Trabalho apresentado no XLI CNMAC, Unicamp - Campinas - SP, 2022.

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics
Preprint

Construindo testes de divisibilidade para inteiros representados numa base qualquer

Vagner T. do Couto,[1] Gilson J. da Silva Jr.,[2] Ricardo M. C. de Souza[3]
Departamento de Eletrônica e Sistemas/UFPE, Recife, PE

Resumo. Este artigo apresenta um método de construir algoritmos rápidos para teste de divisibilidade para números inteiros representados numa base numérica arbitrária. São apresentados testes de divisibilidade por 7, 13, 17 e 19 para a base decimal, bem como testes de divisibilidade por 3, 5 e 7 em bases binárias.

Palavras-chave. Divisibilidade, Aritmética modular, Algoritmo rápido, Representação decimal

1 Introdução

Em 2019 um menino de onze anos (Chika Ofili) encontrou um algoritmo simples para o teste de divisibilidade pelo número sete [4]. O resultado, não muito popular, já era conhecido [3], mas é surpreendente o fato de uma criança ter redescoberto a técnica.

Testes simples de divisibilidade são úteis quando se quer fatorar pequenos números inteiros sem a utilização de um computador, tarefa executada em diversas ações do dia a dia, como por exemplo verificar se a quantidade de doces é divisível pelo número de crianças de uma festa.

Uma questão importante é sobre a aplicação de tal técnica em cenários computacionais práticos. Uma aplicação de testes de divisibilidade em algoritmos de criptografia ocorre na busca por números primos grandes para geração de chaves RSA [5]. Esses testes são utilizados para descartar números compostos múltiplos de primos pequenos, evitando assim um uso excessivo de testes mais complexos computacionalmente. Nesse caso, algoritmos criados para a base decimal são, em sua maioria, ineficientes, pois os computadores trabalham com representação binária (ou potência de dois).

Este artigo apresenta o teste de divisibilidade apresentado por Chika Ofili, bem como um método sistemático de construir um teste de divisibilidade para qualquer inteiro na base decimal. Exemplos são apresentados. Além disso, são apresentados testes de divisibilidade em bases binárias, o que é útil para implementação em computadores digitais. Exemplos de algoritmos de testes de divisibilidade em representação binária são apresentados.

2 Preliminares

Quase todos os métodos de teste de divisibilidade conhecidos são derivados a partir de teoria dos números, mais especificamente da teoria de congruências [1]. O princípio básico desta teoria é o bem conhecido teorema da divisibilidade apresentado a seguir.

Teorema 2.1. *Se a e n são números inteiros, $n > 0$, então existem números inteiros, únicos, q e r, chamados de quociente e resto respectivamente, tais que*

$$a = qn + r, \tag{1}$$

[1] vagner.couto@ufpe.br
[2] gilson.silvajr@ufpe.br
[3] ricardo.csouza@ufpe.br

em que $0 \leq r < n$.

A prova desse teorema pode ser encontrada em [1]. Para certos valores de a e n, o valor de r em (1) é zero e, nesse caso, diz-se que n divide a, representado por $n|a$.

Pode-se agora introduzir o conceito de congruência, apresentado a seguir.

Definição 2.1. *Sejam a e b números inteiros, e n um inteiro positivo, diz-se que a é congruente a b módulo n, representado por $a \equiv b \ (mod\ n)$, se $n|(a-b)$.*

Essa relação de equivalência apresenta diversas propriedades e teoremas que fazem parte de uma disciplina conhecida como Teoria dos Números. Entre as diversas propriedades, destacam-se as seguintes.

Teorema 2.2. *Se a, b, c e n são números inteiros, com $n > 0$, as seguintes propriedades são válidas [1].*

1. $a \equiv 0 \ (mod\ n) \Leftrightarrow n|a$,
2. $a \equiv b \ (mod\ n) \Rightarrow ac \equiv bc \ (mod\ n)$,
3. $a \equiv b \ (mod\ n) \Rightarrow a^k \equiv b^k \ (mod\ n)$, *para qualquer inteiro positivo k.*

Pode-se então multiplicar ambos os membros de uma congruência por um inteiro ou pode-se elevar ambos os membros a uma potência positiva, preservando a congruência. Entretanto, não é sempre possível dividir ambos os membros preservando a congruência.

É possível mostrar que a congruência linear

$$xa \equiv 1 \ (\text{mod}\ n), \tag{2}$$

apresenta solução única para x módulo n, dados a e n, se $\text{MDC}(a, n) = 1$, isto é, se a e n são relativamente primos [1]. Essa solução para x é denotada por a^{-1} modulo n e pode ser obtida computacionalmente por meio do algoritmo de Euclides estendido [2, 5].

A partir do Teorema 2.2, é possível demonstrar o seguinte teorema.

Teorema 2.3. *Seja*

$$p(x) = d_0 + d_1 x + \ldots + d_\ell x^\ell \tag{3}$$

um polinômio com coeficientes d_0, d_1, ..., d_ℓ, todos inteiros; se $a \equiv b \ (mod\ n)$, então $p(a) \equiv p(b) \ (mod\ n)$.

Uma demonstração detalhada é apresentada em [1]. Esse teorema, em conjunto com a representação decimal, é utilizado para demonstrar os testes de divisibilidade mais populares.

A representação decimal pode ser vista como um vetor de dígitos decimais que representa um número inteiro. Seja $(d_\ell, d_{\ell-1}, \ldots, d_1, d_0)$ a representação decimal de um número d, isto é,

$$d = d_0 + d_1 10 + d_2 10^2 + \ldots + d_\ell 10^\ell,$$

em que $0 \leq d_i < 10$. Pode-se definir o polinômio $D(x)$ cujos coeficientes são os dígitos d_i, $i = 0, 1, 2, \ldots, \ell$, isto é,

$$D(x) = d_0 + d_1 x + d_2 x^2 + \ldots + d_\ell x^\ell. \tag{4}$$

Então, $d = D(10)$. Suponha que deseja-se testar se o número d é divisível por um número inteiro positivo n. Deseja-se então saber se $d \equiv 0 \ (\text{mod}\ n)$, o que ocorre se, e somente se, $D(10) \equiv 0 \ (\text{mod}\ n)$. Essa é a premissa para os testes de divisibilidade por 3, 9 e 11, apresentados nos teoremas a seguir.

DOI: 10.5540/03.2022.009.01.0243

Teorema 2.4 (Teste de divisibilidade por 3)**.** *Seja* $(d_\ell, d_{\ell-1}, \ldots, d_1, d_0)$ *a representação decimal de um número inteiro* d*,* $0 \leq d_i < 10$*. Então*

$$3|d \Leftrightarrow 3|\sum_{i=0}^{\ell} d_i.$$

Demonstração. Definindo $D(x) = d_0 + d_1 x + d_2 x^2 + \ldots + d_\ell x^\ell$, então $d = D(10)$. Mas $10 \equiv 1 \pmod 3$, então

$$d \equiv D(1) \equiv \sum_{i=0}^{\ell} d_i \pmod 3,$$

e

$$d \equiv 0 \pmod 3 \Leftrightarrow \sum_{i=0}^{\ell} d_i \equiv 0 \pmod 3, \tag{5}$$

e, pelo item 1 do Teorema 2.2, a demonstração está completa. □

Teorema 2.5 (Teste de divisibilidade por 9)**.** *Seja* $(d_\ell, d_{\ell-1}, \ldots, d_1, d_0)$ *a representação decimal de um número inteiro* d*,* $0 \leq d_i < 10$*. Então*

$$9|d \Leftrightarrow 9|\sum_{i=0}^{\ell} d_i.$$

A demonstração segue a mesma argumentação do Teorema 2.4 pois $10 \equiv 1 \pmod 9$.

Teorema 2.6 (Teste de divisibilidade por 11)**.** *Seja* $(d_\ell, d_{\ell-1}, \ldots, d_1, d_0)$ *a representação decimal de um número inteiro* d*,* $0 \leq d_i < 10$*. Então*

$$11|d \Leftrightarrow 11|\sum_{i=0}^{\ell} (-1)^i d_i.$$

Demonstração. Definindo $D(x) = d_0 + d_1 x + d_2 x^2 + \ldots + d_\ell x^\ell$, então $d = D(10)$. Mas $10 \equiv -1 \pmod{11}$, então

$$d \equiv D(-1) \equiv \sum_{i=0}^{\ell} (-1)^i d_i \pmod{11},$$

e a prova segue. □

Esse último teste é basicamente uma soma alternada dos dígitos decimais. Esses testes simples vêm diretamente da aplicação da teoria de congruências na representação decimal dos números inteiros. Técnicas mais sofisticadas, baseadas no teste da divisão por 7 e 13 [3], são apresentadas na próxima seção.

DOI: 10.5540/03.2022.009.01.0243

3 Teste de divisibilidade por separação de dígito decimal

Seja d um inteiro com representação decimal $(d_\ell, d_{\ell-1}, \ldots, d_1, d_0)$. Pode-se aplicar o Teorema 2.1, dividindo esse número por uma potência de 10, para separar os dígitos menos significativos dos demais. Assim

$$d = q10^i + r, \tag{6}$$

em que q é um número inteiro com representação decimal dada por $(d_\ell, d_{\ell-1}, \ldots, d_i)$ e r possui representação decimal $(d_{i-1}, d_{i-2}, \ldots, d_1, d_0)$. Seja um número n, tal que $\text{MDC}(n, 10) = 1$. Então existe z, inverso módulo n para 10^i, isto é, $z \equiv 10^{-i}$ módulo n. Aplicando a congruência por n em (6) e multiplicando ambos os membros por z, tem-se

$$dz \equiv q + rz \pmod{n}. \tag{7}$$

Note que, como $z \neq 0 \pmod{n}$, então

$$d \equiv 0 \pmod{n} \Leftrightarrow q + rz \equiv 0 \pmod{n}.$$

Essa é a técnica utilizada nos testes de divisão por 7 e 13, apresentados a seguir.

Teorema 3.1 (Teste de divisibilidade por 7)**.** *Seja $(d_\ell, d_{\ell-1}, \ldots, d_1, d_0)$ a representação decimal de um número inteiro d, $0 \leq d_i < 10$, com $d = q10 + d_0$. Então*

$$7|d \Leftrightarrow 7|(q - 2d_0).$$

Demonstração. É suficiente verificar que $-2 \equiv 10^{-1} \pmod{7}$ e utilizar (7). Então

$$d(-2) \equiv q - 2d_0 \pmod{7},$$

e, claramente,

$$d \equiv 0 \pmod{7} \Leftrightarrow q - 2d_0 \equiv 0 \pmod{7},$$

e o teorema está demonstrado. □

Note ainda que é possível utilizar $z = 5, 12$ ou qualquer outro número congruente a -2 módulo 7, como no caso do teste elaborado por Chika Ofili, em que foi utilizado $z = 5$ [4]. Um ponto importante é que essa técnica pode ser utilizada recursivamente, isto é, aplica-se a mesma regra a $q - 2d_0$ para saber se o número d é divisível por 7 [3].

Teorema 3.2 (Teste de divisibilidade por 13)**.** *Seja $(d_\ell, d_{\ell-1}, \ldots, d_1, d_0)$ a representação decimal de um número inteiro d, $0 \leq d_i < 10$, com $d = q10 + d_0$. Então*

$$13|d \Leftrightarrow 13|(q + 4d_0).$$

Demonstração. É suficiente verificar que $4 \equiv 10^{-1} \pmod{13}$ e, utilizando (7), a prova segue como no Teorema 3.1. □

Teorema 3.3 (Teste de divisibilidade por 17)**.** *Seja $(d_\ell, d_{\ell-1}, \ldots, d_1, d_0)$ a representação decimal de um número inteiro d, $0 \leq d_i < 10$, com $d = q10 + d_0$. Então*

$$17|d \Leftrightarrow 17|(q - 5d_0).$$

Demonstração. Verifica-se que $-5 \equiv 10^{-1} \pmod{17}$ e, utilizando (7), a prova segue como no Teorema 3.1. □

DOI: 10.5540/03.2022.009.01.0243

Teorema 3.4 (Teste de divisibilidade por 19)**.** *Seja* $(d_\ell, d_{\ell-1}, \ldots, d_1, d_0)$ *a representação decimal de um número inteiro* d*,* $0 \leq d_i < 10$*, com* $d = q10 + d_0$*. Então*

$$19|d \Leftrightarrow 19|(q + 2d_0).$$

Demonstração. Verifica-se que $2 \equiv 10^{-1} \pmod{19}$ e, utilizando (7), a prova segue como no Teorema 3.1. □

Nota-se que a Equação (7) pode ser utilizada para construir testes de divisibilidade para qualquer número n relativamente primo com 10. A seguir, um exemplo de teste de divisibilidade por 7 para números maiores do que mil, que são chamados de "grandes", no teorema a seguir.

Teorema 3.5 (Teste de divisibilidade por 7 para números "grandes")**.** *Seja* $(d_\ell, d_{\ell-1}, \ldots, d_1, d_0)$ *a representação decimal de um número inteiro* d*,* $0 \leq d_i < 10$*, com* $d = q10^3 + r$*. Então*

$$21|d \Leftrightarrow 21|(q - r).$$

Demonstração. Verifica-se que $-1 \equiv 10^{-3} \pmod{7}$ e, utilizando (7),

$$d(-1) \equiv q - r \pmod{7}$$

e, portanto,

$$d \equiv 0 \pmod{7} \Leftrightarrow q - r \equiv 0 \pmod{7}.$$

□

Combinando os Teoremas 3.5 e 3.1, é possível verificar se um número "grande" é divisível por 7 em poucos passos.

Como exemplo, seja $d = 36876105$ e deseja-se descobrir se $7|d$. Pode-se utilizar o Teorema 3.5, assim, $7|d$ se $7|(36876-105)$ ou $7|36771$, que ocorre se $7|(36-771)$ ou $7|(-735)$ ou equivalentemente $7|735$. Como o número em teste agora é menor que 1000, utiliza-se o Teorema 3.1, assim, $7|735$ se $7|(73 - 2 \times 5)$ ou $7|63$, que ocorre se $7|(6 - 2 \times 3)$ ou $7|0$ (o qual é verdade) e, portanto, $7|d$.

A eficiência desses testes para a representação decimal está no fato de que a divisão por 10, em (6), consiste simplesmente em separar os i-ésimos dígitos menos significativo dos demais. Essa separação não seria tão simples em um computador que trabalha com uma base binária. Entretanto, modificando a base na Equação (7), é possível construir testes de divisibilidade para máquinas digitais.

4 Teste de divisibilidade para uma base B

Seja d um inteiro com representação na base B dada por $(d_\ell, d_{\ell-1}, \ldots, d_1, d_0)_B$. Assim,

$$d = d_0 + d_1 B + d_2 B^2 + \ldots + d_\ell B^\ell,$$

em que $0 \leq d_i < B$, para $i = 0, 1, \ldots, \ell$. Se a base B é uma potência de dois, então essa representação pode ser vista como um agrupamento de bits na representação binária. Por exemplo, o número $d = 1995$ é representado na base binária por $(11111001011)_2$ ou, equivalentemente, na representação base 4, por $(133023)_4 = ((01)_2(11)_2(11)_2(00)_2(10)_2(11)_2)_4$, que é um arranjo em dois bits, ou ainda $(7cb)_{16} = ((0111)_2(1100)_2(1011)_2)$ na representação hexadecimal, que é um arranjo em 4 bits.

DOI: 10.5540/03.2022.009.01.0243

A representação por meio de concatenação de dígitos vale para qualquer representação na base B [2]. Pode-se aplicar o Teorema 2.1, dividindo esse número por B^i, para separar os i-ésimos dígitos menos significativos dos demais. Assim

$$d = qB^i + r, \tag{8}$$

em que q possui representação na base B dada por $(d_\ell, d_{\ell-1}, \ldots, d_i)_B$ e r a representação $(d_{i-1}, d_{i-2}, \ldots, d_0)_B$. Seja um número n, tal que $\text{MDC}(n, B) = 1$. Então, existe z inverso módulo n para B^i, isto é, $z \equiv B^{-i} \pmod{n}$. Aplicando a congruência por n em (8) e multiplicando ambos os membros por z, tem-se

$$dz \equiv q + rz \pmod{n}. \tag{9}$$

Da mesma forma que anteriormente,

$$d \equiv 0 \pmod{n} \Leftrightarrow q + rz \equiv 0 \pmod{n}.$$

Considerando o teste de divisibilidade de um número d por um número ímpar n, se B é uma potência de 2, então $\text{MDC}(n, B) = 1$ e, logo, existe um inteiro k tal que $B^k \equiv 1 \pmod{n}$, sendo o menor inteiro positivo k, que satisfaz à congruência, a ordem de B módulo n [1]. Com isso, é sempre possível escolher uma potência de dois adequada para construir testes de divisibilidade em máquinas digitais e a mesma ideia pode ser reproduzida em qualquer base.

A seguir, alguns testes de divisibilidade, considerando a representação binária, são apresentados.

Teorema 4.1 (Teste de divisibilidade por 3 na base 4)**.** *Seja $(d_\ell, d_{\ell-1}, \ldots, d_1, d_0)_4$ a representação base 4 de um número inteiro d, $0 \leq d_i < 4$. Então*

$$3|d \Leftrightarrow 3|\sum_{i=0}^{\ell} d_i.$$

Demonstração. Definindo $D(x) = d_0 + d_1 x + d_2 x^2 + \ldots + d_\ell x^\ell$, então $d = D(4)$. Mas $4 \equiv 1 \pmod{3}$, então

$$d \equiv D(1) \equiv \sum_{i=0}^{\ell} d_i \pmod{3},$$

e

$$d \equiv 0 \pmod{3} \Leftrightarrow \sum_{i=0}^{\ell} d_i \equiv 0 \pmod{3}, \tag{10}$$

e, pelo item 1 do Teorema 2.2, a demonstração está completa. □

Por exemplo, se $d = 1995 = (133023)_4$, então $3|d$ se $3|(1 + 3 + 3 + 2 + 3)$ ou $3|12$, mas $12 = (30)_4$, então $3|12$ se $3|(3 + 0)$ ou $3|3$. Com isso, $3|d$.

Utilizando o mesmo princípio, pode-se construir testes de divisibilidade para vários números primos, como mostrado nos teoremas a seguir.

Teorema 4.2 (Teste de divisibilidade por 5 na base 4)**.** *Seja $(d_\ell, d_{\ell-1}, \ldots, d_1, d_0)_4$ a representação base 4 de um número inteiro d, $0 \leq d_i < 4$. Então*

$$5|d \Leftrightarrow 5|\sum_{i=0}^{\ell} (-1)^i d_i.$$

Teorema 4.3 (Teste de divisibilidade por 7 na base 8)**.** *Seja* $(d_\ell, d_{\ell-1}, \ldots, d_1, d_0)_8$ *a representação base 8 de um número inteiro* d*,* $0 \leq d_i < 8$*. Então*

$$7|d \Leftrightarrow 7|\sum_{i=0}^{\ell} d_i.$$

Além do teste do Teorema 4.2, existe uma outra alternativa para construir um teste, baseado em (9), como mostrado a seguir.

Teorema 4.4 (Teste alternativo de divisibilidade por 5 na base 4)**.** *Seja* $(d_\ell, d_{\ell-1}, \ldots, d_1, d_0)_4$ *a representação na base 4 de um número inteiro* d*,* $0 \leq d_i < 4$*, com* $d = q4 + d_0$*. Então*

$$5|d \Leftrightarrow 5|(q - d_0).$$

Demonstração. Verifica-se que $-1 \equiv 4 (\text{mod } 5)$ e, utilizando (9),

$$-1d \equiv q - d_0 \text{ (mod 5)},$$

e

$$d \equiv 0 \text{ (mod 5)} \Leftrightarrow q - d_0 \equiv 0 \text{ (mod 5)}.$$

□

Como exemplo, para testar se $d = 1995 = (11111001011)_2$ pode ser dividido por 5, então $5|d$ se $5|(111110010 - 11)_2$ ou $5|(111101111)_2$, que ocorre se $5|(1111011 - 11)_2$ ou $5|(1111000)_2$, que ocorre se $5|(11110 - 00)_2$ ou $5|(11110)_2$, que ocorre se $5|(111 - 10)_2$ ou $5|(101)_2$, que ocorre se $5|(1 - 01)_2$ ou $5|(0)_2$, o que implica que $5|d$.

5 Considerações Finais

Este artigo apresentou as principais ideias envolvidas em testes de divisibilidade, as quais podem ser utilizadas para criar testes de divisibilidade para qualquer número, representado em qualquer base numérica. Demonstrações e exemplos dos testes de divisibilidade por 3, 5, 7, 11, 13, 17 e 19 para a base decimal, bem como testes de divisibilidade por 3, 5 e 7 em bases binárias foram apresentados. Esses testes podem ser utilizados na criação de algoritmos eficientes na busca por chaves criptográficas (RSA por exemplo [5]) e na geração de sequências pseudo-aleatórias [2].

Referências

[1] D. M. Burton. **Teoria Elementar dos Números**. 7a ed. LTC, 2016.

[2] D. E. Knuth. **The Art of Computer Programming: Volume 2: Seminumerical Algorithms**. 3ª ed. Vol. 2. Addison-Wesley, 1997.

[3] F. J. Mueller. "Divisibility by Seven and Thirteen". Em: **The Arithmetic Teacher** 5.5 (1958), pp. 267–268. ISSN: 0004136X. URL: http://www.jstor.org/stable/41184089.

[4] L. Pestana e R. Fonseca (matéria do "Correio Braziliense"). **Menino de 12 anos descobre fórmula matemática que ajuda o estudo da divisão**. Online. Postado em 19/11/2019. URL: https://www.correiobraziliense.com.br/app/noticia/mundo/2019/11/19/interna_mundo,807535/menino-de-12-anos-descobre-formula-matematica-que-ajuda-o-estudo-da-di.shtml. (acessado em 18/06/2022).

[5] R. Terada. **Segurança de Dados: Criptografia em Rede de Computador**. 2a. ed. Blucher, 2008. ISBN: 9788521204398.

