


# Montando critérios de divisibilidade diferentes

Bruno Ribeiro 

Talysson Paulo da Silva 

## Resumo

Crítérios de divisibilidade são tópicos de bastante interesse dos professores e alunos pois servem como exercícios elementares de aritmética, geralmente divertidos e curiosos. Propomos neste artigo a criação, demonstração e exemplificação de critérios de divisibilidade diferentes dos usuais, baseados na ideia de “quebrar” um número, retirando parte de seus algarismos e manipulando algebricamente essa quebra para formar números menores, cujas divisibilidades sejam equivalentes à divisibilidade do número original.

**Palavras-chave:** Critérios de Divisibilidade; Números Primos; Aritmética Modular.

## Abstract

Divisibility rules are topics of great interest to teachers and students as they serve as elementary arithmetic exercises, usually fun and curious. We propose in this article the creation, demonstration and exemplification of divisibility criteria different from the usual ones, based on the idea of “breaking” a number, removing part of its digits and algebraically manipulating this break to form smaller numbers, whose divisibilities are equivalent to the divisibility of the original number.

**Keywords:** Divisibility rules, Modular Arithmetics, Prime Numbers

## 1. Introdução

Recentemente, foi bastante noticiado na imprensa brasileira e internacional o feito de um menino nigeriano, Chika Ofili, de 12 anos, que descobriu um novo critério de divisibilidade por 7. Um feito tido por muitos como fantástico e surpreendente. Se você está lendo esse artigo numa época próxima a sua publicação, poderá procurar em qualquer *site* de busca estas notícias; veja por exemplo em [2, 5]. Caso contrário, não importa. Nosso objetivo não é dissertar especificamente sobre tal descoberta e sim mostrar como obtê-la (e várias outras que você leitor queira criar). O critério desenvolvido pelo garoto Ofili pode ser assim descrito: pegue um número inteiro positivo qualquer,  $n$ . Retire dele seu algarismo da unidade e ao número resultante some a quantia de 5 vezes esse algarismo. Com um exemplo: se  $n = 623$  então faça  $62 + 5 \cdot 3$ . O resultado, igual a 77, é um número bem menor que o original e mais fácil de checar possível divisibilidade por 7. O que ele afirmou é que  $n$  é divisível por 7 se e somente se o número menor também for (é o caso aí nesse exemplo). A proposta deste artigo é mostrar que a aritmética básica aliada à poderosa linguagem notacional de congruência “módulo  $n$ ”, introduzida no século 19 por Carl Friedrich Gauss, podem ser usadas para criar e demonstrar princípios e critérios de divisibilidade semelhantes para quaisquer

primos  $p$  que se queira. Por exemplo, Ofili poderia ter multiplicado por  $-2$  em vez de  $5$ , criando um novo critério (que seria até melhor pois o número resultante ficaria ainda menor). Cabe ressaltar que de maneira alguma os autores pretendem diminuir o feito do garoto. Apenas pretende-se mostrar que a Matemática em geral, quando bem esclarecida, é bem mais simples do que parece.

Este artigo não tem pretensões de originalidade. Resultados semelhantes e ideias equivalentes podem ser encontrados, por exemplo, em [1]. No entanto, acreditamos que o material é escasso em língua portuguesa e vale a pena ser explorado. Avisamos também ao leitor que é necessário o domínio de alguns preliminares algébricos e aritméticos básicos, principalmente envolvendo a aritmética modular e a notação desenvolvida por Gauss. Para uma boa introdução a esses conceitos elementares, indicamos os livros do A. Hefez, [3] e do J. Plínio de Oliveira [6]. Sugerimos também um bom livro introdutório à aritmética modular para se inserir já no ensino fundamental, por Kersonowsky [4]. No entanto, colocamos numa seção de preliminares os principais resultados utilizados, para que a leitura seja tão autossuficiente quanto possível.

A ideia central deste trabalho é elaborar critérios para mostrar que um determinado primo  $p$  divide um certo inteiro  $n$  se, e somente se,  $p$  divide  $m$ , um inteiro devidamente construído através de somas de múltiplos de algarismos da unidade (e dezena e centena) retirados de  $n$ . Esclarecemos essa ideia nas próximas seções.

## 2. Algumas notações e resultados preliminares

Como mencionado na introdução, precisaremos de algumas notações e definições da aritmética modular básica, bem como alguns resultados elementares, para que a leitura e entendimento dos critérios de divisibilidade que iremos propor sejam bem compreendidos. De qualquer forma, em vez de exigir que o leitor busque em outras fontes tais conceitos, colocaremos aqui o básico.

**Definição 1.** Seja  $m$  um inteiro não nulo, positivo. Dois inteiros  $a$  e  $b$  serão ditos *congruentes módulo  $m$*  se os restos de  $a$  e  $b$  por  $m$  forem iguais. Quando  $a$  e  $b$  são congruentes módulo  $m$ , escrevemos

$$a \equiv b \pmod{m}.$$

Quando os números não forem congruentes, utilizamos a notação óbvia  $a \not\equiv b \pmod{m}$ . Um fato crucial e elementar de se observar é o seguinte: Se  $a, b, m \in \mathbb{Z}$ , tem-se que  $a \equiv b \pmod{m}$  se, e somente se,  $a - b$  é múltiplo de  $m$ . Ou seja, em vez de buscar restos da divisão de  $a$  por  $m$  e de  $b$  por  $m$  e compará-los, podemos fazer a diferença  $a - b$  e verificar se este número é múltiplo de  $m$ . Por exemplo,  $25 \equiv 1 \pmod{6}$  já que  $6$  divide  $25 - 1 = 24$  e  $15 \not\equiv 5 \pmod{4}$  pois  $4$  não divide  $10 = 15 - 5$ . Além disso, essa notação de congruência é compatível com as operações elementares de soma e multiplicação, de várias maneiras que elencamos (sem demonstração) abaixo. Para uma prova destas afirmações, indicamos [3, 4].

Sejam  $a, b, c, d, m, n \in \mathbb{Z}$  e  $n \geq 1$ . Temos que:

1. Se  $a \equiv b \pmod{m}$  e  $c \equiv d \pmod{m}$  então  $a + c \equiv b + d \pmod{m}$ ;
2.  $a + c \equiv b + c \pmod{m} \Leftrightarrow a \equiv b \pmod{m}$ ;
3. Se  $a \equiv b \pmod{m}$  e  $c \equiv d \pmod{m}$ , então  $a \cdot c \equiv b \cdot d \pmod{m}$ ;
4. Se  $a \equiv b \pmod{m}$ , então  $a^n \equiv b^n \pmod{m}$ .

Para efeito de curiosidade, note que não é verdade a “lei do corte” para a multiplicação, analogamente ao item 2 acima: Se  $a \cdot c \equiv b \cdot c \pmod{m}$  então não necessariamente teremos  $a \equiv b \pmod{m}$ . Esse corte vale caso  $m$  e  $c$  sejam coprimos, ou seja, não possuam divisores comuns além do 1 e  $-1$ .

Um conceito importante que vamos utilizar nos critérios de divisibilidade que iremos propor adiante é o de inverso multiplicativo módulo  $m$ .

**Definição 2.** Seja  $m$  um inteiro não nulo, positivo e  $a$  um inteiro qualquer. Dizemos que  $x$  é um inverso multiplicativo de  $a$  módulo  $m$  se vale a igualdade

$$a \cdot x \equiv 1 \pmod{m}.$$

Cabem aqui algumas observações importantes: fixado um  $m > 1$ , não é verdade que qualquer número inteiro possua inverso multiplicativo módulo  $m$ . Por exemplo, é impossível encontrar um  $x$  tal que  $6 \cdot x \equiv 1 \pmod{4}$ . Na verdade, é direto checar que existe inverso multiplicativo de  $a$  módulo  $m$  se e somente se  $a$  e  $m$  forem coprimos. Além disso, inversos multiplicativos módulo  $m$ , caso existam, nunca são únicos. Veja: 5 é inverso multiplicativo de 3 módulo 7, assim como também é  $-2$ , 12, 19, etc. Todas essas afirmações podem ser verificadas com suas demonstrações em [3, 6].

Para finalizar essas preliminares, deixamos aqui uma propriedade fundamental de um número primo  $p$ , que iremos usar bastante no decorrer deste artigo:

**Afirmção:** Sejam  $a, b, p \in \mathbb{Z}$ , com  $p$  primo. Se  $p$  divide o produto  $a \cdot b$  e  $p$  não divide  $a$  então obrigatoriamente  $p$  divide  $b$ .

Isso significa, trazendo para a linguagem de congruências, que se  $a \cdot b \equiv 0 \pmod{p}$  e  $a$  não é múltiplo de  $p$  então  $b \equiv 0 \pmod{p}$ .

### 3. Construindo critérios de divisibilidade

Nesta seção apresentamos o método geral que utilizamos para desenvolver alguns critérios de divisibilidade curiosos (e tornar possível você desenvolver seu próprio critério!). Para estabelecer se um dado número natural  $n$  é divisível por um primo  $p$  a ideia é reduzir o problema checando a divisibilidade por  $p$  de um outro número  $m$  construído adequadamente a partir de  $n$ , obtido ao retirar-se de  $n$  algarismos de sua representação decimal. O método mostra-se efetivo porque  $m$  tem ordem de grandeza menor do que  $n$  e a propriedade de ser divisível por  $p$  será equivalente para esses dois números.

#### 3.1. Quebra na unidade

Sejam  $r \geq 1$  e  $n = a_r a_{r-1} a_{r-2} \dots a_1 a_0$  um número natural, onde os  $a_i$  são os algarismos da representação decimal de  $n$ . Ou seja, esta representação significa que os  $a_i$  são algarismos entre 0 e 9 posicionados nesta sequência de acordo com sua ordem de grandeza decimal.

$$n = a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + a_{r-2} \cdot 10^{r-2} + \dots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0.$$

Assim, por exemplo, o número 7340 pode ser escrito como  $7340 = 7 \cdot 10^3 + 3 \cdot 10^2 + 4 \cdot 10 + 0$ . Quebrar  $n$  em relação à unidade consiste em considerar um número da forma  $m = a_r a_{r-1} a_{r-2} \dots a_1 + x \cdot a_0$

para algum inteiro  $x$ . Assim, para estabelecer a divisibilidade de  $n$  por um número primo  $p$  a ideia é encontrar um valor para  $x$  de tal forma que  $p$  divide  $n$  se, e somente se,  $p$  também divide  $m$ . Como a propriedade de ser divisível por  $p$ , vale para  $n$  se, e somente se, vale para  $m$ , a existência do inteiro  $x$  permite repetir o argumento sucessivamente até obtermos um número  $m$  cuja relação de divisibilidade por  $p$  possa ser mais facilmente verificada.

Temos o seguinte resultado:

**Teorema 1** (uma quebra na unidade). *Sejam  $n = a_r a_{r-1} a_{r-2} \dots a_2 a_1 a_0$  um número natural,  $p$  um número primo (diferente de 2 e 5) e  $x \in \mathbb{Z}$  tal que  $10 \cdot x \equiv 1 \pmod{p}$ . Ou seja,  $x$  é um inverso multiplicativo de 10 módulo  $p$ . O critério de divisibilidade então é o seguinte: se  $m = a_r a_{r-1} a_{r-2} \dots a_2 a_1 + x \cdot a_0$  então  $p$  divide  $n$  se e somente se  $p$  divide  $m$ .*

*Prova:* A notação  $n = a_r a_{r-1} a_{r-2} \dots a_2 a_1 a_0$  e  $m = a_r a_{r-1} a_{r-2} \dots a_2 a_1 + x \cdot a_0$  significa que

$$n = a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + a_{r-2} \cdot 10^{r-2} + \dots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$$

$$m = a_r \cdot 10^{r-1} + a_{r-1} \cdot 10^{r-2} + a_{r-2} \cdot 10^{r-3} + \dots + a_2 \cdot 10 + a_1 + x \cdot a_0,$$

de onde segue que

$$n = 10 \cdot m + (1 - 10 \cdot x) \cdot a_0.$$

Note que como  $x$  é um inverso multiplicativo de 10 módulo  $p$ , então o termo  $(1 - 10 \cdot x)$  que aparece do lado direito da equação acima é divisível por  $p$ . Portanto, não importa quem é  $a_0$ , temos certeza que

$$n \equiv 10 \cdot m \pmod{p}. \quad (1)$$

A equação acima afirma que  $n$  é divisível por  $p$  se, e somente se  $10 \cdot m$  também é divisível por  $p$ . No entanto, como  $p$  é primo e  $p$  não divide 10 (já que  $p$  não é igual a 2 nem 5), então temos que  $p$  divide  $n$  se, e somente se,  $p$  divide  $m$ .  $\square$

Que tal um critério de divisibilidade por 3 diferente? Tudo bem, é bem verdade que o bom e velho critério de somar os algarismos é extremamente prático e melhor que este que apresentaremos, mas fica o registro (mesmo que por pura curiosidade):

**Corolário 1** (divisibilidade por 3). *Um número natural  $n = a_r a_{r-1} a_{r-2} \dots a_2 a_1 a_0$  é divisível por 3 se, e somente se 3 divide  $m = a_r a_{r-1} a_{r-2} \dots a_2 a_1 + a_0$ .*

*Prova.* De fato, uma vez que  $10 \cdot 1 \equiv 1 \pmod{3}$ , segue que um inverso multiplicativo de 10 módulo 3 é 1. Então basta fazer  $x = 1$  no Teorema 1.  $\square$

Exemplos são sempre bons: pegue  $n = 273$ . Então a divisibilidade por 3 desse número ocorre pois  $27 + 3 = 30$  e 30 é divisível por 3.

Uma observação curiosa é que esse critério de divisibilidade por 3 acima, quando aplicado sucessivas vezes até se esgotarem os algarismos do número original, é precisamente o critério usual da soma dos algarismos.

Vamos agora para o 7.

**Corolário 2** (divisibilidade por 7). *Um número natural  $n = a_r a_{r-1} a_{r-2} \dots a_2 a_1 a_0$  é divisível por 7 se, e somente se, 7 divide  $m = a_r a_{r-1} a_{r-2} \dots a_2 a_1 + 5 \cdot a_0$ .*

*Prova.* Note que  $10 \cdot 5 = 50 = 49 + 1$ . Daí, segue que um inverso multiplicativo de 10 módulo 7 é 5. Ou seja, tome  $x = 5$  no Teorema 1.  $\square$

Cabe um comentário:  $-2$  também é um inverso multiplicativo de  $10$  módulo  $7$ , portanto, o critério de  $7$  pode ser com  $-2$  no lugar do  $5$ , caso prefira. Observe ser esse exatamente o critério que mencionamos na introdução deste artigo.

Exemplos? Vamos lá: Será que  $652$  é divisível por  $7$ ? Bem, é divisível caso  $65 + 5 \cdot 2$  também seja. Mas,  $65 + 5 \cdot 2 = 75$  e portanto,  $652$  não é múltiplo de  $7$ .

E  $1428$ ? vamos usar o  $-2$  agora. Talvez uma figura com passo a passo ajude, já que vamos implementar a ideia de quebra mais de uma vez, nesse caso. Observe a Figura 1.

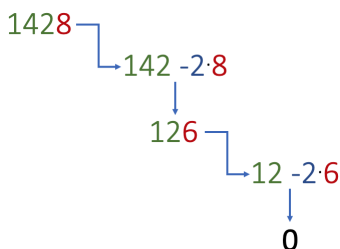


Figura 1: Esquema de verificação de divisibilidade por 7

Como  $0$  é obviamente múltiplo de  $7$ , temos que  $1428$  também é.

**Corolário 3** (divisibilidade por  $11$ ). *Um número natural  $n = a_r a_{r-1} a_{r-2} \dots a_2 a_1 a_0$  é divisível por  $11$  se, e somente se,  $11$  divide  $m = a_r a_{r-1} a_{r-2} \dots a_2 a_1 - a_0$ .*

*Prova.* De fato, desde que  $10 \cdot 10 = 100 = 9 \cdot 11 + 1$ , segue que um inverso multiplicativo de  $10$  módulo  $11$  é  $10 \equiv -1 \pmod{11}$ . Então basta fazer  $x = -1$  no Teorema 1.  $\square$

Poderíamos também escolher  $x = 10$  neste critério, mas o número obtido ao quebrar a unidade e somá-lo com  $10$  vezes o valor dela fica demasiado grande em comparação com a escolha do  $-1$ .

Vamos verificar se  $n = 22737$  é divisível por  $11$ . Aplicando o critério de divisibilidade estabelecido acima,  $n$  é divisível por  $11$  se, e somente se,  $m = 2273 - 7 = 2266$  também é. Como ainda não é evidente se  $m$  é ou não divisível por  $11$ , aplicamos o critério novamente agora sobre esse  $m$ . O número  $m$  é divisível por  $11$  se, e somente se,  $226 - 6 = 220$  também é. Mais uma vez, isso ocorre se, e somente se,  $22 - 0 = 22$  é divisível por  $11$ . Como  $11$  divide  $22$ , segue que  $n = 22737$  também é divisível por  $11$ .

O critério de divisibilidade por  $11$  mais conhecido consiste em fazer uma soma de algarismos trocando o sinal alternadamente entre as ordens: por exemplo, pode-se começar somando a unidade, subtraindo a dezena, somando a centena etc. O resultado obtido é congruente módulo  $11$  ao número original. No caso acima,  $n = 22737$  faríamos  $2 - 2 + 7 - 3 + 7 = 11$ , concluindo que este  $n$  é múltiplo de  $11$ .

Vamos continuar nossa brincadeira formando critérios para outros números primos maiores, mesmo que corramos o risco de ficar um pouco repetitivo a partir de agora.

**Corolário 4** (divisibilidade por  $13$ ). *Um número natural  $n = a_r a_{r-1} a_{r-2} \dots a_2 a_1 a_0$  é divisível por  $13$  se, e somente se,  $13$  divide  $m = a_r a_{r-1} a_{r-2} \dots a_2 a_1 + 4 \cdot a_0$ .*

*Prova.* Como usual, tudo que precisamos é tomar um inverso multiplicativo de 10 módulo 13 mais apropriado. No caso,  $x = 4$ . □

Cansados de exemplos? Só mais um: vamos mostrar que  $n = 15678$  é divisível por 13. De novo, para quebrar a monotonia dos textos, vamos fazer um esquema mais dinâmico com auxílio de recursos gráficos. Veja a próxima figura.

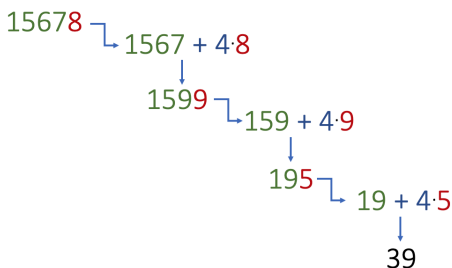


Figura 2: Esquema de verificação de divisibilidade por 13

Como claramente 39 é divisível por 13, segue que 15678 também é.

Enfim, vamos fazer o último desses critérios com essa quebra da unidade:

**Corolário 5** (divisibilidade por 17). *Um número natural  $n = a_r a_{r-1} a_{r-2} \dots a_2 a_1 a_0$  é divisível por 17 se, e somente se, 17 divide  $m = a_r a_{r-1} a_{r-2} \dots a_2 a_1 - 5 \cdot a_0$ .*

*Prova.* Novamente, basta notar que  $-5$  é um inverso multiplicativo de 10 módulo 17. □

Convidamos o leitor a verificar com exemplos este critério. Poderíamos continuar com critérios para quaisquer primos seguintes, como 19, 23 etc. Mas acreditamos que o caminho já está claro para todos que queiram agora desenvolver tais critérios.

Antes de continuar, cabe aqui uma observação importante: os critérios baseados no Teorema 1 são apenas para divisibilidade. Diferentemente de alguns critérios tradicionais, que determinam a congruência  $n \equiv m \pmod{p}$ , os critérios acima são consequência da equação (1). Isso significa que vários critérios usuais não são apenas de divisibilidade mas também servem para cálculos de restos quando os números não forem divisíveis. Por exemplo, aquele critério usual do 3, de somar os algarismos, não só diz que um número é divisível por 3 quando a soma dos algarismos for, mas também estabelece que o resto da divisão do número por 3 é o mesmo resto da divisão desta mesma soma por 3. Em nosso caso, isso não é verdade. Se o número obtido pela quebra da unidade, em qualquer exemplo acima, não for divisível pelo primo em questão, então o seu resto não será igual ao resto do número original (note que temos um fator 10 multiplicando a congruência entre  $n$  e  $m$ ). Veja o caso do 652 no exemplo que trouxemos para a divisibilidade por 7 acima. Enquanto que o resto da divisão de 652 por 7 é 1, o resto de  $65 + 5 \cdot 2 = 75$  é 5.

### 3.2. Quebra na dezena

Podemos ampliar a ideia da última seção. Em vez de quebrar apenas o algarismo da unidade e somar o número quebrado a um múltiplo desta unidade, propomos quebrar o número nos algarismos

da unidade e da dezena, diminuindo ainda mais a ordem do número resultante. Sejam  $r \geq 2$  e  $n = a_r a_{r-1} a_{r-2} \dots a_1 a_0$  um número natural. De maneira análoga à quebra do algarismo da unidade, consideremos números da forma  $m = a_r a_{r-1} a_{r-2} \dots a_2 + y \cdot a_1 + x \cdot a_0$  para certos inteiros  $x$  e  $y$ . Agora a “brincadeira” consiste em encontrar valores para  $x$  e  $y$  de maneira que a divisibilidade de  $n$  por um primo  $p$  seja equivalente à divisibilidade de  $m$  por este  $p$ .

O leitor atento pode pensar: parece um critério ruim de se aplicar, porque exige uma operação complexa de calcular dois múltiplos dos algarismos retirados e somar ao número quebrado, tornando um pouco difícil o cálculo mental. Nossa resposta à eventual pergunta: o leitor está coberto de razão. Não é um critério que poderíamos chamar de prático, mas serve como um exercício de aritmética interessante e pode ser útil para números primos relativamente grandes.

Segue o resultado.

**Teorema 2** (quebra na dezena). *Sejam  $r \geq 2$ ,  $n = a_r a_{r-1} a_{r-2} \dots a_2 a_1 a_0$  e  $p$  um número primo diferente de 2 e 5. Sejam  $x$  e  $y$  soluções inteiras das seguintes equações de congruência:*

$$\begin{cases} 10 \cdot y \equiv 1 \pmod{p} \\ 100 \cdot x \equiv 1 \pmod{p} \end{cases} \quad (2)$$

Então  $n$  é múltiplo de  $p$  se e somente se  $m = a_r a_{r-1} a_{r-2} \dots a_2 + y \cdot a_1 + x \cdot a_0$  é múltiplo de  $p$ .

*Prova.* Considerando o sistema de representação decimal de  $n = a_r a_{r-1} a_{r-2} \dots a_2 a_1 a_0$  e  $m = a_r a_{r-1} a_{r-2} \dots a_2 + y \cdot a_1 + x \cdot a_0$ , podemos escrever

$$n = a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + a_{r-2} \cdot 10^{r-2} + \dots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$$

$$100 \cdot m = a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + a_{r-2} \cdot 10^{r-2} + \dots + a_2 \cdot 10^2 + 100 \cdot y \cdot a_1 + 100 \cdot x \cdot a_0,$$

de onde segue que

$$n - 100 \cdot m = 10 \cdot a_1 - 100 \cdot y \cdot a_1 + a_0 - 100 \cdot x \cdot a_0 = (10 - 100 \cdot y) \cdot a_1 + (1 - 100 \cdot x) \cdot a_0.$$

Assim, uma vez que  $p$  divide  $10 \cdot (1 - 10 \cdot y) \cdot a_1$  e  $(1 - 100 \cdot x) \cdot a_0$  (hipótese do teorema), temos que

$$n \equiv 100 \cdot m \pmod{p}.$$

Mas  $p$  não é 2 nem 5. Ou seja,  $p$  não divide 100. Sendo assim, o fato de  $p$  dividir  $100 \cdot m$  é equivalente a dividir  $m$ . Portanto,  $p$  divide  $n$  se e somente se  $p$  divide  $m$ .  $\square$

Note que  $y$  deve ser um inverso multiplicativo de 10 módulo  $p$  e  $x$  um inverso multiplicativo de 100 módulo  $p$ .

A única restrição para  $p$  é não ser igual a 2 ou 5. Então podemos formar novos critérios para divisibilidade por 3, por 7 etc, assim como fizemos na seção anterior. Tudo que precisamos resolver são as equações em (2) para o primo  $p$  em questão. Por exemplo, para o 3, tomaríamos  $x = 1$  e  $y = 1$ . Para o 7,  $x = 4$  e  $y = 5$  serviriam (ou  $x = -3$  e  $y = -2$ ). Como aplicação desse teorema, vamos, porém, propor critérios para primos maiores pois imaginamos que esta quebra só parece fazer sentido para números grandes.

**Corolário 6** (divisibilidade por 13). *Um número natural  $n = a_r a_{r-1} a_{r-2} \dots a_2 a_1 a_0$  é divisível por 13 se, e somente se, 13 divide  $m = a_r a_{r-1} a_{r-2} \dots a_2 + 4 \cdot a_1 + 3 \cdot a_0$ .*





**Teorema 3** (quebra na centena). *Sejam  $r \geq 3$ ,  $n = a_r a_{r-1} a_{r-2} \dots a_2 a_1 a_0$  e  $p$  um número primo diferente de 2 e 5. Sejam  $x$ ,  $y$  e  $z$  soluções inteiras das seguintes equações de congruência:*

$$\begin{cases} 10 \cdot z \equiv 1 \pmod{p} \\ 100 \cdot y \equiv 1 \pmod{p} \\ 1000 \cdot x \equiv 1 \pmod{p} \end{cases} \quad (3)$$

Então  $n$  é múltiplo de  $p$  se, e somente se,  $m = a_r a_{r-1} a_{r-2} \dots a_3 + z \cdot a_2 + y \cdot a_1 + x \cdot a_0$  é múltiplo de  $p$ .

*Prova.* Escrevendo

$$n = a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + a_{r-2} \cdot 10^{r-2} + \dots + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$$

$$1000 \cdot m = a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \dots + a_3 \cdot 10^3 + 1000 \cdot z \cdot a_2 + 1000 \cdot y \cdot a_1 + 1000 \cdot x \cdot a_0,$$

temos que

$$n - 1000 \cdot m = (100a_2 + 10a_1 + a_0) - (1000za_2 + 1000ya_1 + 1000xa_0)$$

ou seja,

$$n - 1000m = 100 \cdot (1 - 10 \cdot z) \cdot a_2 + 10 \cdot (1 - 100 \cdot y) \cdot a_1 + (1 - 1000 \cdot x) \cdot a_0.$$

Note que  $p$  divide todas as parcelas do lado direito da equação acima por causa de (3). Sendo assim, temos que  $n \equiv 1000 \cdot m \pmod{p}$ . Mas  $p$  não divide 1000, já que  $p \neq 2$  e  $p \neq 5$ . Portanto, a divisão exata de  $n$  por  $p$  ocorre se e somente se também ocorrer a divisão de  $m$  por  $p$ .  $\square$

Aqui percebemos o padrão, pois  $z$  deve ser um inverso multiplicativo de 10 módulo  $p$ ,  $y$  deve ser um inverso de 100 e  $x$  um inverso de 1000. Ou seja, se quiséssemos continuar com quatro quebras, cinco, ou mais, já saberíamos o que fazer, certo?

Então, vamos a nosso último critério.

**Corolário 9** (divisibilidade por 23). *Um número natural  $n = a_r a_{r-1} a_{r-2} \dots a_2 a_1 a_0$  é divisível por 23 se, e somente se, 23 divide  $m = a_r a_{r-1} \dots a_3 + 7 \cdot a_2 + 3 \cdot a_1 - 2 \cdot a_0$*

*Prova.* Tome  $z = 7$ ,  $y = 3$  e  $x = -2$ , pois esses números resolvem as equações (3) das hipóteses do Teorema 3.  $\square$

Para terminar, vamos mostrar que  $n = 9867359812$  é divisível por 23. Aplicando o critério de divisibilidade acima, o número  $n$  é divisível por 23 se, e somente se, 23 divide  $9867359 + 7 \cdot 8 + 3 \cdot 1 - 2 \cdot 2 = 9867414$ . Esse número, por sua vez, é divisível por 23 se, e somente se, 23 divide  $9867 + 7 \cdot 4 + 3 \cdot 1 - 2 \cdot 4 = 9890$ . Por sua vez, esse número é divisível por 23 se, e somente se, 23 divide  $9 + 7 \cdot 8 + 3 \cdot 9 - 2 \cdot 0 = 92$ . Como 92 é divisível por 23, segue que  $n = 9867359812$  também é divisível por 23.

## Agradecimentos

Este artigo foi parcialmente desenvolvido durante a elaboração da dissertação de Mestrado do segundo autor quando era discente do Profmat UFPB. O autor agradece à instituição e a todos os envolvidos na organização deste programa pela excelente formação recebida.

## Referências

- [1] CONRAD, K. *Universal divisibility test*, <<https://kconrad.math.uconn.edu/blurbs/ugradnumthy/universaldivtest.pdf>> Acesso em: 19 de março de 2020.
- [2] ELLIS, M. *Chika's Test*. Disponível em: <<https://www.westminsterunder.org.uk/chikas-test/>> Acesso em: 30 de janeiro de 2020.
- [3] HEFEZ, A. *Elementos de Aritmética*, Sociedade Brasileira de Matemática (Coleção Textos Universitários). Rio de Janeiro: 2005.
- [4] KERSNOWSKY, I. *A Aritmética Modular como Ferramenta para as Séries Finais do Ensino Fundamental*. Edição. Rio de Janeiro, 2013.
- [5] PESTANA, L. *Menino de 12 anos descobre fórmula matemática que ajuda o estudo da divisão*. Disponível em: <[https://www.em.com.br/app/noticia/internacional/2019/11/19/interna\\_internacional,1102274/menino-de-12-anos-descobre-formula-matematica-que-ajuda-o-estudo-da-di.shtml](https://www.em.com.br/app/noticia/internacional/2019/11/19/interna_internacional,1102274/menino-de-12-anos-descobre-formula-matematica-que-ajuda-o-estudo-da-di.shtml)>. Acesso em: 30 de janeiro de 2020.
- [6] SANTOS, J. P. O. *Introdução à Teoria dos Números*. Sociedade Brasileira de Matemática (Coleção Textos Universitários). 3ª Edição. Rio de Janeiro: 2017.

Bruno Ribeiro  
Universidade Federal da Paraíba  
<[bruno@mat.ufpb.br](mailto:bruno@mat.ufpb.br)>

Talysson Paulo da Silva  
Universidade Federal da Paraíba  
<[talys1991@gmail.com](mailto:talys1991@gmail.com)>

Recebido: 12/02/2020  
Publicado: 20/04/2020