Divisibilidade e Números Inteiros

Introdução à Aritmética Modular

Samuel Jurkiewicz

Sobre o autor. Samuel Jurkiewicz é carioca e Doutor em Matemática pela Universidade Pierre et Marie Curie, em Paris. Atualmente é professor da Escola de Engenharia da UFRJ. Já atuou como docente em todos os níveis, inclusive no pré-escolar. Além do ensino de graduação e pós-graduação, tem desenvolvido atividades junto a professores e alunos do Ensino Médio através das Oficinas de Matemática Discreta.

Antes de Começar

Caros Professores e Estudantes

É com grande satisfação que levamos às suas mãos este primeiro volume de uma série destinada a acompanhá-los durante o Estágio dos Alunos Premiados da 1^a Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP-2005). O principal motivo desta satisfação é saber que as mãos que irão recebê-lo são de pessoas que gostam de pensar, praticar, descobrir e se divertir com a Matemática. Isso representa para nós grande responsabilidade: a de manter vivo esse gosto pelo conhecimento e pelo estudo. Aqueles que estão recebendo este material mostraram, além de competência, que o prazer de aprender e de resolver problemas já está presente. Nossa intenção é fazer com que este sentimento cresça e se espalhe. Felizmente, a Matemática nos oferece muitas escolhas e não faltaria a nós assunto para muitas páginas.

Ao pensar que tipo de material seria adequado, tivemos em mente três aspectos: o conteúdo, a forma e a profundidade adequadas. No caso do conteúdo pensamos em abordar temas clássicos, como divisibilidade, Geometria, conjuntos numéricos; temas menos frequentes no currículo habitual, como a Combinatória; e alguns temas ligados à fundamentação da Matemática, como a argumentação lógica. Nossa intenção é contemplar, sempre que possível, aspectos originais da Matemática que por diversos motivos não se encontram facilmente nos livros didáticos do Ensino Fundamental e Médio. Claro, não poderemos fugir aos conhecimentos centrais da Matemática, mas procuraremos nos valer de sua versatilidade para oferecer material que desperte interesse além do que já conhecemos.

Na questão da forma, os fascículos terão sempre algumas características comuns: exposição de conteúdos, exercícios resolvidos, exercícios propostos, propostas de atividades e curiosidades relativas ao tema em estudo.

O ponto mais delicado é o da profundidade, por estarmos nos dirigindo a uma população com idades e história escolar bastante diversificadas. É certamente um desafio oferecer material que seja

adequado a todos. Optamos por dividir o material em duas partes, com dificuldades variadas.

A divisibilidade, a decomposição em números primos, a divisibilidade, a obtenção do mínimo múltiplo comum e do máximo divisor comum, tudo isto é bem familiar aos alunos do Ensino Fundamental e Médio. Entretanto, como esses são temas fundamentais da Matemática achamos importante revisitá-los. Um motivo adicional é o renovado interesse sobre estes assuntos na Matemática superior e nas aplicações computacionais, como a Criptografia e a codificação de informações. Este é o material da primeira parte.

A segunda parte se dedica à Aritmética modular, que será novidade para a maior parte dos alunos. Ela se apoia nos conteúdos fundamentais de que falamos, mas trazendo um aspecto generalizador que é a base da Álgebra abstrata moderna. Procuramos manter esta parte em nível acessível, trabalhando "passo a passo".

Incentivamos o professor a complementar o trabalho com outras idéias e outros textos, uma vez que o assunto é vasto e rico de aspectos interessantes que não caberiam num fascículo deste porte. Ao estudante lembramos que nada substitui a iniciativa e a imaginação.

Direção Acadêmica da OBMEP

Conteúdo

Capítulo 1

Divisão de números naturais

Se quisermos dividir 3 queijos por duas pessoas não teremos problemas, cada pessoa ficará com 1 queijo e meio. A operação matemática que fizemos foi dividir 3 por 2:

$$3 : 2 = \frac{3}{2}$$

Observação: podemos indicar a divisão com os símbolos /, : e ÷ . Usaremos $5 : 7$ **para indicar "5 dividido por 7".**

Mas nem todos os problemas podem ser resolvidos com divisões fracionárias. Se quisermos dividir 27 livros por 4 alunos, não temos a opção de cortar um livro em pedaços. Por isso, é interessante que estudemos as divisões com números naturais. Nas páginas seguintes estaremos falando sempre de números inteiros, positivos ou negativos.

Aqui vale a pena fazer uma observação; o conjunto $\mathbb{N}$ dos números naturais é o conjunto dos números que usamos para contar. Muitos professores incluem o 0 (zero) no conjunto $\mathbb{N}$, mas isso não é obrigatório. No nosso caso o conjunto dos números naturais será $\mathbb{N} = \{1, 2, 3, 4, \ldots\}$ mas o zero será utilizado pois tem um papel importante. Então você verá frequentemente este conjunto expresso como $\mathbb{N} \cup \{0\}$ (os naturais e o zero). Em alguns casos, trabalharemos

também com o conjunto dos números inteiros negativos, $\{-1, -2, -3, \ldots\}$. Vamos então voltar ao problema de dividir os livros.

Vamos colocar um livro de cada vez na pilha do aluno 1, depois na pilha do aluno 2, depois na pilha do aluno 3 e depois na pilha do aluno 4. Voltamos ao aluno 1 e assim por diante. Quando paramos? Paramos quando, depois de colocar um livro para o aluno 4, sobram menos do que 4 livros. No nosso caso cada aluno ficou com 6 livros e ainda sobraram 3 livros. Essa situação pode ser retratada matematicamente como:

$$27 : 4 = 6 \text{ com resto } 3.$$

Note que podemos descobrir o número de livros que tínhamos no começo se soubermos:

- quantos alunos receberão livros (4);
- quantos livros cada aluno recebeu (6) e
- quantos livros sobraram (3).

De fato, basta fazer a conta $4 \times 6 + 3 = 24 + 3 = 27$.

Observação: embora seja bastante comum simbolizar a multiplicação por um ponto (como em $7 \cdot 8 = 56$) usaremos com freqüência o símbolo $\times$ (como em $7 \times 8 = 56$). Em geral, só usaremos o ponto para indicar multiplicação entre símbolos literais.

Estamos prontos para entender o que é a divisão entre números naturais. Temos:

- um número que queremos dividir (chamado de **dividendo** — no nosso caso, o 27);
- um número que vai dividir o dividendo (chamado de **divisor** — no nosso caso, o 4). Lembre-se: O divisor é sempre **diferente de 0**;
- o maior número de vezes que conseguimos colocar o divisor dentro do dividendo (chamado de **quociente ou resultado** — no nosso caso, o 6); e

- o número de unidades que resta (chamado de **resto** e que deve ser **menor que o divisor** — no nosso caso, o 3).

Usando os símbolos:

- D para dividendo;
- d para divisor (que deve ser diferente de 0);
- q para quociente; e
- r para resto (que deve ser menor que d),

podemos resumir o que está acima:

$$D = d \times q + r \quad , \quad r < d \quad , \quad d > 0 \quad , \quad D, d, q, r \in \mathbb{N} \cup \{0\} \quad (1.1)$$

O fato de que, dados dois números naturais D e d seja **sempre** possível encontrar números q e r dentro das condições acima é um **teorema** (que não demonstraremos aqui) e que se baseia no **Princípio da Boa Ordenação**. É uma prova interessante e que se apoia no **algoritmo da divisão**.
A restrição $r < d$ assegura que o **quociente** q é **único**, o que nos permite trabalhar com tranquilidade.
Veremos mais adiante, que esta equação dá origem a um algoritmo para o cálculo do **máximo divisor comum** entre dois números.
Tanto a equação como o algoritmo aparecem pela primeira vez, de forma organizada, nos "Elementos", de Euclides de Alexandria.

Exemplo:

> Uma caixa de 33 lápis deve ser dividida entre 7 pessoas. Quanto cada um receberá? Quantos lápis sobrarão? Descreva a situação usando a equação de Euclides, nossa equação (1).
>
> Solução: $33 : 7 = 4$ com resto 5. Cada pessoa receberá 4 lápis. Sobrarão 5 lápis. A situação pode ser descrita por:
>
> $$33 = 4 \times 7 + 5$$

Exercícios:

1. Efetue as divisões e descreva o resultado na forma da equação de Euclides (equação (1)).

   (a) 44 : 5
   (b) 44 : 7
   (c) 353 : 3
   (d) 483 : 438
   (e) 1253 : 125
   (f) 757 : 75
   (g) 21 : 10
   (h) 1210 : 10
   (i) 210 : 100
   (j) 1285 : 100
   (k) 1285 : 1000
   (l) 11285 : 10
   (m) 157325 : 10000
   (n) 157325 : 1000
   (o) 57325 : 100
   (p) 57325 : 10

2. Efetue as divisões e descreva o resultado na forma da equação de Euclides (equação (1)). O que observa na seqüência dos restos?

   (a) 48 : 4
   (b) 47 : 4
   (c) 46 : 4
   (d) 45 : 4
   (e) 44 : 4
   (f) 43 : 4
   (g) 42 : 4
   (h) 41 : 4
   (i) 40 : 4

3. Porque o resto tem que ser menor do que o divisor?

1.1 Múltiplos, fatores e divisores

Com freqüência desejamos que a divisão dê "certinha". Ou melhor, que ela seja exata. O que queremos dizer com isso? Queremos que não sobre nada, queremos que o resto seja 0.

45 : 7 é uma divisão exata? Não, pois o quociente é 6 mas ainda temos o resto de 3.

45 : 9 é uma divisão exata? Sim, pois o quociente é 5 e o resto é 0.

Porque é tão importante que o resto seja 0?

Para responder a esta pergunta observemos que quando $r = 0$ a equação de Euclides (nossa equação (1)).

$$D = d \times q + r, \qquad r < d, \qquad d > 0, \qquad D, d, q, r \in \mathbb{N} \cup \{0\} \quad (1.1)$$

se reduz a

$$D = d \times q, \qquad d > 0, \qquad D, d, q \in \mathbb{N} \cup \{0\} \quad (1.2)$$

Isto é, temos que tratar somente com multiplicação. Se a divisão tem resto 0 dizemos que o dividendo é **múltiplo** do divisor. Mais ainda, como os números do lado direito da igualdade da equação (2) podem ser trocados (pois a multiplicação é uma operação **comutativa**), o dividendo também é múltiplo do quociente.

No nosso simples exemplo:

$$45 = 9 \times 5 \Rightarrow 45 \text{ é múltiplo de } 9 \text{ e } 45 \text{ é múltiplo de } 5.$$

Podemos dizer também que 5 é divisor de 45, e que 9 é divisor de 45. De certa maneira os números 5 e 9 constroem o número 45, por multiplicação. Os números 5 e 9 fazem o número 45 e por isso dizemos também que:

5 e 9 são **fatores** de 45.

Demos bastante ênfase a esta nomenclatura, pois vamos usá-la com freqüência.

Exemplo: Quais os fatores do número 12?

1 e 12, pois $12 = 1 \times 12$;
2 e 6, pois $12 = 2 \times 6$;
3 e 4, pois $12 = 3 \times 4$;
Conjunto dos divisores de 12: $D_{12} = \{1, 2, 3, 4, 6, 12\}$.

Observação: É bastante freqüente usar a notação:

$$D_{12} \equiv \text{conjunto dos divisores de 12.}$$

Essa forma nos será conveniente em alguns casos.

Exercícios:

1. Determine os fatores de
   (a) 42
   (b) 6
   (c) 18
   (d) 15
   (e) 25
   (f) 100
   (g) 13
   (h) 23
   (i) 37
   (j) 101
   (k) 1001
2. Quais os fatores de 2471? Você testou até que divisor?

1.2 Critérios de divisibilidade e o sistema de numeração

Em alguns casos, não precisaremos tentar dividir para saber se um número é ou não múltiplo de outro. Para isso usaremos as características de nosso sistema de numeração e algumas propriedades do resto de uma divisão. Vamos lembrar alguns fatos.

Fato 1: No nosso sistema usamos 10 algarismos $(0, 1, 2, 3, 4, 5, 6, 7, 8, 9)$ cujo valor aumenta ou diminui conforme sua posição.
Exemplo:

$$12948 = 8 + 4 \times 10 + 9 \times 100 + 2 \times 1000 + 1 \times 10000$$

Fato 2: Se um número é fator de dois outros números, ele é divisor da sua soma (e da sua diferença).
Exemplo:

6 é fator de 30
6 é fator de 48
Então, 6 é fator de $30 + 48 = 78$.
E 6 também é fator de $48 - 30 = 18$ (pois $18 = 6 \times 3$).

Fato 3: Dividimos dois números por um mesmo divisor; se a soma (diferença) dos restos for menor que o divisor ela será igual ao resto da soma (diferença) dos dois números.
Exemplo:

Soma
$22 : 7 = 3$ e o resto é 1
$33 : 7 = 4$ e o resto é 5
A soma dos restos é 6 (que é menor que 7).
$22 + 33 = 55$
$55 : 7 = 7$ e o resto é 6

Diferença
$5 - 1 = 4$
$33 - 22 = 11$
$11 : 7 = 1$ e o resto é 4

Observação: se a diferença for um número negativo, somamos o divisor.

Exemplo:

$44 : 7 = 6$ e o resto é 2
$26 : 7 = 3$ e o resto é 5
$2 - 5 = -3$

$-3 + 7 = 4$
$44 - 26 = 18$
$18 : 7 = 2$ e o resto é 4

Fato 4: Dividimos dois números por um mesmo divisor; se a soma dos restos for maior que o divisor, subtraímos o valor do divisor e o resultado será o resto da soma dos dois números.

Exemplo:

$26 : 7 = 3$ e o resto é 5
$32 : 7 = 4$ e o resto é 4
A soma dos restos é 9 (que é maior que 7). $9 - 7 = 2$
$26 + 32 = 58$
$58 : 7 = 8$ e o resto é 2

Pergunta-exercício: a diferença entre os restos pode ser maior que o divisor? Em algum caso necessitaremos adicionar o divisor mais do que uma vez?

Exercício: Sem executar a soma, determine o resto das divisões:

(a) $(47 + 73) : 7$
(b) $(354 + 432) : 10$
(c) $(47 + 73) : 8$
(d) $(35 + 46) : 6$
(e) $(123 + 258) : 10$
(f) $(16 + 22 + 35) : 3$
(g) $(43 + 49) : 3$
(h) $(200 + 40 + 7) : 3$
(i) $(100 + 40 + 7) : 3$
(j) $(100 + 20 + 4) : 9$
(k) $(400 + 10 + 7) : 9$
(l) $(400 + 10 + 4) : 9$

1.2.1 Divisibilidade por 2; números pares e ímpares

O critério de divisibilidade mais conhecido é a divisão por 2. Para determinar se um número é divisível por 2 (isto é, par) ou não (ímpar)

só precisamos verificar se o último algarismo é par ou ímpar. Observe que:

$10 = 2 \times 5$
$100 = 2 \times 50$
$1000 = 2 \times 500$ e assim por diante.

Então, por exemplo:

$456 = 4 \times 100 + 5 \times 10 + 6$
$400 = 200 \times 2$ é par (divisível por 2)
$50 = 25 \times 2$ é par (divisível por 2)
$6 = 3 \times 2$ é par (divisível por 2)
E 456 é par

7568142635 é ímpar (não é divisível por 2)
7568142636 é par (divisível por 2)

Um fato importante é que todos os fatores de um número ímpar são ímpares. Basta um fator par para que o número seja par.

1.2.2 Divisibilidade por 4 e 8

Observe que:

$100 = 4 \times 25$
$1000 = 4 \times 250$
E assim por diante
$1000000 = 4 \times 250000$

Isto é, as potências de 10, a partir de 100, são todas divisíveis por 4. Mas 10 não é divisível por 4.

Então, para saber se um número é divisível por 4 não precisamos nos preocupar com as centenas, milhares, e assim por diante. Estas classes já têm o 4 como fator.

Para saber se um número é divisível por 4, basta saber se os dois últimos algarismos formam um número divisível por 4.

Para saber o resto da divisão de um número por 4, basta saber o resto da divisão dos seus dois últimos algarismos por 4.

Exemplos:

1. 125867432 é divisível por 4?
   Basta verificar para 32
   $32 = 4 \times 8$ com resto 0
2. Qual o resto de $35971659 : 4$?
   Basta verificar o resto de $59 : 4$.
   $59 : 4 = 14$ com resto 3

A divisibilidade por 8 segue o mesmo padrão. Observe que:

1. $1000 = 8 \times 125$
   $10000 = 8 \times 1250$
   E assim por diante:
   $1000000 = 8 \times 125000$

Isto é, as potências de 10, a partir de 1000, são todas divisíveis por 8. Mas 10 não é divisível por 8 e 100 também não é divisível por 8.

Então, para saber se um número é divisível por 8 não precisamos nos preocupar com os milhares, dezenas de milhares e assim por diante. Estas classes já têm o 8 como fator.

Para saber se um número é divisível por 8, basta saber se os três últimos algarismos formam um número divisível por 8.

Para saber o resto da divisão de um número por 8, basta saber o resto da divisão dos seus três últimos algarismos por 8.

Exemplos:

1. 125867344 é divisível por 8?
   Basta verificar para 344.
   $344 = 8 \times 43$ com resto 0

2. Qual o resto de $35971659 : 8$?
   Basta verificar o resto de $659 : 8$.
   $659 : 8 = 82$ com resto 3.

Exercício: Calcule o resto das divisões:

(a) $1425782 : 2$
(b) $1425782 : 4$

(c) $1425782 : 8$
(d) $658591 : 2$
(e) $658591 : 4$
(f) $658591 : 8$

1.2.3 Divisibilidade por 5 e por 10

As mesmas idéias da divisibilidade por 2 podem ser usadas na divisibilidade por 5 e por 10. Basta observar que

$$10 = 5 \times 2$$
$$100 = 5 \times 10 \times 2$$
$$1000 = 5 \times 100 \times 2$$

e assim por diante. Isso mostra que:

- Um número é divisível por 5 se (e só se) o último algarismo for 5 ou 0.
- Um número é divisível por 10 se (e só se) o último algarismo for 0.

Para saber o resto da divisão de um número por 5, basta saber o resto da divisão do seu último algarismo por 5.

Para saber o resto da divisão de um número por 10, basta saber o resto da divisão do seu último algarismo por 10, isto é, basta saber o seu último algarismo.

Exemplos:

1. Sem executar a soma, determine o resto das divisões:
   (a) $(457 + 378 + 19) : 10$
   Os últimos algarismos somam 24, logo o resto da divisão é 4.
   (b) $(358 + 57917 + 123) : 5$
   Os últimos algarismos somam 18, logo o resto da divisão é 3.

2. Se somarmos todos os números de 1 a 587 qual o resto da divisão por 5?
   A soma dos algarismos de 1 a 9 (1+2+3+4+5+6+7+8+9+0) é 45, logo até 580 a soma dos números será um múltiplo de 45 (58×45), logo um múltiplo de 5. Só precisamos nos preocupar com o último algarismo dos sete últimos números: $1+2+3+4+5+6+7 = 28$. O último algarismo é 8 e o resto da soma é 3.

3. Se somarmos todos os números de 1 a 536 qual o resto da divisão por 10?
   A soma dos algarismos de 1 a 9 (1+2+3+4+5+6+7+8+9+0) é 45, logo até 530 a soma dos últimos algarismos dos números será 53×45, um número com último algarismo igual a 5. Só precisamos nos preocupar com este 5 e com o último algarismo dos seis últimos números: $5+1+2+3+4+5+6 = 26$. O último algarismo é 6 e o resto da soma é 6.

Exercícios:

1. Sem executar a soma, determine o resto das divisões:
   (a) $(3257 + 12378 + 1569) : 10$
   (b) $(354567 + 356 + 1) : 10$
   (c) $(5 + 15 + 25 + 35 + 45) : 5$
   (d) $(1 + 3 + 5 + 7 + 9 + 11 + 13) : 2$
   (e) $(1 + 3 + 5 + 7 + 9 + 11 + 13) : 5$
   (f) $(1 + 3 + 5 + 7 + 9 + 11 + 13) : 10$

2. Se somarmos todos os números de 121 a 587 qual o resto da divisão desta soma por 5?

3. Se somarmos todos os números de 131 a 536 qual o resto da divisão desta soma por 10?

1.2.4 Divisibilidade por 3 e por 9

Vamos lembrar alguns exercícios que já fizemos: Qual o resto de $(200 + 40 + 7) : 3$?

$200 : 3 = 66$ com resto 2 - o mesmo resto de $2 : 3$.
$40 : 3 = 13$ com resto 1 - o mesmo resto de $4 : 3$
$7 : 3 = 2$ com resto 1 - o mesmo resto de $7 : 3$

O resto de $247 : 3$ é o mesmo resto de $(2 + 4 + 7) : 3$, isto é, o mesmo resto de $13 : 3$. E $13 : 3 = 4$ com resto 1.

Vamos investigar um pouco.

$1 : 3 = 0$ com resto 1
$10 : 3 = 3$ com resto 1
$100 : 3 = 33$ com resto 1
E assim por diante:
$1000000 : 3 = 333333$ com resto 1

O resto das potências de 10 quando divididas por 3, é sempre 1. Cada classe contribui com uma unidade para o resto da divisão por 3. Por exemplo, 4000 contribui com 4 unidades para o resto da divisão $4573 : 3$.

Resumindo:

> O resto da divisão de um número por 3 é o mesmo resto da divisão da soma de seus algarismos por 3.

Exemplo:

> O resto de $4573 : 3$ é
> o resto de $4 \times 1000 + 5 \times 100 + 7 \times 10 + 3$,
> isto é, o mesmo resto que $4 \times 1 + 5 \times 1 + 7 \times 1 + 3$,
> ou ainda, $4 + 5 + 7 + 3 = 19$. O resto é 1.

Exemplos:

1. O resto da divisão de 4567 por 3 é o resto da divisão de $4+5+6+7 = 22$ por 3, isto é o resto da divisão de $2 + 2 = 4$ por 3, isto é (finalmente) 1. De fato, $4567 = 1522 \times 3 + 1$
2. Se somarmos todos os números de 1 a 536 qual o resto da divisão por 3? O resto de $(1+2+3) : 3$ é 0; o resto de $(4+5+6) : 3$ é 0; e assim por diante, sempre indo de três em três até o próximo múltiplo de 3.

Temos que nos preocupar apenas com os números após o último múltiplo de 3, no caso 534 (pois $5+3+4=12$). Basta verificar a soma $535+536$. A soma dos algarismos é 27, que é múltiplo de 3. Logo, o resto será 0.

Exercícios:

1. Qual o resto das divisões indicadas?

   (a) $(3257+12378+1569):3$
   (b) $(354567+356+1):3$
   (c) $(5+15+25+35+45):3$
   (d) $(1+3+5+7+9+11+13):3$

2. Se somarmos todos os números de 121 a 587 qual o resto da divisão por 3?
3. Se somarmos todos os números de 131 a 536 qual o resto da divisão por 3?

Para a divisibilidade por 9 podemos usar a mesma idéia. Vejamos um exemplo:

$(400+80+7):9$
$400:9=44$ com resto 4 - o mesmo resto de $4:9$
$80:9=8$ com resto 8 - o mesmo resto de $8:9$
$7:9=1$ com resto 7 - o mesmo resto de $7:9$
O resto de $487:9$ é o mesmo resto de $(4+8+7):9$ - o mesmo resto de $19:9$.
$19:9=2$ com resto 1.

Vamos investigar um pouco.

$1:9=0$ com resto 1
$10:9=1$ com resto 1
$100:9=11$ com resto 1
E assim por diante:
$1000000:9=111111$ com resto 1

O resto das potências de 10 quando divididas por 9, é sempre 1. Cada classe contribui com uma unidade para o resto da divisão por 9.

Por exemplo, 4000 contribui com 4 unidades para o resto da divisão $4585 : 3$.

Resumindo:

> O resto da divisão de um número por 9 é o mesmo resto da divisão da soma de seus algarismos por 9.

Exemplo:

> O resto de $4585 : 9$ é
> o resto de $4 \times 1000 + 5 \times 100 + 8 \times 10 + 5$,
> isto é, o mesmo resto que $4 \times 1 + 5 \times 1 + 8 \times 1 + 5$,
> ou ainda $4 + 5 + 8 + 5 = 22$. O resto é 4.

Resumindo:

> O resto da divisão de um número por 9 é o mesmo resto da divisão da soma de seus algarismos por 9.

Exemplos:

1. O resto da divisão de 4567 por 9 é o resto da divisão de $4+5+6+7 = 22$ por 9, isto é, o resto da divisão de $2 + 2 = 4$ por 9, isto é (finalmente) 4.
   De fato, $4567 = 507 \times 9 + 4$.
2. Se somarmos todos os números de 1 a 536 qual o resto da divisão desta soma por 9?
   O resto de $(1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9) : 9$ é o mesmo de $45 : 9$ que é 0;
   o resto de $(10 + 11 + 12 + 13 + 14 + 15 + 16 + 17 + 18) : 9$ é o mesmo de $126 : 9$ que é 0; e assim por diante.

   Temos que nos preocupar apenas com os números após o último múltiplo de 9, no caso 531 (pois $5 + 3 + 1 = 9$). Basta verificar a soma $532 + 533 + 534 + 535 + 536$. A soma dos algarismos é 60. O resto de $60 : 9$ é 6, logo o resto da soma é 6.

Exercícios:

1. Qual o resto das divisões indicadas?

(a) $(3257 + 12378 + 1569) : 9$
(b) $(354567 + 356 + 1) : 9$
(c) $(5 + 15 + 25 + 35 + 45) : 9$
(d) $(1 + 3 + 5 + 7 + 9 + 11 + 13) : 9$

2. Se somarmos todos os números de 121 a 587 qual o resto da divisão por 9?
3. Se somarmos todos os números de 131 a 536 qual o resto da divisão por 9?

1.3 Outras propriedades dos restos: multiplicação e potenciação

Vimos que quando dividimos dois números pelo mesmo divisor, a soma (ou diferença) dos restos é igual ao resto da soma (ou diferença) dos números - eventualmente temos que "corrigir" a soma ou diferença, somando ou subtraindo o valor do divisor.

Exemplos: Veja os exemplos no Fato 2 e no Fato 3 mais acima.

Mas será que a mesma idéia permanece se usarmos a multiplicação? Veremos que sim, e para isso teremos que usar nossa velha equação de Euclides (a equação (1)):

$$D = d \times q + r, \qquad , r < d, \qquad d > 0, \qquad D, d, q, r \in \mathbb{N} \cup \{0\} \quad (1.1)$$

em que:

- D é o dividendo;
- d é o divisor (que deve ser diferente de 0);
- q é o quociente; e
- r é o resto (que deve ser menor que d)

Vamos experimentar um exemplo:

$45 : 7 = 6$ com resto 3
$37 : 7 = 5$ com resto 2
$45 \times 37 = 1665$
$1665 : 7 = 237$ com resto 6

Observe que o produto dos restos é igual ao resto do produto!

Outro exemplo:

$40 : 6 = 6$ com resto 4
$29 : 6 = 4$ com resto 5
$40 \times 29 = 1160$
$1160 : 6 = 193$ com resto 2

O que aconteceu? O produto dos restos é 20, muito maior do que o divisor. Vamos retirando 6 unidades até obter um resto menor do que 6, isto é, $20 - 6 - 6 - 6 = 2$. Na verdade dividimos $20 : 6 = 3$ com resto 2.

São exemplos de que podemos conhecer o resto de uma multiplicação por um dado divisor, sabendo o resto da divisão dos fatores deste número pelo mesmo divisor. Vamos entender porque isso acontece.

Digamos que tenho dois números D_1 e D_2 que vamos dividir pelo mesmo divisor d. Pela equação de Euclides (equação (1)) podemos escrever:

$$D_1 = d \times q_1 + r_1, \qquad r_1 < d, \qquad d > 0, \qquad D_1, d, q_1, r_1 \in \mathbb{N} \cup \{0\}$$

$$D_2 = d \times q_2 + r_2, \qquad r_2 < d, \qquad d > 0, \qquad D_2, d, q_2, r_2 \in \mathbb{N} \cup \{0\}$$

e daí tirar:

$$D_1 = d \times q_1 + r_1, \qquad \text{com} \qquad 0 \leq r_1 < d, \qquad D_1, d, q_1, r_1 \in \mathbb{N} \cup \{0\}$$

$$D_2 = d \times q_2 + r_2, \qquad \text{com} \qquad 0 \leq r_2 < d, \qquad D_2, d, q_2, r_2 \in \mathbb{N} \cup \{0\}$$

Observe que não precisamos colocar índice no divisor d pois ele é igual nas duas equações.

Vamos fazer a multiplicação $D_1 \times D_2$:

$D_1 = d \times q_1 + r_1,$
$D_2 = d \times q_2 + r_2,$

donde

$$D_1 \times D_2 = (d \times q_1 + r_1) \cdot (d \times q_2 + r_2) = d^2 \cdot q_1 \cdot q_2 + r_1 \cdot d \cdot q_2 + r_2 \cdot d \cdot q_1 + r_1 \cdot r_2$$

Observe que $d^2 \cdot q_1 \cdot q_2$, $r_1 \cdot d \cdot q_2$ e $r_2 \cdot d \cdot q_1$ têm d como fator. Pelos fatos citados lá no começo, vemos que o resto da divisão $(D1 \times D2) : d$ é o mesmo resto da divisão $(r_1 \cdot r_2) : d$.

Exemplos:

1. Qual o resto da divisão $(6779 \times 3846) : 9$?
   Calculamos os restos das divisões $6799 : 9$ e $3486 : 9$;
   $6779 : 9$ deixa resto 2 pois a soma dos algarismos é 29 (e $29 - 27 = 2$);
   $3486 : 9$ deixa resto 3 pois a soma dos algarismos é 21 (e $21 - 18 = 3$);
   O resto de $(6779 \times 3846) : 9$ é $2 \times 3 = 6$

2. Qual o resto da divisão $(297 \times 684 \times 128) : 5$?
   Calculando os restos:
   $297 : 5$ deixa resto 2 $(7 - 5 = 2)$
   $684 : 5$ deixa resto 4
   $128 : 5$ deixa resto 3 $(8 - 5 = 3)$
   O produto dos restos é $2 \times 4 \times 3 = 24$
   O resto de $24 : 5 = 4$
   O resto $(297 \times 684 \times 128) : 5$ também é 4

3. Qual o resto da divisão $(295 \times 63 \times 128) : 3$?
   Poderíamos fazer todas as contas, mas basta observar que 63 é múltiplo de 3, logo o resto de $63 : 3$ é 0. O produto dos restos será 0, e o resto pedido será 0. De fato, como 3 é fator de 63, 3 será fator do produto $295 \times 63 \times 128$; isso quer dizer que o produto também é múltiplo de 3 (e logo, o resto da divisão por 3 será 0).

Exercício: Sem efetuar os produtos, calcule o resto das divisões:

(a) $(43 \times 27 \times 38 \times 537) : 2$
(b) $(453 \times 127 \times 38) : 9$
(c) $(45 \times 37 \times 91) : 9$
(d) $(24 \times 48 \times 96) : 5$
(e) $(1289 \times 2365 \times 1589) : 5$

(f) $(37 \times 43 \times 57) : 10$

Já que conseguimos mostrar que os restos são "bem comportados" quanto à multiplicação, podemos também usar as propriedades dos restos para a potenciação.

Exemplos:

1. Qual o resto de $12^5 : 5$?
   $12^5 = 12 \times 12 \times 12 \times 12 \times 12$
   O resto de $12 : 5$ é 2
   $2 \times 2 \times 2 \times 2 \times 2 = 32$
   O resto de $32 : 5$ é 2
   logo, o resto de $12^5 : 5$ é 2

2. Qual o resto de $3^7 : 2$?
   Como 3 é ímpar, 3^7 também é ímpar e o resto de de $3^7 : 2$ é 1.

3. Qual o resto de $3^7 : 5$?
   Note que só nos interessa o último algarismo:
   $3 = 3$
   $3 \times 3 = 9$
   $9 \times 3 = 27$ último algarismo: 7
   $7 \times 3 = 21$ último algarismo: 1
   $1 \times 3 = 3$
   $3 \times 3 = 9$ ...e os últimos algarismos continuam a se repetir nesta ordem: 3; 9; 7; 1; 3; ...
   Como os últimos algarismos se repetem de 4 em 4, 3^5 terá 3 como último algarismo e 3^7 terá 7 como último algarismo. Logo, o resto de $3^7 : 5$ é 2 (pois $7 - 5 = 2$).

4. Qual o resto de $3^{62} : 5$?
   Usando a mesma idéia do exemplo anterior, vemos que o último algarismo se repete a cada 4 potências de 3. Como $62 : 4 = 15$ com resto 2, vemos que o ciclo 3; 9; 7; 1 ...se repete 15 vezes e as duas últimas potências produzem um número com final 9. Logo, o resto de $3^{62} : 5$ é 4 (pois $9 - 5 = 4$).

1.4 Números primos e números compostos

Estamos trabalhando com o conceito de múltiplos, divisores (que também chamamos de fatores) e podemos perceber que alguns números têm muitos fatores, como por exemplo, o 24. O conjunto D_{24} dos fatores de 24 é:

$$D_{24} = \{1, 2, 3, 4, 6, 8, 12, 24\}$$

O número 1 é divisor de todos os números. Observe que o número que tem só um divisor é 1, pois

$$D_1 = \{1\}$$

Por outro lado, há números que têm apenas dois fatores, como por exemplo o número 7. De fato:

$$D_7 = \{1, 7\}$$

Os números que só têm dois fatores distintos (o 1 e ele próprio), são chamados **números primos**. O único divisor diferente de 1 de um número primo é ele mesmo.

Os números diferentes de 1 e que não são primos, são chamados de **compostos**.

Um fato bem conhecido é que podemos escrever qualquer número natural diferente de 1 como um produto de números primos — é a chamada **decomposição em números primos**. Mais ainda, se colocarmos os fatores em ordem crescente, só há uma única forma de fazer esta decomposição.
Este fato é importante, pois nos permite comparar as decomposições dos números inteiros e deduzir propriedades.
Embora já conhecido há mais tempo, Euclides apresenta uma demonstração na sua obra "Os Elementos".
Devido à sua larga utilização, é comumente chamado

Teorema Fundamental da Aritmética

Observação: o número 1 é especial. O motivo é que ele divide todos os números naturais. Quais os divisores de um natural que interessam? Apenas os divisores diferentes de 1. Procuramos os divisores diferentes de 1. Os números primos são os números naturais, diferentes de 1, com o menor número de divisores, apenas dois divisores. Com os números primos construímos os números compostos.

Exemplos:

1. Os números 2, 3, 5, 37, 3413 e 7919 são primos. À medida que os números vão crescendo, vai ficando mais difícil determinar se um número é primo ou composto.
2. 512 é composto.
   Sua decomposição é $512 = 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2$.
   É mais cômodo escrever $512 = 2^9$.
3. 825 é composto pois $825 = 3 \times 5 \times 5 \times 11$, ou melhor, $825 = 3 \times 5^2 \times 11$.
4. 296783 é composto pois $296783 = 463 \times 641$. Observe que 463 e 641 são números primos. Pode ser bastante difícil a decomposição em fatores primos.

Exercícios:

1. Determine se os números abaixo são primos ou compostos. Caso sejam compostos decomponha-os em fatores primos.
   (a) 35
   (b) 43
   (c) 105
   (d) 131
   (e) 1001
   (f) 625
   (g) 6480
   (h) 1961
   (i) 5292
   (j) 3003

1.4.1 O crivo de Eratóstenes

O nome não deve assustar o leitor. "Crivo" quer dizer "peneira" e Eratóstenes foi o sábio grego a quem se atribui sua invenção. É uma "peneira" de números. Vamos peneirar os números divisíveis por 2, por 3 e assim sucessivamente. Com este crivo podemos obter ao menos os primeiros números primos, ou melhor todos os números primos **até um certo número**. No nosso exemplo vamos peneirar até 50.

Começamos por riscar de 2 em 2, tirando os múltiplos de 2 (mas não riscamos o 2 — ele é primo):

1	**2**	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~
11	~~12~~	13	~~14~~	15	~~16~~	17	~~18~~	19	~~20~~
21	~~22~~	23	~~24~~	25	~~26~~	27	~~28~~	29	~~30~~
31	~~32~~	33	~~34~~	35	~~36~~	37	~~38~~	39	~~40~~
41	~~42~~	43	~~44~~	45	~~46~~	47	~~48~~	49	~~50~~

Retiramos os números que passaram na "peneira" do 2. O próximo primo é o 3. Riscamos de 3 em 3, tirando os múltiplos de 3 (mas não riscamos o 3 — ele é primo):

1	**2**	**3**		5		7		~~9~~	
11		13		~~15~~		17		19	
~~21~~		23		25		~~27~~		29	
31		~~33~~		35		37		~~39~~	
41		43		~~45~~		47		49	

Retiramos os números que passaram na "peneira" do 3. O próximo primo é o 5. Riscamos de 5 em 5, tirando os múltiplos de 5 (mas não riscamos o 5 — ele é primo):

1	**2**	**3**		**5**		7			
11		13				17		19	
		23		~~25~~				29	
31				~~35~~		37			
41		43				47		49	

Retiramos os números que passaram na "peneira" do 5. O próximo primo é o 7. Riscamos de 7 em 7, tirando os múltiplos de 7 (mas não riscamos o 7 — ele é primo):

1	**2**	**3**		**5**		**7**			
11		13				17		19	
		23						29	
31						37			
41		43				47		~~49~~	

Retiramos o 49, que não passou na "peneira" do 7.

Aqui paramos. Por quê? O próximo primo seria o 11, mas qualquer número (até 50) dividido por 11 vai nos dar um quociente menor do que 11 pois 11×11 é maior do que 50. Quando aplicamos o crivo ou examinamos se um determinado número é primo, basta verificar até o maior número que, elevado ao quadrado, não ultrapasse o número examinado. No nosso caso $7 \times 7 = 49$, e 7 é o maior número que, elevado ao quadrado, ainda é menor que 50. Na nossa peneira então só sobraram os números primos. Lembramos que 1 não é primo.

Primos até 50:$P_{50} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47\}$

Nem sempre é fácil procurar fatores. O crivo funciona bem com números pequenos, mas um número primo grande pode complicar a nossa vida. Por exemplo: 34020977 é primo ou composto? Ele é composto mas sua decomposição é $34020977 = 5077 \times 6701$. Imagine o tamanho da peneira que você teria que usar!

1.5 Maior divisor comum

Uma das principais utilizações da decomposição em números primos é a determinação do maior divisor comum (mdc) e do menor múltiplo comum (mmc).

Vamos supor que temos que remeter duas encomendas de sabonete para dois compradores diferentes. Um pediu 420 sabonetes e outro 480 sabonetes. Queremos fazer uma embalagem que sirva para os dois compradores. Estamos procurando um número de sabonetes que seja divisor (ou fator) de 420, mas também seja um divisor (fator) de 480. Isto é: um fator comum (ou divisor comum) de 420 e 480. Isso é fácil, basta usar embalagens de 10 sabonetes (10 é um fator de 420 e de

480). O primeiro comprador receberia 42 embalagens e o segundo 48 embalagens.

Mas gostaríamos de usar poucas embalagens, ou melhor de colocar mais sabonetes em cada embalagem. Então não queremos apenas um divisor comum; queremos o **maior divisor comum**. Vamos usar a decomposição para isso:

$$420 = 2^2 \times 3 \times 5 \times 7$$

$$480 = 2^5 \times 3 \times 5$$

Quais os fatores comuns? 2, 3 e 5.

Mas o 2 pode ser usado duas vezes, pois em ambos os números ele aparece duas vezes. Embora ele apareça mais vezes como fator de 480, só podemos utilizá-lo duas vezes, o número de vezes que o 2 aparece como fator no 420.

Enfim, o maior divisor que podemos obter será:

$$mdc(420, 480) = 2^2 \times 3 \times 5 = 60$$

De fato, 60 é fator de 420 e de 480, e não é possível haver um fator maior. Podemos fazer embalagens com 60 sabonetes: o primeiro comprador receberá 7 embalagens e o segundo 8 embalagens. Note que 7 é o quociente que obtemos ao dividirmos 420 por $2^2 \times 3 \times 5$ e que $8 = 2^3$ é o quociente que obtemos ao dividir 480 por $2^2 \times 3 \times 5$.

Exemplos:

1. Calcular $mdc(30, 45)$.
   $30 = 2 \times 3 \times 5$
   $45 = 3^2 \times 5$
   Tomando os fatores comuns, temos $mdc(30, 45) = 3 \times 5 = 15$.
2. Podemos calcular o mdc de mais de dois números simultaneamente:
   $mdc(84, 72, 180)$
   $84 = 2^2 \times 3 \times 7$
   $72 = 2^3 \times 3^2$
   $180 = 2^4 \times 3^2 \times 5$
   $mdc(84, 72, 180) = 2^2 \times 3 = 12$

3. $mdc(16, 45)$
   $16 = 2^4$ e $45 = 3^2 \times 5$
   Não há fator comum a não ser o 1.
   $mdc(16, 45) = 1$
   Observação: neste caso dizemos que 16 e 45 são **primos entre si**.

Exercício: Calcular

(a) $mdc(49, 84)$
(b) $mdc(36, 60, 72)$
(c) $mdc(8, 32, 128)$
(d) $mdc(13, 39, 21)$
(e) $mdc(45, 135, 81)$
(f) $mdc(343, 91, 169)$
(g) $mdc(7, 11, 13)$
(h) $mdc(1800, 2700, 4500)$
(i) $mdc(1001, 1002)$
(j) $mdc(1001, 1078)$

Já vimos que às vezes pode ser complicado encontrar uma decomposição em fatores primos. Mas a nossa boa e velha equação de Euclides (equação (1)) nos dá uma outra forma de calcular o mdc entre dois números.

Vamos supor que quero encontrar o $mdc(168, 49)$. A equação de Euclides (equação (1)) nos diz que

$$168 = 3 \times 49 + 21$$

Ora, estou procurando um divisor de 168 e de 49. A equação acima mostra que ele terá que ser também um divisor de 21. Então, posso resolver meu problema procurando o mdc de 49 e 21. Mas

$$49 = 2 \times 21 + 7.$$

Pelo mesmo raciocínio posso procurar o $mdc(21, 7)$. Mas

$$21 = 3 \times 7, \text{ sem resto.}$$

Logo, 7 divide 21, isto é $mdc(7, 21) = 7$. Voltando passo a passo, $mdc(21, 49) = 7$, e finalmente $mdc(168, 49) = 7$.

O procedimento acima permite encontrar o mdc de números grandes sem o uso da decomposição.

Exemplo:

mdc(4873, 275) $4873 = 17 \times 275$ com resto 198
$275 = 1 \times 198$ com resto 77
$198 = 2 \times 77$ com resto 44
$77 = 1 \times 44$ com resto 33
$44 = 1 \times 33$ com resto 11
$33 = 3 \times 11$ sem resto
$mdc(4873, 275) = 11$

Esse procedimento é chamado "algoritmo de Euclides" para determinação do mdc. Ele pode ser apresentado de uma forma gráfica:

Quociente	17	1	2	1	1	3
4873	275	198	77	44	33	11
Resto	198	77	44	33	11	0

Note que o quociente não nos interessa neste algoritmo. Basta o resto.

Exercício: Calcular, usando o algoritmo de Euclides:

(a) $mdc(1176, 471)$
(b) $mdc(57, 36)$
(c) $mdc(175, 98)$
(d) $mdc(2536, 938)$
(e) $mdc(12578, 6248)$
(f) $mdc(1589, 3584)$

1.6 Menor múltiplo comum

Outra utilização da decomposição em números primos é a determinação do menor múltiplo comum.

Vejamos um exemplo. Três amigos passeiam de bicicleta, na mesma direção, em torno de uma pista circular. Para dar uma volta completa um deles demora 15 minutos, outro demora 18 minutos e o terceiro demora 21 minutos. Eles partem juntos e combinam interromper o passeio quando os três se encontrarem pela primeira vez no ponto de partida.

Já que eles vão dar voltas completas, o tempo gasto será múltiplo de 15 minutos, por causa do primeiro amigo. Será também um múltiplo de 18 e de 21 por causa dos outros amigos. Procuramos, portanto um múltiplo comum. Não há problema em conseguir um múltiplo comum de 15, 18 e 21; basta multiplicá-los: $15 \times 18 \times 21 = 5670$. Mas o que queremos saber é a primeira vez que todos se encontram no ponto de partida; queremos o **menor múltiplo comum**.

Vamos examinar as decomposições:

$15 = 3 \times 5$; um múltiplo de 15 deve ter 3 e 5 como fatores.
$18 = 2 \times 3^2$; um múltiplo de 18 deve ter 2 e 3^2 como fatores.
$21 = 3 \times 7$; um múltiplo de 15 deve ter 3 e 7 como fatores.

Um múltiplo comum de 15, 18 e 21 deve ter esse fatores todos (2, 3, 5 e 7), mas podemos "economizar" fatores:

- a potência mais alta de 2 que precisamos é 2^1
- a potência mais alta de 3 que precisamos é 3^2
- a potência mais alta de 5 que precisamos é 5^1
- a potência mais alta de 7 que precisamos é 7^1

Resumindo, o menor múltiplo comum de 15, 18 e 21 é:

$$mmc(15, 18, 21) = 2^1 \times 3^2 \times 5^1 \times 7^1 = 630$$

Os três amigos se encontrarão na linha de partida depois de 630 minutos. Isso quer dizer que eles vão pedalar durante 10 horas e meia! Ou eles são muito bons na bicicleta ou alguma coisa está errada nos dados do problema!

Isso acontece com freqüência nos livros de Matemática. A gente se preocupa com a Matemática e esquece do bom senso... O mais correto seria pensar em uma pista rápida, e que os amigos fizessem o contorno em 15, 18 e 21 segundos. Assim, a solução nos daria um

tempo de 630 segundos, isto é, 10 minutos e meio. Agora sim...

Exemplos:

1. $mmc(25, 15, 9)$
   $9 = 3^2; 15 = 3 \times 5; 25 = 5^2$
   $mmc(25, 15, 9) = 3^2 \times 5^2 = 225$
2. $mmc(16, 27)$
   $16 = 2^4$
   $27 = 3^3$
   $mmc(16, 27) = 2^4 \times 3^3 = 432$
   Note que os números não tem fatores comuns, logo o mmc é o produto dos dois números.
3. $mmc(6, 8, 24)$
   $6 = 2 \times 3$
   $8 = 2^3$
   $24 = 2^3 \times 3 = 24$
   Note que 24 é múltiplo de 6 e de 8, logo é ele mesmo o menor múltiplo comum.

Exercício: Calcular

(a) $mmc(49, 84)$
(b) $mmc(36, 60, 72)$
(c) $mmc(8, 32, 128)$
(d) $mmc(13, 39, 21)$
(e) $mmc(45, 135, 81)$
(f) $mmc(343, 91, 169)$
(g) $mmc(1800, 2700, 4500)$
(h) $mmc(7, 11, 13)$
(i) $mmc(1001, 1002)$
(j) $mmc(1001, 1078)$

O algoritmo de Euclides, que utilizamos para calcular o mdc de dois números, pode ser utilizado para calcular o mmc se lançarmos mão do seguinte fato.

Fato 5: Dados dois números naturais, seu produto é igual ao produto do seu mmc pelo seu mdc.
Por exemplo: 12 e 18

$mdc(12, 18) = 6$
$mmc(12, 18) = 36$
$36 \times 6 = 216$
$12 \times 18 = 216$

Não faremos uma prova formal deste fato. Mas vamos observar o que acontece neste caso:

$12 = 2^2 \times 3$
$18 = 2 \times 3^2$

Usamos as maiores potências para o mmc e as menores para o mdc. Assim

$mdc(12, 18) = 2 \times 3$
$mmc(12, 18) = 2^2 \times 3^2$

Observe que todas as potências foram usadas uma e só uma vez. Isso explica o Fato 5.

Se um dos números não tiver uma das potências colocamos à potência 0 (todo número elevado a 0 é igual a 1).

Exemplo: 45 e 21

$21 = 3^1 \times 5^0 \times 7^1$
$45 = 3^2 \times 5^1 \times 7^0$
$mdc(21, 45) = 3^1 \times 5^0 \times 7^0 = 3 \times 1 \times 1 = 3$
$mmc(21, 45) = 3^2 \times 5^1 \times 7^1 = 9 \times 5 \times 7 = 315$

Outra vez, todas as potências foram usadas uma e só uma vez.
$21 \times 45 = 3 \times 315 = 945$

Atenção: Esta propriedade só vale para dois números. Para três ou mais números ela pode falhar. Veja:

Tomemos os números 6, 8 e 12.
$mdc(6, 8, 12) = 2$
$mmc(6, 8, 12) = 24$

Mas $6 \times 8 \times 12 = 576$ e $2 \times 24 = 48$. Os valores são bem diferentes.

Exemplo:

Calcule o $mmc(4873, 275)$.
Agora sabemos que $4873 \times 275 = mmc \times mdc$.
Já calculamos antes o $mdc(4873, 275) = 11$

Quociente	17	1	2	1	1	3
4873	275	198	77	44	33	11
Resto	198	77	44	33	11	0

Temos então:
$4873 \times 275 = mmc \times 11$
$1340075 = 11 \times mmc$
$mmc = 1340075 : 11 = 121825$

Exercício: Calcular usando o algoritmo de Euclides e o Fato 5:

(a) $mmc(1176, 471)$
(b) $mmc(57, 36)$
(c) $mmc(175, 98)$
(d) $mmc(2536, 938)$
(e) $mmc(12578, 6248)$
(f) $mmc(1589, 3584)$

1.7 Um truque de divisibilidade

Pense num número de 3 algarismos (por exemplo 347). Escreva ele duas vezes formando um número de 6 algarismos (no nosso exemplo 347 347). Divida esse número por 13. (No nosso exemplo, o resultado é 26719). Divida esse número por 11. (No nosso exemplo, o resultado é 2429.) Divida esse número por 7. (No nosso exemplo, o resultado é ... 347.) Experimente com seu número agora. Você verá que:

- as divisões são exatas e
- o número final é o que você escolheu.

Por que isto acontece?

Bem, se fizemos divisões exatas e obtivemos o mesmo número, é porque o número "duplicado" é múltiplo do número original. O que fizemos? 327 327 é a mesma coisa que $1000 \times 327 + 327$. Ou melhor: $327\ 327 = 327 \times 1001$. Você já fatorou o 1001 num exercício anterior: $1001 = 7 \times 11 \times 13$

Está explicado o "mistério". Ao duplicar o número (sempre de 3 algarismos), você multiplicou o número por 7, por 11 e por 13.

Uma variação deste truque é usar um número de dois algarismos mas colocando um zero na duplicação:

$$35 \rightarrow 35035$$

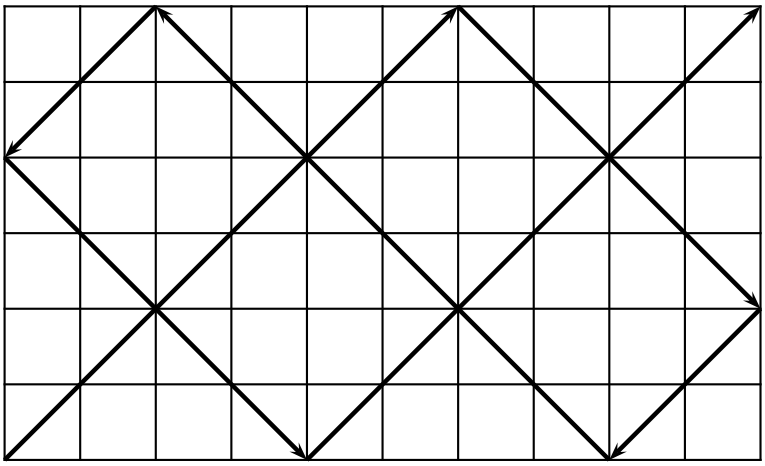
$$35035 : 13 = 2695$$

$$2695 : 11 = 245$$

$$245 : 7 = 35$$

1.8 Uma aplicação geométrica

Um retângulo de lados inteiros 6 e 10 é dividido em quadrados de lado 1, como mostra a figura abaixo.



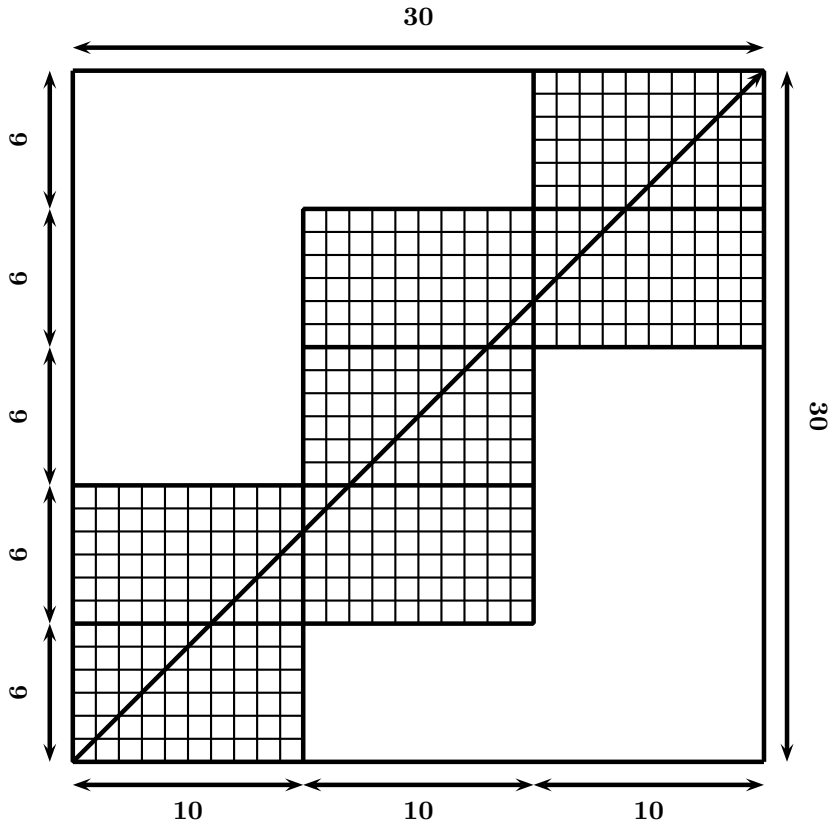
Um raio de luz entra no retângulo por um dos vértices, na direção da bissetriz do ângulo reto, e é refletido sucessivamente nos lados do retângulo. Quantos quadrados são atravessados pelo raio de luz?

Observe que seja qual for o trajeto, o raio deve atravessar um múltiplo de 6 quadrados, cada vez que vai do lado de baixo até o lado de cima, ou de cima para baixo (mesmo ricocheteando). Isso também é verdade para os trajetos que vão de um lado para outro, só que aí deve ser um múltiplo de 10 quadrados. Na primeira vez que o raio atinge um vértice (depois da entrada) ele percorreu um número de quadrados múltiplo de 10 e de 6, na verdade o menor múltiplo comum pois é a primeira vez que isso acontece. Como $mmc(10, 6) = 30$, o raio percorreu 30 quadrados.

Pergunta 1. Se eu quiser que o raio atravesse todos os quadrados, que dimensões deve ter o meu retângulo?

Pergunta 2. Se eu quiser que o raio atravesse o retângulo sem ricochetear, que dimensões deve ter o meu retângulo?

Uma outra forma de visualizar o problema é "pavimentar" o plano com cópias do retângulo (veja figura adiante). Fica bastante aparente que tenho que percorrer 3 vezes a largura ($3 \times 10 = 30$) e 5 vezes a altura ($5 \times 6 = 30$) do retângulo. Esta visualização dá uma pista para responder à pergunta 2 acima.


30
6
6
6
6
6
30
10
10
10

Capítulo 2

Aritmética Modular
Uma introdução passo a passo

Os conceitos de divisibilidade, mdc e mmc que acabamos de ver podem parecer bem simples, mas são a semente de uma parte muito interessante da Matemática. Vamos abordar algumas idéias através de questões e respostas, passo a passo.

1 A tabela da página seguinte mostra os números naturais (e o zero) até 115 colocados em determinada ordem. Você acha que todos os números naturais poderiam entrar nesta tabela? (se tivéssemos papel e tempo suficiente, é claro).

2 Em que coluna você colocaria:

1. o número 116?
2. o número 117?
3. o número 119?
4. o número 200?
5. o número 223?
6. o número 15792732 ?
7. o número 1359735?

3 Nessa tabela qual o número que fica:

0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15
16	17	18	19
20	21	22	23
24	25	26	27
28	29	30	31
32	33	34	35
36	37	38	39
40	41	42	43
44	45	46	47
48	49	50	51
52	53	54	55
56	57	58	59
60	61	62	63
64	65	66	67
68	69	70	71
72	73	74	75
76	77	78	79
80	81	82	83
84	85	86	87
88	89	90	91
92	93	94	95
96	97	98	99
100	101	102	103
104	105	106	107
108	109	110	111
112	113	114	115

1. imediatamente abaixo do número 53?
2. imediatamente acima do número 107?
3. imediatamente abaixo do número 563?
4. imediatamente acima do número 107?
5. imediatamente acima do número 15792732?
6. imediatamente abaixo do número 15792732?
7. 5 linhas abaixo do número 114 (mas na mesma coluna)?
8. 5 linhas acima do número 1421 (mas na mesma coluna)?

4 Como você descreveria os números da coluna do 0?

5 Se você somar dois números quaisquer da coluna do 0, em que coluna vai cair o resultado?

6 Observe que a tabela apresentada pode ser considerada como uma

"tabuada". Se quisermos saber a soma de $84 + 3$ basta encontrar o número que está na linha do 84 e na coluna do 3, isto, é 87.

7 Na questão 3 você deu uma descrição da primeira coluna: são os múltiplos naturais de 4 (lembre-se que estamos incluindo o 0). Podemos escrever isso em "Matematiquez":

> "O conjunto dos números da forma $4n$, onde n é um número natural",

ou ainda,

$$\{4 \cdot n \mid n \in \mathbb{N}\}$$

Se quisermos descrever os números da $2^{\underline{a}}$ coluna (a coluna do 1) podemos escrever:

> "O conjunto dos números naturais que, quando divididos por 4, dão resto 1"

ou

> "O conjunto dos números da forma $4 \cdot n + 1$, onde $n \in \mathbb{N}$",

ou ainda,

$$\{4 \cdot n + 1 \mid n \in \mathbb{N}\}$$

Observação: Você deve ter notado que passamos a usar a notação de ponto para indicar a multiplicação. Isso se deve a que agora estamos indicando multiplicação entre símbolos literais (letras), em que o símbolo $\times$ poderia gerar confusão. Para indicar a multiplicação entre números continuaremos a usar $\times$, pois o ponto poderia nos confundir — embora usemos vírgulas para números decimais menores do que 1, as máquinas de calcular que usamos utilizam o ponto.

Como você descreveria os elementos da coluna embaixo do 2? E os da coluna embaixo do 3?

8

1. Se você escolher dois números da coluna do 3 e subtrair o menor do maior, em que coluna estará a diferença?

2. Se você escolher dois números da coluna do 2 e subtrair o menor do maior, em que coluna estará a diferença?
3. Como você escreveria um resultado geral que se aplique a pares que estão na mesma coluna?

9 Se você escolher dois números da coluna do 3, em que coluna estará a soma desses números?

10 Se você escolher um número da coluna do 2 e um número da coluna do 3, em que coluna estará a soma desses números?

11 Vamos organizar uma tabela de adição: algumas casas estão preenchidas, outras ficaram para você:

+ mod4	números na coluna do 0	números na coluna do 1	números na coluna do 2	números na coluna do 3
números na coluna do 0				
números na coluna do 1		números na coluna do 2		
números na coluna do 2			números na coluna do 0	números na coluna do 1
números na coluna do 3				

12 Essa tabela é chamada de **"adição módulo 4"**, ou **"soma módulo 4"**. Quando dois números têm o mesmo resto quando divididos por 4, dizemos que eles são **congruentes módulo 4**. Os números congruentes módulo 4 são aqueles que estão na mesma coluna da tabela da primeira página.

Em geral escrevemos $47 \equiv 43 \bmod 4$. Isto quer dizer que o resto de $47 : 4$ é o mesmo de $43 : 4$. Usando a questão 8 podemos escrever:

$$47 \equiv 43 \bmod 4$$

É o mesmo que dizer que

$$47 - 43 \text{ é múltiplo de } 4$$

13 Exemplo: Mostre que $107 \equiv 83 \bmod 4$.
Solução: $107 - 83 = 24$ e 24 é múltiplo de 4.
Agora experimente você:

1. Mostre que $158 \equiv 126 \bmod 4$.
2. Mostre que $113 \equiv 77 \bmod 4$.
3. Mostre que $15107 \equiv 34803 \bmod 4$.
4. Mostre que $99999 \equiv 55555 \bmod 4$.
5. Mostre que $15807 \equiv 4575 \bmod 4$.

14 Outra forma de escrever a tabela acima é (você completa o resto):

$\overset{+}{\bmod 4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$				
$\overline{1}$				
$\overline{2}$				$\overline{1}$
$\overline{3}$		$\overline{0}$		

Para que o **tracinho** em cima dos números? Note que não estamos falando do **número 1** mas de qualquer número que esteja na coluna do 1 na tabela do **módulo 4**. A soma também não é a soma que estamos acostumados. Depois de somarmos temos que verificar em que coluna estará o resultado.
Exemplo:

$473 + 487$
$473 \equiv 1 \bmod 4$
$486 \equiv 2 \bmod 4$
$473 + 486 = 959 \equiv 3 \bmod 4$

O resultado estará na coluna do 3.

15 A tabela adiante tem 5 colunas (e não 4 como a da primeira página). Você conseguiria fazer uma tabela semelhante àquela que fizemos para a primeira tabela, como no item 11?

0	1	2	3	4
5	6	7	8	9
10	11	12	13	14
15	16	17	18	19
20	21	22	23	24
25	26	27	28	29
30	31	32	33	34
35	36	37	38	39
40	41	42	43	44
45	46	47	48	49
50	51	52	53	54
55	56	57	58	59
60	61	62	63	64
65	66	67	68	69

16 Exemplo: Mostre que $107 \equiv 82 \bmod 5$.
Solução: $107 - 82 = 25$ e 25 é múltiplo de 5.
Experimente você:

1. Mostre que $158 \equiv 123 \bmod 5$.
2. Mostre que $112 \equiv 77 \bmod 5$.
3. Mostre que $1510 \equiv 34805 \bmod 5$.
4. Mostre que $12380 \equiv 55555 \bmod 5$.
5. Mostre que $15801 \equiv 4576 \bmod 5$.

17 A esta altura dos acontecimentos você já percebeu que podemos fazer tabelas para todos os números naturais. Na primeira tabela escrevemos os números de 4 em 4. Mostramos que todos os números naturais podem ser escritos na forma:

$$4 \cdot n \text{ ou } 4 \cdot n + 1 \text{ ou } 4 \cdot n + 2 \text{ ou } 4 \cdot n + 3 \text{ em que } n \in \mathbb{N}$$

18 Na segunda tabela vimos que todos os naturais podem ser escritos na forma

$$5 \cdot n \text{ ou } 5 \cdot n + 1 \text{ ou } 5 \cdot n + 2 \text{ ou } 5 \cdot n + 3 \text{ ou } 5 \cdot n + 4 \text{ em que } n \in \mathbb{N}$$

1. Se nossa tabela tivesse 7 colunas até que número iria a primeira linha?
2. Em que coluna estaria o número 48?
3. Em que coluna estaria o número 1001?
4. Que formas essa tabela nos sugeriria para escrever os números naturais (como aí acima e no item 17)?

19 Até agora só trabalhamos com os números naturais e incluímos o 0. Será que poderíamos estender nossa tabela para os números negativos?

-20	-19	-18	-17
-16	-15	-14	-13
-12	-11	-10	-9
-8	-7	-6	-5
-4	-3	-2	-1
0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15
16	17	18	19
20	21	22	23
24	25	26	27
28	29	30	31

A tabela acima mostra que isto é possível; acabamos de estender a tabela da primeira página "para trás" e agora não temos só números naturais - podemos perceber que poderemos incluir nesta tabela todos os números inteiros, positivos, 0 e negativos. Estamos lidando com o conjunto dos números inteiros, o conjunto $\mathbb{Z}$.
Quais os números que estão na coluna do 0?
Ainda são os múltiplos de 4.
Mas a divisão que trabalhamos até agora não deixa resto negativo. Lembre-se da equação de Euclides (a nossa equação (1)):

$$D = d \times q + r, \qquad r < d, \qquad d > 0, \qquad D, d, q, r \in \mathbb{N} \cup \{0\} \quad (2.1)$$

Em que:

- D é o dividendo;
- d é o divisor (que deve ser diferente de 0);
- q é o quociente; e
- r é o resto (que deve ser menor que d)

Entretanto, ainda podemos falar em módulo d !
Exemplo 1: $34 \equiv -14 \bmod 4$, pois $34 - (-14) = 34 + 14 = 48$ e 48 é múltiplo de 4.
Exemplo 2: $-9 \equiv -33 \bmod 4$, pois $-9 - (-33) = -9 + 33 = 24$ e 24 é múltiplo de 4.
Agora é com você:

1. mostre que $36 \equiv -36 \bmod 4$
2. mostre que $-34 \equiv +14 \bmod 4$
3. mostre que $334 \equiv -714 \bmod 4$
4. mostre que $45 \equiv -35 \bmod 4$
5. mostre que $31 \equiv -17 \bmod 4$
6. mostre que $31 \equiv -1017 \bmod 4$

20 Observe que, na tabela do item 19, o número 3 e o número -3 estão em colunas diferentes, mas os números 22 e -22 estão na mesma coluna; isso mostra que devemos ter cuidado - as situações variam de tabela para tabela.

Uma forma simples de localizar números negativos na tabela é usar um artifício conhecido, somar o divisor, no caso 4.

Exemplo: Em que coluna estará o número -1437?

Se fosse -1436 a resposta seria fácil: na coluna do 0 pois 1436 é múltiplo de 4. Se aceitarmos que o resto possa ser negativo, desde que não fique maior do que -3, poderemos escrever uma equação parecida com a equação (1) que chamaremos de equação (3):

$$D = d \times q + r, \quad -d < r < d, \quad d > 0, \quad D, q, r \in \mathbb{Z}, \quad d \in \mathbb{N} \quad (2.3)$$

Repare que os números D, q e r agora podem ser negativos, d continuará sendo positivo (por conveniência) e o resto r pode ir de $-d$ a d.

No nosso exemplo: $-1437 = 4 \times (-359) - 1$. Nosso resto agora é -1. Para saber em que coluna ele estará, basta somar 4.
-1 estará na coluna $(-1) + 4 = 3$ e -1437 também estará na coluna do 3.

Agora é com você. Em que coluna da tabela do módulo 4 se encontra:

1. o número -147?
2. o número -1487?
3. o número -140?
4. o número -473?
5. o número -4732 ?

Observação: Note que, ao aceitarmos valores negativos para r perdemos a **unicidade**. De fato, agora temos a possibilidade de um resto positivo e um resto negativo. Isso não é um problema, na verdade isso é necessário para podermos localizar os números negativos na nossa tabela.

21 Vamos estender a tabela do 5?

-10	-9	-8	-7	-6
-5	-4	-3	-2	-1
0	1	2	3	4
5	6	7	8	9
10	11	12	13	14
15	16	17	18	19

Em que coluna da tabela do 5 você colocaria:

1. o número -147?
2. o número -1487?
3. o número -140?
4. o número -473?

5. o número -4732 ?

22 Vamos estender a tabela do 7?

-14	-13	-12	-11	-10	-9	-8
-7	-6	-5	-4	-3	-2	-1
0	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20

Estenda a tabela nos dois sentidos (positivo e negativo). Em que coluna da tabela do módulo 7 se encontra:

1. o número -147?
2. o número -1487?
3. o número -140?
4. o número -473?
5. o número -4732?

23 Até agora nos aproveitamos do fato de que dois números na mesma coluna têm a mesma forma. Por exemplo, na tabela do 4:
473 fica na coluna do 1, pois é da forma $4 \times 118 + 1$.
1013 também fica na coluna do 1, pois é da forma $4 \times 253 + 1$.
Os dois são da forma $4 \cdot n + 1$.
Se subtraímos dois números desta forma temos:
$(4a + 1) - (4b + 1) = 4a + 1 - 4b - 1 = 4(a - b)$ que será sempre um múltiplo de 4.
A soma também "se comportou bem", pois os números estão sendo representados pelo resto da divisão por 4. Por exemplo:
$473 = 4 \times 118 + 1 \rightarrow$ 473 fica na coluna do $1 \rightarrow$ 473 é representado pelo $\overline{1}$.
$1027 = 4 \times 256 + 3 \rightarrow$ 1027 fica na coluna do $3 \rightarrow$ 1027 é representado

pelo $\overline{3}$.
A soma $473 + 1027$ ficará na coluna do 0, pois na tabela que construímos:

$$\overline{1} + \overline{3} = \overline{0}$$

Vamos tentar estender nossas idéias para a **multiplicação modular**.

24 Usaremos uma pequena porção da tabela do 4.

0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15
16	17	18	19
20	21	22	23

1. Escolha um número da coluna do 1 e outro da coluna do 3. Multiplique estes dois números. Em que coluna caiu o produto? Exemplo: $9 \times 7 = 63$; 63 está na coluna do 3, pois $63 = 4 \times 15 + 3$.
2. Repita a experiência. O produto cai sempre na mesma coluna?
3. Experimente pegar dois números da coluna do 3. Em que coluna cai o produto? Repita a experiência.
   Se você fez as contas direito reparou que nos itens a) e b) o resultado cai na coluna do 3; nenhuma surpresa, pois $1 \times 3 = 3$.
   Já no item c) os produtos recaem na coluna do 1. Como $3 \times 3 = 9$ e $9 \equiv 1 \bmod 4$, podemos desconfiar que a multiplicação também vai se "comportar direitinho" na nossa aritmética dos módulos. Em vez de desconfiar, vamos demonstrar.

Vamos primeiro ver um caso simples. Vamos escolher um número da coluna do 2 e um número da coluna do 3. Eles podem ser escritos como:

$$4 \cdot a + 2 \text{ e } 4 \cdot b + 3$$

O seu produto é

$$(4 \cdot a + 2) \cdot (4 \cdot b + 3) = 16 \cdot a \cdot b + 12 \cdot a + 8 \cdot b + 6$$

Observe que os termos literais (que contém letras) são todos múltiplos de 4. Resta-nos o 6, que está na coluna do 2, pois $6 \equiv 2 \bmod 4$. Podemos fazer o mesmo raciocínio para todos os números e fabricar uma tabuada de **multiplicação** módulo 4.

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

25 Você pode usar a tabela do 5 para fabricar a tabuada de multiplicação módulo 5. Já colocamos alguns resultados, você preenche o resto.

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

26

1. Fabrique a tabela do 7.
2. Fabrique a tabuada de **adição** módulo 7.
3. Fabrique a tabuada de **multiplicação** módulo 7.

27 Exemplo: qual o resto de $7^{12} : 4$?
Poderíamos calcular $7^{12} = 13841287201$ e verificar que o resto é 1; mas podemos fazer de forma mais simples.
$7 \equiv 3 \bmod 4$, então podemos trabalhar com 3^{12}.
$3^{12} = 3 \times 3 \times 3 \times 3 \times 3 \times 3 \times 3 \times 3 \times 3 \times 3 \times 3 \times 3$
Mas olhando a tabuada de multiplicação módulo 4, verificamos que $3 \times 3 \equiv 1 \bmod 4$. Chegamos à conclusão que
$7^{12} \equiv 1 \times 1 \times 1 \times 1 \times 1 \times 1 \bmod 4$, isto é, $7^{12} \equiv 1 \bmod 4$.
O resto de $7^{12} : 4$ é 1.

28 Exemplo: Qual o resto de $4^{15} : 7$? Se você fez a tabuada de multiplicação módulo 7 podemos calcular:
$4^2 \equiv 2 \bmod 7$,
$4^3 \equiv 2 \times 4 \bmod 7 \equiv 8 \bmod 7 \equiv 1 \bmod 7$,
$4^{15} = \left(4^3\right)^5 \equiv 1^5 \bmod 7 \equiv 1 \bmod 7$.
O resto de $4^{15} : 7$ é 1.

29 Não precisaremos sempre formar a tabuada.
Exemplo: Qual o resto de $7^{30} : 11$?
Vamos calcular passo-a-passo:
$7^2 = 49 \equiv 5 \bmod 11$ (pois $49 = 4 \times 11 + 5$)
$7^4 \equiv 5^2 \bmod 11 \equiv 25 \bmod 11 \equiv 3 \bmod 11$
$7^8 \equiv 3^2 \bmod 11 \equiv 9 \bmod 11$
$7^{16} \equiv 9^2 \bmod 11 \equiv 81 \bmod 11 \equiv 4 \bmod 11$
$7^{30} = 7^{(16+8+4+2)} = 7^{16} \times 7^8 \times 7^4 \times 7^2 \equiv 4 \times 9 \times 3 \times 5 \bmod 11$
$7^{30} \equiv 36 \times 15 \bmod 11 \equiv 3 \times 4 \bmod 11 \equiv 12 \bmod 11 \equiv 1 \bmod 11$
O resto de $7^{30} : 11$ é 1.

30 Exemplo: Mostre que 41 divide $2^{20} - 1$. (Sugestão: prove que $2^{20} \equiv 1 \bmod 41$)
Solução (uma delas):
$2^{10} = 1024 \equiv 40 \bmod 41$
Mas $40 \equiv -1 \bmod 41$
$2^{20} = 2^{10} \times 2^{10} \equiv -1 \times -1 \bmod 41 \equiv 1 \bmod 41$
Como $2^{20} \equiv 1 \bmod 41$
$2^{20} - 1$ é múltiplo de 41.

31 Exercício: Diga se é Verdadeiro ou Falso

1. $19 \equiv 7 \bmod 2$
2. $52 \equiv -18 \bmod 10$
3. $1213 \equiv 212 \bmod 13$
4. Se $1066 \equiv 1776 \bmod m$, quais são os possíveis valores de m?
5. Ache todos os inteiros x, tais que $0 < x < 15$ e $3 \cdot x \equiv 6 \bmod 15$.
6. Dê todos os inteiros positivos x menores que 100, tais que $x \equiv 8 \bmod 13$.
7. Ache o resto da divisão $2^{50} : 7$
8. Mostre que 89 divide $2^{44} - 1$.
   (Sugestão: prove que $2^{44} \equiv 1 \bmod 89$.)

Apêndice A

Para saber mais

Para saber mais você pode consultar os artigos abaixo, publicados na *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