

1 Equações modulares não lineares

Consideramos agora equações modulares gerais de grau superior a 1, ou seja, equações da forma

$$f(x) \equiv 0 \pmod{m},$$

onde

$$f(x) = \sum_{i=0}^n a_i x^i$$

é um polinómio com coeficientes inteiros.

Convém no entanto precisar a noção de grau neste contexto: o polinómio $5x^3 + 2x^2 + 1$, por exemplo, tem grau 3, se o consideramos como polinómio com coeficientes inteiros, mas tem grau 2 se o considerarmos como polinómio com coeficientes em $\mathbb{Z}/5$.

Definimos portanto grau de um polinómio $f(x)$ como o maior expoente k tal que a_k não é congruente com 0 módulo m . Se a for uma classe de congruência módulo p , diferente de 0, o grau do polinómio “constante” $f(x) = a$ é zero, enquanto que o grau do polinómio nulo é definido por convenção como sendo $-\infty$, embora este símbolo não tenha aqui outro significado do que satisfazer, por convenção, as propriedades

$$-\infty < 0 \text{ e } -\infty + m = -\infty \quad \forall m \in \mathbb{N}.$$

É claro que se os coeficientes de um polinómio f são todos divisíveis por m , e portanto f se identifica, enquanto polinómio com coeficientes módulo p , com o polinómio nulo, a equação modular

$$f(x) \equiv 0 \pmod{m}$$

tem todas as classes de congruência como solução.

Nota 1.1 *É importante compreender bem os diferentes significados da congruência entre dois polinómios.*

Quando consideramos polinómios numa variável real (ou racional, ou inteira)

dizemos, por exemplo, que $f(x) = g(x)$ se, quando representados sob a forma de uma soma de monómios, os coeficientes de f e de g de cada x^k são iguais. Essa condição é equivalente, por sua vez, a que f e g são iguais como funções, ou seja, tomam o mesmo valor para cada escolha de um valor para a variável x .

Quando consideramos polinómios definidos em \mathbb{Z}/m , e com coeficientes nesse conjunto, estas duas noções já não são equivalentes: se f e g têm os mesmos coeficientes (mais precisamente, se os coeficientes de f e de g de x^k são congruentes \pmod{m} para todo o k) eles representam a mesma função, ou seja tomam o mesmo valor para cada valor de x ; mas, por exemplo, se p é primo, o Teorema de Fermat diz-nos que os polinómios representados por x^p e por x representam a mesma função em \mathbb{Z}/p , e, no entanto, não têm os mesmos coeficientes.

Resumindo,

$$f(x) \equiv g(x) \pmod{m}$$

(congruência dos coeficientes) implica

$$f(x) \equiv g(x) \pmod{m} \forall x$$

mas a recíproca não é verdadeira.

No que se segue, esta distinção não levanta problemas, mas usaremos estas duas formas e a expressão “congruentes como polinómios” ou outra semelhante para frisar os casos em que dois polinómios são idênticos no sentido mais forte referido.

Nota 1.2 *Pode parecer que estamos a introduzir uma restrição à teoria por considerarmos apenas polinómios e não outras funções. O que se passa é que qualquer função*

$$f : \mathbb{Z}/m \rightarrow \mathbb{Z}/m$$

pode ser representada por um polinómio com coeficientes em \mathbb{Z}/m . Esse facto (cuja demonstração é deixada como exercício) não é assim tão surpreendente se nos lembrarmos que para qualquer conjunto finito $\{(a_i, b_i) \in \mathbb{Z} \times \mathbb{Z} : 0 \leq$

$i < m\}$, existe um polinómio $f(x)$ com coeficientes inteiros e grau menor ou igual a m tal que $f(a_i) = b_i$ para todo o i .

O Teorema Chinês dos Restos implica que para resolver equações do tipo

$$f(x) \equiv 0 \pmod{m}$$

é suficiente resolvê-las no caso

$$f(x) \equiv 0 \pmod{p^j}$$

com p primo.

Vamo-nos concentrar no caso mais simples de equações da forma

$$f(x) \equiv 0 \pmod{p}$$

com p primo.

O problema de determinar em que condições e como obter soluções de

$$f(x) \equiv 0 \pmod{p^j}$$

para os diversos expoentes j , será tratado separadamente.

1.1 Aritmética dos polinómios com coeficientes em \mathbb{Z}_p

O estudo da resolução de equações módulo p (com p primo) é substancialmente simplificado se começarmos por analisar as propriedades aritméticas do conjunto dos polinómios com coeficientes em \mathbb{Z}_p , que designamos por $\mathbb{Z}_p[x]$. Note-se que consideramos os polinómios como expressões algébricas da forma

$$f(x) = \sum_{i=0}^m a_i x^i,$$

sem atribuir necessariamente valores a x , ou seja, de acordo com a observação feita atrás, *não* estamos a identificar um polinómio com a função correspondente

$$f : \mathbb{Z}/p \rightarrow \mathbb{Z}/p, \quad f(u) \equiv \sum_{i=0}^m a_i u^i \pmod{p}.$$

Estão definidas neste conjunto as operações de soma e produto: se

$$f(x) = \sum_{i=0}^m a_i x^i, \quad g(x) = \sum_{i=0}^n b_i x^i,$$

com, por exemplo, $m \geq n$, então

$$f(x) + g(x) \equiv \sum_{i=0}^m (a_i + b_i) x^i$$

e

$$f(x)g(x) = \sum_{i=0}^{m+n} \left(\sum_{k=0}^i a_k b_{i-k} \right) x^i$$

convencionando que nestas expressões $a_k \equiv 0$ para $k > m$ e $b_{i-k} \equiv 0$ se $i - k > n$.

Estas operações satisfazem as mesmas condições verificadas pelas mesmas operações entre inteiros: ambas são comutativas e associativas; o produto é distributivo sobre a soma; existe um elemento neutro para a soma (polinómio 0) e todo o polinómio $f(x)$ tem inverso para a soma, que é $-f(x)$; existe um elemento neutro para o produto (o polinómio 1); vale a lei do corte: se $g(x)h(x) \equiv 0$ e $g(x)$ não é o polinómio nulo, então $h(x) \equiv 0$. Note-se que esta última propriedade decorre de o grau do produto de dois polinómios ser igual à soma dos graus dos factores, como se verifica directamente pela definição de produto (e usando as convenções sobre $-\infty$ referidas no início).

Em particular, temos uma versão do Lema da Divisão:

Lema 1.3 *Dados polinómios $f(x) = \sum_{i=0}^m a_i x^i$ com grau m e $g(x) = \sum_{i=0}^n b_i x^i$ com grau $n \geq 0$, existem um polinómio $q(x)$ e um polinómio $r(x)$ com grau menor que n , unicamente determinados, tais que*

$$f(x) \equiv q(x)g(x) + r(x) \pmod{p}.$$

Sublinhamos mais uma vez que a congruência no enunciado deve ser entendida como congruência dos coeficientes de cada x^i .

Demonstração 1.4 *A demonstração consiste essencialmente na verificação da validade do algoritmo de divisão, que pode ser descrito informalmente do seguinte modo:*

1. se $m < n$, definimos $q(x) = 1$ e $r(x) = f(x)$;
2. caso contrário, inicializamos variáveis $q(x)$, $r(x)$, u e c como

$$q(x) = 0; r(x) = f(x); u = m; c = a_m$$

e, enquanto $u \geq n$, repetimos a rotina

- (a) substituir $r(x)$ por $r(x) - cb_n^{-1}x^{u-n}g(x)$;
- (b) substituir $q(x)$ por $q(x) + cb_n^{-1}x^{u-n}$;
- (c) substituir u pelo grau de $r(x)$ e c pelo coeficiente do termo de maior grau de $r(x)$;

3. os $q(x)$ e $r(x)$ finais são os polinômios pretendidos.

Note-se que b_n^{-1} designa a solução (única módulo p) de $b_n x \equiv 1 \pmod{p}$. O algoritmo está bem definido uma vez que a sucessão de valores da variável u é estritamente decrescente.

Resta verificar a unicidade dos polinômios quociente e resto: o conjunto de polinômios $\{f(x) - s(x)g(x) : s(x) \in \mathbb{Z}/p[x]\}$ contém polinômios com grau mínimo, e o algoritmo mostra que esse grau mínimo é menor que n ; se esse grau mínimo for $-\infty$, ou seja, se existe $q(x)$ tal que $f(x) \equiv q(x)g(x)$, temos $r(x) \equiv 0$ que é o único polinômio com o seu grau, e, pela lei do corte, $q(x)$ é também único. Caso contrário, se existissem $r_1(x)$ e r_2 , ambos com grau mínimo r , e $q_1(x)$ e $q_2(x)$ tais que

$$f(x) \equiv q_1(x)g(x) + r_1(x) \equiv q_2(x)g(x) + r_2(x)$$

então

$$(q_1(x) - q_2(x))g(x) \equiv r_2(x) - r_1(x);$$

se os polinómios $r_i(x)$ fossem distintos, e portanto os $q_i(x)$ também, o polinómio do lado esquerdo tem grau maior ou igual a n , mas o polinómio do lado direito tem grau menor ou igual a $r < n$, uma contradição.

Exemplo 1.5 Se, por exemplo, $p = 13$, $f(x) = x^7 + 3x^5 + 2x^4 + x + 7$ e $g(x) = 2x^2 + x + 3$, temos sucessivamente

$$\begin{aligned}
 x^7 + 3x^5 + 2x^4 + x + 7 &\equiv 7x^5(2x^2 + x + 3) + 6x^6 + 8x^5 + 2x^4 + x + 7 \\
 &\equiv (7x^5 + 3x^4)(2x^2 + x + 3) + 5x^5 + 6x^4 + x + 7 \\
 &\equiv (7x^5 + 3x^4 + 9x^3)(2x^2 + x + 3) + 10x^4 + 12x^3 + x + 7 \\
 &\equiv (7x^5 + 3x^4 + 9x^3 + 5x^2)(2x^2 + x + 3) + 7x^3 + 11x^2 + x + 7 \\
 &\equiv (7x^5 + 3x^4 + 9x^3 + 5x^2 + 10x)(2x^2 + x + 3) + x^2 + 10x + 7 \\
 &\equiv (7x^5 + 3x^4 + 9x^3 + 5x^2 + 10x + 7)(2x^2 + x + 3) + 3x + 12
 \end{aligned}$$

A validade do Lema da Divisão em $\mathbb{Z}/p[x]$ permite agora copiar para este conjunto a construção da teoria da aritmética dos inteiros, com algumas pequenas adaptações: o algoritmo de Euclides pode ser definido, para dois polinómios não nulos $f(x)$ e $g(x)$, exactamente da mesma forma, e tem como resultado um polinómio $d(x)$ que divide ambos, e polinómios $u(x)$ e $v(x)$ tais que

$$d(x) \equiv u(x)f(x) + v(x)g(x),$$

ou seja, $d(x)$ é um máximo divisor comum de $f(x)$ e $g(x)$, uma vez que é um múltiplo de qualquer divisor comum destes dois polinómios.

A verificação da validade do algoritmo é idêntica, e baseia-se mais uma vez no facto de que nas sucessivas divisões

$$r_{j-1}(x) \equiv q_{j+1}(x)r_j(x) + r_{j+1}(x)$$

a sucessã dos graus dos $r_j(x)$ é estritamente decrescente, pelo que se obtém, para algum m , $r_m(x) \equiv 0$. Além disso, podemos tal como no caso dos inteiros, verificar que existem polinómios $u_j(x)$ e $v_j(x)$ que satisfazem

$$u_j(x)f(x) + v_j(x)g(x) \equiv r_j(x)$$

e que, se definirmos, tal como se fez para \mathbb{Z} , $r_{-1}(x) = f(x)$ e $r_0(x) = g(x)$, satisfazem as recorrências

$$u_{-1}(x) = 1, \quad v_{-1}(x) = 0, \quad e \quad u_0(x) = 0, \quad v_0(x) = 1$$

$$u_{j+1}(x) \equiv u_{j-1}(x) - q_{j+1}(x)u_j(x), \quad v_{j+1}(x) \equiv v_{j-1}(x) - q_{j+1}(x)v_j(x).$$

Exemplo 1.6 *Considere-se mais uma vez $p = 13$ e*

$$f(x) = 7x^6 + 5x^4 + x + 2, \quad g(x) = 4x^5 + 5x^3 + 3x^2 + 6.$$

r_i	q_i	u_i	v_i
$7x^6 + 5x^4 + x + 2$		1	0
$4x^5 + 5x^3 + 3x^2 + 6$		0	1
$6x^4 + 11x^3 + 10x + 2$	$5x$	1	$8x$
$4x^3 + 5x^2 + 8x + 7$	$5x + 6$	$8x + 7$	$12x^2 + 4x + 1$
$8x^2 + 12x + 4$	$8x + 9$	$x^2 + 2x + 3$	$8x^3 + 3x^2 + 3x + 4$
$x + 1$	$7x + 8$	$6x^3 + 4x^2 + 10x + 9$	$9x^4 + 6x^3 + 6x^2 + 4x + 8$
0	$8x + 4$	$4x^4 + 9x^3 + 9x^2 + 7x + 6$	$6x^5 + 7x^4 + x^3 + 12x^2 + x + 11$

Portanto, $d(x) \equiv x + 1$ é um máximo divisor de $f(x)$ e $g(x)$, em $\mathbb{Z}_{/13}[x]$, e

$$x + 1 \equiv (6x^3 + 4x^2 + 10x + 9)f(x) + (9x^4 + 6x^3 + 6x^2 + 4x + 8)g(x).$$

No caso dos inteiros, definimos o máximo divisor comum de a e b como o inteiro *positivo* d que satisfaz aquela propriedade, e o algoritmo de Euclides tem como resultado exactamente este d . No caso presente, não temos essa noção de positividade; o que se passa é que, enquanto em \mathbb{Z} só existem dois elementos invertíveis, 1 e -1 , em $\mathbb{Z}_{/p}[x]$ os elementos invertíveis são os polinómios de grau 0, ou seja, as "constantes" não nulas; por isso, se $d(x) = \text{mdc}(f(x), g(x))$, para qualquer $a \in \mathbb{Z}_{/p} \setminus \{0\}$, o polinómio $ad(x)$ também é um máximo divisor comum de $f(x)$ e $g(x)$; se quisermos ter um máximo divisor comum unicamente definido, podemos escolher o polinómio mónico, ou seja com coeficiente de maior grau igual a 1, mas isso não é necessário, não acrescenta nada de útil à teoria, e esse polinómio não é, em geral, o que resulta do algoritmo de Euclides.

Da existência e propriedades do máximo divisor comum deduzem-se, sempre como no caso de \mathbb{Z} , a existência e propriedades dos elementos primos de $\mathbb{Z}/p[x]$, que são os polinómios irredutíveis, ou seja, que não podem ser factorizados em factores de grau positivo. Estes incluem naturalmente os polinómios da forma $x - a$, com $a \in \mathbb{Z}/p$, mas também muitos outros; por exemplo, $f(x) = x^2 + x + 1$ ou $g(x) = x^3 + 2x + 3$ são primos em $\mathbb{Z}_{13}[x]$, mas $x^5 + x^4 + 3x^3 + 5x^2 + 5x + 3 \equiv f(x)g(x)$ não o é, embora não tenha raízes módulo 13.

É claro que se $f(x)$ for irredutível, também $af(x)$ o é, para qualquer $a \in \mathbb{Z}/p^\times$. Podemos convencionar tomar como elementos primos em $\mathbb{Z}/p[x]$ os polinómios irredutíveis mónicos. Com essa convenção, podemos enunciar o Teorema Fundamental da Aritmética para $\mathbb{Z}/p[x]$: todo o polinómio $f(x) \in \mathbb{Z}/p[x]$ tem uma factorização

$$f(x) \equiv ap_1^{k_1}(x) \cdots p_t^{k_t}(x),$$

com $a \in \mathbb{Z}/p$, $p_i(x)$ primo e $k_i > 0$, para todo o $1 \leq i \leq t$, e essa factorização é única a menos da ordem dos factores.

Nota 1.7 *Toda esta linha de raciocínio foi possível porque tomámos p primo. De facto, sem essa hipótese, a divisão de polinómios nem sempre pode ser feita: considere-se por exemplo*

$$f(x) = x^4 - 1 \quad \text{e} \quad g(x) = 2x^2 - 1$$

como polinómios com coeficientes em $\mathbb{Z}/8$. E a teoria desenvolvida acima deixa de valer: por exemplo, um polinómio pode ter mais do que uma factorização em factores irredutíveis: é o que acontece, mais uma vez em $\mathbb{Z}/8[x]$, com

$$x^2 - 1 \equiv (x - 1)(x + 1) \equiv (x - 3)(x + 3).$$

Claro que a propriedade que diferencia \mathbb{Z}/p com p primo dos outros \mathbb{Z}/m é o facto de todos os elementos não nulos terem inverso, ou seja, o facto de \mathbb{Z}/p ser um corpo.

Por outro lado, tudo o que foi dito se aplicaria ao caso de polinómios com

coeficientes num qualquer corpo, por exemplo \mathbb{Q} , etc. Estas ideias serão desenvolvidas e esclarecidas noutros cursos.

Exercícios V.1

1. Seja p primo e $g : \mathbb{Z}/p \rightarrow \mathbb{Z}/p$ uma função qualquer. Verificar que o polinómio definido por

$$F(x) = \sum_{k=0}^{p-1} g(k) (1 - (x - k)^{p-1})$$

satisfaz a condição

$$F(x) \equiv g(x) \pmod{p} \quad \forall x$$

2. Calcular o produto $f(x)g(x)$ com $f(x) = 3x^3 + x^2 + 4x + 1$ e $g(x) = 2x^2 + 3x + 2$ polinómios com coeficientes em $\mathbb{Z}/5$.
3. Resolver o problema anterior considerando os polinómios como tendo coeficientes em $\mathbb{Z}/7$.
4. Aplicar o algoritmo da divisão aos polinómios com coeficientes em \mathbb{Z}_5 $f(x) = x^6 - x$ e $g(x) = 2x^3 + x + 4$.
5. Dados $f(x), g(x) \in \mathbb{Z}_5[x]$,

$$f(x) = 2x^5 + x^3 + 4x^2 + 2x + 1, \quad g(x) = x^3 + 3x + 1,$$

calcular, pelo algoritmo de Euclides estendido para polinómios, um máximo divisor comum $d(x)$ e polinómios $u(x)$ e $v(x)$ satisfazendo

$$d(x) = u(x)f(x) + v(x)g(x).$$

1.2 Equações com módulo primo

Regressamos agora ao problema da resolução de equações modulares com módulo primo.

Proposição 1.8 *Se $f(x) \in \mathbb{Z}/p$ tem grau $n \geq p$, então ou existe um polinómio $g(x)$ com grau $n - p$ tal que se tem a congruência de polinómios*

$$f(x) \equiv (x^p - x)g(x) \pmod{p}$$

e todas as classes de congruência são solução da equação

$$f(x) \equiv 0 \pmod{p},$$

ou existe um polinómio $r(x)$ de grau $< p$ tal que a equação

$$r(x) \equiv 0 \pmod{p}$$

tem exactamente as mesmas soluções que a anterior.

Demonstração 1.9 *Fazemos a divisão de polinómios*

$$f(x) = (x^p - x)g(x) + r(x)$$

onde r será um polinómio de grau estritamente menor que p ; se os seus coeficientes forem todos divisíveis por p temos a congruência

$$f(x) \equiv (x^p - x)g(x) \pmod{p}$$

e como, pelo Teorema de Fermat, todas as classes de congruência são zeros do segundo membro, têm também que o ser do primeiro. Caso contrário temos a congruência

$$f(x) \equiv (x^p - x)g(x) + r(x) \pmod{p}$$

e se $f(a) \equiv 0$, como $a^p - a \equiv 0$ também, temos necessariamente $r(a) \equiv 0$. Reciprocamente, se $r(a) \equiv 0$, temos pelo mesmo raciocínio que $f(a) \equiv 0$.

Na prática, se estamos apenas interessados na resolução da equação, não precisamos de efectuar a divisão de polinómios, e basta reduzir os expoentes superiores a $p - 1$ por intermédio do Teorema de Fermat.

Exemplo 1.10 Com $p = 17$,

$$x^{23} + 3x^{19} + x^3 + 2 \equiv x^7 + 4x^3 + 2 \pmod{17} \quad \forall x$$

Podemos chegar a essa conclusão aplicando repetidamente o Teorema de Fermat ou fazendo a divisão de polinômios para concluir que

$$x^{23} + 3x^{19} + x^3 + 2 \equiv (x^{17} - x)(x^6 + 3x^2) + x^7 + 4x^3 + 2 \pmod{17}.$$

Nota 1.11 No exemplo anterior, temos mesmo uma igualdade de polinômios de coeficientes inteiros. O lema da divisão aplica-se à divisão entre polinômios de coeficientes inteiros, desde que o divisor seja mônico. Portanto podemos realizar a divisão como se se tratasse de polinômios com coeficientes inteiros e só reduzir os coeficientes módulo p no fim, ou, em alternativa, como fizemos na secção anterior, podemos considerar sempre que os coeficientes são classes de congruência.

Podemos portanto considerar apenas equações

$$f(x) \equiv 0 \pmod{p}$$

de grau menor que p e podemos até assumir que o coeficiente do termo de maior grau é 1 (caso contrário, dividimos a congruência por esse coeficiente, ou seja, multiplicamos pelo seu inverso \pmod{p}).

Lema 1.12 *Seja*

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$

um polinômio com coeficientes inteiros.

Se $f(c) \equiv 0 \pmod{p}$, então existe um polinômio $g(x)$ de coeficientes inteiros, mônico e de grau $n - 1$, tal que

$$f(x) \equiv (x - c)g(x) \pmod{p}$$

Demonstração 1.13 *Temos*

$$\begin{aligned} f(x) &\equiv f(x) - f(c) \equiv \\ &\equiv x^n - c^n + a_{n-1}(x^{n-1} - c^{n-1}) + \cdots + a_1(x - c) \pmod{p} \end{aligned}$$

Ora, para qualquer $k > 0$,

$$\begin{aligned} x^k - c^k &= (x - c)(x^{k-1} + x^{k-2}c + \cdots + xc^{k-2} + c^{k-1}) = \\ &= (x - c) \sum_{i=0}^{k-1} x^{k-1-i} c^i \end{aligned}$$

o que nos dá a factorização desejada, restando verificar que o polinómio $g(x)$ assim obtido é de facto mónico e tem grau $n - 1$.

A teoria desenvolvida na secção anterior implica que se $f(x)$ é um polinómio de grau n , a equação

$$f(x) \equiv 0 \pmod{p}$$

não pode ter mais do que n soluções distintas: de facto essas soluções correspondem a factores da forma $(x - c)$ na factorização de $f(x)$ em factores primos. Podemos mesmo deduzir

Proposição 1.14 *Um polinómio $f(x)$ de grau n pode ser factorizado na forma*

$$f(x) \equiv (x - c_1)^{k_1} (x - c_2)^{k_2} \cdots (x - c_t)^{k_t} h(x) \pmod{p}$$

com $h(x)$ um polinómio mónico de grau $n - k_1 - k_2 - \cdots - k_t$, sem raízes módulo p .

Em particular, o número de raízes, contando as multiplicidades, é sempre menor ou igual que n .

Proposição 1.15 *Seja $f(x)$ de grau $n < p$. Se na divisão de $x^p - x$ por f*

$$x^p - x = f(x)g(x) + r(x)$$

$r(x) \equiv 0$, a equação

$$f(x) \equiv 0 \pmod{p}$$

tem exactamente n soluções. Caso contrário, todas as soluções desta equação são também soluções de

$$r(x) \equiv 0 \pmod{p}$$

Demonstração 1.16 No primeiro caso temos a congruência

$$x^p - x \equiv f(x)g(x) \pmod{p}$$

onde f tem grau n e g tem grau $p - n$; pela proposição anterior f não pode ter mais que n zeros e g não pode ter mais que $n - p$ zeros módulo p . Mas pelo Teorema de Fermat o seu produto tem exactamente p zeros; isso só pode acontecer se cada um dos factores tiver n e $p - n$ zeros respectivamente.

No segundo caso temos a congruência

$$x^p - x \equiv f(x)g(x) + r(x) \pmod{p}$$

e se $f(a) \equiv 0$ temos

$$r(a) \equiv f(a)g(a) + r(a) \equiv a^p - a \equiv 0 \pmod{p}$$

A aplicação repetida desta proposição pode ajudar a restringir o possível número de soluções de uma congruência módulo p .

Exemplo 1.17 Para determinar o número de soluções de $x^7 + 4x^3 + 2 \equiv 0 \pmod{11}$, podemos começar por calcular

$$x^{11} - x = (x^7 + 4x^3 + 2)(x^4 - 4) + (-2x^4 + 16x^3 - x + 8)$$

e concluímos que todas as soluções daquela equação são também soluções de

$$-2x^4 + 16x^3 - x + 8 \equiv 0 \pmod{11} \Leftrightarrow x^4 + 3x^3 - 5x + 7 \equiv 0 \pmod{11}$$

E se quisermos simplificar ainda mais podemos dividir de novo verificando que

$$x^{11} - x \equiv (x^4 + 3x^3 - 5x + 7)(x^7 + 8x^6 + 9x^5 + 3x + 2) + 5x^3 + 4x^2 + 10x + 8 \pmod{11} \quad \forall x$$

e que portanto é suficiente encontrar as soluções de

$$5x^3 + 4x^2 + 10x + 8 \equiv 0 \pmod{11}$$

e assim por diante.

Um procedimento mais eficiente seria o de aplicar o algoritmo de Euclides para $\mathbb{Z}/_{11}[x]$ aos polinómios $x^{11} - x$ e $f(x) = x^7 + 4x^3 + 2$; o máximo divisor comum é o produto $a(x - c_1)(x - c_2) \cdots (x - c_t)$ onde c_1, c_2, \dots, c_t são as raízes distintas de $f(x)$ módulo p , se existirem, ou uma constante não nula caso contrário, caso em que $f(x)$ e $x^{11} - x$ são primos entre si.

Um exemplo particularmente importante de aplicação daquele resultado:

Corolário 1.18 *Dado p primo, se $d \mid (p - 1)$ então a equação*

$$x^d \equiv 1 \pmod{p}$$

tem exactamente d soluções.

Demonstração 1.19 *De facto, se $p - 1 = de$ temos a factorização*

$$x^{p-1} - 1 = (x^d - 1)(x^{d(e-1)} + \cdots + x^d + 1)$$

Exercícios V.2

1. Notando que $7^2 \equiv 5 \pmod{11}$, determinar, sem ser por tentativa e erro, quais as soluções de

$$x^{12} + 3x^{11} + 5 \equiv 0 \pmod{11}$$

2. Determinar (sem esforço...) a única solução da equação

$$47x^{120} + 7x^{100} + 54x^{20} + 25x + 2 \equiv 0 \pmod{101}$$

3. Verificando que

$$x^{11} - x \equiv (x^3 + 2x^2 + 5x + 6)(x^8 - 2x^7 - x^6 + 6x^5 + 3x^4 + 3x^3 - 2x^2 + 4x + 6) + 2x^2 - 3$$

determinar se existem e quais são as soluções de $x^3 + 2x^2 + 5x + 6 \equiv 0 \pmod{11}$.

4. Mostrar que, se

$$1 + \frac{1}{2} + \cdots + \frac{1}{p-1} = \frac{a}{b},$$

onde p é um primo ímpar, então $p \mid a$.

Sugestão : Notar que

$$x^{p-1} - 1 \equiv (x-1) \cdots (x-(p-1)) \pmod{p}$$

1.3 Ordem de um inteiro módulo p e raízes primitivas

Se a é primo com p sabemos que $a^{p-1} \equiv 1 \pmod{p}$. No entanto pode haver outros valores de k para os quais se verifique $a^k \equiv 1 \pmod{p}$.

Designamos *ordem* de a módulo p o menor inteiro positivo $ord_p(a)$ que satisfaz essa condição. Se não houver dúvidas em relação a qual o módulo usaremos a notação abreviada $ord(a)$.

Evidentemente $ord_p(1) = 1$ e $ord_p(-1) = 2$ para todo o primo p ímpar. Outros exemplos:

$$ord_5(3) = 4, \quad ord_7(2) = 3, \quad ord_{11}(4) = 5$$

Exemplo 1.20 *Seja por exemplo $p = 11$. A tabela seguinte apresenta as potências $x^k \pmod{11}$, com o valor de x nas linhas e o de k nas colunas*

	1	2	3	4	5	6	7	8	9	10
1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	5	10	9	7	3	6	1
3	3	9	5	4	1	3	9	5	4	1
4	4	5	9	3	1	4	5	9	3	1
5	5	3	4	9	1	5	3	4	9	1
6	6	3	7	9	10	5	8	4	2	1
7	7	5	2	3	10	4	6	9	8	1
8	8	9	6	4	10	3	2	5	7	1
9	9	4	3	5	1	9	4	3	5	1
10	10	1	10	1	10	1	10	1	10	1

Conclui-se que

$$\text{ord}_{11}(2) = \text{ord}_{11}(6) = \text{ord}_{11}(7) = \text{ord}_{11}(8) = 10$$

enquanto que

$$\text{ord}_{11}(3) = \text{ord}_{11}(4) = \text{ord}_{11}(5) = \text{ord}_{11}(9) = 5.$$

Proposição 1.21 Fixando um primo p ,

- 1) Se $\text{ord}(a) = k$ e $a^h \equiv 1 \pmod{p}$ então $k \mid h$. Em particular $\text{ord}(a) \mid p-1$.
- 2) Se $\text{ord}(a) = k$ e $ab \equiv 1 \pmod{p}$ então $\text{ord}(b) = k$.
- 3) Se $\text{ord}(a) = k$ então $\text{ord}(a^j) = \frac{k}{d}$ em que $d = \text{mdc}(k, j)$.
- 4) Se $\text{ord}(a) = k$, $\text{ord}(b) = h$ e $\text{mdc}(k, h) = 1$ então $\text{ord}(ab) = kh$.

Demonstração 1.22 1) dividindo h por k temos $h = qk + r$ com $0 \leq r < k$; então

$$1 \equiv a^h = a^{qk+r} = (a^k)^q a^r \equiv a^r \pmod{p}$$

porque $a^k \equiv 1 \pmod{p}$; mas pela definição de ordem tem que ser $r = 0$.

3) por um lado

$$(a^j)^{\frac{k}{d}} = (a^k)^{\frac{j}{d}} \equiv 1 \pmod{p}$$

e portanto $\text{ord}_p(a^j) \mid \frac{k}{d}$. Mas por outro se $\text{ord}_p(a^j) = l$,

$$1 \equiv (a^j)^l = a^{jl} \pmod{p},$$

logo $k \mid (jl)$ o que implica

$$\frac{k}{d} \mid \frac{j}{d}l \implies \frac{k}{d} \mid l$$

uma vez que $\text{mdc}(\frac{k}{d}, \frac{j}{d}) = 1$.

4) em primeiro lugar, uma vez que

$$(ab)^{kh} = a^{kh}b^{kh} \equiv 1 \pmod{p}$$

é evidente, por **1** que $\text{ord}(ab) \mid kh$. Mas, se $\text{ord}(ab) = j$ então

$$a^{jh} \equiv a^{jh}b^{jh} \equiv 1 \pmod{p}$$

e de novo por **1** temos que $k \mid jh$; como k e h são primos entre si isso implica que $k \mid j$. Do mesmo modo conclui-se que $h \mid j$ e portanto, mais uma vez porque k e h são primos entre si, $(kh) \mid j$.

A demonstração de 2) é deixada como exercício.

A definição de ordem e as propriedades aritméticas enunciadas generalizam-se a módulos compostos m , naturalmente para classes de congruência primas com m .

Definição 1.23 Uma classe de congruência módulo m com ordem $\text{ord}_m(a) = \phi(m)$ chama-se uma **raiz primitiva** de m .

O conhecimento de raízes primitivas de um módulo, ou até o mero conhecimento da sua existência, pode contribuir em muito, como veremos mais adiante, para a compreensão e a resolução de certas equações.

Vamos em seguida mostrar que um módulo p primo tem sempre raízes primitivas.

Seja q^j um factor de $p-1$ com q primo; por um Corolário de uma Proposição anterior sabemos que existem q^j classes de congruência que são solução de

$$x^{q^j} \equiv 1 \pmod{p}$$

ou seja, cuja ordem módulo p divide q^j . Dada uma dessas soluções a , teremos $\text{ord}_p(a) = q^j$ se e só se $a^{q^{j-1}}$ não for congruente com 1. Mas o mesmo corolário garante que existem q^{j-1} soluções de

$$x^{q^{j-1}} \equiv 1 \pmod{p}$$

Conclui-se portanto que

Proposição 1.24 *Se q^j é um factor de $p-1$ com q primo, existem $q^j - q^{j-1}$ classes com ordem q^j módulo p .*

Se $p-1 = q_1^{j_1} q_2^{j_2} \cdots q_r^{j_r}$ for a factorização em factores primos de $p-1$, por cada escolha de classes a_1 com ordem $q_1^{j_1}$, a_2 com ordem $q_2^{j_2}$, etc., a classe

$$a = a_1 a_2 \cdots a_r$$

terá, pela propriedade 4 da proposição acima, ordem $q_1^{j_1} q_2^{j_2} \cdots q_r^{j_r} = p-1$. Uma vez que existem $q_i^{j_i} - q_i^{j_i-1}$ escolhas para cada a_i e que

$$\prod_{i=1}^r (q_i^{j_i} - q_i^{j_i-1}) = \phi(p-1)$$

concluimos que

Teorema 1.25 *Dado p primo, existem $\phi(p-1)$ raízes primitivas para o módulo p .*

Prova-se que m tem raízes primitivas se e só se

$$m \in \{1, 2, 4, p^k, 2p^k | p \text{ primo ímpar}\}$$

Nota 1.26 *Existem numerosos problemas em aberto relacionados com raízes primitivas. O mais significativo é talvez a*

Conjectura de Artin Generalizada: *Todo o inteiro diferente de -1 e que não seja um quadrado perfeito é uma raiz primitiva para infinitos primos.*

Embora se tenha provado que existem no máximo três inteiros para os quais a conjectura é falsa, continua por provar até a conjectura original de Artin (formulada há mais de 80 anos)

Conjectura de Artin: *Existem infinitos primos para os quais 2 é uma raiz primitiva.*

O conhecimento de uma raiz primitiva de p permite muitas vezes simplificar os cálculos e os raciocínios acerca de equações modulares. Eis um exemplo:

1.4 Raízes módulo p

Voltemos à equação

$$x^k \equiv b \pmod{p}$$

agora com módulo primo. Sabemos que se $\text{mdc}(k, p-1) = 1$ a solução é única e pode ser determinada por aplicação do algoritmo de Euclides e do cálculo de potências módulo p . Vamos deduzir uma generalização desse resultado.

Suponhamos que g é uma raiz primitiva de p e que $g^j \equiv b$. Se x for uma solução da equação e $x \equiv g^i$, aquela reduz-se a

$$g^{ki} \equiv g^j \pmod{p}$$

e esta congruência, como g é raiz primitiva, equivale a

$$ki \equiv j \pmod{p-1}$$

Recorde-se que se $d = \text{mdc}(k, p-1)$ esta equação tem d soluções se $d \mid j$ e não tem soluções caso contrário. Mas se $d \mid j$ então

$$b^{\frac{p-1}{d}} \equiv g^{j\frac{p-1}{d}} \equiv \left(g^{j/d}\right)^{p-1} \equiv 1 \pmod{p}$$

Reciprocamente se $b^{\frac{p-1}{d}} \equiv g^{j\frac{p-1}{d}} \equiv 1 \pmod{p}$ então

$$(p-1) \mid j\frac{p-1}{d}$$

o que implica que $d \mid j$.

Deduzimos portanto a

Proposição 1.27 (Critério de Euler): *Seja p primo, b primo com p , $k > 1$ e $d = \text{mdc}(k, p-1)$. Então a equação*

$$x^k \equiv b \pmod{p}$$

tem d soluções se

$$b^{\frac{p-1}{d}} \equiv 1 \pmod{p}$$

e não tem soluções caso contrário.

A designação de critério de Euler é normalmente usada apenas para o caso $k = 2$. Usamo-la aqui para o caso geral para facilitar a identificação do resultado.

O critério generaliza-se também ao caso de um módulo m para o qual exista uma raiz primitiva, com as condições b primo com m e $d = \text{mdc}(k, \phi(m))$.

Exemplo 1.28 *Mostrar que a equação*

$$x^5 \equiv 6 \pmod{101}$$

tem 5 soluções.

Uma vez que $\text{mdc}(5, 100) = 5$ basta mostrar que $6^{20} \equiv 1 \pmod{101}$.

Note-se que o critério de Euler não permite calcular as soluções. Mas se soubermos que 2 é uma raiz primitiva de 101 e que $2^{70} \equiv 6 \pmod{101}$, a dedução feita diz-nos que as soluções são as classes 2^i com i solução de

$$5i \equiv 70 \pmod{100} \Leftrightarrow i \equiv 14 \pmod{20}$$

ou seja são as classes 2^{14+20l} com $l \in \{0, 1, 2, 3, 4\}$.

Exercícios V.3

1. Se g é raiz primitiva de p , para que valores de k é que g^k também é raiz primitiva?

2. Mostrar que se $a = b^2$ então a não pode ser raiz primitiva de um primo p ímpar.

Sugestão: se a é raiz primitiva, então existe $s < p - 1$ tal que $a^s \equiv b \pmod{p}$.

3. Sabendo que 5 é uma raiz primitiva de 47 e que $5^{16} \equiv 17 \pmod{47}$, determinar as soluções da equação “exponencial”

$$25^x \equiv 17 \pmod{47}$$

4. Se p é um primo ímpar, para quantos $a \in \mathbb{Z}/p$ é que

$$x^2 \equiv a \pmod{p}$$

tem solução?

Sugestão: Seja g uma raiz primitiva de p e $g^k \equiv a$. Estudar a existência de solução em função da paridade de k .

5. Mostrar que se p é primo ímpar então

$$x^2 \equiv -1 \pmod{p}$$

tem solução se e só se $p \equiv 1 \pmod{4}$.

6. Mostrar que existem infinitos primos congruentes com 1 módulo 4.

Sugestão: Dados primos p_1, p_2, \dots, p_k congruentes com 1 módulo 4, considerar os factores primos de

$$(p_1 p_2 \cdots p_k)^2 + 1$$

7. Mostrar que se p e q são primos ímpares diferentes e a é primo com pq ,

$$a^{\phi(pq)/2} \equiv 1 \pmod{pq}.$$

Concluir que pq não tem raízes primitivas.

8. Usar o critério de Euler para determinar quais das seguintes equações têm solução e qual o seu número

a) $x^{12} \equiv 16 \pmod{17}$;

b) $x^{20} \equiv 13 \pmod{17}$;

c) $x^{48} \equiv 9 \pmod{17}$;

d) $x^{11} \equiv 9 \pmod{17}$;

9. Mostrar que $3^8 \equiv -1 \pmod{17}$. Justificar porque é que podemos concluir que 3 é raiz primitiva de 17.

Usar uma lista das classes de congruência de $3^i \pmod{17}$ para encontrar as soluções do problema anterior.

10. 3 é raiz primitiva módulo 31 e $3^{12} \equiv 8 \pmod{31}$. Determinar as soluções de

$$x^4 \equiv 8 \pmod{31}.$$

11. Neste exercício vamos verificar que se p é um primo ímpar, existem raízes primitivas módulo p^k , para todo o $k > 0$. Mais precisamente, se a é raiz primitiva módulo p , provamos que ou a ou $a + p$ é raiz primitiva módulo p^k .

a) Justificar que as ordens de a e de $a + p$ módulo p^k são divisíveis por $p - 1$ e portanto são da forma $p^j(p - 1)$ com $j < k$.

b) Mostrar, usando o Teorema do binómio de Newton, que

$$(a + p)^{\phi(p^{k-1})} \equiv a^{\phi(p^{k-1})} - p^{k-1} a^{\phi(p^k)-1} \pmod{p^k}.$$

Sugestão: Tem que se mostrar que, para $j \geq 2$,

$$\binom{\phi(p^{k-1})}{j} p^j \equiv 0 \pmod{p^k};$$

começar por mostrar que p^{j-1} não divide $j!$.

c) Concluir que, se a não é raiz primitiva módulo p^k , então

$$(a + p)^{\phi(p^{k-1})} \not\equiv 1 \pmod{p^k},$$

e deduzir que, nesse caso, $(a + p)$ é raiz primitiva módulo p^k .

12. Mostrar que, se p é primo e $a, b \in \mathbb{Z}$,

$$(a + b)^p \equiv a^p + b^p \pmod{p}.$$

13. Recorde-se a dedução do critério e fórmula resolvente para polinómios de grau 2: suponhamos que

$$f(x) = ax^2 + bx + c$$

e $a > 0$; então

$$f(x) = 0 \Leftrightarrow x^2 + \frac{b}{a}x + \frac{c}{a} = 0$$

Mas

$$\begin{aligned} x^2 + \frac{b}{a}x + \frac{c}{a} &= x^2 + 2\frac{b}{2a}x + \frac{b^2}{4a^2} + \frac{c}{a} - \frac{b^2}{4a^2} = \\ &= \left(x + \frac{b}{2a}\right)^2 + \frac{4ac - b^2}{4a^2} \end{aligned}$$

Portanto, $f(x) = 0$ se e só se

$$\left(x + \frac{b}{2a}\right)^2 = \frac{b^2 - 4ac}{4a^2}$$

Se $b^2 - 4ac < 0$ não existe solução em \mathbb{R} ; se $b^2 - 4ac = 0$, existe uma única solução $x = -\frac{b}{2a}$; se $b^2 - 4ac > 0$ existem duas soluções:

$$x = -\frac{b}{2a} \pm \sqrt{\frac{b^2 - 4ac}{4a^2}} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Supondo agora que p é um primo ímpar, e a, b, c são inteiros, deduzir um critério e uma fórmula semelhante para a congruência

$$f(x) \equiv 0 \pmod{p}$$

1.4.1 A Lei da Reciprocidade Quadrática: uma breve introdução

No caso de uma equação de grau 2, o critério de Euler, para um módulo primo ímpar p , pode enunciar-se do seguinte modo:

Proposição 1.29 *Se p é um primo ímpar e $a \in \mathbb{Z}$ é primo com p , então ou*

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

e a equação $x^2 \equiv a \pmod{p}$ tem duas soluções; ou

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

e a equação $x^2 \equiv a \pmod{p}$ não tem solução.

Definição 1.30 *Dado p primo ímpar e $a \in \mathbb{Z}$ primo com p , a diz-se um **resíduo quadrático** \pmod{p} se $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.*

O critério de Euler permite portanto determinar, para um dado p , quais os seus resíduos quadráticos, e é fácil verificar que existem exactamente $\frac{p-1}{2}$. Mas quer o aprofundamento da Teoria Aritmética dos Inteiros (e da Teoria dos Números Algébricos), quer as aplicações práticas, como por exemplo o desenvolvimento de algoritmos de factorização, conduzem, entre outras, à pergunta inversa:

Dado um inteiro a , quais os primos para os quais a é resíduo quadrático?

Exemplo 1.31 *Um problema aritmético relacionado com este é o seguinte: uma forma quadrática em duas variáveis (nos inteiros) é uma função*

$$f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}, \quad f(x, y) = ax^2 + bxy + cy^2,$$

onde $a, b, c \in \mathbb{Z}$. O problema fundamental sobre formas quadráticas é a existência de soluções (diferentes de $(0, 0)$) da equação $f(x, y) = 0$.

Uma condição necessária evidente para que a equação tenha solução é que

$$f(x, y) \equiv 0 \pmod{p}$$

para todo o primo p .

No caso de a não ser múltiplo de p , a última equação é equivalente (exercício)

$$(2ax + by)^2 - (b^2 - 4ac)y^2 \equiv 0 \pmod{p}$$

que tem soluções não triviais se e só se o discriminante $b^2 - 4ac$ for um resíduo quadrático módulo p .

De facto (exercício), a é resíduo quadrático módulo p se e só se existem x e y co-primos satisfazendo

$$p \mid (x^2 - ay^2).$$

Notação 1.32 No que se segue, p e q designam sempre primos ímpares.

O matemático francês Legendre (1752-1833) introduziu, no decurso das suas investigações sobre este tipo de problemas, a seguinte notação:

Definição 1.33 Dado p e $a \in \mathbb{Z}$, o símbolo $(a|p)$ define-se como

$$(a|p) = \begin{cases} 0 & \text{se } p \mid a \\ 1 & \text{se } a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \\ -1 & \text{se } a^{\frac{p-1}{2}} \equiv -1 \pmod{p} \end{cases}$$

Ou seja, $(a|p) \in \{-1, 0, 1\}$ e $(a|p) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

O símbolo de Legendre tem as seguintes propriedades, de verificação imediata a partir da definição:

1. $(1|p) = 1$ para todo o p ;
2. $(-1|p) = 1$ se $p \equiv 1 \pmod{4}$, e $(-1|p) = -1$ se $p \equiv 3 \pmod{4}$;
3. $(a + kp|p) = (a|p)$;
4. $(ab|p) = (a|p)(b|p)$.

É possível determinar diversas relações entre $(a|p)$ e a multiplicação de a pelos elementos de \mathbb{Z}/p . Uma delas, descoberta por Gauss, é a seguinte:

Definição 1.34 Um conjunto $S \subset \mathbb{Z}$ com $\frac{p-1}{2}$ elementos diz-se um conjunto de Gauss módulo p se $S \cup -S \cup \{0\}$ constituir um sistema completo de resíduos módulo p , onde

$$-S = \{-x : x \in S\}.$$

Exemplo 1.35 Dois exemplos simples de conjuntos de Gauss módulo p são

- $\{1, 2, \dots, \frac{p-1}{2}\} = \{i : 1 \leq i \leq \frac{p-1}{2}\};$
- $\{1, 3, \dots, p-2\} = \{2i-1 : 1 \leq i \leq \frac{p-1}{2}\}.$

Pela definição de conjunto de Gauss, vemos imediatamente que, fixando a , para cada $x \in S$ existem $u(x) \in S$ e $e(x) \in \{1, -1\}$ (dependentes de a , claro), únicos, tais que

$$ax \equiv e(x)u(x) \pmod{p};$$

mas, além disso, a função

$$s_a : S \rightarrow S, \quad s_a(x) = u(x)$$

é uma bijecção: se $x, y \in S$ e $u(x) = u(y)$, então, módulo p ,

$$ay \equiv e(y)u(y) = e(y)u(x) = e(y)e(x)e(x)u(x) \equiv \pm ax,$$

e portanto, como a é primo com p ,

$$x \equiv \pm y \pmod{p};$$

mas isso só pode acontecer se $x = y$.

Em consequência, $\prod_{x \in S} x = \prod_{x \in S} u(x)$; multiplicando por $a^{\frac{p-1}{2}}$,

$$\begin{aligned} a^{\frac{p-1}{2}} \prod_{x \in S} x &= \prod_{x \in S} ax \equiv \prod_{x \in S} e(x)u(x) = \\ &= \prod_{x \in S} e(x) \prod_{x \in S} u(x) = \prod_{x \in S} e(x) \prod_{x \in S} x, \end{aligned}$$

e dividindo ambos os lados da congruência por $\prod_{x \in S} x$, obtemos $a^{\frac{p-1}{2}} \equiv \prod_{x \in S} e(x)$, mod p .

Demonstrámos assim o

Proposição 1.36 (Critério de Gauss) *Seja $p = 2m + 1$, a primo com p e S um conjunto de Gauss módulo p . Seja t o número de $x \in S$ tais que $e(x) = -1$ (ou seja, aqueles para os quais $ax \equiv -x' \pmod{p}$ para algum $x' \in S$). Então $(a|p) = (-1)^t$.*

Nota 1.37 *Cada escolha de conjunto de Gauss corresponde a uma definição particular de t . Por exemplo, se $S = \{2i - 1 : 1 \leq i \leq \frac{p-1}{2}\}$, e definirmos $b(i)$ pela condição*

$$a(2i - 1) \equiv b(i) \pmod{p} \text{ e } 0 < b(i) < p,$$

é fácil ver (exercício) que

$$e(2i - 1) = -1 \Leftrightarrow b(i) \text{ é par.}$$

Esta escolha de conjunto de Gauss será útil mais adiante.

Exemplo 1.38 *Sejam por exemplo $p = 13$ e $a = 5$; a tabela abaixo mostra os valores dos $b(i)$:*

$2i - 1$	1	3	5	7	9	11
$b(i)$	5	2	12	9	6	3

Há três $b(i)$ pares, e portanto $(5|13) = (-1)^3 = -1$, como se pode comprovar verificando que $5^6 \equiv -1 \pmod{13}$.

Esta proposição já permite esclarecer o valor de $(2|p)$: consideremos o conjunto de Gauss

$$S = \left\{ i : 1 \leq i \leq \frac{p-1}{2} \right\};$$

neste caso, $2i \equiv e(i)u(i) \pmod{p}$ implica que

$$e(i) = -1 \Leftrightarrow \frac{p-1}{2} < 2i \leq p-1 \Leftrightarrow \frac{p-1}{4} < i \leq \frac{p-1}{2};$$

o número t de inteiros i satisfazendo estas desigualdades é

$$\begin{cases} \frac{p-1}{4} & \text{se } p \equiv 1 \pmod{4} \\ \frac{p+1}{4} & \text{se } p \equiv 3 \pmod{4} \end{cases}$$

Como se verifica facilmente,

- se $p \equiv 1 \pmod{4}$ então

t é par se $p \equiv 1 \pmod{8}$,

t é ímpar se $p \equiv 5 \pmod{8}$;

- se $p \equiv 3 \pmod{4}$ então

t é par se $p \equiv 7 \pmod{8}$,

t é ímpar se $p \equiv 3 \pmod{8}$.

Resumindo,

$$(2|p) = \begin{cases} 1 & \text{se } p \equiv \pm 1 \pmod{8} \\ -1 & \text{se } p \equiv \pm 3 \pmod{8} \end{cases}.$$

Deixa-se como exercício a demonstração deste resultado usando o conjunto de Gauss $S = \{2i - 1 : 1 \leq i \leq \frac{p-1}{2}\}$.

Pelas propriedades elementares enunciadas atrás e por este último resultado, o cálculo do símbolo de Legendre reduz-se ao do caso $(q|p)$ para q primo. O caso $q = 2$ poderia sugerir que deveríamos poder determinar $(q|p)$ através de algumas condições modulares sobre q e p . O que se verifica é que o que podemos obter é uma relação entre os símbolos $(q|p)$ e $(p|q)$: concretamente, a análise de diversos casos particulares conduziu Euler, Legendre e Gauss a conjecturar a seguinte

Teorema 1.39 (Lei da Reciprocidade Quadrática) *Dados primos ímpares p e q*

$$(p|q)(q|p) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}.$$

Por outras palavras, $(q|p) = (p|q)$ se pelo menos um dos dois primos é congruente com 1 módulo 4; se p e q são ambos congruentes com 3 módulo 4, então $(q|p) = -(p|q)$.

Gauss foi o primeiro a conseguir provar este resultado, tendo apresentado várias demonstrações.

Demonstração 1.40 *Fixamos os conjuntos de Gauss*

$$S_p = \{2i - 1 : 1 \leq i \leq \frac{p-1}{2}\}, \quad S_q = \{2i - 1 : 1 \leq i \leq \frac{q-1}{2}\}.$$

De acordo com a observação feita atrás sobre estes conjuntos de Gauss, $(q|p) = (-1)^t$ onde t é o número de $x \in S_p$ tais que $qx = py + u$ com $0 < u < p$ par. Notamos que para isso acontecer y tem que ser ímpar e $0 < y \leq q-2$ (exercício), ou seja, $y \in S_q$. Reciprocamente, se $x \in S_p$, $y \in S_q$ e $0 < qx - py < p$ então existe $x' \in S_p$ tal que $qx \equiv -x' \pmod{p}$, ou seja, $e(x) = -1$ e x é um dos elementos de S_p que contribui para t .

Do mesmo modo, $(p|q) = (-1)^s$ onde s o número de $y \in S_q$ tais que $py = qx + v$ com $0 < v < q$ par. De acordo com a discussão anterior, s é portanto o número de $y \in S_q$ para os quais existe $x \in S_p$ tal que $-q < qx - py < 0$.

Esta observação leva-nos a considerar a função

$$R : S_p \times S_q \rightarrow \mathbb{Z}, \quad R(x, y) = qx - py;$$

$R(x, y)$ só toma valores pares não nulos e

$$q - p(q - 2) \leq R(x, y) \leq q(p - 2) - p;$$

além disso, há t pares (x, y) tais que $0 < R(x, y) < p$ e s pares tais que $-q < R(x, y) < 0$, ou seja, há $t + s$ pares (x, y) tais que $-q < R(x, y) < p$.

Mas se $-q < R(x, y) < p$, verifica-se (exercício) que $(p - 1 - x, q - 1 - y) \in S_p \times S_q$ e que $-q < R(p - 1 - x, q - 1 - y) < p$. Portanto $t + s$ é par, a menos que exista um $(x, y) \in S_p \times S_q$ (necessariamente único) tal que

$$p - 1 - x = x, \quad q - 1 - y = y,$$

ou seja que $x = \frac{p-1}{2}$ e $y = \frac{q-1}{2}$ sejam ambos ímpares o que acontece se e só se p e q forem ambos congruentes com 3 módulo 4.

Ilustramos através de um exemplo como, juntamente com as outras propriedades do símbolo de Legendre, o teorema anterior simplifica a determinação do valor de $(a|p)$ e permite responder à pergunta apresentada no início desta secção. O exemplo ilustra igualmente a vantagem da notação de Legendre:

Exemplo 1.41

$$\begin{aligned}
 (42|101) &= (2|101)(3|101)(7|101) = -(3|101)(7|101) \text{ porque } 101 \equiv 5 \pmod{8} \\
 &= -(101|3)(101|7) \text{ porque } 101 \equiv 1 \pmod{4} \\
 &= -(2 + 3 \times 33|3)(3 + 7 \times 14|7) = -(2|3)(3|7) \\
 &= (3|7) \text{ porque } 2 \text{ não é resíduo quadrático } \pmod{3} \\
 &= -(7|3) \text{ porque } 3 \equiv 7 \equiv 3 \pmod{4} \\
 &= -(1 + 3 \times 2|3) = -(1|3) = -1
 \end{aligned}$$

donde se conclui que 42 não é resíduo quadrático módulo 101.