1 Potências e raízes em Aritmética Modular

1.1 Os Teoremas de Fermat e Euler

Seja p primo e a um inteiro primo com p; a aplicação

$$\mathbb{Z}_{/p} \to \mathbb{Z}_{/p}, \qquad x \to ax$$

definida pela multiplicação por a (ou mais precisamente pela sua classe de congruência) é uma bijecção: de facto, como a é primo com p, existe a' tal que $a'a \equiv 1 \mod p$ e portanto

$$ax \equiv ay \mod p \Leftrightarrow a'ax \equiv a'ay \mod p \Leftrightarrow x \equiv y \mod p$$

Por exemplo, para $p = 5$ e $a = 2$ temos

x	0	1	2	3	4
ax	0	2	4	1	3

Se fizermos o produto dos ax para todas as classes de congruência primas com p (ou seja, todas menos a de 0) obtemos portanto

$$1 \cdot 2 \cdots (p-1) \equiv (a \cdot 1)(a \cdot 2) \cdots (a \cdot p - 1) \equiv a^{p-1} \cdot (1 \cdot 2 \cdots (p-1)) \mod p$$

uma vez que $(a \cdot 1)(a \cdot 2) \cdots (a \cdot p - 1)$ é o produto das mesmas $p-1$ classes de congruência por uma ordem diferente. Como $1 \cdot 2 \cdots (p-1) = (p-1)!$ não é equivalente a 0 módulo p, podemos dividir ambos os lados por $(p-1)!$ (ou seja multiplicar pelo seu inverso) e concluímos que

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

Deduzimos portanto o seguinte

Teorema 1.1 *Teorema de Fermat: Dado um primo p tem-se*

$$a^{p-1} \equiv 1 \mod p \qquad \forall a : mdc(a, p) = 1$$

Note-se que o teorema pode ser enunciado de forma equivalente, e mais simples, como

Teorema 1.2 *Teorema de Fermat: Dado um primo p tem-se*

$$a^p \equiv a \mod p \qquad \forall a$$

uma vez que, por um lado, a congruência anterior implica esta última para a primo com p, enquanto que para a múltiplo de p, esta é evidentemente verdadeira; e por outro, se $a^p \equiv a \mod p$ e a for primo com p, então temos que p divide $a^p - a = a(a^{p-1} - 1)$ e como não divide a tem que dividir o segundo factor.

Exemplo 1.3 *: Calcular o resto da divisão de 7^{203} por 17:*

$$7^{213} = 7^{13\times 16+5} = \left(7^{16}\right)^{13} 7^5 \equiv 7^5 \mod 17$$

e como $7^2 = 49 \equiv 15 \equiv -2 \mod 17$, temos

$$7^5 \equiv (-2)^2 \times 7 \equiv 11 \mod 17$$

Seja agora m um módulo qualquer e a primo com m. O resultado do teorema de Fermat já não vale em geral; por exemplo

$$5^{11} \equiv 5 \mod 12$$

e

$$3^{19} \equiv 7 \mod 20$$

Podemos no entanto repetir o raciocínio feito para o teorema de Fermat desde que consideremos apenas as classes de congruência primas com m; designamos por

$$\mathbb{Z}_m^\times$$

o conjunto das classes de congruência módulo m primas com m; por exemplo

$$\mathbb{Z}_{12}^\times = \{1, 5, 7, 11\}$$

Notamos que o produto de duas classes primas com m é ainda uma classe prima com m.

Definição 1.4 *: A função ϕ de Euler é definida como*

$$\phi : \mathbb{N} \to \mathbb{N}, \qquad \phi(m) = \left|\mathbb{Z}_m^\times\right|$$

ou seja $\phi(m)$ é o número de classes de congruência módulo m primas com m.

Se a representa, mais uma vez, uma classe de congruência módulo m e prima com m, a aplicação

$$\mathbb{Z}_{/m}^\times \to \mathbb{Z}_{/m}^\times, \qquad x \to ax$$

é de novo uma bijecção, já que

$$ax \equiv ay \mod m \Leftrightarrow m \mid a(x-y)$$

e como $mdc(a,m) = 1$ isso implica $m \mid (x-y)$, ou seja x e y representam a mesma classe de congruência módulo m.
Se

$$x_1, \cdots, x_{\phi(m)}$$

representarem as classes primas com m, temos

$$a^{\phi(m)} x_1 \cdots x_{\phi(m)} = (ax_1) \cdots (ax_{\phi(m)}) \equiv x_1 \cdots x_{\phi(m)} \mod m$$

Como o produto $x_1 \cdots x_{\phi(m)}$ é primo com m, tem um inverso módulo m e podemos multiplicar ambos os lados da congruência por esse inverso e obter o

Teorema 1.5 *Teorema de Euler: Se a é primo com m então*

$$a^{\phi(m)} \equiv 1 \mod m$$

Como $\phi(p) = p-1$ para p primo, o Teorema de Fermat é de facto um caso particular deste último.

Exemplo 1.6 *: Tendo em conta que, como vimos atrás,* $\phi(12) = 4$*, tem-se*

$$5^{35} = 5^{32+3} = 5^{4\cdot 8}5^3 = \left(5^4\right)^8 5^3 \equiv 5^3 \equiv 5 \mod 12$$

Ou seja, qualquer potência de base a prima com m é congruente módulo m com uma potência de expoente menor que $\phi(m)$: para cada k, $a^k \equiv a^r \mod m$ onde $0 \leq r < \phi(m)$ e $r \equiv k \mod \phi(m)$.

Nota 1.7 *: O Teorema de Euler fornece uma alternativa para resolver equações lineares: se* $mdc(a, m) = 1$*, a solução de*

$$ax \equiv b \mod m$$

pode ser calculada multiplicando ambos os lados da equação por $a^{\phi(m)-1}$*.*

Para aplicar o Teorema de Euler é necessário calcular $\phi(m)$.
Recorde-se que o Teorema Chinês dos Restos nos diz que se $m = m_1 \cdots m_k$ e $mdc(m_i, m_j) = 1$ se $i \neq j$, então a aplicação

$$\psi : \mathbb{Z}_{/m} \to \mathbb{Z}_{/m_1} \times \mathbb{Z}_{/m_k}$$

definida por

$$\psi(a) = (a \mod m_1, \cdots, a \mod m_k)$$

é uma bijecção.

Note-se também que a é primo com m se e só se o é com cada m_i. Isso mostra que

$$\phi(m) = \phi(m_1) \cdots \phi(m_k)$$

ou seja ϕ é uma função *multiplicativa*:

Definição 1.8 *: Uma função* $f : \mathbb{N} \to \mathbb{N}$ *diz-se multiplicativa se*

$$mdc(m, n) = 1 \implies f(m \cdot n) = f(m)f(n)$$

Conclui-se que se $m = p_1^{k_1} \cdots p_r^{k_r}$ for a factorização de m em factores primos,

$$\phi(m) = \phi\left(p_1^{k_1}\right) \cdots \phi\left(p_r^{k_r}\right)$$

Mas é fácil verificar que, para p primo

$$\phi(p^k) = p^k - p^{k-1}.$$

De facto, as classes módulo p^k que não são primas com p^k são as dos múltiplos de p:

$$0, p, 2p, \cdots, (p^{k-1} - 1)p$$

(o múltiplo de p seguinte seria $p^k \equiv 0$).

Portanto

$$\phi(m) = \left(p_1^{k_1} - p_1^{k_1-1}\right) \cdots \left(p_r^{k_r} - p_r^{k_r-1}\right) = m \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

Exemplo 1.9 *: suponhamos que queremos determinar* $0 < x < 279$ *tal que*

$$x \equiv (25)^{681} \mod 279.$$

Como $279 = 9 \times 31$*, temos*

$$\phi(279) = \phi(9)\phi(31) = 6 \cdot 30 = 180.$$

E portanto, como 25 *é obviamente primo com* 279*,*

$$(25)^{681} = (25)^{3\times 180+149} = \left((25)^{180}\right)^3 (25)^{149} \equiv (25)^{149} \mod 279$$

Mas podemos ainda simplificar mais o cálculo desta potência: aplicando o algoritmo de Euclides, verificamos que

$$1 = 67 \times 25 - 6 \times 279$$

ou seja

$$67 \times 25 \equiv 1 \mod 279$$

Usando mais uma vez o Teorema de Euler

$$(25)^{149} \equiv (25)^{149}(67)^{180} \equiv (25 \times 67)^{149}(67)^{31} \equiv (67)^{31} \mod 279$$

que nos reduz ao cálculo de uma potência de expoente menor.

Ou seja, para a primo com m e sendo b um qualquer representante da classe de congruência inversa da de a, temos

$$a^k \equiv b^{\phi(m)-k} \mod m$$

que é o análogo da bem conhecida expressão

$$a^k = \left(a^{-1}\right)^{-k}$$

Note-se finalmente que mesmo o cálculo da última potência poderia ser simplificado pelo uso do Teorema Chinês dos Restos:

$$\begin{aligned} x \equiv (67)^{31} \mod 279 &\Leftrightarrow \\ \Leftrightarrow \begin{cases} x \equiv (67)^{31} \mod 9 \\ x \equiv (67)^{31} \mod 31 \end{cases} &\Leftrightarrow \\ \Leftrightarrow \begin{cases} x \equiv 4^{31} \mod 9 \\ x \equiv 5^{31} \mod 31 \end{cases} &\Leftrightarrow \\ \Leftrightarrow \begin{cases} x \equiv 4 \mod 9 \\ x \equiv 5 \mod 31 \end{cases} & \end{aligned}$$

onde, no último passo, voltámos a usar o Teorema de Euler.

Esta aplicação do Teorema Chinês dos Restos podia, bem entendido, ter sido feita logo no início.

Exercícios IV.1

1. Determinar

   a) $0 \leq a < 73$ satisfazendo $a \equiv 9^{794} \mod 73$.

b) $0 \leq a < 83$ satisfazendo $a \equiv 7^{670} \mod 83$.

2. Quais são os algarismos das unidades e das dezenas de 2^{1000}? E de 7^{888}?

3. Mostrar que $n^7 - n$ é divisível por 42, para todo o inteiro n.

4. Mostrar que se p é um primo diferente de 2 e de 5, então p divide infinitos inteiros do conjunto $\{9, 99, 999, 9999, \cdots\}$.

5. Sendo m o seu número de aluno, seja n o número definido por

$$0 \leq n < 10^3, \qquad n \equiv m \mod 10^3$$

Calcular $\phi(n)$.

6. Sejam m e n inteiros positivos. Mostrar que se todo o primo que divide n também divide m, então

$$\phi(nm) = n\phi(m).$$

7. a) Para que valores de m se verifica $\phi(m) = \dfrac{m}{2}$?

b) Existe algum n tal que $\phi(n) = 50$?

c) Para que valores de m é que $\phi(m)$ divide m?

Nota 1.10 *Teorema de Euler e dízimas periódicas*

Os teoremas de Fermat e Euler permitem ver a uma nova luz certas propriedades elementares da representação decimal de números racionais. Embora o que se segue não desempenhe qualquer papel no desenvolvimento da teoria da aritmética modular, veremos mais uma vez como os seus conceitos aparecem naturalmente na discussão de problemas aritméticos.
Um argumento elementar (usando o Lema da Divisão) mostra que uma dízima $0.a_1a_2\cdots$ *(com* $0 \leq a_i < 10$ *para todo o* i*) representa um número racional se e só se a sequência* a_i *é eventualmente periódica, ou seja, existem* $t \geq 0$ *e* $n > 0$ *tais que* $a_{t+i+jn} = a_{t+i}$ *para todo o* $1 \leq i \leq n$ *e* $j \geq 0$*. Que racionais* x *têm representação decimal puramente periódica, isto é, com* $t = 0$*? Notamos que isso é equivalente à existência de um inteiro* I *(a parte inteira de* x*), de um* $n > 0$ *(o período) e de um* $0 \leq N < 10^n$ *tais que*

$$x = I + \frac{N}{10^n} + \frac{N}{10^{2n}} + \cdots = I + N\sum_{j\geq 1} \frac{1}{10^{jn}},$$

ou seja, usando a fórmula para a soma da série geométrica, $x = I + \dfrac{N}{10^n - 1}$.
Uma aplicação muito simples do Teorema de Euler esclarece completamente a questão. Obviamente, basta considerar o caso $I = 0$ *e supor que* x *é representado por uma fracção reduzida, ou seja, com numerador e denominador primos entre si.*

Seja então $0 < \frac{a}{m} < 1$ *e suponhamos que* $mdc(m, 10) = 1$. *Então, pelo Teorema de Euler, se* $\phi(m) = n$, *temos* $10^k \equiv 1 \mod m$, *ou seja, existe* M *tal que* $10^n - 1 = Mm$. *Deduzimos que* $\frac{a}{m} = \dfrac{aM}{10^n - 1}$, *e como se tem forçosamente* $aM < 10^n$, *concluímos que* $\frac{a}{m}$ *tem representação decimal puramente períodica e que o período será um divisor de* $\phi(m)$ *(de facto, pode acontecer que o bloco periódico de comprimento* n *representado por* aM *seja a concatenação de várias cópias de um bloco de comprimento* p, *com* $p \mid n$, *ou seja que* $aM = b(1 + 10^p + 10^{2p} + \cdots + 10^{(l-1)p})$ *onde* $n = pl$ *e* $0 < b < 10^p$*).*

Mas, reciprocamente, se $0 < \frac{a}{m} < 1$ *tem representação decimal puramente períodica, com período mínimo* n, *isso significa, pelo mesmo raciocínio, que existe* M *tal que* $a(10^n - 1) = Mm$; *como* $mdc(a, m) = 1$, *temos* $10^n \equiv 1 \mod m$ *e* n *é o menor inteiro positivo satisfazendo essa equação. Isso implica imediatamente que* $mdc(m, 10) = 1$, *mas além disso, como* $10^{\phi(m)} \equiv 1 \mod m$, *podemos escrever* $\phi(m) = qn + r$, *com* $0 \leq r < n$ *e concluímos que também* $10^r \equiv 1 \mod m$, *o que, pela propriedade de* n, *implica* $r = 0m$, *ou seja, o período da representação decimal de* $\frac{a}{m}$ *tem que ser um divisor de* $\phi(m)$.

Terminamos esta breve digressão com duas observações. Verifica-se que quando o denominador m *é primo e o período* n *da representação decimal é par, o bloco peri'odico tem a propriedade de que a soma das suas "metades" é da forma* $99...9$. *Por exemplo*

$$\frac{3}{7} = \frac{428571}{10^6 - 1} \text{ e } 428 + 571 = 999,$$

$$\frac{2}{13} = \frac{153846}{10^6 - 1} \text{ e } 153 + 846 = 999.$$

A justificação deste facto pode ser feita por uma aplicação igualmente simples das mesmas ideias e é deixada como exercício.

A segunda observação é que nada do que se disse depende essencialmente de representarmos os números na base 10. *É portanto possível deduzir propriedades semelhantes para a representação de números em qualquer base inteira* b, *ou seja, no caso* $0 < x < 1$, *na forma* $x = \sum_{i \geq 1} c_i b^{-i}$ *com* $0 \leq c_i < b$ *para todo o* i.

1.2 Nota sobre o cálculo eficiente de potências

Mesmo com todas as simplificações descritas anteriormente, somos irremediavelmente conduzidos, na resolução de equações modulares, à determinação da classe de congruência de potências por vezes com expoente muito grande.

Naturalmente, o cálculo de potências deve ser feito iterativamente, reduzindo módulo m em cada passo; por exemplo, para calcular 2^{12} módulo 19, teríamos sucessivamente

$$2^2 = 4; 2^3 = 8; 2^4 = 16; 2^5 = 32 \equiv 13; 2^6 \equiv 2 \cdot 13 \equiv 7;$$

$$2^7 \equiv 14; 2^8 \equiv 28 \equiv 9; 2^9 \equiv 18 \equiv -1; 2^{10} \equiv -2; 2^{11} \equiv -4; 2^{12} \equiv -8 \equiv 11$$

Estes cálculos podem ainda ser simplificados e no caso de módulos e expoentes grandes, essa simplificação ganha maior importância; uma das maneiras de calcular eficientemente

$$a^n \mod m$$

passa por escrever o expoente como uma soma de potências de 2

$$n = 2^{k_1} + 2^{k_2} + \cdots 2_{k_r}, \qquad k_1 < k_2 < \cdots < k_r$$

calcular

$$a^{2^k} \mod m$$

para cada k, levantando sucessivamente ao quadrado a potência anterior, e multiplicar os valores correspondentes.

Por exemplo, para calcular $7^{327} \mod 853$, calculando primeiro as potências

7^{2^k} módulo 853

$$\begin{aligned}
7^2 &= 49 \\
7^4 = 49^2 &= 2401 \equiv 695 \\
7^8 \equiv 695^2 &= 483025 \equiv 227 \\
7^{16} \equiv 227^2 &= 51529 \equiv 349 \\
7^{32} \equiv 349^2 &= 121801 \equiv 675 \\
7^{64} \equiv 675^2 &= 455625 \equiv 123 \\
7^{128} \equiv 123^2 &= 15129 \equiv 628 \\
7^{256} \equiv 628^2 &= 394384 \equiv 298
\end{aligned}$$

e como $327 = 1 + 2 + 2^2 + 2^6 + 2^8$, temos usando a tabela anterior

$$7^{327} \equiv \cdot 7 \cdot 49 \cdot 695 \cdot 123 \cdot 298 \equiv 286$$

Note-se que neste processo nunca usamos números superiores a m^2. Se calculássemos directamente 7^{327} obteríamos um número com 277 algarismos que teria depois que ser reduzido $\mod 853$. E mesmo que reduzíssemos $\mod 853$ a cada multiplicação, como no exemplo anterior, teríamos 327 multiplicações, enquanto que deste modo temos 12 multiplicações (mais as divisões para determinar a decomposição do expoente em soma de potências de 2).

Na implementação deste algoritmo, mesmo no cálculo manual, as tarefas anteriores (determinar a representação na base 2 do expoente n

$$n = b_0 + b_1 2 + b_2 2^2 + \cdots + b_l 2^l \qquad b_i \in \{0, 1\}$$

calcular as potências $a^{2^k} \mod m$ e multiplicar as que correspondem a potências 2^k com $b_k = 1$), descritas separadamente para clarificação da ideia envolvida, devem ser levadas a cabo ao mesmo tempo; eis uma descrição esquemática do algoritmo para calcular $a^n \mod m$:

1. Inincializamos variáveis $j = n$, $x = 1$ e $c = a$;
2. enquanto $j > 0$,

a) se j é par, substituir j por $\frac{j}{2}$ e c por c^2 e reduzir $\mod m$;

b) se j é ímpar substituir j por $j-1$ e x por cx e reduzir $\mod m$

3. se $j=0$, $x \equiv a^n \mod m$.

A ideia do algoritmo é que se $n = \sum_{i=0}^{r} b_i 2^i$ é a representação binária do expoente, se tem

$$a^n = a^{b_0} \left(a^2\right)^{b_1} \left(a^4\right)^{b_2} \cdots \left(a^{2^r}\right)^{b_r}$$

e que esses produtos se podem fazer, passo a passo, ao mesmo tempo que vamos deduzindo os b_i.

A variável x representa os sucessivos valores que o produto vai tomando e é naturalmente inicializado em 1; se n é ímpar, ou seja $b_0 = 1$, temos

$$a^n = a \cdot a^{n-1}$$

enquanto que para n par (e portanto $b_0 = 0$)

$$a^n = (a^2)^{n/2}$$

No primeiro caso actualizamos o produto e no segundo a base; o novo expoente é sempre menor que o anterior pelo que este processo termina.

Exemplo 1.11 *: Calcular* 3^{21} *módulo* 37*; no quadro seguinte apresentamos à esquerda os passos do algoritmo com os sucessivos valores das variáveis, sempre reduzidos módulo* 37*, acompanhados à direita pela sua tradução no cálculo; note-se nesta coluna que o valor de* 3^{21} *módulo* 37 *é sucessivamente representado pelo produto de um primeiro factor que corresponde ao valor de* x *nesse passo, e um segundo que é a parte ainda por calcular.*

j	c	x	
21	3	1	$3^{21} =$
20	3	3	$= 3 \times 3^{20}$
10	9	3	$= 3 \times (3^2)^{10}$
5	7	3	$= 3 \times (3^4)^5$
4	7	21	$= (3 \cdot 3^4) \times (3^4)^4$
2	12	21	$= (3 \cdot 3^4) \times (3^8)^2$
1	33	21	$= (3 \cdot 3^4) \times 3^{16}$
0	33	27	$= 3 \cdot 3^4 \cdot 3^{16}$

1.3 Testes de primalidade

O Teorema de Fermat está na base de testes de primalidade: seja $m > 1$ e a primo com m. Se a^{m-1} não for congruente com 1 módulo m então m não é primo.
Por exemplo, se $m = 299$ e $a = 2$, o cálculo de $2^{298} \mod 299$ dá-nos, pelo método descrito anteriormente

j	c	x
298	2	1
149	4	1
148	4	4
74	16	4
37	256	4
36	256	127
18	55	127
9	35	127
8	35	259
4	29	259
2	243	259
1	146	259
0	146	140

e portanto $2^{298} \equiv 140 \mod 299$ comprovando que o módulo em questão não é primo.

Se $a^{m-1} \equiv 1 \mod m$ então o teste é inconclusivo. Por exemplo $2^{340} \equiv 1 \mod 341$ mas 341 não é primo, como se pode comprovar repetindo o teste com base 3 já que $3^{340} \equiv 56 \mod 341$.

No entanto, existem inteiros m compostos para os quais o teste falha para *todas* as bases primas com m. Esses números designam-se por números de Carmichael (em homenagem ao matemático R. Carmichael que identificou os primeiros exemplos em 1910) e o menor deles é $561 = 3 \times 11 \times 17$
(ver o exercício **IV.2.1.**).

A conjectura de que existem infinitos números de Carmichael (avançada pelo próprio Carmichael em 1910) foi comprovada em 1994 por Alford, Granville e Pomerance. Prova-se também o seguinte

Proposição 1.12 *Critério de Korselt: Um inteiro composto m é um número de Carmichael se e só se for ímpar e, para cada primo p que divida m se verificam as condições*

p^2 *não divide* m*;*

$(p-1) \mid (m-1)$*;*

É no entanto possível deduzir critérios de primalidade mais eficazes: suponhamos que m é primo e que

$$m - 1 = 2^k q$$

com q ímpar. Dado a primo com m, ou bem que

$$a^q \equiv 1 \mod m$$

ou então existe $0 < j \leq k$ tal que

$$a^{2^j q} \equiv 1 \mod m \qquad \text{e} \qquad a^{2^{j-1} q} \equiv -1 \mod m$$

De facto, se a^q não for congruente com 1, tem que existir um primeiro j tal que $a^{2^j q} \equiv 1$, já que pelo menos para $j = k$ isso acontece de certeza (sempre supondo que m é primo, bem entendido). Mas então, pondo $b = a^{2^{j-1} q}$, temos que $b^2 \equiv 1 \mod m$ o que implica $b \equiv \pm 1 \mod m$ (porque m é primo!). Como por hipótese b não é congruente com 1, tem que ser $b \equiv -1$. Este raciocínio conduz ao

Proposição 1.13 *Critério de Rabin-Miller: Seja* m *ímpar e* $m-1 = 2^k q$ *com* q *ímpar. Se, para algum* a *primo com* m*, se verificam ambas as condições*

a^q *não é congruente com* 1 *módulo* m*,*

$a^{2^j q}$ *não é congruente com* -1 *módulo* m*, para* $j = 0, 1, \cdots, k-1$

então m *é composto.*

Este critério é muito mais eficaz para determinar que um inteiro é composto, nomeadamente porque se pode provar que para qualquer m composto, pelo menos 3/4 de todos os a primos com m permitem verificar esse facto através do Critério de Rabin-Miller.

Um outro exemplo de aplicação do Teorema de Fermat como teste de primalidade é apresentado no exercício **IV.2.5**

Exercícios IV.2

1. Usando a factorização $561 = 3 * 11 * 17$ mostrar que $a^{561} \equiv a \mod 561$ para todo o inteiro a.
2. Mostrar, usando o Teorema de Fermat (e um computador...), que os inteiros 1763, 1387, 11051 e 294409 não são primos.
3. Dizemos que n é um pseudo-primo para a base 2 se $2^{n-1} \equiv 1 \mod n$ mas n não for primo. Mostrar que n é um pseudo-primo para a base 2, então $2^n - 1$ também o é.
   Sugestão: Mostrar que $2^n - 1$ divide $2^{2^n-2} - 1$.
4. Provar metade do Critério de Korselt: msotrar que se m é o produto de primos ímpares distintos e
   $$p \mid m \implies (p-1) \mid (m-1)$$
   então m é um número de Carmichael.
5. Seja p primo ímpar. Mostrar que um factor primo q de $2^p - 1$ é da forma $q = 1 + 2kp$.
   Sugestão : Justificar que q divide $2^{q-1} - 1$ e usar o exercício **II.2.5.**. Notar que q é ímpar.

1.4 Raizes módulo m

O Teorema de Euler permite igualmente abordar a resolução de equações do tipo

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

Suponhamos primeiro que b é primo com m e que k é primo com $\phi(m)$; então existem inteiros u, v tais que

$$ku - \phi(m)v = 1$$

portanto

$$x^k \equiv b \Rightarrow x^{ku} \equiv b^u \Rightarrow x x^{\phi(m)v} \equiv b^u \mod m$$

Mas se x for solução da equação terá que ser primo com m logo, pelo Teorema de Euler, temos

$$x^k \equiv b \Rightarrow x \equiv b^u \mod m$$

que é de facto a solução da equação:

$$(b^u)^k = b^{1+\phi(m)v} \equiv b \mod m$$

Proposição 1.14 *: Se*

$$mdc(b, m) = 1 \text{ e } mdc(k, \phi(m)) = 1,$$

a equação

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

tem a solução única b^u onde u é um inteiro satisfazendo

$$ku \equiv 1 \mod \phi(m)$$

Nota 1.15 *: A equação anterior tem solução única mesmo se $mdc(b, m) > 1$, desde que $mdc(k, \phi(m)) = 1$ e que m seja livre de quadrados, isto é, que m seja o produto de primos distintos.*
Sem essas condições, a solução da equação pode não existir ou não ser única, como teremos oportunidade de ver mais adiante.

Exemplo 1.16 *: Resolver $x^{29} \equiv 2 \mod 117$; $117 = 13 \times 9$ e portanto*

$$\phi(117) = \phi(13)\phi(9) = 12 \times 6 = 72$$

Estamos nas condições da proposição; aplicando o algoritmo de Euclides verificamos que

$$1 = 5 \times 29 - 2 \times 72$$

Logo a única solução da equação é $2^5 = 32$.

É claro que pode ser mais útil começar por aplicar o Teorema Chinês dos Restos:

Exemplo 1.17 *: Como* $91 = 7 \times 13$*, a resolver a equação* $x^{55} \equiv 17 \mod 91$ *é equivalente a resolver o sistema*

$$\begin{cases} x^{55} \equiv 17 \mod 7 \\ \\ x^{55} \equiv 17 \mod 13 \end{cases} \Leftrightarrow \begin{cases} x \equiv 3 \mod 7 \\ \\ x^7 \equiv 4 \mod 13 \end{cases}$$

Nota 1.18 *: A resolução deste tipo de equações modulares passa, como vimos, por levantar ambos os membros da equação a uma mesma potência; por exemplo, na segunda equação do exemplo anterior, temos*

$$x^7 \equiv 4 \mod 13 \Leftrightarrow x^{7\times 7} \equiv 4^7 \ mod 13 \Leftrightarrow x \equiv 4^7 \mod 13,$$

uma vez que $7 \times 7 = 49 = 4 \times 12 + 1$*.*
Será que podemos, em geral, usar esta operação de levantar ambos os membros de uma equação a uma mesma potência para obter uma equação mais simples? Tal como na situação bem conhecida de uma equação sobre $\mathbb{R}$*, isso tem que ser feito com cuidado: no nosso exemplo, a primeira passagem é uma equivalência porque a potência usada é prima com* $\phi(13)$*; se não for assim, temos apenas uma implicação. Por exemplo*

$$x^3 \equiv 3 \mod 5 \implies x^6 \equiv 9 \mod 5 \Leftrightarrow x^2 \equiv 4 \mod 5;$$

mas esta última equação tem claramente duas soluções, as classes de congruência módulo 5 *de* 2 *e de* 3*, enquanto que a equação original só tem uma.*

Exercícios IV.3

1. Resolver a equação ou mostrar que não existe solução

   a) $x^{85} \equiv 6 \mod 29$

b) $x^{87} \equiv 5 \mod 29$

c) $x^{39} \equiv 3 \mod 13$

d) $x^{123} \equiv 5 \mod 24$

e) $x^{19} \equiv 5 \mod 111$

2. Seja m um número natural livre de quadrados, isto é, existem primos p_i (com $1 \leq i \leq k$) tais que se $i \neq j$ então $p_i \neq p_j$ e $m = p_1 p_2 \cdots p_k$. Supondo que $mdc(k, \phi(m)) = 1$, mostrar que a equação

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

tem uma única solução, mesmo que $mdc(b, m) > 1$.

Sugestão: usar o Teorema Chinês dos Restos.

1.4.1 Aplicação à Criptografia

A única dificuldade na resolução da equação

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

nas condições da proposição anterior está na determinação de $\phi(m)$, que depende do conhecimento da factorização de m. Mas essa dificuldade é, de um modo geral, muito grande. O problema está em que, apesar de existirem métodos para procurar os factores de um inteiro muito mais eficazes do que tentar sistematicamente a divisão por primos, não existe ainda um algoritmo eficaz para factorizar um inteiro $m > 10^{400}$, por exemplo.

Essa deficiência da Teoria dos Números acabou por ser aproveitada para a implementação de um sistema de codificação, o algoritmo RSA (dos nomes dos seus criadores Rivest, Shamir e Andleman). Ao contrário de outros sistemas de codificação em que o método de codificar uma mensagem, a chamada

chave de codificação, tem que ser mantido secreto, o RSA é um sistema de chave pública, isto é, qualquer pessoa pode codificar uma mensagem.

O sistema RSA consiste muito resumidamente no seguinte: escolhem-se dois primos p e q grandes, define-se $m = p \times q$ e escolhe-se um expoente k primo com $\phi(m) = (p-1)(q-1)$.
Tornam-se públicos m e k que são os elementos necessários à codificação: uma mensagem é transformada numa sequência de inteiros $0 < a < m$; a codificação de a é o inteiro $b \equiv a^k \mod m$.
O problema de descodificar uma mensagem equivale ao de, dado um inteiro b, resolver

$$a^k \equiv b \mod m$$

Ora, para m muito grande, sem conhecer os factores de m é virtualmente impossível determinar $\phi(m)$ e portanto resolver a equção.
Evidentemente, a implementação prática desta ideia geral exige vários cuidados; para mencionar apenas um, se $k^t \equiv 1 \mod \phi(m)$ para t pequeno, qualquer pessoa pode descoficiar uma mensagem, recodificando-a $t-1$ vezes.