1 Aritmética Modular

Vamos considerar alguns exemplos de problemas sobre números inteiros como motivação para o que se segue.

1. O que podemos dizer sobre a imagem da função

$$f : \mathbb{Z} \to \mathbb{Z}, \qquad f(x) = x^2 + x + 1?$$

Uma possível abordagem a este problema começa pela observação de que f só toma valores ímpares; para o verificar basta evidentemente considerar os dois casos x par e x ímpar.
Desenvolvendo esta ideia, podíamos perguntar quais os posíveis restos da divisão de $f(x)$ por 3; mais uma vez, esta pergunta é fácil de responder se notarmos que para qualquer inteiro x se tem

$$f(x + 3k) = (x + 3k)^2 + x + 3k + 1 = x^2 + x + 1 + 6kx + 9k^2 + 3k$$

ou seja, se somarmos a um certo x um múltiplo de 3, o valor de f muda mas também por um múltiplo de 3 e portanto o resto da divisão do valor de f por 3 não muda; de facto este resto só depende do resto da divisão de x por 3.
Como qualquer inteiro é igual a 0, 1 ou 2 mais um múltiplo de 3, para responder à pergunta basta calcular $f(0) = 1$, $f(1) = 3$ e $f(2) = 7$ e os respectivos restos na divisão por 3 que são 1, 0 e 1 novamente. Concluímos que 2 nunca é resto na divisão de $f(x)$ por 3 e portanto $f(x)$ não toma nenhum dos valores

$$\cdots, -4, -1, 2, 5, 8, 11, \cdots$$

Naturalmente, o mesmo raciocínio se podia aplicar a outro inteiro em vez de 3 e do mesmo modo a outra função polinomial

$$f : \mathbb{Z} \to \mathbb{Z}$$

2. Será que 20131400046549674927 é um quadrado perfeito em $\mathbb{Z}$, ou seja, existe algum inteiro m tal que

$$m^2 = 20131400046549674927\,?$$

Conseguimos dar uma resposta com um mínimo de cálculos fazendo o seguinte raciocínio:
todo o inteiro m se pode escrever na forma $m = 4q+r$ com $r \in \{0, 1, 2, 3\}$; nesse caso $m^2 = 16q^2 + 8qr + r^2$ e, portanto, o resto na divisão de m^2 por 4 é igual ao resto na divisão de r^2 por 4 (já que a diferença entre m^2 e r^2 é um múltiplo de 4). A tabela

r	0	1	2	3
resto na divisão de r^2 por 4	0	1	0	1

mostra-nos então que o resto na divisão de m^2 por 4 é sempre 0 ou 1, para qualquer inteiro m. Mas o resto na divisão de 20131400046549674927 por 4 é igual a 3:

$$20131400046549674927 = 20131400046549674900 + 27 =$$

$$= (201314000465496749 \times 25 + 6) \times 4 + 3,$$

e portanto aquele número não pode ser igual a m^2 com m inteiro.
Note-se que se a mesma pergunta fosse feita antes sobre o número

$$20131400046549674928,$$

que tem resto 0 na divisão por 4, a ideia usada anteriormente já não se poderia aplicar directamente: embora todos os m^2 tenham resto 0 ou 1 na divisão por 4, não é verdade que todos os números com resto 0 ou 1 na divisão por 4 sejam quadrados perfeitos. Mas se verificássemos por exemplo que o resto na divisão de 20131400046549674928 por 7 é 3, a tabela

r	0	1	2	3	4	5	6
resto na divisão de r^2 por 7	0	1	4	2	2	4	1

mostra-nos, por um raciocínio semelhante ao anterior, que 2013140004654967 também não é um quadrado perfeito.

3. Será que
$$32070004559 \mid (2^{16035002279} - 1)\,?$$
Não vamos por enquanto responder a esta pergunta mas notamos o seguinte: o que torna, à partida, esta pergunta tão difícil, ou mesmo impossível, de responder, é o facto de o número $2^{16035002279} - 1$, e portanto também o seu quociente na divisão por 32070004559, serem muito grandes (vários milhões de dígitos em representação decimal...).
Mas o que nos interessa aqui é apenas o *resto* daquela divisão, que é portanto menor que o "pequeno" 32070004559, e é possível, como veremos adiante, calcular aquele resto nunca usando números maiores que este.

1.1 A relação de congruência

Estes três exemplos mostram que na abordagem a alguns problemas aritméticos pode ser útil considerar apenas os restos na divisão por um certo inteiro fixo, escolhido de forma conveniente. Vamos agora clarificar com uma notação adequada esta ideia de trabalhar apenas com os restos da divisão por um certo inteiro.

Definição 1.1 *Seja $m \in \mathbb{N}$. Dois inteiros a e b dizem-se* ***congruentes*** *módulo m*
$$a \equiv b \mod m$$
se m divide $a - b$.

Como se verifica facilmente, a congruência é uma relação de equivalência em $\mathbb{Z}$, para qualquer escolha do módulo m. A classe de congruência de a é

$$\cdots, a-3m, a-2m, a-m, a, a+m, a+2m, a+3m, \cdots$$

e cada classe de congruência tem um e um só representante no conjunto

$$[m] = \{0, 1, \cdots, m-1\}$$

Um conjunto com esta propriedade chama-se um **sistema completo de resíduos** $\mod m$:

Definição 1.2 *: Um sistema completo de resíduos módulo m é um conjunto*

$$\{n_0, n_1, \cdots, n_{m-1}\} \subset \mathbb{Z}$$

tal que se $i \neq j$ então n_i e n_j não são congruentes $\mod m$.

Podemos também descrever um sistema completo de resíduos módulo m como um conjunto

$$\{n_0, n_1, \cdots, n_{m-1}\} \subset \mathbb{Z}$$

tal que $n_i \equiv i \mod m$.
Existem evidentemente infinitos sistemas completos de resíduos para um módulo dado.

O conjunto das classes de congruência módulo m é representado por $\mathbb{Z}/m\mathbb{Z}$ ou mais simplesmente por $\mathbb{Z}_{/m}$. Uma congruência entre números módulo m corresponde portanto a uma igualdade entre classes, ou seja entre elementos de $\mathbb{Z}_{/m}$.
A propriedade fundamental da relação de congruência está contida na proposição seguinte, cuja demonstração se deixa como exercício.

Proposição 1.3 *: Se $a \equiv b \mod m$ e $c \equiv d \mod m$ então*

$$a + c \equiv b + d \mod m \qquad ac \equiv bd \mod m$$

ou seja, a classe de congruência da soma ou do produto de dois inteiros depende apenas das classes de congruência destes (e não dos representantes particulares dentro de cada classe); estão portanto bem definidas em $\mathbb{Z}_{/m}$ as operações de soma e produto.

Exemplo 1.4 *: as tabuadas de soma e multiplicação de* $\mathbb{Z}_{/4}$ *são*

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

e de $\mathbb{Z}_{/5}$

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Nota 1.5 *: Para se ser mais preciso, devíamos distinguir a classe de congruência dos seus representantes; pode-se por exemplo usar a notação* $\overline{a}$ *para designar a classe de congruência de* a*.*
Mas quando não há perigo de confusão usamos um número para representar a sua classe de congruência; é no entanto crucial que esteja sempre claro quando é que isso acontece; por exemplo, é verdade que

$$7^{14} \equiv 2^{14} \mod 5$$

e portanto podemos usar qualquer dos dois números para representar a respectiva classe. No entanto o expoente 14 *não representa uma classe de*

congruência módulo 5*; ele indica que estamos a multiplicar a classe de* 2 *por si mesma* 14 *vezes e embora* $14 \equiv 4 \mod 5$*,* ***não é verdade*** *que* 2^{14} *seja congruente com* 2^4 *módulo* 5*.*

Uma equação sobre classes de congruência módulo m chama-se também uma *equação modular*. Uma solução de uma tal equação pode ser vista como um elemento de $\mathbb{Z}_{/m}$ ou como o conjunto dos números inteiros contidos nessa classe.

Conforme sugerido pelos exemplos iniciais, a relação de congruência e as suas propriedades permitem apresentar de forma mais sucinta e resolver de modo mais simples certos problemas da aritmética dos inteiros:

Exemplo 1.6 *Um inteiro é divisível por* 3 *se e só se a soma dos seus dígitos (da representação decimal habitual) também é divisível por* 3*. A explicação desse facto elementar é óbvia à luz da noção de congruência: se* $x = (a_s \cdots a_1\, a_0)$ *então*

$$x = \sum_{k=0}^{s} a_k 10^k \equiv \sum_{k=0}^{s} a_k \mod 3$$

uma vez que $10 \equiv 1$ *módulo* 3*.*

Exemplo 1.7 *: A solução do segundo problema apresentado no início pode agora ser traduzida do seguinte modo:*

$$20131400046549674927 \equiv 3 \mod 4$$

e como, para todo o $x \in \mathbb{Z}$*,* $x^2 \equiv 0$ *ou* $1 \mod 4$*, aquele número não é um quadrado perfeito.*

Exemplo 1.8 *Considere-se o seguinte problema, semelhante ao encontrado no terceiro dos exemplos iniciais: qual o resto na divisão de* 2^{41} *por* 7*? Temos* $2^{41} = (2^3)^{13} \times 2^2$ *e como* $2^3 \equiv 1 \mod 7$*, concluímos que*

$$2^{41} \equiv 2^2 \mod 7$$

ou seja o resto pedido é 4*.*

Exercícios III.1

1. Construir as tabelas da soma e multiplicação para as classes de congruência módulo 7 e módulo 8.
2. Em que classes de congruência mod 8 estão os quadrados perfeitos? 4926834923 poderá ser a soma de dois quadrados perfeitos?
3. Determinar um sistema completo de resíduos módulo 11
   a) constituído por números pares;
   b) constituído por números primos
4. Mostrar que se
$$n = a_0 + a_1 10 + a_2 10^2 + \cdots + a_k 10^k$$
então
$$n \equiv a_0 - a_1 + a_2 - \cdots + (-1)^k a_k \mod 11$$
5. Se p_1, p_2, p_3 e q são primos e
$$q = p_1^2 + p_2^2 + p_3^2$$
justificar, usando congruências módulo 3, que um dos p_i é 3.
Se $n^2 - 2$ e $n^2 + 2$ são ambos primos, justificar que $3 \mid n$.
6. Mostrar que $\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15}$ é inteiro para qualquer $n \in \mathbb{Z}$.
7. Mostrar que se $a, b, c \in \mathbb{Z}$ satisfazem
$$a^2 + b^2 = c^2$$
então um deles é múltiplo de 3, um deles é múltiplo de 4 e um deles é múltiplo de 5.
Sugestão: pode ser necessário usar o resultado do exercício **II.4.6.**.

Dados módulos m e n, não é possível, em geral, estabelecer uma relação entre as respectivas classes de congruência. Mas no caso de $n \mid m$ há uma

relação simples e importante entre $\mathbb{Z}_{/m}$ e $\mathbb{Z}_{/n}$: seja $m = nd$; em primeiro lugar é óbvio que

$$x \equiv y \mod m \implies x \equiv y \mod n;$$

por outro lado, se $x \equiv y \mod n$ é porque existe $k \in \mathbb{Z}$ tal que $y = x + kn$; e verificamos que a classe de congruência $\mod m$ de y só depende da classe de congruência de k módulo d.
Conclui-se que a classe de congruência $\mod n$ de x é a união das d classes de congruência $\mod m$ com representantes

$$x, \qquad x + n, \cdots x + (d-1)n$$

1.2 A equação linear numa variável

Consideramos a equação

$$ax \equiv b \mod m$$

De acordo com as definições dadas, um inteiro x será uma solução se existir $y \in \mathbb{Z}$ tal que $ax - b = my$. Seja $d = mdc(a, m)$; resulta directamente da última equação que para que exista solução é necessário que $d|b$ pois $b = ax - my$.

Por outro lado, sabemos que existem inteiros x_0 e y_0 tais que

$$ax_0 + my_0 = d$$

x_0 e y_0 podem ser determinados por aplicação do algoritmo de Euclides com que se calcula d.

Mas então, se $d|b$, temos que

$$ax_0\frac{b}{d} + my_0\frac{b}{d} = b$$

e vemos que a equação modular tem a solução $x = x_0\frac{b}{d}$ (ou, mais precisamente, a classe de congruência deste número).

Que outras soluções (não congruentes com esta, claro) existem? suponhamos que z e w satisfazem igualmente $az - mw = b$; então

$$az - mw = ax - my \Leftrightarrow a(z-x) = m(w-y) \Leftrightarrow \frac{a}{d}(z-x) = \frac{m}{d}(w-y)$$

mas, como $\frac{a}{d}$ e $\frac{m}{d}$ são primos entre si, isso implica que

$$\frac{m}{d}|(z-x)$$

ou seja

$$z = x + k\frac{m}{d}$$

Duas soluções desta forma serão congruentes módulo m se $d|k$. Temos portanto d soluções distintas, correspondendo aos valores $0 \leq k < d$. Resumindo,

Proposição 1.9 *: Para $m \in \mathbb{N}$, a inteiro e $d = mdc(a, m)$, a equação*

$$ax \equiv b \mod m$$

tem d soluções distintas se $d|b$ e não tem soluções caso contrário.
Se x_0 e y_0 são inteiros satisfazendo $ax_0 + my_0 = d$, as soluções do primeiro caso são

$$x_0\frac{b}{d} + k\frac{m}{d}, \qquad 0 \leq k < d$$

Exemplo 1.10 *: Determinar as soluções de*

$$210x \equiv 10 \mod 745$$

Usando o algoritmo de Euclides

$$\begin{aligned} 745 &= 3 \times 210 + 115 \\ 210 &= 1 \times 115 + 95 \\ 115 &= 1 \times 95 + 20 \\ 95 &= 4 \times 20 + 15 \\ 20 &= 1 \times 15 + 5 \end{aligned}$$

deduzimos que

$$mdc(210, 745) = 5 = 11 \times 745 - 39 \times 210$$

Aplicando a proposição anterior, concluímos que as soluções da equação modular são dadas pela expressão

$$2 \times (-39) + k\frac{745}{5}, \qquad 0 \leq k < 5$$

ou seja, as soluções são (as classes de congruência de)

$$-78, 71, 220, 369, 518$$

É importante notar a seguinte interpretação deste resultado no caso $d = 1$; $mdc(a, m) = 1$ significa que a classe de a é invertível para a multiplicação em $\mathbb{Z}_{/m}$: se $au + mv = 1$, então a classe de u é a inversa da classe de a módulo m; a solução da congruência

$$ax \equiv b \mod m$$

é, como numa equação "habitual", $x = a^{-1}b$ (em que a^{-1} designa a classe inversa da de a).

Por outro lado, no caso geral, se $d = mdc(a, m)$ divide b podemos observar que

$$ax \equiv b \mod m \Leftrightarrow m|(ax - b) \Leftrightarrow \frac{m}{d}|\left(\frac{a}{d}x - \frac{b}{d}\right) \Leftrightarrow \frac{a}{d}x \equiv \frac{b}{d} \mod \frac{m}{d}$$

Assim, podemos começar por encontrar a solução (única) t desta última congruência e notar que as soluções da congruência inicial são as classes $\mod m$ dadas por $t + k\frac{m}{d}$ com $0 \leq k < d$, que são as classes de congruência módulo m que estão contidas na classe de $t \mod \frac{m}{d}$.

Exemplo 1.11 *:* $15x \equiv 21 \mod 72$ *tem* 3 *soluções uma vez que* $mdc(15, 72) = 3$ *e* $3|21$*;*

$$15x \equiv 21 \mod 72 \Leftrightarrow 5x \equiv 7 \mod 24$$

Como $5\dot{5} - 1 \cdot 24 = 1$ *(ou seja o inverso de* 5 *módulo* 24 *é o próprio* 5*) deduzimos que a solução desta última congruência é* $x \equiv 5 \cdot 7 \equiv 11 \mod 24$*.*

Finalmente, $x \equiv 11 \mod 24 \Leftrightarrow x \equiv 11 \vee x \equiv 35 \vee x \equiv 59 \mod 72$*.*

Nota 1.12 *É importante notar que multiplicar ambos os lados de uma congruência por um inteiro só resulta numa congruência* equivalente *(ou seja, com as mesmas soluções) se esse inteiro for primo com o módulo. Caso contrário, temos apenas uma implicação.*
Por exemplo se multiplicarmos por 3 *ambos os lados da congruência*

$$7x \equiv 2 \mod 18,$$

obtemos

$$21x \equiv 6 \mod 18 \Leftrightarrow 3x \equiv 6 \mod 18;$$

esta última equação tem a solução evidente $x \equiv 2 \mod 18$*, que não é solução da equação original. Podemos apenas dizer que a solução da equação original (que existe e é única) está entre as soluções da última, que são as classes de congruência de* 2*,* 8 *e* 14 *módulo* 18*. E de facto*

$$7 \times 6 \equiv 2 \mod 18.$$

Exercícios III.2

1. Resolver as seguintes congruências (encontrar todas as soluções ou justificar que não existem):

   a) $5x \equiv 3 \mod 11$;

   b) $12x \equiv 2 \mod 33$;

   c) $9x \equiv 21 \mod 12$;

   d) $110x \equiv 40 \mod 575$;

   e) $1011x \equiv 1101 \mod 1110$;

   f) $501x \equiv 345 \mod 72$;

2. Justificar que se $ac \equiv bc \mod m$ e $d = mdc(c, m)$, então $a \equiv b \mod m/d$.

3. Mostrar que todo o inteiro da forma $4k + 3$ tem algum factor da mesma forma. Deduzir que existem infinitos primos congruentes com 3 módulo 4.
   Podemos aplicar o mesmo raciocínio para inteiros da forma $4k+1$? E da forma $6k + 5$?

4. Seja p primo. Notando que para cada $1 < a < p - 1$ existe um (único) $1 < a' < p-1$ tal que $aa' \equiv 1 \mod p$, demonstrar o Teorema de Wilson:

$$(p - 1)! \equiv -1 \mod p$$

   se e só se p é primo.
   Usar o resultado anterior para mostrar que

$$61! + 1 \equiv 0 \mod 71.$$

1.3 O Teorema Chinês dos Restos

Começamos com um exemplo simples que está na origem do resultado que vamos apresentar:

Exemplo 1.13 *Um camponês tem um certo número de ovos; quandos os divide por* 3*, sobra-lhe* 1*; quando os divide por* 4*, sobram* 2 *ovos; e quando os divide por* 5*, sobram* 3*. Quantos ovos tem o camponês?*
O que queremos aqui é a solução simultânea de um sistema de equações modulares

$$\begin{cases} x \equiv 1 & \mod 3 \\ x \equiv 2 & \mod 4 \\ x \equiv 3 & \mod 5 \end{cases}$$

Começando pela primeira equação, temos que qualquer solução x do sistema tem que satisfazer

$$x = 1 + 3y$$

para algum $y \in \mathbb{Z}$; substituindo na segunda equação ficamos com

$$3y + 1 \equiv 2 \mod 4 \Leftrightarrow 3y \equiv 1 \mod 4 \Leftrightarrow y \equiv 3 \mod 4$$

e portanto $y = 3 + 4z$ e $x = 1 + 3(3 + 4z) = 10 + 12z$, onde, mais uma vez, z representa uma nova incógnita inteira; substituindo de novo na terceira equação

$$12z + 10 \equiv 3 \mod 5 \Leftrightarrow 2z \equiv 3 \mod 5 \Leftrightarrow z \equiv 4 \mod 5$$

Concluímos que $z = 4 + 5w$ e portanto a solução do nosso sistema é

$$x = 10 + 12(4 + 5w) = 58 + 60w.$$

A resposta à pergunta é portanto que o camponês poderia ter 58 *ovos ou* 118 *ou* 178*, etc.*

Que a solução do sistema só fica determinada módulo 60 é evidente, uma vez que, como 60 é múltiplo de 3, de 4 e de 5, se x for solução, qualquer inteiro da forma $x + 60w$ também seria solução. Por outro lado, se x e y forem duas soluções do sistema, então $x - y$ será divisível por 3, por 4 e por 5, e como estes são primos dois a dois, $x - y$ tem que ser divisível pelo seu produto 60. Podemos também observar que o facto de 3, 4 e 5 serem primos entre si dois a dois nos garantiu que ao substituir o valor de x na segunda e depois

na terceira equação, ficaríamos sempre com uma equação com soluções, uma vez que o coeficiente de y e depois de z é primo com o módulo da equação respectiva.

Vamos agora enunciar um resultado fundamental para a simplificação da resolução de equações modulares:

Teorema 1.14 *(**Teorema Chinês dos Restos**) : Sejam $m_1, m_2, \cdots, m_k$ inteiros positivos primos dois a dois (ou seja, se $1 \leq i < j \leq k$ então $mdc(m_i, m_j) = 1$) e $M = \prod_{i=1}^{k} m_i$. Então, dados $a_1, a_2, \cdots, a_k$ quaisquer, o sistema de congruências*

$$\begin{cases} x \equiv a_1 & \mod m_1 \\ x \equiv a_2 & \mod m_2 \\ \vdots & \\ x \equiv a_k & \mod m_k \end{cases}$$

tem solução que é única módulo M.

Demonstração 1.15 *Comecemos por notar que a observação feita a propósito do exemplo, vale em geral: dada uma solução do sistema ela é única módulo M, uma vez que se x e y são soluções, temos $m_i \mid (x - y)$ para todo o i e como os m_i são primos dois a dois isso implica $M \mid (x - y)$.*
O método iterativo de solução usado no exemplo pode ser usado para fazer uma demonstração por indução: dado um sistema com duas equações

$$\begin{cases} x \equiv a_1 & \mod m_1 \\ x \equiv a_2 & \mod m_2 \end{cases}$$

a solução pode ser determinada como já vimos substituindo na segunda equação x por $a_1 + m_1 y$; a equação

$$m_1 y \equiv a_2 - a_1 \mod m_2$$

tem solução única módulo m_2 uma vez que $mdc(m_1, m_2) = 1$.
Suponhamos agora, como hipótese de indução, que o resultado do teorema é válido para um certo k e seja

$$\begin{cases} x \equiv a_1 & \mod m_1 \\ x \equiv a_2 & \mod m_2 \\ \vdots & \\ x \equiv a_k & \mod m_k \\ x \equiv a_{k+1} & \mod m_{k+1} \end{cases}$$

Chamemos n ao produto $m_1 \times \cdots \times m_k$. Por hipótese de indução, o sistema constituído pelas primeiras k equações tem solução única $c \mod n$; podemos então resolver o sistema de duas equações

$$\begin{cases} x \equiv c & \mod n \\ x \equiv a_{k+1} & \mod m_{k+1} \end{cases}$$

a sua solução, única módulo $n \times m_{k+1} = M$, é a desejada solução do sistema de $k+1$ equações.

III.3

1. Resolver os sistemas de equações

$$\begin{cases} x \equiv 2 & \mod 3 \\ x \equiv 3 & \mod 5 \\ x \equiv 5 & \mod 2 \end{cases} \qquad \begin{cases} x \equiv 1 & \mod 4 \\ x \equiv 0 & \mod 3 \\ x \equiv 5 & \mod 7 \end{cases}$$

2. Ao tentar formar grupos de trabalho numa turma, conclui-se que se os grupos tiverem 3 elementos ficam dois alunos de fora, se tiverem quatro fica 1 de fora, mas que se consegue formar grupos de 5 elementos desde que o professor faça parte de um deles. Quantos alunos terá a turma?

3. Determinar 3 inteiros consecutivos tais que um é divisível pelo quadrado de um primo, outro é divisível pelo cubo de um primo e o terceiro é divisível pela quarta potência de um primo.

4. Mostrar que, dados inteiros positivos m_1 e m_2, o sistema

$$\begin{cases} x \equiv a_1 & \mod m_1 \\ x \equiv a_2 & \mod m_2 \end{cases}$$

tem solução se e só se $a_1 \equiv a_2 \mod mdc(m_1, m_2)$, e que nesse caso a solução é única módulo $mmc(m_1, m_2)$.

5. Determinar, se existirem, as soluções do sistema

$$\begin{cases} 5x \equiv 1 & \mod 6 \\ 4x \equiv 13 & \mod 15 \end{cases}$$

O Teorema Chinês dos Restos permite reduzir a resolução de uma congruência à de um sistema de congruências mais simples:

Exemplo 1.16 *: Considere-se a equação*

$$327x \equiv 171 \mod 520;$$

Calculando $mdc(327, 520) = 1$ *podemos deduzir que existe uma única solução e aplicar o método explicado mais atrás. No entanto, notando que* $520 = 5 \cdot 8 \cdot 13$*, passamos ao sistema*

$$\begin{cases} 327x \equiv 171 & \mod 5 \\ 327x \equiv 171 & \mod 8 \\ 327x \equiv 171 & \mod 13 \end{cases} \Leftrightarrow \begin{cases} 2x \equiv 1 & \mod 5 \\ 7x \equiv 3 & \mod 8 \\ 2x \equiv 2 & \mod 13 \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} x \equiv 3 & \mod 5 \\ x \equiv 5 & \mod 8 \\ x \equiv 1 & \mod 13 \end{cases}$$

Qualquer solução da equação inicial terá que ser também solução de cada uma das equações do sistema e reciprocamente, pelo Teorema Chinês dos Restos, qualquer solução do sistema é solução da equação inicial.

Usamos o mesmo método de solução do exemplo anterior: pela primeira equação $x = 3 + 5y$*; substituindo na segunda temos*

$$5y \equiv 2 \mod 8 \Leftrightarrow y \equiv 2 \mod 8$$

portanto $y = 2 + 8z$ *e* $x = 13 + 40z$*, o que nos dá, na última equação,*

$$40z \equiv 1 \mod 13 \Leftrightarrow z \equiv 1 \mod 13$$

donde se deduz finalmente que $x = 53 + 520w$*.*

É possível demonstrar o teorema de outra forma, que nos fornece igualmente um método prático de solução: Dado o sistema no enunciado, calcula-se, para cada $1 \leq i \leq k$, um inteiro b_i tal que

$$\frac{M}{m_i} b_i \equiv 1 \mod m_i$$

Note-se que isto é possível, uma vez que $mdc(\frac{M}{m_i}, m_i) = 1$, ficando b_i determinado naturalmente módulo m_i. Verificamos que x definido por

$$x = \sum_{i=1}^{k} \frac{M}{m_i} b_i a_i$$

é solução do sistema; fixemos um índice $1 \leq j \leq k$; nas parcelas do somatório com $i \neq j$ temos que $m_j \mid \frac{M}{m_i}$ (m_i e m_j são primos entre si) e portanto essas parcelas anulam-se módulo m_j; na parcela de índice j, devido ao modo como escolhemos b_j, temos

$$\frac{M}{m_j} b_j a_j \equiv a_j \mod m_j$$

Este método de solução torna-se mais útil quando temos que resolver não um mas vários sistemas de equações com os mesmos módulos $m_1, \cdots, m_k$, como veremos a seguir.

O próximo exemplo envolve equações modulares de grau maior que 1 para pôr em evidência as vantagens do segundo método de solução de um sistema.

Exemplo 1.17 *: Procuramos as soluções simultâneas do sistema de equações*

$$\begin{cases} x^2 \equiv 2 & \mod 7 \\ x^3 \equiv 1 & \mod 9 \\ x^4 \equiv 3 & \mod 11 \end{cases}$$

Como não temos (por enquanto) nenhuma forma mais eficaz de tratar estas equações, procuramos as suas soluções directamente, calculando a^2 *em que* a *percorre todas as classes de congruência módulo* 7*, e do mesmo modo para as outras equações. Concluímos que a primeira equação tem duas soluções* 3 *e* 4 *módulo* 7*, a segunda tem três soluções módulo* 9*:* 1*,* 4 *e* 7*, e a terceira tem duas soluções* 4 *e* 7*. Teríamos portanto que resolver os* 12 *sistemas de* 3 *equações da forma*

$$\begin{cases} x \equiv a_1 & \mod 7 \\ x \equiv a_2 & \mod 9 \\ x \equiv a_3 & \mod 11 \end{cases}$$

onde $a_1 \in \{3, 4\}$*,* $a_2 \in \{1, 4, 7\}$ *e* $a_3 \in \{4, 7\}$*.*
Em alternativa, podemos usar o outro método: designando $M = 7 \times 9 \times 11 = 693$*, resolvemos as equações da forma*

$$\frac{M}{m_i} y \equiv 1 \mod m_i$$

Temos

$$99y \equiv 1 \mod 7 \Leftrightarrow y \equiv 1 \mod 7$$

e portanto podemos escolher $b_1 = 1$*. As outras equações são*

$$77y \equiv 1 \mod 9 \Leftrightarrow 5y \equiv 1 \mod 9 \Leftrightarrow y \equiv 2 \mod 9$$

e

$$63y \equiv 1 \mod 11 \Leftrightarrow 8y \equiv 1 \mod 11 \Leftrightarrow y \equiv 7 \mod 11$$

e portanto $b_2 = 2$ *e* $b_3 = 7$*. Substituindo os valores dos* a_i *na expressão*

$$\sum_{i=1}^{3} \frac{M}{m_i} b_i a_i = 99a_1 + 154a_2 + 441a_3$$

obtemos as doze soluções pretendidas.
Recorde-se que os b_i são calculados módulo m_i; podemos portanto, por exemplo, pôr $b_3 = -4$; as soluções obtidas são as mesmas módulo M, ainda que representadas por outros inteiros.

Exercícios III.4

1. Determinar, usando o Teorema Chinês dos Restos, as soluções, se existirem, das equações

$$507x \equiv 312 \mod 3025$$
$$264x \equiv 31 \mod 1573$$
$$732x \equiv 84 \mod 504$$

2. Determinar directamente as soluções de

$$x^3 + 2x - 3 \equiv 0 \mod 5$$

e de

$$x^3 + 2x - 3 \equiv 0 \mod 9$$

e usar as soluções encontradas para determinar as de

$$x^3 + 2x - 3 \equiv 0 \mod 45$$

3. Sabendo que $1144 = 8 \times 11 \times 13$, determinar, ou mostrar que não existem, as soluções das congruências seguintes

   a) $68x \equiv 28 \mod 1144$

   b) $24x \equiv 44 \mod 1144$

4. a) Determinar os pares de inteiros consecutivos tais que a sua soma é divisível por 9 e o seu produto é divisível por 11.

   b) Determinar o primeiro par de inteiros positivos ímpares consecutivos em que o menor deles é múltiplo de 17 e o maior é múltiplo de 11.

O Teorema Chinês dos Restos pode ser enunciado alternativamente do seguinte modo:

Teorema 1.18 *: Se* $M = m_1 \times \cdots \times m_k$ *e* $mdc(m_i, m_j) = 1$ *se* $i \neq j$*, então a aplicação*

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

definida por

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

é uma bijecção.

A existência de solução para qualquer sistema da forma

$$\begin{cases} x \equiv a_1 & \mod m_1 \\ x \equiv a_2 & \mod m_2 \\ \vdots & \\ x \equiv a_k & \mod m_k \end{cases}$$

é equivalente a ψ ser sobrejectiva; por outro lado, a propriedade de ψ ser injectiva é equivalente a aquela solução ser única módulo M.

Quando enunciado desta forma, o Teorema Chinês dos Restos é de demonstração ainda mais simples: de facto, basta provar que ψ é injectiva, sendo a sobrejectividade uma consequência imediata de o domínio e o contra-domínio desta aplicação terem o mesmo número de elementos. Mas ψ é injectiva uma vez que

$$x \equiv y \mod m_i \, \forall i \in \{1, \cdots, k\} \Leftrightarrow x \equiv y \mod M.$$

Por outro lado, este raciocínio não nos indica como resolver na prática um sistema, ou seja, dados $a_i \in \mathbb{Z}_{/m_i}$, como determinar

$$\psi^{-1}(a_1, \cdots, a_k)$$

É isso que as outras demonstrações fazem. De facto, a segunda dessas demonstrações dá-nos uma fórmula para a função inversa de ψ:

$$\psi^{-1}(a_1, \cdots, a_k) = \sum_{i=1}^{k} \frac{M}{m_i} b_i a_i$$

ou mais precisamente a classe de congruência módulo M deste inteiro.

Nota 1.19 *Uma aplicação ao cálculo aritmético, particularmente útil quando é preciso realizar um grande número de cálculos envolvendo inteiros pertencentes a um intervalo fixo mas grande, é a seguinte: suponhamos, por exemplo, que queremos multiplicar dois inteiros* $10^{50} < x, y < 10^{100}$*; podemos escolher um conjunto de inteiros* $m_1, \cdots, m_l$*, primos entre si dois a dois, tais que* $\prod_{i=1}^{l} m_i > 10^{200}$*, reduzir* x *e* y *e calcular o produto* xy *módulo cada* m_i*, e obter o resultado final por aplicação do Teorema Chinês dos Restos.*