’ = a’ * a = e.

Se (G, *) é um grupo, a função * é a operação binária do grupo. Se o par (G, *) satisfazer a * b = b * a para todo a, b pertencente a G, então dizemos que (G, *) é um grupo comutativo ou abeliano. Também é dito que um grupo (G, *) é finito se G é finito.

O conjunto $\mathbb{Z}_n^*$ é um grupo com a operação produto. Para que $\mathbb{Z}_n^*$ seja um grupo, vamos verificar as propriedades acima.

1. (Fechado). Dados $\bar{a}, \bar{b} \in \mathbb{Z}$, sabemos que o $mdc\ (a,n) = 1$ e $mdc\ (b,n) = 1$, logo o $mdc\ (a.b,n) = 1$. Portanto $\bar{a}, \bar{b} \in \mathbb{Z}_n^*$.
2. (Elemento neutro). O elemento $\bar{1} \in \mathbb{Z}_n^*$ e dado qualquer elemento $\bar{a} \in \mathbb{Z}_n^*$ temos que $\bar{a}\ .\bar{1} = \bar{1}\ .\bar{a} = \bar{a}$. Logo, $\bar{1}$ é o elemento neutro.
3. (Associatividade). Dados $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n^*$, temos que $(\bar{a}\ .\bar{b}\ ).\bar{c} = \overline{(a\ .b).c} = \overline{a\ .(b\ .c)} = \bar{a}\ .(\bar{b}\ .\bar{c}\ )$.
4. (Elemento inverso). Dado $\bar{a} \in \mathbb{Z}_n^*$ sabemos que $mdc\ (a,b) = 1$ e também que $\bar{a}$ é inversível. Portanto, existe $\overline{a'}$ tal que $\bar{a}\ .\overline{a'} = \bar{1} = \overline{a'}\ .\bar{a}$.

A.4 ALGORITMO DE EUCLIDES

Um algoritmo é uma sequência de passos no qual dada uma entrada, é realizado um processamento e se obtém uma saída. Como por exemplo uma receita de bolo, dados os ingredientes, o bolo é feito utilizando métodos e no final se obtém o bolo pronto. Vamos apresentar o algoritmo de Euclides utilizado para calcular o mdc no algoritmo de Shor. O algoritmo de Euclides calcula o máximo divisor de dois números inteiros positivos.

Entrada: números inteiros positivos distintos a e b

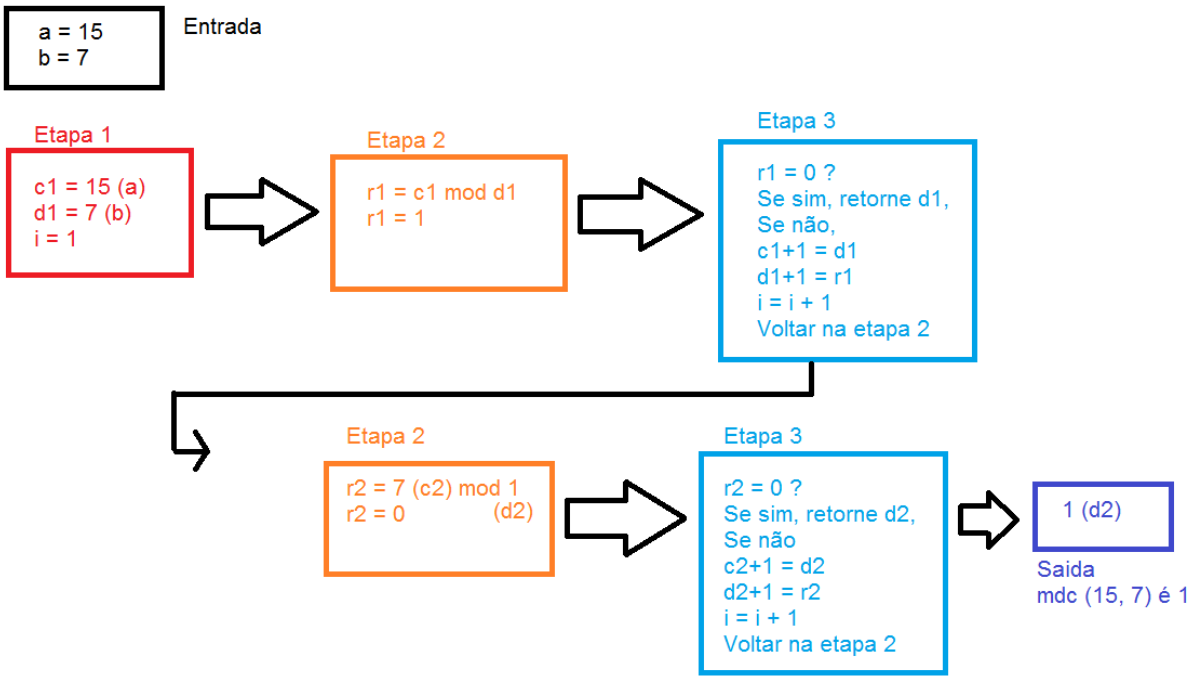
Saída: $mdc(a, b)$

Etapa 1: Comece fazendo $c_1 = a$, $d_1 = b$ e $i = 1$

Etapa 2: utilize o algoritmo da divisão para dividir c_i por d_i e retornar r_i.

Etapa 3: Se $r_i = 0$ retorne d_i, caso contrário faça $c_{i+1} = d_i$, $d_{i+1} = r_i$, acrescente 1 ao contador i e volte a etapa 2.

Abaixo está uma representação do funcionamento do algoritmo de Euclides.



REFERÊNCIAS

MATTIELO, Felipe et al. Decifrando a computação quântica. **Caderno de Física da UEFS**, v. 10, p. 31-44, 2012.

CARDONHA, Carlos Henrique; DE CARLI SILVA, Marcel Kenji; FERNANDES, Cristina Gomes. **Computação quântica: Complexidade e algoritmos**. IME-USP, 2005.

BASALO, Ana Luiza Domingues Fernandez; GNANN, William Alexandre Miura. **Computação quântica para leigos.** IME-USP, 2011.

FREITAS, Adriana Xavier. **Algoritmo de Shor e sua aplicação à fatoração de números inteiros.** UFMG, 2010.