1 Equações modulares não lineares

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

$$f(x) \equiv 0 \mod m,$$

onde

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

é um polinómio com coeficientes em $\mathbb{Z}_m$. Designamos o espaço dos polinómios numa variável x, com coeficientes em $\mathbb{Z}_m$, por $\mathbb{Z}_m[x]$.
Tal como para polinómios com coeficientes reais, definimos 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 m, 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 s'imbolo não tenha aqui outro significado do que satisfazer, por convenção, as propriedades

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

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 $\mod m$ 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, $f(x) = g(x)$ em $\mathbb{Z}_m[x]$ (congruência dos coeficientes) implica

$$f(x) \equiv g(x) \mod m \, \forall x$$

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*

$$f : \mathbb{Z}_{/m} \to \mathbb{Z}_{/m}$$

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

$$f(x) \equiv 0 \mod m$$

é suficiente resolvê-las no caso

$$f(x) \equiv 0 \mod p^j$$

com p primo.

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

$$f(x) \equiv 0 \mod p$$

com p primo.
O problema de determinar em que condições e como obter soluções de

$$f(x) \equiv 0 \mod p^j$$

para os diversos expoentes j, será tratado separadamente.

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

Em $\mathbb{Z}_p[x]$ estão definidas as operações de soma e produto: se

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

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).
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*

$$f(x) \equiv q(x)g(x) + r(x) \mod p.$$

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 de polinómios, 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 polinómios pretendidos.*

Note-se que b_n^{-1} designa a solução (única módulo p) de $b_n x \equiv 1 \mod p$. O algoritmo está bem definido uma vez que a sucessão de valores da variável u é estritamente decrescente.
Resta verificar a unicidade dos polinómios quociente e resto: o conjunto de polinómios $\{f(x) - s(x)g(x) : s(x) \in \mathbb{Z}_{/p}[x]\}$ contém polinómios 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 polinómio com o seu grau, e, pela lei do corte, $q(x)$ é també 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*

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

Nota 1.6 *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: temos um algoritmo de Euclides, a definição e existência de máximo divisor comum, a definição de elementos "primos", um teorema fundamental da aritmética, etc.*
Não vamos usar esses resultados, que são deixados para um possível estudo complementar.

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*

$$f(x) = x^4 - 1 \;\; e \; g(x) = 2x^2 - 1$$

como polinómios com coeficientes em $\mathbb{Z}_{/8}$.

Exercícios V.1

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

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

   satisfaz a condição

   $$F(x) \equiv g(x) \mod p \; \forall x$$

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 $g(x) = 2x^3 + x + 4$.

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*

$$f(x) \equiv (x^p - x)\, g(x) \mod p$$

e todas as classes de congruência são solução da equação

$$f(x) \equiv 0 \mod p,$$

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

$$r(x) \equiv 0 \mod p$$

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*

$$f(x) \equiv (x^p - x)\, g(x) \mod p$$

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

$$f(x) \equiv (x^p - x)\, g(x) + r(x) \mod p$$

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* $p = 17$*,*

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

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

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

Nota 1.11 *No exemplo anterior, temos mesmo uma igualdade de polinómios de coeficientes inteiros. O lema da divisão aplica-se à divisão entre polinómios de coeficientes inteiros, desde que o divisor seja mónico. Portanto podemos realizar a divisão como se se tratasse de polinómios 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

$$f(x) \equiv 0 \mod p$$

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 $\mod p$).

Lema 1.12 *Seja*

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0$$

um polinómio com coeficientes inteiros.
Se $f(c) \equiv 0 \mod p$, *então existe um polinómio* $g(x)$ *de coeficientes inteiros, mónico e de grau* $n-1$, *tal que*

$$f(x) \equiv (x-c)g(x) \mod p$$

Demonstração 1.13 *Temos*

$$f(x) \equiv f(x) - f(c) \equiv$$

$$\equiv x^n - c^n + a_{n-1}(x^{n-1} - c^{n-1}) + \cdots a_1(x-c) \mod p$$

Ora, para qualquer $k > 0$,

$$x^k - c^k = (x-c)(x^{k-1} + x^{k-2}c + \cdots + xc^{k-2} + c^{k-1}) =$$

$$= (x-c)\sum_{i=0}^{k-1} x^{k-1-i}c^i$$

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

Este lema permite provar, por indução no grau, a seguinte

Proposição 1.14 *Um polinómio* $f(x) \in \mathbb{Z}_p[x]$ *de grau* n *não pode ter mais do que* n *raizes distintas.*

Proposição 1.15 *Seja* $f(x) \in \mathbb{Z}_p[x]$ *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*

$$f(x) \equiv 0 \mod p$$

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

$$r(x) \equiv 0 \mod p$$

Demonstração 1.16 *No primeiro caso temos a congruência*

$$x^p - x \equiv f(x)g(x) \mod p$$

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

$$x^p - x \equiv f(x)g(x) + r(x) \mod p$$

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

$$r(a) \equiv f(a)g(a) + r(a) \equiv a^p - a \equiv 0 \mod p$$

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* $x^7 + 4x^3 + 2 \equiv 0 \mod 11$, *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

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

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

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

e que portanto é suficiente encontrar as soluções de

$$5x^3 + 4x^2 + 10x + 8 \equiv 0 \mod 11$$

e assim por diante.

Um exemplo particularmente importante de aplicação daquele resultado:

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

$$x^d \equiv 1 \mod p$$

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 $7^2 \equiv 5 \mod 11$, determinar, sem ser por tentativa e erro, quais as soluções de

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

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

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

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 $x^3 + 2x^2 + 5x + 6 \equiv 0 \mod 11$.

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

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

1.3 Ordem de um inteiro módulo p e raízes primitivas

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

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

Exemplo 1.20 *Seja por exemplo* $p = 11$. *A tabela seguinte apresenta as potências* $x^k \mod 11$, *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

$$ord_{11}(2) = ord_{11}(6) = ord_{11}(7) = ord_{11}(8) = 10$$

enquanto que

$$ord_{11}(3) = ord_{11}(4) = ord_{11}(5) = ord_{11}(9) = 5.$$

Proposição 1.21 *Fixando um primo* p,

1) Se $ord(a) = k$ *e* $a^h \equiv 1 \mod p$ *então* $k \mid h$. *Em particular* $ord(a) \mid p-1$.

2) Se $ord(a) = k$ *e* $ab \equiv 1 \mod p$ *então* $ord(b) = k$.

3) Se $ord(a) = k$ *então* $ord(a^j) = \frac{k}{d}$ *em que* $d = mdc(k, j)$.

4) Se $ord(a) = k$, $ord(b) = h$ *e* $mdc(k, h) = 1$ *então* $ord(ab) = kh$.

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

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

porque $a^k \equiv 1 \mod p$*; mas pela definição de ordem tem que ser* $r = 0$.
3) por um lado

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

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

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

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

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

uma vez que $mdc(\frac{k}{d}, \frac{j}{d}) = 1$.
4) em primeiro lugar, uma vez que

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

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

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

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* $ord_m(a) = \phi(m)$ *chama-se uma* ***raiz primitiva*** *de* m.

Consultando a tabela acima verifica-se, por exemplo, que 2 ou 7 são raizes primitivas módulo 11.

O conhecimento de raizes 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 raizes 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

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

ou seja, cuja ordem módulo p divide q^j. Dada uma dessas soluções a, teremos $ord_p(a) = q^j$ 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

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

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

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

concluímos que

Teorema 1.25 *Dado p primo, existem $\phi(p-1)$ raizes 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.*

Dada uma raiz primitiva g módulo p, todos os elementos de $\mathbb{Z}_p^\times$ (ou seja, os elementos não nulos de $\mathbb{Z}_p$) são iguais a uma potência de g, e o expoente é único módulo $p-1$.
Esse facto permite, se tivermos uma tabela com a correspondência bijectiva entre os elementos $a \in \mathbb{Z}_p^\times$ e os expoentes $0 \leq k < p-1$ tais que $a \equiv g^k \ mod p$, transformar multiplicações em somas:

Exemplo 1.27 *A tabela estabelece essa bijecção para módulo 13 e a raiz primitiva 2:*

k	1	2	3	4	5	6	7	8	9	10	11	12
2^k	2	4	8	3	6	12	11	9	5	10	7	1

$$9 \times 7 \equiv 2^8 \times 2^{11} \equiv 2^{8+11} \equiv 2^7 \equiv 11 \mod 13$$

Este cálculo é análogo à utilização para números reais dos logaritmos (que foram aliás inventados exactamente com esse fim).

1.4 Raizes módulo p

Voltemos à equação

$$x^k \equiv b \mod p$$

agora com módulo primo. Sabemos que se $mdc(k, p-1) = 1$ 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

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

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

$$ki \equiv j \mod p-1$$

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

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

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

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

o que implica que $d \mid j$.
Deduzimos portanto a

Proposição 1.28 ***(Critério de Euler):*** *Seja p primo, b primo com p, $k > 1$ e $d = mdc(k, p-1)$. Então a equação*

$$x^k \equiv b \mod p$$

tem d soluções se

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

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 $d = mdc(k, \phi(m))$.

Exemplo 1.29 *Mostrar que a equação*

$$x^5 \equiv 6 \mod 101$$

tem 5 *soluções.*

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

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* $2^{70} \equiv 6 \mod 101$, *a dedução feita diz-nos que as soluções são as classes* 2^i *com* i *solução de*

$$5i \equiv 70 \mod 100 \Leftrightarrow i \equiv 14 \mod 20$$

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 $a^s \equiv b \mod p$.
3. Sabendo que 5 é uma raiz primitiva de 47 e que $5^{16} \equiv 17 \mod 47$, determinar as soluções da equação "exponencial"

$$25^x \equiv 17 \mod 47$$

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

$$x^2 \equiv a \mod p$$

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

$$x^2 \equiv -1 \mod p$$

tem solução se e só se $p \equiv 1 \mod 4$.

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

Sugestão: Dados primos $p_1, p_2, \cdots, p_k$ 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,

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

Concluir que pq não tem raizes primitivas.

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

   a) $x^{12} \equiv 16 \mod 17$;
   b) $x^{20} \equiv 13 \mod 17$;
   c) $x^{48} \equiv 9 \mod 17$;
   d) $x^{11} \equiv 9 \mod 17$;

9. Mostrar que $3^8 \equiv -1 \mod 17$. Justificar porque é que podemos concluir que 3 é raiz primitiva de 17.
   Usar uma lista das classes de congruência de $3^i \mod 17$ para encontrar as soluções do problema anterior.

10. 3 é raiz primitiva módulo 31 e $3^{12} \equiv 8 \mod 31$. Determinar as soluções de
$$x^4 \equiv 8 \mod 31.$$

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
    $$(a + p)^{\phi(p^{k-1})} \equiv a^{\phi(p^{k-1})} - p^{k-1}a^{\phi(p^k)-1} \mod p^k.$$
    Sugestão: Tem que se mostrar que, para $j \geq 2$,
    $$\binom{\phi(p^{k-1})}{j} p^j \equiv 0 \mod p^k;$$
    começar por mostrar que p^{j-1} não divide $j!$.

    c) Concluir que, se a não é raiz primitiva módulo p^k, então
    $$(a + p)^{\phi(p^{k-1})} \not\equiv 1 \ mod p^k,$$
    e deduzir que, nesse caso, $(a + p)$ é raiz primitiva módulo p^k.

12. Mostrar que, se p é primo e $a, b \in \mathbb{Z}$,
$$(a + b)^p \equiv a^p + b^p \mod p.$$

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

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

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

$$f(x) \equiv 0 \mod p$$

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

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

e a equação $x^2 \equiv a \mod p$ tem duas soluções; ou

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

e a equação $x^2 \equiv a \mod p$ não tem solução.

Definição 1.31 *Dado p primo ímpar e $a \in \mathbb{Z}$ primo com p, a diz-se um* ***resíduo quadrático*** $\mod p$ *se* $a^{\frac{p-1}{2}} \equiv 1 \mod p$.

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

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

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

$$f(x, y) \equiv 0 \mod p$$

para todo o primo p.
No caso de a não ser múltiplo de p, a última equação é equivalente (exercício) a

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

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 1.33 *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 1.34 *Dado p e $a \in \mathbb{Z}$, o símbolo $(a|p)$ define-se como*

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

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

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 $p \equiv 1 \mod 4$, e $(-1|p) = -1$ se $p \equiv 3 \mod 4$;
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 1.35 *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 1.36 *Dois exemplos simples de conjuntos de Gauss módulo p são*

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

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

$$ax \equiv e(x)u(x) \mod p;$$

mas, além disso, a função

$$s_a : S \to S, \qquad s_a(x) = u(x)$$

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,

$$x \equiv \pm y \mod p;$$

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

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

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

$$= \prod_{x\in S} e(x) \prod_{x\in S} u(x) = \prod_{x\in S} e(x) \prod_{x\in S} x,$$

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 1.37 (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 $ax \equiv -x' \mod p$ para algum $x' \in S$). Então $(a|p) = (-1)^t$.*

Nota 1.38 *Cada escolha de conjunto de Gauss corresponde a uma definição particular de t. Por exemplo, se $S = \{2i - 1 :\leq i \leq \frac{p-1}{2}\}$, e definirmos $b(i)$ pela condição*

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

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 1.39 *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* $5^6 \equiv -1 \mod 13$.

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

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

neste caso, $2i \equiv e(i)u(i) \mod p$ 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

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

Como se verifica facilmente,

- se $p \equiv 1 \mod 4$ então

  t é par se $p \equiv 1 \mod 8$,

  t é ímpar se $p \equiv 5 \mod 8$;

- se $p \equiv 3 \mod 4$ então

  t é par se $p \equiv 7 \mod 8$,

  t é ímpar se $p \equiv 3 \mod 8$.

Resumindo,

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

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 1.40 (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 1.41 *Fixamos os conjuntos de Gauss*

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

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 $qx \equiv -x' \mod p$, 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

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

$R(x, y)$ *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*

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

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 1.42

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

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