Routo Terada

July 27, 2004

1. Resíduo quadrático mod n

Seja $a \in Z_n^*$. a é um resíduo quadrático módulo n (ou um quadrado módulo n) se existir um $x \in Z_n^*$ tal que $x^2 = a \bmod n$. Se tal x não existir, diz-se que a é um não-resíduo quadrático módulo n. O conjunto de todos os resíduos quadráticos módulo n é Q_n, e os não-resíduos quadráticos é $\overline{Q}_n$. Observe que como $0 \notin Z_n^*$, $0 \notin Q_n$ e $0 \notin \overline{Q}_n$. Em resumo:

$$\boxed{a \in Z_n^* \text{.é resíduo quadrático mod } n \iff \exists x \in Z_n^* : x^2 = a \bmod n}$$

Por exemplo, em Z_{11}^*, $Q_{11} = \{1, 3, 4, 5, 9\}$ como se vê na tabela a seguir:

x	1	2	3	4	5	6	7	8	9	10
$x^2 \bmod 11$	1	4	9	5	3	3	5	9	4	1

Seja $g \in Z_p^*$ um gerador de Z_p^* no caso particular de p ser um primo ímpar. Neste caso, $a \in Z_p^*$ é um resíduo quadrático se e só se $a = g^i \bmod p$ para um i inteiro par. Portanto,

$$|Q_p| = (p-1)/2 \text{ e } |\overline{Q}_p| = (p-1)/2.$$

Em resumo:

$$\boxed{\begin{array}{l}\text{se } p > 2 \text{ primo, então:} \\ a \in Z_p^* \text{ é resíduo quadrático mod } n \\ \Updownarrow \\ a = g^i \bmod p : i \text{ par, } g \text{ gerador de } Z_p^*\end{array}}$$

Por exemplo sendo $g = 2$ um gerador de Z_{11}^*, tem-se:

i	0	1	2	3	4	5	6	7	8	9
$2^i \bmod 11$	1	2	4	8	5	10	9	7	3	6

Portanto, $Q_{11} = \{1, 3, 4, 5, 9\}$ e $\overline{Q}_{11} = \{2, 6, 7, 8, 10\}$.

Se $n = pq$ onde p e q são dois primos ímpares distintos, então $a \in Z_n^*$ é um resíduo quadrático módulo n se e só se $a \in Q_p$ e $a \in Q_q$. Logo, deduz-se que

$$|Q_n| = |Q_p| \times |Q_q| = (p-1)(q-1)/4 \text{ e } |\overline{Q}_n| = 3(p-1)(q-1)/4.$$

Em resumo:

se $p, q > 2$ primos ímpares distintos, então:

$$a \in Z_{pq}^* \text{ é resíduo quadrático } \bmod n$$
$$\Updownarrow$$
$$a \in Q_p \text{ e } a \in Q_q \tag{1.1}$$

Por exemplo para $n = 3 \times 5 = 15$, $Q_3 = \{1\}$ e $\overline{Q}_3 = \{2\}$, e $Q_5 = \{1, 4\}$ e $\overline{Q}_5 = \{2, 3\}$. $Q_{15} = \{1, 4\}$. $\overline{Q}_{15} = \{2, 7, 8, 11, 13, 14\}$. Verifique pela tabela a seguir.

x	1	2	3	4
$x^2 \bmod 3$	1	1	0	$1 = 4^2 \bmod 3$

x	1	2	3	4	5	6
$x^2 \bmod 5$	1	4	4	1	0	$1 = 6^2 \bmod 5$

Seja $a \in Q_n$. Se $x \in Z_n^*$ satisfaz $x^2 = a \bmod n$, diz-se que x é raiz quadrada de a módulo n. Por exemplo, se $n = 15$ tem-se a tabela a seguir: (Na tabela a seguir, observe que $6, 9, 10 \notin Q_{15}$ e $6, 9, 10 \notin \overline{Q}_{15}$ pois $6, 9, 10 \notin Z_{15}^*$.)

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$x^2 = a \bmod 15$	1	4	9	1	10	6	4	4	6	10	1	9	4	1

Quanto ao número de raízes quadradas, tem-se:

1. Se p é um primo ímpar e $a \in Q_p$, então a possui exatamente duas raízes quadradas módulo p.

2. Se $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ onde os p_j são primos ímpares distintos e cada $\alpha_j > 0$ e se $a \in Q_n$, então a possui exatamente 2^k raízes quadradas distintas módulo n. No caso particular de $n = pq$, onde $p, q > 2$ são primos distintos, há quatro raízes quadradas $\bmod n$.

Por exemplo, as duas raízes quadradas de 5 módulo 41 são 13 ($13^2 \bmod 41 = 5$) e 28 ($28^2 \bmod 41 = 5$). E as raízes quadradas de 16 módulo 21($21 = 3 \times 7$) são: $4, 10, 11$ e 17, conforme a tabela a seguir.

$1^2 \bmod 21 = 1$	$2^2 \bmod 21 = 4$	$3^2 \bmod 21 = 9$	$4^2 \bmod 21 = 16$
$5^2 \bmod 21 = 4$	$6^2 \bmod 21 = 15$	$7^2 \bmod 21 = 7$	$8^2 \bmod 21 = 1$
$9^2 \bmod 21 = 18$	$10^2 \bmod 21 = 16$	$11^2 \bmod 21 = 16$	$12^2 \bmod 21 = 18$
$13^2 \bmod 21 = 1$	$14^2 \bmod 21 = 7$	$15^2 \bmod 21 = 15$	$16^2 \bmod 21 = 4$
$17^2 \bmod 21 = 16$	$18^2 \bmod 21 = 9$	$19^2 \bmod 21 = 4$	$20^2 \bmod 21 = 1$

2. Símbolo de Legendre

(Adrien-Marie Legendre, 1752-1833)

Seja p um inteiro primo ímpar, e seja Q_p o conjunto dos inteiros $a \in Z$ que são resíduos quadráticos mod p, isto é, existe um inteiro $x \in Z_p^*$ tal que $x^2 = a \bmod p$. Símbolo de Legendre é por definição:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 \text{ se } p|a \text{ (i.e., } mdc(p,a) \neq 1) \\ 1 \text{ se } a \in Q_p \\ -1 \text{ se } a \in \overline{Q}_p \end{cases}$$

O símbolo $\left(\frac{a}{p}\right)$ possui as seguintes propriedades, supondo $p > 2$ ser um inteiro primo ímpar, e $a, b \in Z$:

1. (Critério de Euler) $\boxed{\text{se } mdc(a,p) = 1\text{: } \left(\frac{a}{p}\right) = a^{(p-1)/2} \bmod p}$
   Por exemplo, $4^{(11-1)/2} \bmod 11 = 1$ e $4 \in Q_{11}$; e $7^{(11-1)/2} \bmod 11 = 10 = -1$ e $7 \in \overline{Q}_{11}$.
   Em particular $\left(\frac{1}{p}\right) = 1$ e $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$. Portanto

   $$-1 \in Q_p \text{ se } p = 1 \bmod 4 \text{ e } -1 \in \overline{Q}_p \text{ se } p = 3 \bmod 4.$$

2. $\boxed{\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)}$ pois $\left(\frac{ab}{p}\right) = (ab)^{(p-1)/2} \bmod p = a^{(p-1)/2} b^{(p-1)/2} \bmod p = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. Por exemplo $\left(\frac{4\times 7}{11}\right) = \left(\frac{4}{11}\right)\left(\frac{7}{11}\right) = 1(-1) = -1$
   Portanto, se $mdc(a,p) = 1$: $\left(\frac{a^2}{p}\right) = 1$ e $\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$.

3. se $a = b \bmod p$, então $\boxed{\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)}$ Esta propriedade é conseqüência da definição de Símbolo de Legendre.

4. $\boxed{\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}}$ Por exemplo $\left(\frac{2}{11}\right) = (-1)^{(121-1)/8} = (-1)^{15} = -1$
Logo

$$\left(\frac{2}{p}\right) = 1 \text{ se } p = 1 \bmod 8 \text{ ou } p = 7 \bmod 8.$$
$$\left(\frac{2}{p}\right) = -1 \text{ se } p = 3 \bmod 8 \text{ ou } p = 5 \bmod 8.$$

5. (Reciprocidade, Gauss 1796) Sejam $p, q > 2$ primos distintos, então

$$\boxed{\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{(p-1)(q-1)/4}}$$

Ou seja:

$$\boxed{\left(\frac{p}{q}\right) = \begin{cases} -\left(\frac{q}{p}\right) \text{ se } p = 3 \bmod 4 \text{ e } q = 3 \bmod 4 \\ \left(\frac{q}{p}\right) \text{ caso contrário} \end{cases}}$$

Por exemplo $\left(\frac{11}{7}\right) = -\left(\frac{7}{11}\right) = -(-1) = 1$.

3. Símbolo de Jacobi

(Karl Gustav Jacob Jacobi, 1804 - 1851)

O Símbolo de Jacobi é uma generalização do Símbolo de Legendre para um módulo ímpar, não necessariamente primo.

Seja $a \in Z$, e seja $n > 0$ um inteiro ímpar com fatoração $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ onde os $p_j \geq 3$ são primos ímpares distintos e cada $\alpha_j > 0$. O Símbolo de Jacobi é por definição:

$$\begin{cases} \left(\frac{a}{1}\right) = 1 \\ \left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \left(\frac{a}{p_2}\right)^{\alpha_2} \dots \left(\frac{a}{p_k}\right)^{\alpha_k} \text{ se } n > 1 \text{ ímpar} \end{cases}$$

No caso particular $n = pq$ onde p e q são dois primos ímpares distintos, $\left(\frac{a}{pq}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right)$.

Para inteiros ímpares $m \geq 3, n \geq 3$ e $a, b \in Z$, o Símbolo de Jacobi possui as seguintes propriedades:

1. Pela definição: $\left(\frac{0}{1}\right) = 1$ e $\left(\frac{0}{n}\right) = 0$ se $n \neq 1$.

2. Pela definição: $\boxed{\left(\frac{a}{n}\right) = 0, 1, \text{ ou } -1}$ Ademais

$$\left(\frac{a}{n}\right) = 0 \Leftrightarrow mdc(a, n) \neq 1$$

pois $mdc(a, n) = p \neq 1 \Rightarrow \left(\frac{a}{p}\right) = 0$ pela definição de Símbolo de Legendre $\Rightarrow \left(\frac{a}{n}\right) = 0$.

3. $\boxed{\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)}$. Esta propriedade é conseqüência da Propriedade 2. Portanto se $a \in Z_n^*$ (como $\left(\frac{a}{n}\right) \neq 0$), então $\left(\frac{a^2}{n}\right) = 1$.

4. $\boxed{\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)}$

5. se $a = b \bmod n$, então $\boxed{\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)}$. Esta propriedade é conseqüência da Propriedade 3.

6. $\boxed{\left(\frac{1}{n}\right) = 1}$

7. $\boxed{\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}}$ Logo

$$\left(\frac{-1}{n}\right) = 1 \text{ se } n = 1 \bmod 4 \text{ e } \left(\frac{-1}{n}\right) = -1 \text{ se } n = 3 \bmod 4.$$

8. $\boxed{\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}}$ Logo

$$\left(\frac{2}{n}\right) = 1 \text{ se } n = 1 \bmod 8 \text{ ou } n = 7 \bmod 8.$$
$$\left(\frac{2}{n}\right) = -1 \text{ se } n = 3 \bmod 8 \text{ ou } n = 5 \bmod 8.$$

9. (Reciprocidade) Se $mdc(m, n) = 1$ e $m > 2, n > 2$ são inteiros ímpares, então $\boxed{\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)(-1)^{(m-1)(n-1)/4}}$ Ou seja:

$$\boxed{\left(\frac{m}{n}\right) = \begin{cases} -\left(\frac{n}{m}\right) & \text{se } n = 3 \bmod 4 \text{ e } m = 3 \bmod 4 \\ \left(\frac{n}{m}\right) & \text{caso contrário (i.e., } m = 1 \bmod 4 \text{ ou } n = 1 \bmod 4) \end{cases}}$$

Corollary 3.1. $mdc(a, n) = 1 \Rightarrow$

$$\left(\frac{a}{n}\right) \neq 0 \Rightarrow \left(\frac{a^2}{n}\right) = \left(\frac{a}{n}\right)^2 = \left(\frac{a}{n^2}\right) = 1 \tag{3.1}$$

pelas Propriedades 3 e 4

Corollary 3.2. $mdc(a, n) = 1 \Rightarrow$

$$\begin{cases} \left(\frac{a^2 b}{n}\right) = \left(\frac{b}{n}\right) & \text{pelo Corolário 3.1 e pela Propriedade 3} \\ \left(\frac{a}{mn}\right) = \left(\frac{a}{n}\right) & \text{pelo Corolário 3.1 e pela Propriedade 4} \end{cases} \tag{3.2}$$

Corollary 3.3. Seja $a = 2^e n'$ com $e \geq 0$ e n' ímpar, e seja $a' = n \bmod n'$ (i.e., $n = qn' + a'$ para algum inteiro $q \geq 0$). O Símbolo de Jacobi é dado por:

$$\left(\frac{a}{n}\right) = \left(\frac{a'}{n'}\right) (-1)^{e \times \frac{n^2-1}{8} + \frac{n-1}{2}\frac{n'-1}{2}} \tag{3.3}$$

Demonstração

$$\begin{aligned} \left(\frac{a}{n}\right) &= \left(\frac{2^e n'}{n}\right) \\ &= \left(\frac{2^e}{n}\right)\left(\frac{n'}{n}\right) && \text{pela Propriedade 3} \\ &= (-1)^{e \times \frac{n^2-1}{8}} \left(\frac{n'}{n}\right) && \text{pela Propriedade 8} \\ &= (-1)^{e \times \frac{n^2-1}{8}} \left(\frac{n}{n'}\right) (-1)^{\frac{n-1}{2}\frac{n'-1}{2}} && \text{pela Propriedade 9, porque } mdc(n, n') = 1 \text{ (pois } n = a' \bmod n') \text{ e } n' > 0 \text{ é ímpar.} \end{aligned}$$

Observe que mesmo quando $mdc(a, n) > 1$ a igualdade 3.3 é válida pois os dois lados são iguais a zero.

Como $a' < n' \leq a < n$ o lado direito da igualdade 3.3 envolve argumentos estritamente menores. Portanto aplicando-se a igualdade 3.3 sucessi vamente, fatalmente teremos $a' = 0$ e o cálculo de $\left(\frac{a}{n}\right)$ termina. Esta aplicação sucessiva é a idéia básica do algoritmo a seguir para calcular o Símbolo de Jacobi. Note que neste algoritmo não há necessidade de se conhecer a fatoração de n:

Algoritmo $Jacobi(A, N)$ **para calcular o Símbolo de Jacobi** $\left(\frac{A}{N}\right)$
Entrada: inteiro ímpar $N > 0$, e inteiro $A : 0 < A < N$.
Saída: $\left(\frac{A}{N}\right)$, Símbolo de Jacobi; se N primo, então Símbolo de Legendre.

1. $temp \leftarrow 1$;

2. **enquanto (**$A \neq 0$) {

   2.1 **enquanto (**$A \bmod 2 = 0$){
   (* depois deste laço, $A = n'$ no Corolário 3.3 *)

   2.1.1 $A \leftarrow A/2$;

   2.1.2 **se**($N \bmod 8 = 3$ ou $N \bmod 8 = 5$) $temp \leftarrow -temp$;
   (* $(n^2 - 1)/8$ é ímpar *)
   }

   2.2 $X \leftarrow A; A \leftarrow N; N \leftarrow X$;
   (* troca A e N, e $A = n, N = n'$ ímpar no Corolário 3.3 *)

   2.4 **se (**$A \bmod 4 = 3$ e $N \bmod 4 = 3$) $temp \leftarrow -temp$;
   (* $(n - 1)/2 \times (n' - 1)/2$ é ímpar *)

   2.5 $A \leftarrow A \bmod N$;
   (* $A = n \bmod n'$ no Corolário 3.3 *)
   }

3. **se** ($N = 1$) resposta é $temp$ **senão** resposta é 0;

Este algoritmo em linguagem MatLab é como segue:

```
function [resp] = Jacobi(A,N)
% calcula Simbolo de Jacobi de int A:0<A<N, N>0 impar
if(rem(N,2)==0)
  resp =-99; % N par -> erro
  else
  temp=1; % inicia sinal com 1
  while (A~=0)
    while(rem(A,2)==0) % depois deste laco, A=n'
      A=A/2;
      if(rem(N,8)==3 | rem(N,8)==5) % (n^2-1)/8 impar
        temp=-temp;
      end % if
    end % while

    X=A; A=N; N=X; % troca A e N, A=n, N=n' impar
    if( (rem(A,4)==3 & rem(N,4)==3) ) temp = -temp;
        % (n-1)(n'-1)/2 impar
    end %if
    if(N~=0)A=rem(A,N);
    end% A= n mod n'
  end % while
  if(N==1) resp=temp
  else resp=0
  end
end % if inicial
```

4. Caso particular de $\left(\frac{a}{pq}\right)$, $p = q = 3 \bmod 4$

No caso particular $n = pq$ onde p e q são dois primos ímpares distintos, pela definição de Símbolo de Legendre, $\left(\frac{a}{pq}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right)$.

Lemma 4.1. Sejam $p > 2$ primo, $p = 3 \bmod 4$ e $a \in \overline{Q}_p$. Então $\left(\frac{-a}{p}\right) = +1$.

Demonstração $\left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right)$ pela Propriedade 3 de Símbolo de Jacobi. Como por hipótese $p = 3 \bmod 4$, pela Propriedade 1 de Símbolo de Legendre $\left(\frac{-1}{p}\right) = -1$. Como $a \in \overline{Q}_p$, ou seja, $\left(\frac{a}{p}\right) = -1$, conclui-se este lema. 2

Lemma 4.2. Sejam $p > 2, q > 2$ primos distintos, $p = q = 3 \bmod 4$ e inteiro $a \neq 0$. Se $\left(\frac{a}{pq}\right) = 1$, então ou $a \in Q_{pq}$ ou $-a \in Q_{pq}$.

Demonstração Como $\left(\frac{a}{pq}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right)$ e como por hipótese $\left(\frac{a}{pq}\right) = 1$, tem-se: $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$. Há duas alternativas:

1. $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = +1$ e portanto $a \in Q_{pq}$.
2. $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = -1$. Neste caso, pelo Lema 4.1 tem-se $\left(\frac{-a}{p}\right) = \left(\frac{-a}{q}\right) = +1$, e portanto $-a \in Q_{pq}$. Esta alternativa ocorre porque $p = q = 3 \bmod 4$ por hipótese, e portanto pela Propriedade 1 de Símbolo de Legendre $\left(\frac{-1}{p}\right) = \left(\frac{-1}{q}\right) = -1$. Então $\left(\frac{-a}{pq}\right) = \left(\frac{-a}{p}\right)\left(\frac{-a}{q}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right)\left(\frac{-1}{q}\right)\left(\frac{a}{q}\right) = +1$. 2

5. Exercícios

1. Calcular os seguintes Símbolos de Jacobi:
    1. $\left(\frac{8}{15}\right) = +1$
    2. $\left(\frac{37}{59}\right) = -1$
    3. $\left(\frac{133}{401}\right) = -1$
    4. $\left(\frac{7331}{9859}\right) = +1$
    5. $\left(\frac{7411}{9283}\right) = -1$
2. Provar que para n composto
    1. se $a \in Q_n$ então $\left(\frac{a}{n}\right) = 1$
    2. se $\left(\frac{a}{n}\right) = 1$, então não é necessário que $a \in Q_n$

6. Pseudo-primos

Seja $n > 3$ um inteiro ímpar. Seja $J_n = \{a \in Z_n^* : \left(\frac{a}{n}\right) = 1\}$. Como visto no Exercício, o conjunto $J_n - Q_n$ não é vazio, e é chamado Conjunto dos Pseudo-primos módulo n.

Index