Divisibilidade e números Inteiros

Introdução à aritmética Modular

Material Complementar

Soluções e Observações

Samuel Jurkiewicz

Sumário

Capítulo 1

Material complementar

A seqüência de Fibonacci

A seqüência de Fibonacci é:

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots$$

isto é, cada termo é igual à soma dos dois anteriores (com excessão dos dois primeiros que são iguais a 1. Costumamos simbolizar os termos desta seqüência por F_n. Assim, $F_1 = 1$, $F_7 = 13$. A formação da seqüência pode ser expressa por:

$$F_n = F_{n-1} + F_{n-2}, \quad n \in \mathbb{Z}.$$

1. Mostre que dois termos seguidos da seqüência de Fibonacci são primos entre si, i.é., $mdc(F_n, F_{n-1}) = 1$.

   Solução

   Utilizando o algorítmo de Euclides obtemos a seguinte seqüência:

   $F_n = F_{n-1} + F_{n-2}$ onde F_{n-2} é o resto;

   $F_{n-1} = F_{n-2} + F_{n-3}$ onde F_{n-3} é o resto;

   ...e assim por diante. Esta seqüência terminará invariavelmente com resto 1.

   Por exemplo, calculando o $mdc(89, 55)$:

$$89 = 55 + 34$$
$$55 = 34 + 21$$
$$34 = 21 + 13$$
$$21 = 13 + 8$$
$$13 = 8 + 5$$
$$8 = 5 + 3$$
$$5 = 3 + 2$$
$$3 = 2 + 1$$

2. Mostre que dois números alternados da seqüência de Fibonacci são primos entre si, i.é., $mdc(F_n, F_{n-2}) = 1$.

   Solução

   Utilizando o algorítmo de Euclides obtemos a seguinte seqüência:

   $F_n = F_{n-1} + F_{n-2} \Rightarrow F_n = F_{n-2} + F_{n-3} + F_{n-2}$

   $F_n = 2 \cdot F_{n-2} + F_{n-3}$ onde F_{n-3} é o resto;

   $F_{n-2} = F_{n-3} + F_{n-4}$ onde F_{n-3} é o resto;

   ...e o problema se reduz ao ítem anterior.

3. Mostre que F_{5k} é múltiplo de 5 para qualquer valor de k.

   Solução

   Queremos mostrar que F_{5k} é múltiplo de 5. Usaremos a indução sobre k.

   Se $k = 1$, $F_{5k} = F_5 = 1$.

   Se F_{5k} é múltiplo de 5 o que acontece com $F_{5(k+1)} = F_{5k+5}$?

   $F_{5k+5} = F_{5k+4} + F_{5k+3} = F_{5k+3} + F_{5k+2} + F_{5k+2} + F_{5k+1}$

   $F_{5k+5} = F_{5k+3} + 2 \cdot F_{5k+2} + F_{5k+1}$

   $F_{5k+5} = F_{5k+2}+F_{5k+1}+2\cdot F_{5k+1}+2\cdot F_{5k}+F_{5k+1} = F_{5k+2}+4\cdot F_{5k+1}+2\cdot F_{5k}$

   $F_{5k+5} = F_{5k+1} + F_{5k} + 4 \cdot F_{5k+1} + 2 \cdot F_{5k} = 5 \cdot F_{5k+1} + 2 \cdot F_{5k}$

   As duas parcelas à direita são múltiplos de 5 (a segunda parcela pela hipótese de indução) logo,F_{5k} é múltiplo de 5 para qualquer valor de k.

4. Mostre que se $10x + y$ é divisível por 7 se e só se $x - 2y$ também for.

   Solução

   $10x + y$ é divisível por 7 $\Leftrightarrow$

   $10x + y - 7x - 7y$ é divisível por 7 $\Leftrightarrow$

   $3x - 6y$ é divisível por 7 $\Leftrightarrow$

   $3(x - 2y)$ é divisível por 7 $\Leftrightarrow$

   $x - 2y$ é divisível por 7.

5. Use o exercício 4 para estabelecer o seguinte critério de divisibilidade por 7:

   Para saber se um número é divisível por 7 multiplicamos o último algarismo do número por 2 e subtraimos o resultado do número obtido do número inicial pela supressão do último algarismo.

   (a) Exemplo: $294 \Rightarrow 29|4 \Rightarrow 29 - 8 = 21 \Rightarrow 294$ é divisível por 7.

   (b) Exemplo: $248738 \Rightarrow 24873 - 16 = 24857 \Rightarrow 2485 - 14 = 2471 \Rightarrow 247 - 2 = 245 \Rightarrow 24 - 10 = 14 \Rightarrow 248738$ é divisível por 7.

   (c) Exemplo: $7557 \Rightarrow 755 - 14 = 741 \Rightarrow 74 - 2 = 72 \Rightarrow 7 - 4 = 3 \Rightarrow 7557$ não é divisível por 7.

Observação

Podemos expressar teóricamente o algorítmo acima. Um número qualquer é expresso por algarismos:

$$ABCDE \cdots KLM$$

Se fizermos $x = ABC \cdots KL$ e $y = M$, teremos

$$ABCDE \cdots KLM = 10x + y$$

que só será divisível or 7 se $x - 2y = ABC \cdots KL - 2M$ também for.

6. Invente seus exemplos. Verifique que, ao contrário dos algorítmos usuais, esse critério **NÃO** permite descobrir o resto de uma divisão por 7.

   Observação

   De fato, no exemplo anterior

   $7557 \Rightarrow 755 - 14 = 741 \Rightarrow 74 - 2 = 72 \Rightarrow 7 - 4 = 3 \Rightarrow 7557$ não é divisível por 7.

   Mas o resto da divisão de 7557 por 7 é 4 e não 3.

7. Na apostila 1, ná página 45, ítem 25 você construiu a tabela de multiplicação módulo 5.

$\overset{\times}{\text{mod}5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

   Observe que para obter $\overline{0}$ tivemos que ter $\overline{0}$ como fator. No ítem 24 fabricamos a tabela da multiplicação módulo 4.

$\overset{\times}{\text{mod}4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

   Você consegue encontrar um produto que dê $\overline{0}$ com os dois fatores diferentes de $\overline{0}$? Isto é o que chamamos um **divisor de** $\overline{0}$.

8. Você encontra divisores de $\overline{0}$ na tabela de multiplicação módulo 7 ?

   Solução

   Não há divisores de $\overline{0}$ na tabela de multiplicação módulo 7.

9. Você encontra divisores de $\overline{0}$ na tabela de multiplicação módulo 6 ?

   Solução

   Sim, o $\overline{2}$ e o $\overline{3}$.

10. Em que tabelas você encontra divisores de $\overline{0}$? e quem são os divisores $\overline{0}$?

    Solução

    Encontramos divisores de $\overline{0}$ na tabela de multiplicação módulo n se e só se n for primo. Se o número n for composto os divisores de $\overline{0}$ são os números m para os quais $mdc(m, n) > 1$.

A função ϕ de Euler

A função ϕ de Euler

Dizemos que um número n é **co-primo** com m se $mdc(m, n) = 1$, isto é, se m e n são **primos entre si**. A função ϕ de Euler conta, para um número natural n, os números, também naturais, menores que n e que são co-primos com êle.

Exemplo: $\phi(6) = 2$ pois :
$mdc(1, 6) = 1,$
$mdc(2, 6) = 2,$
$mdc(3, 6) = 3,$
$mdc(4, 6) = 2,$
$mdc(5, 6) = 1.$

Exemplo: $\phi(8) = 4$ pois :
$mdc(1, 8) = 1,$
$mdc(2, 8) = 2,$
$mdc(3, 8) = 1,$
$mdc(4, 8) = 4,$
$mdc(5, 8) = 1,$
$mdc(6, 8) = 2,$
$mdc(7, 8) = 1.$

Calcule:

(a) $\phi(1) =$

(b) $\phi(2) =$

(c) $\phi(3) =$

(d) $\phi(4) =$

(e) $\phi(5) =$

(f) $\phi(6) =$

(g) $\phi(7) =$

(h) $\phi(8) =$

(i) $\phi(9) =$

(j) $\phi(10) =$

(k) $\phi(11) =$
(l) $\phi(12) =$

Solução

(a) $\phi(1) = 1$, o conjunto de co-primos é $\{1\}$
(b) $\phi(2) = 1$, o conjunto de co-primos é $\{1\}$
(c) $\phi(3) = 2$, o conjunto de co-primos é $\{1; 2\}$
(d) $\phi(4) = 2$, o conjunto de co-primos é $\{1; 3\}$
(e) $\phi(5) = 4$, o conjunto de co-primos é $\{1; 2; 3; 4\}$
(f) $\phi(6) = 2$, o conjunto de co-primos é $\{1; 5\}$
(g) $\phi(7) = 6$, o conjunto de co-primos é $\{1; 2; 3; 4; 5; 6\}$
(h) $\phi(8) = 4$, o conjunto de co-primos é $\{1; 3; 5; 7\}$
(i) $\phi(9) = 6$, o conjunto de co-primos é $\{1; 2; 4; 5; 7; 8\}$
(j) $\phi(10) = 4$, o conjunto de co-primos é $\{1; 3; 7; 9\}$
(k) $\phi(11) = 10$, o conjunto de co-primos é $\{1; 2; 3; 4; 5; 6; 7; 8; 9; 10\}$
(l) $\phi(12) = 4$, o conjunto de co-primos é $\{1; 5; 7; 11\}$

11. Quais são os números naturais n para os quais $\phi(n) = n - 1$?

Solução

n deve ser primo.

Voltaremos a falar da função ϕ de Euler mais adiante

Equações com números inteiros - equações diofantinas

Vamos agora trabalhar com equações com números inteiros. Elas são chamadas **diofantinas** em homenagem a Diophante de Alexandria, matemático grego que viveu nos meados do século III.

Diophante é considerado como um dos fundadores da álgebra. Escreveu uma obra sobre Aritmética em 13 volumes e dos quais apenas seis se preservaram. seus estudos se basearam no uso de símbolos para facilitar a escrita e os cálculos matemáticos.

Os símbolos criados por Diofante fizeram com que as expressões, até então escritas totalmente com palavras, pudessem ser representadas com abreviações.

Procuraremos números inteiros que satisfaçam às expressões algébricas.

12. Determine as soluções **inteiras** da equação:

$$5X + 3Y = 1$$

Solução e observação

Nestes primeiros exemplos, a idéia é procurar por meio de1 tentativa e erro. Os primeiros são simples, depois começa a complicar. Existe mais do que uma solução, logo as respostas devem ser verificadas.

Por exemplo

$$X = -1$$
$$Y = 2$$

13. Determine as soluções **inteiras** da equação:

$$17X + 5Y = 4$$

Solução

Por exemplo

$$X = -3$$
$$Y = 11$$

14. Determine as soluções **inteiras** da equação:

$$3X + 6Y = 4$$

Solução

É impossível. O $mdc(3, 6) = 3$ logo o termo à direita tem que ser múltiplo de 3, o que não acontece.

15. Determine as soluções **inteiras** da equação:

$$119X + 35Y = 6$$

Pista: Qual o $mdc(119, 35)$? Por que isso é importante ?

Solução

É impossível. O $mdc(119, 35) = 7$ logo o termo à direita tem que ser múltiplo de 7, o que não acontece.

16. Determine as soluções **inteiras** da equação:

$$119X + 35Y = 14$$

Solução

O $mdc(119, 35) = 7$ e o termo à direita é múltiplo de 7, logo podemos simplificar para:

$$17X + 5Y = 2$$

Por exemplo

$$X = 1$$
$$Y = -3$$

17. Suponha que $mdc(a, b)$ **não** divida o número inteiro c. Mostre que a equação:

$$aX + bY = c$$

não admite soluções **inteiras**.

Solução

$aX + bY$ será sempre múltiplo de $mdc(a, b)$, logo c também deve ser, caso contrário, a equação não tem solução.

Observação: O que vem a seguir depende do entendimento do Algorítmo de Euclides, abordado na apostila 1.

18. Vamos encontrar uma solução para a equação:

$$5X + 3Y = 1$$

Começamos executando o **algorítmo de Euclides** (veja a apostila 1, nas páginas 25 e 26.

Quociente	1	1	
5	3	2	
Resto	2	1	

$mdc(5,3) = 1$

Quais foram as etapas ?

$$5 = 1 \times 3 + 2 \Rightarrow 2 = 5 - 1 \times 3$$

$$3 = 1 \times 2 + 1 \Rightarrow 1 = 3 - 1 \times 2$$

Vamos "reconstruir" o mdc, no caso 1.

$$1 = 3 - 1 \times 2$$

Substituimos o 2 por seu valor na outra equação:

$$1 = 3 - 1 \times 2 = 3 - 1 \times (5 - 1 \times 3)$$

O que nos dá

$$1 == 3 - 1 \times 5 + 1 \times 3 = 2 \times 3 - 1 \times 5$$

Observe que conseguimos uma solução inteira para nossa equação !

$$X = -1$$

$$Y = 2$$

De fato $5 \cdot (-1) + 3 \cdot 2 = 1$.

Acabamos de encontrar uma solução inteira para

$$5X + 3Y = 1$$

a saber

$$X = -1$$

$$Y = 2$$

19. Encontre soluções para as equações:

Observação: As soluções das equações a seguir se obtém por multiplicação das raízes.

(a)

$$5X + 3Y = 3$$

Solução

$$X = -3$$

$$Y = 6$$

(b)
$$5X + 3Y = 7$$

Solução
$$X = -7$$
$$Y = 14$$

(c)
$$5X + 3Y = -2$$

Solução
$$X = 2$$
$$Y = -4$$

(d)
$$5X + 3Y = -127$$

Solução
$$X = 127$$
$$Y = -254$$

Podemos agora enunciar a seguinte proposição:

Sejam a,b e c números inteiros diferentes de 0. A equação:

$$aX + bY = c$$

admitirá soluções inteiras se e só o $mdc(a, b)$ dividir c.

20. Outro exemplo: Determine números X e Y **inteiros** que satisfaçam às equações (ou mostre que é impossível):

$$24X + 9Y = 6$$

Como $mdc(24, 9) = 3$ e 3 divide 6, a equação terá soluções. mais ainda, a equação é equivalente a:
$$8X + 3Y = 2$$

Quociente	2	1	
8	3	2	
Resto	2	1	

$mdc(8, 3) = 1$

Quais foram as etapas ?

$$8 = 2 \times 3 + 2 \Rightarrow 2 = 8 - 2 \times 3$$
$$3 = 1 \times 2 + 1 \Rightarrow 1 = 3 - 1 \times 2$$

Vamos "reconstruir" o mdc, no caso 1.

$$1 = 3 - 1 \times 2$$

Substituimos o 2 por seu valor na outra equação:

$$1 = 3 - 1 \times 2 = 3 - 1 \times (8 - 2 \times 3)$$

O que nos dá

$$1 == 3 - 1 \times 8 + 2 \times 3 = 3 \times 3 - 1 \times 8$$

Observe que conseguimos uma solução inteira para a equação:

$$8X + 3Y = 1$$

$$X = -1$$

$$Y = 3$$

Mas nossa equação é:

$$8X + 3Y = 2$$

Fazemos:

$$X = -2$$

$$Y = 6$$

De fato $8 \cdot (-2) + 6 \cdot 3 = 2$.

21. Determine números X e Y **inteiros** que satisfaçam às equações (ou mostre que é impossível):

    (a) $7X + 4Y = 5$
    solução
    $mdc(4, 7) = 1$
    Quais foram as etapas ?

    $$7 = 4 + 3$$

    $$4 = 3 + 1$$

    Vamos "reconstruir" o mdc, no caso 1.

    $$1 = 4 - 3$$

    Substituimos o 3 por seu valor na outra equação:

    $$1 = 4 - (7 - 4)$$

    O que nos dá

    $$1 == 2 \times 4 - 1 \times 7$$

    Observe que conseguimos uma solução inteira para a equação:

    $$7X + 4Y = 1$$

    $$X = -1$$

    $$Y = 2$$

Mas nossa equação é:

$$7X + 4Y = 5$$

Fazemos:

$$X = -5$$

$$Y = 10$$

De fato $7 \cdot (-5) + 10 \cdot 4 = 5$.

(b) $8X + 6Y = 12$

solução

$mdc(8, 6) = 2$

Quais foram as etapas ?

$$8 = 6 + 2$$

Vamos "reconstruir" o mdc, no caso 2.

$$2 = 8 - 6$$

O que nos dá

$$2 = 1 \times 8 - 1 \times 6$$

Observe que conseguimos uma solução inteira para a equação:

$$8X + 6Y = 2$$

$$X = 1$$

$$Y = -1$$

Mas nossa equação é:

$$8X + 6Y = 12$$

Fazemos:

$$X = 6$$

$$Y = -6$$

De fato $8 \cdot (6) + 6 \cdot (-6) = 12$.

(c) $8X + 12Y = 18$

solução

$mdc(8, 12) = 4$ que não divide 18. Logo a equação não tem solução.

(d) $7X + 3Y = 2$

solução

$mdc(7, 3) = 1$

Quais foram as etapas ?

$$7 = 2 \times 3 + 1$$

Vamos "reconstruir" o mdc, no caso 2.

$$1 = 7 - 2 \times 3$$

Observe que conseguimos uma solução inteira para a equação:

$$7X + 3Y = 1$$

$$X = 1$$

$$Y = -2$$

Mas nossa equação é:

$$7X + 3Y = 2$$

Fazemos:

$$X = 2$$

$$Y = -4$$

De fato $7 \cdot (2) + 3 \cdot (-4) = 2$.

(e) $8X + 12Y = 16$
solução
$mdc(8, 12) = 4$
Quais foram as etapas ?

$$12 = 8 + 4$$

Vamos "reconstruir" o mdc, no caso 4.

$$4 = 12 - 8$$

Observe que conseguimos uma solução inteira para a equação:

$$8X + 12Y = 4$$

$$X = -1$$

$$Y = 1$$

Mas nossa equação é:

$$14X + 24 = 16$$

Fazemos:

$$X = -4$$

$$Y = 4$$

De fato $8 \cdot (8) - 12 \cdot (-4) = 16$.

(f) $14X + 24Y = 8$
solução
$mdc(14, 24) = 2$
Quais foram as etapas ?

$$24 = 14 + 10$$

$$14 = 10 + 4$$

$$10 = 2 \times 4 + 2$$

Vamos "reconstruir" o mdc, no caso 2.

$$2 = 10 - 2 \times 4$$

$$2 = 10 - 2 \times (14 - 10) = 3 \times 10 - 2 \times 14$$
$$2 = 3 \times (24 - 14) - 2 \times 14 = 3 \times 24 - 5 \times 14$$

Observe que conseguimos uma solução inteira para a equação:

$$14X + 24Y = 2$$

$$X = -5$$
$$Y = 3$$

Mas nossa equação é:

$$14X + 24Y = 8$$

Fazemos:

$$X = -20$$
$$Y = 12$$

De fato $14 \cdot (-20) - 12 \cdot (24) = 8$.

(g) $15X + 12Y = 20$
solução
$mdc(15, 12) = 3$ que não divide 20. Logo a equação não tem solução.

(h) $4X + 6Y = 9$
solução
$mdc(4, 6) = 2$ que não divide 9. Logo a equação não tem solução.

(i) $3X + 6Y = 9$
solução
$mdc(3, 6) = 3$
Quais foram as etapas ?

$$6 = 2 \times 3$$

Vamos "reconstruir" o mdc, no caso 3.
Neste caso a reconstrução é extremamente simples:

$$3 = 3$$

Observe que conseguimos uma solução inteira para a equação:

$$3X + 6Y = 3$$

$$X = 1$$
$$Y = 0$$

Mas nossa equação é:

$$3X + 6Y = 9$$

Fazemos:

$$X = 3$$
$$Y = 0$$

De fato $3 \cdot (3) + 6 \cdot 0 = 9$.

(j) $128X + 64Y = 32$
solução
$mdc(128, 64) = 64$ que não divide 32. Logo a equação não tem solução.

(k) $3X + 2Y = 493$
solução
$mdc(3, 2) = 1$
Quais foram as etapas ?

$$3 = 2 + 1$$

Vamos "reconstruir" o mdc, no caso 2.

$$1 = 3 - 2$$

Observe que conseguimos uma solução inteira para a equação:

$$3X + 2Y = 1$$

$$X = 1$$

$$Y = -1$$

Mas nossa equação é:

$$3X + 2Y = 493$$

Fazemos:

$$X = 493$$

$$Y = -493$$

De fato $3 \cdot (493) - 2 \cdot (493) = 493$.

22. Encontre **todas** as soluções inteiras da equação:

$$5X + 3Y = 1$$

Já temos uma solução (encontrada em itens anteriores):

$$X = -1$$

$$Y = 2$$

Podemos somar e subtrair o mesmo número ao lado esquerdo e a equação será equivalente. Escolherei para somar e subtrair (quem adivinha ?) o $mmc(5, 3) = 15$.

$$5X + 15 + 3Y - 15 = 1$$

$$5(X + 3) + 3(Y - 5) = 1$$

Isso mostra que posso somar/subtrair 3 do valor de X desde que eu subtraia/some 5 ao valor de Y. Por exemplo:

$$X = -1 + 3 = 2$$

$$Y = 2 - 5 = -3$$

também é solução da equação original. Verificando:

$$5(2) + 3(-3) = 10 - 9 = 1$$

Portanto a solução geral da equação

$$5X + 3Y = 1$$

é

$$X = -1 + 3t$$
$$Y = 2 - 5t$$

Onde t é um número inteiro.

Importante : Para obter todas as soluções, é imprescindível que a equação seja reduzida. Por exemplo:

$$4X + 6Y = 18$$

Reduzimos para:

$$2X + 3Y = 9$$

Uma solução é:

$$X = 0$$
$$Y = 3$$

Uma solução geral é $X = 0 + 9t$, $Y = 3 - 9t$. O $mdc(4, 6) = 2$ se encarrega de "produzir" o 18 a partir de $9t$ para cada t escolhido.

23. Encontre **todas** as soluções inteiras da equação:

    Observação: utilizaremos as soluções obtidas em ítens anteriores

    (a) $7X + 4Y = 5$

    Solução

    $$X = -5 + 4t$$
    $$Y = 10 - 7t$$

    t inteiro.

    (b) $8X + 6Y = 12$

    Solução

    Reduzimos para:

    $$4X + 3Y = 6$$

    Uma solução é:

    $$X = 6$$
    $$Y = -6$$

    A solução geral é:

    $$X = 6 + 3t$$
    $$Y = -6 - 4t$$

    t inteiro.

(c) $8X + 12Y = 18$
solução
$mdc(8, 12) = 4$ que não divide 18. Logo a equação não tem solução.

(d) $7X + 3Y = 2$

$$X = 2 + 3t$$
$$Y = -4 - 7t$$

t inteiro.

(e) $14X + 24Y = 8$

$$X = -20 + 24t$$
$$Y = 12 - 14t$$

t inteiro.

(f) $15X + 12Y = 20$
solução
$mdc(15, 21) = 3$ que não divide 20. Logo a equação não tem solução.

(g) $7X + 3Y = 2$

$$X = 1 + 3t$$
$$Y = -2 - 7t$$

t inteiro.

(h) $4X + 6Y = 9$
solução
$mdc(4, 6) = 2$ que não divide 9. Logo a equação não tem solução.

(i) $3X + 6Y = 9$
Reduzimos para:

$$X + 2Y = 3$$

Uma solução é:

$$X = 3$$
$$Y = 0$$

A solução geral é:

$$X = 3 + 2t$$
$$Y = 0 - t$$

t inteiro.
t inteiro.

(j) $128X + 64Y = 32$
solução
$mdc(128, 64) = 64$ que não divide 32. Logo a equação não tem solução.

(k) $3X + 2Y = 493$

$$X = 493 + 2t$$
$$Y = -493 - 3t$$

t inteiro.

Vamos agora utilizar o que já sabemos para resolver equações envolvendo congruências

24. Encontre os valores de X que tornem verdadeira a equação:

$$5X \equiv 17 \bmod 4$$

Solução: Pela definição de mod temos

$$5X \equiv 17 \bmod 4 \Leftrightarrow 5X - 17 = 4Y \Leftrightarrow 5X - 4Y = 17$$

A solução é (já sabemos calcular...):

$$X = 5 + 4t$$

$$Y = 2 + 5t$$

Na verdade, só nos interessa $X = 4t$. Assim os números inteiros $-15, -11, -7, -3, 1, 5, 9, 13$ são todos soluções desta congruência.

Importante: Na equação $aX \equiv b \bmod Y$ tivermos $a \equiv 0 \bmod Y$, a equação só terá solução se $b \equiv 0 \bmod Y$ também. Nesse caso qualquer valor inteiro de X é solução da equação. Se $b \neq 0 \bmod Y$ não haverá solução.

Exemplo:

Na equação $10X \equiv 25 \bmod 5$, qualquer valor inteiro serve para X, pois $10 \equiv 0 \bmod 5$ e $25 \equiv 0 \bmod 5$.

Na equação $10X \equiv 23 \bmod 5$, nenhum valor inteiro serve para X, pois $10 \equiv 0 \bmod 5$ mas $23 \neq 0 \bmod 5$.

25. Encontre os valores de X que tornem verdadeira a equação:

Indicamos a seguir as equações que devem ser resolvidas e o resultado, sem o desenvolvimento

(a) $4X \equiv 3 \bmod 7$

Solução Resolvendo a equação:

$$4X - 7Y = 3$$

Encontramos

$$X = -1$$

$$Y = -1$$

A resposta é $X = -1 + 7t$, t inteiro.

(b) $6X \equiv 10 \bmod 8$
Solução Resolvendo a equação:

$$6X - 8Y = 10$$

reduzida para

$$3X - 4Y = 5$$

Encontramos

$$X = 3$$

$$Y = 1$$

A resposta é $X = 3 + 4t$, t inteiro.

(c) $9X \equiv 2 \bmod 5$
Solução Resolvendo a equação:

$$9X - 5Y = 2$$

Encontramos

$$X = 3$$

$$Y = 5$$

A resposta é $X = 3 + 5t$, t inteiro.

(d) $6X \equiv 7 \bmod 9$
Solução Resolvendo a equação:

$$6X - 9Y = 7$$

Que não tem solução.

(e) $28X \equiv 8 \bmod 12$
Solução Resolvendo a equação:

$$28X - 12Y = 8$$

reduzida para

$$7X - 3Y = 2$$

Encontramos

$$X = 2$$

$$Y = 4$$

A resposta é $X = 2 + 3t$, t inteiro.

(f) $15X \equiv 10 \bmod 12$
Solução Resolvendo a equação:

$$15X - 12Y = 10$$

Que não tem solução.

(g) $4X \equiv 3 \mod 6$
Solução Resolvendo a equação:

$$4X - 6Y = 3$$

que não tem solução.

(h) $64X \equiv 128 \mod 32$
Solução Resolvendo a equação:
Observe que $64 \equiv 0 \mod 32$ e $128 \equiv 0 \mod 32$. Qualquer valor de X tornará a quação verdadeira.

(i) $15X \equiv 3 \mod 18$
Solução Resolvendo a equação:

$$15X - 18Y = 3$$

reduzida para

$$5X - 6Y = 1$$

Encontramos

$$X = -1$$

$$Y = -1$$

A resposta é $X = -1 + 6t$, t inteiro.

(j) $9X \equiv 2 \mod 5$
Solução Resolvendo a equação:

$$9X - 5Y = 2$$

Encontramos

$$X = 3$$

$$Y = 5$$

A resposta é $X = 3 + 5t$, t inteiro.

Promessa é dívida! vamos dar uma olhadinha a mais na função ϕ de Euler

26. Preencha a tabela abixo com os números de 0 a 11 (alguns números já foram colocados como exemplo):

mod3×mod4	0 mod 4	1 mod 4	2 mod 4	3 mod 4
0 mod 3	0			
1 mod 3				7
2 mod 3		5		

Solução

mod3×mod4	0 mod 4	1 mod 4	2 mod 4	3 mod 4
0 mod 3	0	9	6	3
1 mod 3	4	1	10	7
2 mod 3	8	5	2	11

(a) Todas as casas ganharam um número ?

(b) O mesmo número pode ocupar duas casas ?

27. Qual o número que estará na casa $2 \bmod 3$ e $3 \bmod 4$?

    Observe que isso equivale a resolver um sistema:

$$X \equiv 2 \bmod 3$$

$$X \equiv 3 \bmod 4$$

Podemos escrever:

$$X - 2 = 3Y$$

$$X - 3 = 4Z$$

Ou melhor (subtraindo as equações membro a membro:

$$3Y - 4Z = 1$$

Dando a solução geral:

$$Y = -1 + 4t$$

$$Z = -1 + 3t$$

Escolhendo $Y = -1$ obteríamos $X = -1$. Para colocar X entre 0 e 11 somamos 12 (o $mdc(3, 4)$(por que ?), obtendo 11. Voce pode conferir com a tabela que preencheu no item anterior.

Qualquer que fosse a casa, a equação teria solução pois $mdc(3, 4) = 1$. Isso mostra que todas as casas podem ser preenchidas. Como as soluções estão “istantes”12 unidades, cada casa só ganha um número.

28. Preencha a tabela abaixo, do $\bmod 4 \times \bmod 9$ com números inteiros de 0 a 35

mod9 → mod4 ↓	0	1	2	3	4	5	6	7	8
0									
1									
2									
3									

Solução

mod9 $\rightarrow$ mod4 $\downarrow$	0	1	2	3	4	5	6	7	8
0	0	28	20	12	4	32	24	16	8
1	9	1	29	21	13	5	33	25	17
2	18	10	2	30	22	14	6	34	26
3	27	19	11	3	31	23	15	7	35

(a) Todas as casas ganharam um número ?
(b) O mesmo número pode ocupar duas casas ?
(c) Qual o $mdc(4, 9)$?

29. E se tentarmos com dois números que não sejam co-primos (isto é, com $mdc \neq 1$) ?

    Preencha a tabela abaixo, do $\mod 4 \times \mod 6$ com números inteiros de 0 a 23

mod6 $\rightarrow$ 0 mod 4 $\downarrow$	0	1	2	3	4	5
0						
1						
2						
3						

mod6 $\rightarrow$ 0 mod 4 $\downarrow$	0	1	2	3	4	5
0	$0 - 12$		$8 - 20$		$4 - 16$	
1		$1 - 13$		$9 - 21$		$5 - 17$
2	$6 - 18$		$2 - 14$		$10 - 22$	
3		$7 - 19$		$3 - 15$		$11 - 23$

(a) Todas as casas ganharam um número ?
(b) O mesmo número pode ocupar duas casas ?
(c) Qual o $mdc(4, 6)$?

30. Qual o número que fica na casa $2 \mod 4$ e $4 \mod 6$?

    Observe que isso equivale a resolver um sistema:

$$X \equiv 2 \mod 4$$

$$X \equiv 4 \mod 6$$

Podemos escrever:

$$X - 2 = 4Y$$

$$X - 4 = 6Z$$

Ou melhor (subtraindo as equações membro a membro:

$$4Y - 6Z = 2 \Leftrightarrow 2Y - 3Z = 1$$

Dando a solução geral:

$$Y = 2 + 3t$$
$$Z = 1 + 2t$$

Escolhendo $Y = 2$ obteríamos $X = 10$. Mas escolhendo $Y = 5$ obteríamos $X = 22$. As duas respostas estão no limite entre 0 e 23.

31. Por que algumas casas da tabela do $\mod 4 \times \mod 6$ não foram preenchidas ? Por exemplo, qual o número que fica na casa $3 \mod 4$ e $2 \mod 6$?

    Observe que isso equivale a resolver um sistema:

    $$X \equiv 3 \mod 4$$
    $$X \equiv 2 \mod 6$$

    Podemos escrever:

    $$X - 3 = 4Y$$
    $$X - 2 = 6Z$$

    Ou melhor (subtraindo as equações membro a membro:

    $$4Y - 6Z = -1$$

    Como $mdc(6, 4) = 2$ a equação não tem soluçao e esta casa fica sem número.

32. Preencha a tabela abaixo, do $\mod 6 \times \mod 9$ com números inteiros de 0 a 53

    Antes de preencher, responda:

    (a) Qual o $mdc(6, 9)$?

    (b) Todas as casas ganharão um número ? **Quantos ?**
    Solução
    A partir do $mmc(6, 9) = 18$ os números passam a ocupar casas já ocupadas. Assim: $0, 18$ e 36 ocupam a mesma casa. 18 casas são ocupadas com (o $mdc(6, 9) = 3$) números cada e 36 casas permanecem vazias.

    (c) Um mesmo número ocupará duas casas ?

$\mod 9 \rightarrow$ $\mod 4 \downarrow$	0	1	2	3	4	5	6	7	8
0									
1									
2									
3									
4									
5									

33. Voce calculou a função ϕ para alguns números. Será que podemos obter outros valores a partir destes ?

Tome a tabela do $\mod 4 \times \mod 9$ com números inteiros de 0 a 35. Qual será o valor de $\phi(36)$?

mod9 → mod4 ↓	0	1	2	3	4	5	6	7	8
0	0	28	20	12	4	32	24	16	8
1	9	1	29	21	13	5	33	25	17
2	18	10	2	30	22	14	6	34	26
3	27	19	11	3	31	23	15	7	35

Vamos riscar as **linhas** correspondentes aos números co-primos com 4

mod9 → mod4 ↓	0	1	2	3	4	5	6	7	8
0	$\cancel{0}$	$\cancel{28}$	$\cancel{20}$	$\cancel{12}$	$\cancel{4}$	$\cancel{32}$	$\cancel{24}$	$\cancel{16}$	$\cancel{8}$
1	9	1	29	21	13	5	33	25	17
2	$\cancel{18}$	$\cancel{10}$	$\cancel{2}$	$\cancel{30}$	$\cancel{22}$	$\cancel{14}$	$\cancel{6}$	$\cancel{34}$	$\cancel{26}$
3	27	19	11	3	31	23	15	7	35

Observe que todos os números riscados são co-primos com 36.

Vamos riscar as **colunas**(voce adivinhou) correspondentes aos números co-primos com 9.

mod9 → mod4 ↓	0	1	2	3	4	5	6	7	8
0	$\cancel{0}$	$\cancel{28}$	$\cancel{20}$	$\cancel{12}$	$\cancel{4}$	$\cancel{32}$	$\cancel{24}$	$\cancel{16}$	$\cancel{8}$
1	$\cancel{9}$	1	29	$\cancel{21}$	13	5	$\cancel{33}$	25	17
2	$\cancel{18}$	$\cancel{10}$	$\cancel{2}$	$\cancel{30}$	$\cancel{22}$	$\cancel{14}$	$\cancel{6}$	$\cancel{34}$	$\cancel{26}$
3	$\cancel{27}$	19	11	$\cancel{3}$	31	23	$\cancel{15}$	7	35

E agora só sobraram os números que **não** são co-primos com 36. O número de linhas que sobrou é igual a $\phi(4)$ e o número de colunas que sobrou é igual a $\phi(9)$. Como cada casa tem apenas um número, podemos concluir que $\phi(4) \cdot \phi(9) = \phi(36)$. De fato, os números naturais menores que 36 e co-priomos com ele são

$$1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35$$

$$\phi(4) = 2$$

$$\phi(9) = 6$$

$$\phi(36) = 12$$

Esse processo pode ser repetido sempre que os números em questão sejam co-primos (primos entre si). Podemos concluir que:

Se a e b são numeros naturais e $mdc(a, b) = 1$ então

$$\phi(a \cdot b) = \phi(a) \cdot \phi(b)$$

34. Determine (usando a propriedade do item anterior):

    (a) $\phi(21) =$
    (b) $\phi(42) =$
    (c) $\phi(35) =$
    (d) $\phi(63) =$
    (e) $\phi(72) =$
    (f) $\phi(60) =$
    (g) $\phi(84) =$
    (h) $\phi(1260) =$

    Solução

    (a) $\phi(21) = \phi(3)\phi(7) = 2 \times 6 = 12$
    (b) $\phi(42) = \phi(6)\phi(7) = 2 \times 6 = 12$
    (c) $\phi(35) = \phi(5)\phi(7) = 4 \times 6 = 24$
    (d) $\phi(63) = \phi(7)\phi(9) = 6 \times 6 = 36$
    (e) $\phi(72) = \phi(8)\phi(12) = 4 \times 4 = 16$
    (f) $\phi(60) = \phi(5)\phi(12) = 4 \times 4 = 16$
    (g) $\phi(84) = \phi(7)\phi(12) = 6 \times 6 = 24$
    (h) $\phi(1260) = \phi(35)\phi(36) = \phi(35)\phi(4)\phi(9) = 24 \times 2 \times 6 = 288$

35. Mostre que a fórmula da multiplicação **não vale** se os números não forem co-primos. De pelo menos 3 exemplos.

    $\phi(4) \times \phi(6) = 4$ mas $\phi(24) = 8$

Apêndice A

Para saber mais

Números - Uma introdução à Matemática; Millies, Cesar Polcino e Coelho, Sonia Pitta, EDUSP, 2000

Para saber mais você pode consultar os artigos da Revista do Professor de Matemática, editada pela SBM - o número da revista onde o artigo pode ser encontrado está assinalado.

Sobre critérios de divisibilidade – Carmem M. G. Taboas – N.06

Sobre o processo de divisão de inteiros – Jaime M. Cardoso – N.08

Restos, congruência e divisibilidade – Luiz R. Dante – N.10

Outros critérios de divisibilidade – Mário G. P. Guedes – N.12

Um método para o cálculo do mdc e do mmc – Roberto R. Paterlini – N.13

A prova dos noves – Flávio W. Rodrigues – N.14

Divisores, múltiplos e decomposição em fatores primos – Paulo Argolo – N.20

Congruência, divisibilidade e adivinhações – Benedito T. V. Freire – N.22

Uma interpretação geométrica do mdc – Zelci C. de Oliveira – N.29

A escolha do goleiro e o resto de uma divisão – Cláudio Arconcher – N.30

Dispositivo prático para expressar o mdc de dois números como combinação linear deles – José P. Q. Carneiro – N.37

$2 \times 3 = 0$? – Cristina Ochoviet – N.41

Divisibilidade por 7 – Arnaldo Umbelino Jr. – N.43

A prova dos onze – Eric C.B. Guedes – N.44

Os primos esquecidos – Chico Nery e Cláudio Possani – N.47

Uma demonstração de Euclides – Arthur Almeida – N.49

Um exemplo de situação problema: O problema do bilhar – Marcelo Câmara dos Santos – N.50

Um resultado recente: um algoritmo rápido para detectar números primos – Ricardo Bianconi – N.50