Resíduos Quadráticos e Fatoração: uma aplicação à criptoanálise do RSA

Charles F. de Barros

20 de novembro de 2008

Resumo

Faremos uma breve introdução ao conceito de resíduos quadráticos, descrevendo em seguida um algoritmo probabilístico de fatoração. Tal procedimento reforça a tese da equivalência entre quebrar o RSA e fatorar o módulo n, mas ressaltamos que tal equivalência ainda não foi comprovada. Isto nos remete a uma questão crucial: saber se a segurança do RSA[1] de fato reside na dificuldade para fatorar números muito grandes. Se a tese da equivalência fosse refutada, quebrar o RSA *poderia* não ser tão difícil. Por enquanto, o problema está em aberto, e o RSA continua sendo seguro, pois quebrá-lo ainda é tão difícil quanto fatorar.

1 Resíduos quadráticos

No conjunto $\mathbb{Z}_p^*$, onde p é um número primo maior que 2, alguns elementos possuem uma característica especial: são equivalentes ao quadrado de algum outro elemento de $\mathbb{Z}_p^*$, como o que acontece com $\overline{4}$ em $\mathbb{Z}_5^*$, pois

$$4 \equiv 3^2 \pmod 5$$

Tais elementos são denominados *resíduos quadráticos*. Apresentaremos a definição geral deste conceito e enunciaremos de forma breve algumas de suas propriedades fundamentais.

Definição 1.1 *Seja $p > 2$ um número primo e $\overline{a} \in \mathbb{Z}_p^*$. Dizemos que $\overline{a}$ é um resíduo quadrático módulo p se*

$$a \equiv b^2 \pmod p$$

para algum $\overline{b} \in Z_p^*$.

Por exemplo, em $\mathbb{Z}_7^*$ temos os seguintes quadrados:

$$\begin{aligned} 1^2 &\equiv 1 \pmod 7 \\ 2^2 &\equiv 4 \pmod 7 \\ 3^2 \equiv 9 &\equiv 2 \pmod 7 \end{aligned}$$

[1] A segurança do RSA depende ainda de certos detalhes um pouco mais sutis [3], como a escolha adequada dos fatores de n, e também de outros parâmetros. Se estes detalhes não forem levados em conta, vulnerabilidades no sistema poderão ser exploradas [2].

Dizemos assim que $\overline{1}$, $\overline{2}$ e $\overline{4}$ são resíduos quadráticos em $\mathbb{Z}_7^*$. Os demais elementos, $\overline{3}$, $\overline{5}$ e $\overline{6}$, são resíduos não quadráticos módulo 7.

Observe que, para calcular os resíduos quadráticos módulo 7, tomamos os quadrados apenas dos três primeiros elementos de $\mathbb{Z}_7^*$. Por que ignoramos os demais elementos? Ora, é fácil verificar o seguinte:

$$\begin{aligned} 4^2 &\equiv 16 \equiv 2 \pmod 7 \\ 5^2 &\equiv 25 \equiv 4 \pmod 7 \\ 6^2 &\equiv 36 \equiv 1 \pmod 7 \end{aligned}$$

Obtivemos os mesmos resultados! Isto não é mera coincidência. Vejamos mais um exemplo, em $\mathbb{Z}_{11}^*$, tomando apenas os quadrados dos cinco primeiros elementos:

$$\begin{aligned} 1^2 &\equiv 1 \pmod{11} \\ 2^2 &\equiv 4 \pmod{11} \\ 3^2 &\equiv 9 \pmod{11} \\ 4^2 &\equiv 16 \equiv 5 \pmod{11} \\ 5^2 &\equiv 25 \equiv 3 \pmod{11} \end{aligned}$$

E agora, elevando ao quadrado os demais elementos:

$$\begin{aligned} 6^2 &\equiv 36 \equiv 3 \pmod{11} \\ 7^2 &\equiv 49 \equiv 5 \pmod{11} \\ 8^2 &\equiv 64 \equiv 9 \pmod{11} \\ 9^2 &\equiv 81 \equiv 4 \pmod{11} \\ 10^2 &\equiv 100 \equiv 1 \pmod{11} \end{aligned}$$

Mais uma vez, obtivemos os mesmos resíduos quadráticos: $\overline{1}$, $\overline{3}$, $\overline{4}$, $\overline{5}$ e $\overline{9}$.

Estamos vendo que, em $\mathbb{Z}_7^*$, que possui seis elementos, temos exatamente três resíduos quadráticos, e em $\mathbb{Z}_{11}^*$, que possui dez elementos, são cinco resíduos quadráticos. Podemos generalizar este fato, enunciando o seguinte

Lema 1.1 *Dado um número primo $p > 2$, exatamente metade dos elementos de $\mathbb{Z}_p^*$ são resíduos quadráticos.*

Demonstração: Vamos denotar por $\overline{a_1}$, $\overline{a_2}$,..., $\overline{a_{p-1}}$ os elementos de $\mathbb{Z}_p^*$, com $a_1 = 1$, $a_2 = 2$, ..., $a_{p-1} = p - 1$. É fácil observar que

$$a_1 + a_{p-1} = a_2 + a_{p-2} = ... = p$$

Ou seja, a soma de elementos equidistantes dos extremos é sempre igual a p. Por exemplo, em $\mathbb{Z}_{11}^*$, temos

$$1 + 10 = 2 + 9 = 3 + 8 = 4 + 7 = 5 + 6 = 11$$

Então podemos concluir que

$$a_k \equiv -a_{p-k} \pmod p$$

para todo k entre 1 e $p - 1$.

Logo:

$$(a_k)^2 \equiv (-a_{p-k})^2 \equiv (a_{p-k})^2 \pmod p$$

Ou seja, elevando ao quadrado dois elementos equidistantes dos extremos, o resultado módulo p será o mesmo. Como $\mathbb{Z}_p^*$ tem exatamente $p-1$ elementos, teremos $(p-1)/2$ resíduos quadráticos, e a mesma quantidade de resíduos não quadráticos. Assim, para determinar os quadrados em $\mathbb{Z}_p^*$, basta calcular a forma reduzida de $b^2 \pmod{p}$ para $b = 1, 2, ..., (p-1)/2$.

QED

A seguir, enunciaremos uma propriedade[2] que nos permitirá, dado um número primo p, caracterizar se um inteiro é ou não resíduo quadrático módulo p.

Propriedade 1.1 *Seja um número primo $p > 2$ e $a \in \mathbb{Z}$ tal que* $\text{mdc}(p, a) = 1$. *Então*

$$a^{(p-1)/2} \equiv \pm 1 \pmod{p}$$

Em particular, temos

$$a^{(p-1)/2} \equiv 1 \pmod{p}$$

se a for um resíduo quadrático módulo p. Caso contrário,

$$a^{(p-1)/2} \equiv -1 \pmod{p}$$

Vale a pena ressaltar aqui nossa hipótese principal: p **é um número primo**. A idéia agora é mostrar que, quando o módulo for um inteiro n, composto, a propriedade anterior será falsa para pelo menos metade dos elementos de $\mathbb{Z}_n^*$, desde que possamos encontrar um inteiro a que satisfaça

$$a^{(n-1)/2} \not\equiv \pm 1 \pmod{n}$$

Proposição 1.1 *Seja n um número ímpar, composto. Se pudermos assegurar a existência de pelo menos um inteiro a, primo com n, tal que*

$$a^{(n-1)/2} \not\equiv \pm 1 \pmod{n}$$

então isto deve ocorrer para pelo menos metade dos elementos de $\mathbb{Z}_n^*$.

Demonstração: Sejam a_1 e a_2 inteiros, tais que

$$a_1 \equiv \pm 1 \pmod{n}$$

e

$$a_2 \not\equiv \pm 1 \pmod{n}$$

Então

$$(a_1 a_2)^{(n-1)/2} \equiv (a_1)^{(n-1)/2}(a_2)^{(n-1)/2} \equiv \pm(a_2)^{(n-1)/2} \not\equiv \pm 1 \pmod{n}$$

Suponha que os inteiros b_1, b_2, ..., b_k satisfaçam

$$(b_i)^{(n-1)/2} \equiv \pm 1 \pmod{n} \qquad i = 1, 2, ..., k$$

[2]Na verdade, trata-se de um teorema, cuja demonstração omitiremos, por envolver detalhes que não serão abordados aqui. Para obter maiores informações, consulte [1].

Pelo que acabamos de verificar, se existir um inteiro a tal que

$$a^{(n-1)/2} \not\equiv \pm 1 \pmod{n}$$

teremos

$$(ab_i)^{(n-1)/2} \not\equiv \pm 1 \pmod{n} \qquad i = 1, 2, ..., k$$

Ou seja, garantindo a existência de pelo menos um inteiro que não satisfaça a Propriedade 1.1, a quantidade de elementos para os quais ela é falsa será no mínimo igual à quantidade daqueles para os quais ela é verdadeira.

Portanto, pelo menos metade dos elementos de $\mathbb{Z}_n^*$, onde n é um número ímpar composto, não satisfazem a Propriedade 1.1, desde que exista um inteiro a que também não a satisfaça. O que afirmamos, sem demonstração[3], é que *sempre podemos garantir a existência de tal a.*

QED

2 Fatoração de Inteiros e Criptoanálise do RSA

Antes de dar início à nossa discussão, ressaltemos alguns aspectos importantes da criptoanálise do RSA. Em primeiro lugar, é preciso ter em mente que fatorar o módulo n equivale a expor a chave secreta d. De fato, uma vez obtida a fatoração de n, podemos utilizar $\varphi(n)$ e a chave pública e para recuperar o valor de d, lembrando que $ed \equiv 1 \pmod{\varphi(n)}$. No entanto, a fatoração direta de n é impraticável, já que $n = pq$, onde p e q são números primos *muito grandes*, mas se pudermos recuperar o valor de $\varphi(n)$, então poderemos obter os fatores de n, já que $\varphi(n) = (p-1)(q-1)$. Note que, neste caso, estamos supondo a existência de um método que permita calcular $\varphi(n)$ sem fatorar n.

Nossa abordagem partirá do pressuposto de que tenha sido encontrada uma maneira de recuperar diretamente o valor de d, a partir de n e e. Nosso objetivo é demonstrar que isto também equivale a fatorar n, pois, uma vez obtido o valor de d, teremos encontrado um múltiplo de $\varphi(n)$. Isto não é tão bom quanto conhecer o próprio $\varphi(n)$, mas nos permite a fatoração por meio de um método probabilístico. Repare que estamos no centro de uma importante discussão, que consiste em saber se fatorar o módulo n realmente equivale a quebrar o RSA. O problema que permanece em aberto é o da possibilidade de se recuperar uma mensagem criptografada, sem que seja necessário encontrar a chave secreta d. Se isto fosse possível, quebrar o RSA e fatorar n poderiam não ser problemas equivalentes.

Então, suponha que tenhamos conseguido quebrar um sistema RSA, encontrando um inteiro positivo d que satisfaça

$$ed \equiv 1 \pmod{\varphi(n)}$$

Logo, existe um inteiro k tal que $ed - 1 = k\varphi(n)$. Pelo Teorema de Euler sabemos que

$$a^{\varphi(n)} \equiv 1 \pmod{n}, \text{ para todo } a \in \mathbb{Z}_n^*.$$

Então:

[3]Consulte [1], página 52, exercício 21.

$$a^{ed-1} \equiv (a^{\varphi(n)})^k \equiv 1 \pmod{n}$$

para todo a primo com n.

Façamos $ed - 1 = m$. Observe que, como p é ímpar, $\varphi(n)$ é par. Logo, m também é.

Uma vez que conheçamos tal m, o próximo passo é verificar se $m/2$ satisfaz a mesma condição, isto é, se

$$a^{m/2} \equiv 1 \pmod{n}$$

para todo a primo com n.

Seria inviável testar esta congruência para todo $a \in \mathbb{Z}_n^*$. Por isso, escolhemos aleatoriamente diversos valores de a para fazer o teste. Se em todos os casos a congruência for verificada, então será *bastante provável* que isto ocorra para todo a primo com n, e assim poderemos substituir m por $m/2$. Continuamos dividindo o expoente por 2, enquanto a congruência for satisfeita.

Suponha então que, para todo a primo com n, seja válida a relação

$$a^m \equiv 1 \pmod{n}$$

mas que tenhamos encontrado um valor de a tal que

$$a^{m/2} \not\equiv 1 \pmod{n}$$

Isto ocorrerá para pelo menos metade dos elementos de $\mathbb{Z}_n^*$. De fato, se os inteiros b_1, b_2, ..., b_k satisfazem

$$(b_i)^{m/2} \equiv 1 \pmod{n} \qquad i = 1, 2, ..., k$$

então

$$(ab_i)^{m/2} \equiv a^{m/2} \not\equiv 1 \pmod{n} \qquad i = 1, 2, ..., k$$

Portanto, a quantidade de elementos que não satisfazem a congruência é no mínimo igual à quantidade daqueles para os quais ela se verifica.

Assim, quando soubermos que $a^m \equiv 1 \pmod{n}$ para todo a primo com n, e encontrarmos algum $a \in \mathbb{Z}_n^*$ tal que

$$a^{m/2} \not\equiv 1 \pmod{n}$$

teremos duas possibilidades:

1. $m/2$ é múltiplo de $p - 1$ ou $q - 1$, mas não de ambos. Digamos que seja múltiplo somente de $p - 1$. Neste caso, sempre teremos

   $$a^{m/2} \equiv 1 \pmod{p}$$

   De fato, sabemos, por Fermat, que $a^{p-1} \equiv 1 \pmod{p}$. Como $m/2$ é múltiplo de $p - 1$, existe um inteiro k tal que $m/2 = k(p - 1)$. Logo

   $$a^{m/2} \equiv (a^{p-1})^k \equiv 1 \pmod{p}$$

Por outro lado, vimos na seção anterior que apenas metade dos elementos de $\mathbb{Z}_q^*$ satisfaz $a^{(q-1)/2} \equiv 1 \pmod{q}$, enquanto a outra metade deve satisfazer $a^{(q-1)/2} \equiv -1 \pmod{q}$.

O que mostraremos agora é um pouco diferente: metade dos elementos de $\mathbb{Z}_q^*$ devem satisfazer a congruência

$$a^{m/2} \equiv 1 \pmod{q}$$

e para os demais, teremos

$$a^{m/2} \equiv -1 \pmod{q}$$

Isto porque, se a for resíduo quadrático, existe algum inteiro b tal que $a \equiv b^2 \pmod{q}$. Logo:

$$a^{m/2} \equiv b^m \equiv 1 \pmod{q}$$

Por outro lado, sabemos que

$$a^m - 1 = (a^{m/2} - 1)(a^{m/2} + 1)$$

Estamos supondo que $a^m \equiv 1 \pmod{n}$ para todo $a \in \mathbb{Z}_n^*$. Ou seja, $a^m - 1$ é múltiplo de n, logo é múltiplo de q. Então q sempre divide $(a^{m/2} - 1)(a^{m/2} + 1)$. Se a não for resíduo quadrático, q não pode dividir $a^{m/2} - 1$, logo ele *deve* dividir $a^{m/2} + 1$, ou seja, $a^{m/2} \equiv -1 \pmod{q}$.

2. $m/2$ não é múltiplo de $p - 1$ nem de $q - 1$. Neste caso, pelo mesmo argumento utilizado anteriormente, teremos

   $$a^{m/2} \equiv 1 \pmod{p}, \text{ para metade dos elementos de } \mathbb{Z}_p^*$$

   e, para os demais,

   $$a^{m/2} \equiv -1 \pmod{p}$$

   O mesmo se aplica a $\mathbb{Z}_q^*$.

Então podemos resumir nossa análise com as seguintes tabelas de probabilidade:
Para o primeiro caso, em que $m/2$ é múltiplo de $p - 1$, mas não de $q - 1$:

$a^{m/2} \equiv 1 \pmod{p}$	100%
$a^{m/2} \equiv -1 \pmod{q}$	50%
Probabilidade conjunta	50%

Já no segundo caso, em que $m/2$ não é múltiplo nem de $p - 1$ nem de $q - 1$, temos:

$a^{m/2} \equiv 1 \pmod{p}$	50%
$a^{m/2} \equiv -1 \pmod{q}$	50%
Probabilidade conjunta	25%

$a^{m/2} \equiv -1 \pmod{p}$	50%
$a^{m/2} \equiv 1 \pmod{q}$	50%
Probabilidade conjunta	25%

Repare que, em ambos os casos, a probabilidade de que $a^{m/2} - 1$ seja múltiplo de um dos primos, mas não do outro, é de 50%, para cada valor de a que testarmos. Assim, em duas tentativas, esperamos encontrar um $a \in \mathbb{Z}_n^*$ tal que $a^{m/2} - 1$ seja múltiplo de somente um dos fatores de n, digamos p. Então, a fatoração de n poderá ser obtida, pois $\text{mdc}(a^{m/2} - 1, n) = p$.

3 Conclusões

O procedimento que acabamos de descrever constitui um exemplo de *algoritmo probabilístico*, e é mais um argumento apontando na direção de que fatorar o módulo n e quebrar o RSA são problemas equivalentes, embora ainda não seja descartada a possibilidade de se encontrar um método para recuperação de uma mensagem criptografada, sem que seja necessário fatorar n. Como já foi dito aqui, isto só seria possível se tal método excluísse a necessidade de recuperar o valor da chave secreta d, o que até hoje não foi realizado.

Os resultados obtidos aqui devem ser interpretados da seguinte maneira: partindo de um método (hipotético) de obtenção da chave secreta d, chegamos a um algoritmo de fatoração. Como já dissemos, a recíproca é verdadeira, isto é, se fatorarmos n, poderemos recuperar d. Assim mostramos que as duas coisas são equivalentes, ou seja, encontrar o valor de d é tão difícil quanto fatorar números muito grandes, o que nas circunstâncias atuais significa dizer *muito difícil*. Então, a pergunta que permanece sem resposta é: realmente precisamos do valor de d para quebrar o RSA? Se a resposta for negativa, *quebrar o RSA é realmente tão difícil?*

Repare que em nenhum momento afirmamos que seria *fácil* quebrar o RSA, se para isto não fosse necessário encontrar d. Por outro lado, se precisamos do expoente secreto para quebrar o sistema, então esta é uma tarefa difícil, porque até hoje não foi desenvolvido nenhum método eficiente de fatoração. Ou seja, quebrar o RSA ainda é tão difícil quanto fatorar. Alguém até poderia descobrir uma maneira, por exemplo, de calcular diretamente o valor de x a partir da forma reduzida de $x^e \pmod{n}$, sem precisar encontrar d, mas nada nos garante que tal método seria eficiente. Ou seja, mesmo se pudéssemos afirmar que fatorar n e quebrar o RSA não são problemas equivalentes, isto não implicaria necessariamente em dizer que o RSA não é seguro.

Em [4], Boneh e Venkatesan mostram que, sob certas condições, não há equivalência entre fatoração e a quebra do RSA, quando o expoente de codificação tem um valor baixo. Contudo, eles fazem questão de enfatizar que suas conclusões não apontam nenhuma vulnerabilidade do sistema. Portanto, ainda não temos nenhum resultado que ponha em xeque a segurança do RSA.

Referências

[1] KOBLITZ, Neal, *A Course in Number Theory and Cryptography*, Graduate Texts in Mathematics 114, Springer-Verlag, New York, 2^{nd} edition, 1987.

[2] BONEH, Dan, *Twenty Years of Attacks on the RSA Cryptosystem*, Notices of the AMS, February 1999, 203-213.

[3] COUTINHO, S.C., *Números Inteiros e Criptografia RSA*, IMPA, Série de Computação e Matemática, 2^a edição, 2003.

[4] BONEH, Dan *and* VENKATESAN, R., *Breaking RSA may be easier than factoring*. In K. Nyberg, editor, *Advances in Cryptology, EUROCRYPT '98*, NUMBER 1403 in LNCS, 59-71. IACR, Springer, May 1998.