UNIVERSIDADE FEDERAL DA GRANDE DOURADOS

Critérios de Divisibilidade

Autor:
Huilton José Domingues Neto

Orientador:
Me. Rafael Afonso Barbosa

Dourados - MS
2016

UNIVERSIDADE FEDERAL DA GRANDE DOURADOS
MATEMÁTICA

CRITÉRIOS DE DIVISIBILIDADE

Monografia apresentada por Huilton José Domingues Neto à Faculdade de Ciências Exatas e Tecnologias da Universidade Federal da Grande Dourados, para conclusão do curso de graduação em Licenciatura Plena em Matemática.

HUILTON JOSÉ DOMINGUES NETO

Dourados, MS
2016

Dados Internacionais de Catalogação na Publicação (CIP).

D671c Domingues Neto, Huilton Jose

Critérios de Divisibilidade / Huilton Jose Domingues Neto -- Dourados: UFGD, 2016.

63f. : il. ; 30 cm.

Orientador: Rafael Afonso Barbosa

TCC (Graduação em Matemática) - Faculdade de Ciências Exatas e Tecnologia, Universidade Federal da Grande Dourados.

Inclui bibliografia

1. Critérios de Divisibilidade. 2. Dibisibilidade. 3. Congruência. I. Título.

Ficha catalográfica elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).

Monografia defendida em 14/10/2016 e aprovada pela Banca Examinadora:

Prof^{o} Dr. Rogério de Oliveira

Prof^{a} Dra. Ana Cláudia Mendonça

Prof. Me. Rafael Afonso Barbosa

Agradecimentos

Quero, antes de tudo, agradecer ao Profº Me. Rafael Afonso Barbosa, por aceitar me orientar neste trabalho e ter feito com excelência.

Agradecer também à Profª Dra. Ana Cláudia Mendonça e o Profº Dr. Rogério de Oliveira, por aceitarem compor a banca examinadora.

Aos meus pais, por me apoiarem desde a escolha do curso até hoje.

Aos colegas e professores da graduação, que nestes anos todos contribuiram para minha formação.

À Jackeline, minha namorada, por todo carinho e apoio.

À profª Drª Selma Helena Marchiori Hashimoto, por ser está pessoa incrível e contribuir diretamente na minha formação, não só curricular, mas também na formação pessoal.

Por fim, mas não menos importante, agradecer aos amigos Rafael e Letícia, por ajudar na tradução do Resumo.

Resumo

Sabemos que os critérios de divisibilidade são ensinados nas séries iniciais do Ensino Fundamental, sendo eles muito importantes para a resoluções de problemas e exercícios destas séries. Neste trabalho vamos demonstrar alguns critérios de divisibilidade usando as definições e propriedades da teoria de divisibilidade e congruência apresentada no livro Aritmética de HEFEZ, A. Com essa bagagem de conteúdo que o trabalho está abordando, deixamos como proposta o uso deste material como ferramenta de estudo de Aritmética.

Palavras-chave: Critérios de divisibilidade; Congruência; Divisibilidade; Demonstrações.

Abstract

We know that the divisibility criteria are taught in the early grades of elementary school, being very important for the resolution of problems and exercises of these series. In this study we demonstrate some divisibility ideas, using divisibility settings and congruence and thus. With the an insights that the study is addressing, we leave, a proposal, the use of this material as Arithmetic study tool.

Keywords: Divisibility Criteria; Congruence; Divisibility; Demonstration.

Sumário

Capítulo 1

INTRODUÇÃO

Segundo os historiadores, foi Tales de Mileto (640-546 a.C) quem introduziu o estudo da Matemática na Grécia. Tales teria trazido para a Grécia os rudimentos da geometria e da aritmética que aprendera com os sacerdotes egípcios, iniciando a intensa atividade matemática que ali se desenvolveu por mais de 5 séculos. A diferença entre a matemática dos egípcios e a dos gregos era que, para os primeiros, tratava-se de uma arte que os auxiliava em seus trabalhos de engenharia e de agrimensura, enquanto que, com os segundos, assumia um caráter científico, dada a atitude filosófica e especulativa que os gregos tinham face à vida. Em seguida, foram Pitágoras de Samos (580?-500? a.C) e sua escola (que durou vários séculos) que se encarregaram de ulteriormente desenvolver e difundir a Matemática pela Grécia e suas colônias. A escola pitagórica atribuía aos números um poder místico, adotando a aritmética como fundamento de seu sistema filosófico. Quase nada sobrou dos escritos originais dessa fase da matemática grega, chegando até nós apenas referências e comentários feitos por outros matemáticos posteriores. Os gregos tinham uma forte inclinação para a filosofia e a lógica, tendo isto influenciado fortemente toda a sua cultura e, em particular, o seu modo de fazer matemática. Um importante exemplo disso foi a grande influência que sobre ela exerceu Platão (429-348 a.C), que, apesar de não ser matemático, nela via um indispensável treinamento para o filósofo, ressaltando a metodologia axiomático-dedutiva a ser seguida em todos os campos do conhecimento. O domínio da geometria era uma condição necessária aos aspirantes

para o ingresso na sua academia. A preferência de Platão pelos aspectos mais teóricos e conceituais o fazia estabelecer uma clara diferenciação entre a ciência dos números, que chamava aritmética, e a arte de calcular, que chamava logística, a qual desprezava por ser "infantil e vulgar". Com toda esta herança cultural, surge por volta de 300 a.C, em Alexandria, um tratado que se tornaria um dos marcos mais importantes da Matemática, Os Elementos de Euclides. Pouco se sabe sobre os dados biográficos deste grande matemático, tendo chegado a nós, através de sucessivas edições, este tratado composto por treze livros, onde se encontra sistematizada a maior parte do conhecimento matemático da época. Aparentemente, Euclides não criou muitos resultados, mas teve o mérito de estabelecer um padrão de apresentação e de rigor na Matemática jamais alcançado anteriormente, tido como o exemplo a ser seguido nos milênios que se sucederam. Dos treze livros de Os Elementos, dez versam sobre geometria e três, sobre aritmética. Nos três livros de aritmética, Livros VII, $VIII$ e IX, Euclides desenvolve a teoria dos números naturais, sempre com uma visão geométrica (para ele, números representam segmentos e números ao quadrado representam áreas). No Livro VII, são definidos os conceitos de divisibilidade, de número primo, de números perfeitos, de máximo divisor comum e de mínimo múltiplo comum, entre outros. No mesmo livro, além das definições acima, todas bem postas e até hoje utilizadas, encontra-se enunciada (sem demonstração) a divisão com resto de um número natural por outro, chamada divisão euclidiana. Com o uso iterado desta divisão, Euclides estabelece o algoritmo mais eficiente, até hoje conhecido, para o cálculo do máximo divisor comum de dois inteiros chamado de Algoritmo de Euclides, que apresentaremos neste trabalho. Após Euclides, a aritmética estagnou por cerca de 500 anos, ressuscitando com os trabalhos de Diofanto de Alexandria, que viveu por volta de 250 DC. A obra que Diofanto nos legou chama-se Aritmética e foi escrita em treze volumes, dos quais apenas sete nos chegaram. Trata-se do primeiro tratado de álgebra hoje conhecido, pois a abordagem de Diofanto era totalmente algébrica, não sendo revestida de nenhuma linguagem ou interpretação geométrica, como o faziam todos os seus predecessores. A maioria dos problemas estudados por Diofanto em Aritmética visava encontrar soluções em números racionais, muitas vezes contentando-se em encon-

trar apenas uma solução, de equações algébricas com uma ou várias incógnitas. Um dos problemas tratados por Diofanto era a resolução em números racionais, ou inteiros, da equação pitagórica $x^2 + y^2 = z^2$, chegando a descrever todas as suas soluções. Este problema teve o poder de inspirar o matemático francês Pierre Fermat mais de 1300 anos depois, traçando os rumos futuros que a Matemática iria tomar.

Já a aritmética modular (chamada também de aritmética do relógio), na matemática, é um sistema de aritmética para números inteiros, onde os números "voltam pra trás"quando atingem um certo valor, o *módulo.*

O matemático suiço Euler foi o pioneiro na abordagem de congruência por volta de 1750, quando ele explicitamente introduziu a ideia de congruência módulo um número natural ($\mathbb{N}$).

A aritmética modular foi desenvolvida posteriormente por *Carl Friedrich Gauss* em seu livro *Disquisitiones Arithmeticae*, publicado em 1801.

Capítulo 2

DIVISIBILIDADE

Definição 2.1 *Dados dois números inteiros a e b, dizemos que a divide b, quando existir um $q \in \mathbb{Z}$ tal que $b = aq$. Neste caso diremos também que a é um divisor de b, ou ainda, que b é divisível por a.*

Notação: $a \mid b$, lê-se a divide b.

Observe que a notação não representa nenhuma operação em $\mathbb{Z}$, nem representa uma fração. Trata-se de uma sentença que diz ser verdade que b e múltiplo de a. A negação desta sentença é representada por $a \nmid b$.

Proposição 1 *Sejam $a, b \in \mathbb{Z}$*

(i) $1 \mid a$, $a \mid a$ *e* $a \mid 0$.

(ii) $0 \mid a \Leftrightarrow a = 0$.

(iii) $a \mid b \Leftrightarrow |a| \mid |b|$.

(iv) Se $a \mid b$ *e* $b \mid c$ *então* $a \mid c$.

Demonstração.

(i) Isto decorre das igualdades $a = 1a$, $a = a \cdot 1$ e $0 = a \cdot 0$.

(ii) Suponhamos que $0 \mid a$, logo existe um $b \in \mathbb{Z}$ onde $a = 0b \Rightarrow a = 0$. reciprocamente, basta observar que $0 \mid 0$, que foi provado no item anterior.

(iii) Suponhamos que $a \mid b$ então $\exists\ c \in \mathbb{Z}$ tal que $b = ac \Rightarrow |b| = |ac| \Rightarrow |b| = |a||c|$. Logo$|a| \mid |b|$. reciprocamente, temos que se $|a| \mid |b|$ existe $c \in \mathbb{Z}$ tal que $|b| = |a|c \Rightarrow |b| = |ac| \Rightarrow b = ac$ ou $b = -ac$, de qualquer forma $a \mid b$.

(iv) Se $a \mid b$, então $\exists\ q \in \mathbb{Z}$ tal que $b = aq$, e se $b \mid c$ então $\exists\ p \in \mathbb{Z}$ tal que $c = bp$. Assim, temos que $c = aqp \Rightarrow c = at$, com $t = qp$. Portanto $a \mid c$.

■

Do item (i) e (iii) temos que qualquer número inteiro é divisivel por ± 1, por ele mesmo, e seu oposto. Note que $0 \mid 0$, portanto, todo número inteiro divide zero. Sendo assim, zero tem infinitos divisores. Suponha que $a \mid b$ e seja um $q \in \mathbb{Z}$ tal que $b = aq$, com a e $b \in \mathbb{Z}$ e $a \neq 0$. O número inteiro q é chamado de *quociente* de b por a e denotado por $q = b/a$. Observe que b/a só está definido quando $a \neq 0$ e $a \mid b$.

Proposição 2 *Sejam a,b,c e* $d \in \mathbb{Z}$. *Se* $a \mid b$ *e* $c \mid d$ *então* $ac \mid bd$.

Demonstração. De fato, se $a \mid b$ e $c \mid d$, então existem q e $p \in \mathbb{Z}$ tal que $b = aq$ e $d = cp$. Logo, temos então $bd = (aq)(cp) = ac \cdot qp = ac \cdot t$ com $t = qp$. Portanto, $ac \mid bd$. ■

Em particular, se $a \mid b$, então $ac \mid bc$, para todo $c \in \mathbb{Z}$. A demonstração é analoga a proposição acima.

Proposição 3 *Sejam a,b e* $c \in \mathbb{Z}$, *tais que* $a \mid (b \pm c)$. *Então,* $a \mid b \Leftrightarrow a \mid c$.

Demonstração. Suponhamos que $a \mid (b \pm c)$, então $b \pm c = aq$ (I), com $q \in \mathbb{Z}$. Agora, se $a \mid b$, então $b = ap$ (II),com $p \in \mathbb{Z}$. Substituindo (II) na (I), temos:

$$ap \pm c = aq$$

$$\Rightarrow c = a(q \pm p)$$

$\Rightarrow c = at$ com $q \pm p = t$. Então $a \mid c$. A prova da volta da implicação é analoga. ■

Proposição 4 *Se a, b e $c \in \mathbb{Z}$ tais que $a \mid b$ e $a \mid c$, então para todo x e $y \in \mathbb{Z}$ $a \mid (bx + cy)$.*

Demonstração. Como $a \mid b$ e $a \mid c$, então $\exists$ p e $q \in \mathbb{Z}$ onde $b = ap$ e $c = aq$. $bx + cy = ap \cdot x + aq \cdot y = a \cdot (px + qy) = at$ com $t = px + qy$. Portanto $a \mid (bx + cy)$ ■

Proposição 5 *Dados a,$b \in \mathbb{Z}$, onde $b \neq 0$, temos que $a \mid b \Rightarrow |a| \leqslant |b|$.*

Demonstração. Suponha que $a \mid b$, então $\exists$ um $q \in \mathbb{Z}$ onde $b = aq$ com $q \neq 0$ pois $b \neq 0$. Aplicando modulo, temos que $|b| = |a||q|$, então $1 \leqslant |q| \Rightarrow |a| \leqslant |a| \cdot |q|$ e como $|a||q| = |b|$. Portanto $|a| \leqslant |b|$. ■

Proposição 6 *Sejam a e $b \in \mathbb{Z}$, temos que $a - b \mid a^n - b^n$ para todo $n \in \mathbb{N}$.*

Demonstração. Para mostrar isso usaremos indução. Como $a - b \mid 0$, então para $n = 0$ a afirmação é verdadeira. Suponhamos então, que valha para n. Como $a - b \mid a^n - b^n$ então $a^n - b^n = (a - b) \cdot q$ com $q \in \mathbb{Z}$.

$$a^n - b^n = (a - b)q$$

$$\Rightarrow a^n = (a - b)q + b^n.$$

Mostraremos que vale para $n + 1$. E como $a^{n+1} - b^{n+1} = a^n \cdot a - b^{n+1}$. Substituindo o valor de a^n, teremos então

$$a^{n+1} - b^{n+1} = [(a - b)q + b^n]a - b^{n+1}$$

$$\Rightarrow a^{n+1} - b^{n+1} = (a - b)a \cdot q + ab^n - b^{n+1}$$

$$\Rightarrow a^{n+1} - b^{n+1} = (a - b)a \cdot q + (a - b)b^n$$

$$\Rightarrow a^{n+1} - b^{n+1} = (a - b) \cdot (aq + b^n) = (a - b)t$$

com $t = (aq + b^n)$. Logo $a - b \mid a^{n+1} - b^{n+1}$. Portanto $a - b \mid a^n - b^n$ para todo $n \in \mathbb{N}$. ■

Proposição 7 *Sejam a e $b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Temos que $a+b \mid a^{2n+1}+b^{2n+1}$.*

Demonstração. Demonstraremos por indução em n, também. Para $n = 0$ é, obviamente, uma afirmação verdadeira, pois $a^{2n+1} + b^{2n+1} = a^{2\cdot 0+1} + b^{2\cdot 0+1} = a + b$ e $a + b \mid a + b$. Suponhamos que valha para n. Então $a^{2n+1} + b^{2n+1} = (a + b)q$ com $q \in \mathbb{Z}$. Daí, tem-se $a^{2n+1}+b^{2n+1} = (a+b)q \Rightarrow a^{2n+1} = (a+b)q-b^{2n+1}$, chamamos de (I). Agora mostraremos que vale para $n+1$. Como temos que $a^{2(n+1)+1}+b^{2(n+1)+1} = a^{2n+3}+b^{2n+3} = a^{2n+1}a^2+b^{2n+3}$, chamamos de (II). Substituindo (I) na (II), temos então: $a^{2(n+1)+1} + b^{2(n+1)+1} = [(a + b)q - b^{2n+1}]a^2 + b^{2n+3} = (a + b)a^2q - a^2b^{2n+1} + b^{2n+3} = (a + b)a^2q - b^{2n+1}(a^2 - b^2)$ e como $(a^2-b^2) = (a-b)(a+b)$, segue que $a^{2(n+1)+1}+b^{2(n+1)+1} = (a+b)a^2q-b^{2n+1}[(a-b)(a+b)]$. Colocando $(a + b)$ em evidencia, teremos:

$$a^{2(n+1)+1} + b^{2(n+1)+1} = (a + b)[(qa^2) - b^{2n+1}(a - b)].$$

Portanto $a + b \mid a^{2n+1} + b^{2n+1}$ para todo $n \in \mathbb{N}$. ■

Proposição 8 *Sejam a e $b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Temos que $a - b \mid a^{2n} - b^{2n}$.*

Demonstração. Novamente iremos usar indução no n. Veja como a afirmação é válida para $n = 0$, pois $a^{2\cdot n} - b^{2n} = a^0 - b^0 = 1 - 1 = 0$ e pelo item (i) da Proposição 1, temos que qualquer número divide zero. Suponhamos que valha para n, então temos que $a^{2n} - b^{2n} = (a + b)q$ com $q \in \mathbb{Z}$

$$a^{2n} - b^{2\cdot n} = (a + b)q$$

$$a^{2n} = (a + b)q + b^{2n}$$

Iremos mostrar que vale para $n + 1$, isto é,

$$a + b \mid a^{2n+2} - b^{2n+2}.$$

Sabemos que $a^{2n+2}-b^{2n+2} = a^{2n}a^2-b^{2n+2}$. Substituindo os valores, teremos então $a^{2n+2}-b^{2n+2} = [(a+b)q+b^{2n}]a^2-b^{2n+2} = (a+b)a^2q+a^2b^{2n}-b^{2n+2} = (a+b)a^2q+b^{2n}(a^2-b^2)$ e como $(a^2-b^2) = (a+b)(a-b) \Rightarrow a^{2n+2}-b^{2n+2} = (a+b)a^2q+b^{2n}(a+b)(a-b) = (a+b)t+(a+b)p$, com $t = a^2q$ e $p = b^{2n}(a - b)$. Segue da proposição 4, que $a + b \mid a^{2n+2} - b^{2n+2}$. Portanto $a + b \mid a^{2n} - b^{2n}$ para todo $n \in \mathbb{N}$. ■

2.1 Exemplos

Exemplo 2.1 *Mostre que* $13 \mid 2^{70} + 3^{70}$.

Perceba que podemos escrever $13 = 4 + 9 = 2^2 + 3^2$. E podemos escrever também $2^{70}+3^{70} = (2^2)^{35}+(3^2)^{35}$, sendo assim, pela proposição 7, temos que $2^2+3^2 \mid (2^2)^{35}+(3^2)^{35}$.

Exemplo 2.2 *Sabe-se que* $9 \mid 36$ *e ainda* $9 \mid 45$*, mostre que* $9 \mid 1872$.

Podemos escrever $1872 = 17 \cdot 36 + 28 \cdot 45$ e pela proposição 4, temos que $9 \mid 1872$.

Capítulo 3

DIVISÃO EUCLIDIANA

Mesmo quando um número inteiro $a \neq 0$ não divide um $b \in \mathbb{Z}$, Euclides, no seu livro Elementos, sem um enunciado especifíco, traz o fato de que é sempre possível fazer a divisão de b por a, com resto. Esse resultado, cuja a demonstração faremos abaixo, não é só importante na obra de Euclides, como também é um resultado central da teoria.

Proposição 9 *Dado um inteiro b qualquer e um inteiro estritamente positivo a, podem-se determinar dois inteiros*

$$q \text{ e } r, \text{ tais que } b = a \cdot q + r, \text{ com } 0 \leqslant r < a.$$

Demonstração. Como $b > 0$, existe um q satisfazendo:

$$bq \leq a < b(q+1).$$

O que implica $0 \leq a - bq < b$. Desta forma escrevemos $r = a - bq$, temos garantido a existência de q e r. Se $r = 0$ temos que b é múltiplo de a, por definição de divisibilidade. Afim de mostrar a unicidade vamos supor, que pudesse determinar um outro par de inteiros q_1 e r_1, tais que $b = aq_1 + r_1$, com $0 \leq r_1 < a$. Então, $aq + r = aq_1 + r_1$ e, portanto, $a(q - q_1) = r - r_1$, chamamos de (I). Suponhamos que $r_1 > r$. Daí, o segundo membro de (I) seria estritamente negativo, e como $a > 0$, então $q - q_1 < 0$ e, portanto, $q_1 - q \geq 1$. Mas de (I), segue que:

$r = r_1 + a(q_1 - q)$, chamamos de (II).

Levando-se em conta que $a > 0$, $r_1 \geq 0$ e $q_1 - q \geq 1$, de (II) seguiria que $r \geq a$, o que contraria a hipótese. Da mesma forma, prova-se que a desigualdade $r > r_1$ também é impossível. De onde $r_1 = r$ e, consequentemente, $q_1 = q$. ■

Nas condições do teorema anterior, os números q e r são chamados de quociente e resto, respectivamente, da divisão de b por a. O resto r da divisão de b por a será zero se, somente se, $a \mid b$.

Dado um número inteiro $n \in \mathbb{Z}$ qualquer, temos duas possibilidades:

i) O resto da divisão de n por 2 é 0, ou seja, $\exists$ um $q \in \mathbb{Z}$ tal que $n = 2q$; ou

ii) O resto da divisão de n por 2 é 1, ou seja, $\exists$ um $q' \in \mathbb{Z}$ tal que $n = 2q' + 1$.

Portanto, os números inteiros dividem-se em duas classes, a dos números de forma $2q$ para algum $q \in \mathbb{Z}$, chamados de *números pares*, e a dos números de forma $2q' + 1$, chamados de *números impares*. Os naturais são classificados em pares e ímpares desde Pitágoras, 500 a.C.

3.1 Exemplos

Exemplo 3.1 *Iremos mostrar que o resto da divisão de* 10^n *por* 9*, representado por* $r_9(10^n)$*, é sempre 1, qualquer que seja o* $n \in \mathbb{N}$*.*

Será feito por indução. Para $n = 0$ a afirmação é verdadeira, pois $10^0 = 1 = 9 \cdot 0 + 1$ com $q = 0$ e $r = 1$. Suponha que o resultado é válido para um $n \in \mathbb{N}$, ou seja, $10^n = 9 \cdot q + 1$.

Iremos mostrar que pra $n + 1$ a afirmação também é válida. Considere que $10^{n+1} = 10 \cdot 10^n = (9 + 1) \cdot 10^n = 9 \cdot 10^n + 10^n$. Substituindo o valor de 10^n, temos então $10^{n+1} = 9 \cdot 10^n + 9 \cdot q + 1 = 9 \cdot (10^n + q) + 1$, ou seja $10^{n+1} = 9 \cdot q' + 1$, onde $q' = (10^n + q)$ e $r = 1$. Provamos que o resultado vale para $n + 1$ e, consequentemente, vale para todo $n \in \mathbb{N}$.

Exemplo 3.2 *Vamos achar os múltiplos de 5 que se encontram entre 1 e 253.*

Pelo algoritmo da divisão euclidiana, temos que

$$253 = 5 \cdot 50 + 3$$

ou seja, o maior múltiplo de 5 que cabe em 253 é o $5 \cdot 50$, onde 50 é o quociente da divisão de 253 por 5. Portanto, os múltiplos de 5, entre 1 e 253 são

$$1 \cdot 5, 2 \cdot 5, 3, \cdot 5, ..., 49 \cdot 5, 50 \cdot 5$$

consequentemente, são 50 múltiplos de 5 diferentes entre 1 e 253.

Exemplo 3.3 *Discuta a paridade:*

(a) da soma de dois números

(b) do produto de dois números

(c) da potência de um número

(d) da soma de n números ímpares

Dados a, b números pares e c, d números ímpares, sabemos que $a = 2q$, $b = 2q'$, $c = 2p + 1$ e $d = 2p' + 1$, com $q, q', p, p' \in \mathbb{Z}$. Temos,

(a) Vejamos os casos possiveis.

(i) A soma de dois números pares quaisquer é um número par. De fato, $a + b = 2q + 2q' = 2(q + q')$.

(ii) A soma de dois números ímpares quaisquer é um número par. De fato, $c + d = 2q + 1 + 2q' + 1 = 2q + 2q' + 2 = 2(q + q' + 1)$.

(iii) A soma de um número par com um número ímpar é um número ímpar. De fato, $a + d = 2q + 2q' + 1 = 2(q + q') + 1$.

(b) São três casos possiveis, vejamos.

(i) O produto de dois números pares, sempre será par. De fato, $a \cdot b = (2q)(2q') = 4(qq') = 2 \cdot 2(qq')$.

(ii) O produto de dois números ímpares, sempre será ímpar. Veja, $cd = (2q+1)(2q'+1) = 4(qq') + 2q + 2q' + 1 = 2qq' + 2q + 2q' + 1 = 2(qq' + q + q') + 1$.

(iii) O produto de um número par com um número ímpar, sempre será par. De fato, $ad = 2q(2q'+1) = 2 \cdot [2(qq') + q]$.

(c) Os casos possiveis são:

(i) A potência de um número par que, independente da paridade do expoente, sempre será par. Isto segue do fato de que produto de números pares, é sempre par.

(ii) A potência de um número ímpar independente do expoente é sempre ímpar. Demonstração análoga a (i).

(d) Temos dois casos possiveis, estes são:

(i) Quando n for par, a soma de n números ímpares será par. A demonstração vem, a partir, da demonstração no item (a-i).

(ii) Quando n for ímpar, a soma de n números ímpares será ímpar. A demonstração surge a partir da demonstração item (a-i) e (a-iii).

Capítulo 4

SISTEMA DE NUMERAÇÃO

O sistema universalmente utilizado pelas pessoas, no seu dia-a-dia, para representar os números inteiros é o sistema decimal posicional. Esse sistema de numeração, que é uma variante do sistema sexgesimal utilizado pelos babilônios em 1700 anos a.C., foi desenvolvido na China e na índia. Existem documentos do século VI comprovando a utilização deste sistema. Posteriormente, foi se espalhando pelo Oriente Médio, por meio das caravanas, tendo encontrado grande aceitação entre os povos árabes.

Neste capítulo restringir-nos-emos à representação dos números naturais, pois 0 tem seu próprio símbolo e todo número inteiro negativo é representado com um número natural precedido pelo sinal $-$.

No sistema decimal, todo número inteiro é representado por uma sequência formada pelos algarismos

$$1, 2, 3, 4, 5, 6, 7, 8, 9,$$

acrescidos do símbolo 0 (zero), que representa a ausência de algarismo. Por serem dez algarismos, o sistema é chamado de decimal.

O sistema é também chamado posicional, pois cada algarismo, além do seu valor intrínseco, possui um peso que lhe é atribuído em função da posição que ele ocupa no número. Esse peso, sempre uma potência de dez, varia do seguinte modo:

O algarismo da extrema direita tem peso um; o seguinte, sempre da direita pra esquerda, tem peso dez; o seguinte tem peso cem; o seguinte tem peso mil, e assim por diante.

Portanto, os números de um a nove são representados pelos algarismos de 1 a 9, correspondentes. O número dez é representado por 10, o número cem por 100, o numéro mil por 1000.

Por exemplo, o número 13109, na base 10, é a representação de

$1 \cdot 10^4 + 3 \cdot 10^3 + 1 \cdot 10^2 + 0 \cdot 10 + 9 = 1 \cdot 10^4 + 3 \cdot 10^3 + 1 \cdot 10^2 + 9$

Cada algarismo de um número possui uma *ordem* contada da direita para a esquerda. Assim, no exemplo acima, o primeiro 1 que aparece (da direita para a esquerda), é de terceira ordem, enquanto o último é de quinta ordem. O 9 é de primeira ordem, enquanto o 3 é de quarta ordem.

Cada terna de ordens, também contadas da direita pra esquerda, forma uma *classe*. As classes são, às vezes, separadas umas das outras por meio de um ponto.

Os sistemas de numeração posicionais baseiam-se no teorema a seguir, que é uma aplicação da divisão euclidiana.

Proposição 10 *Sejam dados os números inteiros a e b, com $a > 0$ e $b > 1$. Existem números inteiros $n \geq 0$ e $0 \leq r_0, r_1, ..., r_n < b$ com $r_n \neq 0$, univocamente determinados, tais que $a = r_0 + r_1 b + r_2 b^2 + ... + r_n b^n$.*

Demonstração. Vamos demonstrar o teorema por Indução Completa em a. Se $0 < a < b$, basta tomar $n = 0$ e $r_0 = a$. Teremos a afirmação como verdadeira.

Suponhamos que o resultado seja válido para todo natural menor que a, onde $a \geq b$. Vamos prová-lo para a. Pela divisão euclidiana $\exists\ q, r$, únicos tais que

$$a = bq + r \text{ com } 0 \leq r < b$$

Temos que $0 < q < a$, pois a é um produto de q e b, com $b > 1$ por hipótese.

Pela hipótese de indução, segue-se que existem números inteiros $n' \geq 0$ e $0 \leq$

$r_1, r_2, ..., r_{n'+1} < b$, com $r_{n'+1} \neq 0$ univocamente determinados, tais que

$$q = r_1 + r_2 b + ... + r_{n'+1} b^{n'}.$$

Levando em conta as duas igualdades acima, temos que

$$a = bq + r = b(r_1 + r_2 b + ... + r_{n'+1} b^{n'}) + r,$$

faça $r_0 = r$ e $n = n' + 1$ e está demonstrado o que queríamos. ■

4.1 Exemplos

Exemplo 4.1 *Escreva, na base dez, os números a seguir:*

a) 529

b) 2387

c) 456321

d) Generalize o caso para qualquer número

a) O número 529, na base 10, é escrito da forma $5 \cdot 10^2 + 2 \cdot 10 + 9$

b) O número 2387, na base 10, é escrito da forma $2 \cdot 10^3 + 3 \cdot 10^2 + 8 \cdot 10 + 7$

c) O número 456321, na base 10, é escrito da forma $4 \cdot 10^5 + 5 \cdot 10^4 + 6 \cdot 10^3 + 3 \cdot 10^2 + 2 \cdot 10 + 1$

d) Seja o número $s = a_n a_{n-1} a_{n-2} ... a_2 a_1 a_0$ onde cada a_i é um algarismo do número, na base 10, s é escrito da forma $a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + a_{n-2} \cdot 10^{n-2} + ... + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$.

Capítulo 5

ARITMÉTICA DOS RESTOS

Seja $n \in \mathbb{N}$. Diremos que dois números a e b inteiros, são *congruentes* módulo n se os restos de sua divisão euclidiana por n são iguais. Quando os inteiros a e b são congruentes módulo n, escrevemos

$$a \equiv b \mod n$$

Por exemplo, $21 \equiv 13 \mod 2$, já que os restos da divisão por 21 e de 13 por 2 são iguais a 1.

Quando a relação $a \equiv b \mod n$ for falsa, diremos que a e b *não são congruentes*, ou são *incongruentes*, módulo n. Escreveremos, neste caso, $a \not\equiv b \mod n$.

Como o resto da divisão de um número inteiro qualquer por 1 é sempre nulo, temos que $a \equiv b \mod 1$, quais quer que sejam a e $b \in \mathbb{Z}$. Isto torna desinteressante a aritmética dos restos módulo 1. Portanto, consideremos $n > 1$.

Proposição 11 *Seja $n \in \mathbb{N}$. Para todos $a, b, c \in \mathbb{Z}$, tem-se que*

(i) $a \equiv a \mod n$.

(ii) *se* $a \equiv b \mod n$, *então* $b \equiv a \mod n$.

(iii) *se* $a \equiv b \mod n$ *e* $b \equiv c \mod n$, *então* $a \equiv c \mod n$.

A demonstração é direta pela definição de números congruentes.

Para verificar se dois números são congruentes módulo n, não é necessário efetuar a divisão euclidiana de ambos por n para depois comparar os seus restos. É suficiente aplicar o seguinte resultado:

Proposição 12 *Suponha que $a, b, n \in \mathbb{Z}$, com $n > 1$. Tem-se que $a \equiv b \mod n$ se, e somente se, $n \mid b - a$.*

Demonstração. Façamos a divisão euclidiana de a e b por n e obtemos então que $a = nq + r$, e $b = nq' + r'$ onde $q, q', r, r' \in \mathbb{Z}$ e $0 \leq r, r' < n$. Então, temos que

$$b - a = (nq' + r') - (nq + r)$$

$$b - a = n(q' - q) + (r' - r)$$

Portanto, $a \equiv b \mod n$ se, e somente se, $r = r'$, o que, em vista da igualdade acima, é equivalente que $n \mid b - a$, ja que $|r' - r| < n$ ■

Proposição 13 *Sejam $a, b, c, d, n \in \mathbb{Z}$, com $n > 1$.*

(i) Se $a \equiv b \mod n$ e $c \equiv d \mod n$, então $a + c \equiv b + d \mod n$.

(ii) Se $a \equiv b \mod n$ e $c \equiv d \mod n$, então $ac \equiv bd \pmod n$.

Demonstração.

(i) Temos que $n \mid b - a$ e $n \mid d - c$, basta agora observar que $n \mid (b - a) + (d - c)$ e portanto, $n \mid (b + d) - (a + c)$.

(ii) Temos que $n \mid b - a$ e $n \mid d - c$, sendo assim $n \mid (b - a)d$ e $n \mid (d - c)a$, então $n \mid (b - a)d + (d - c)a$ e como,

$$(b - a)d + (d - c)a = bd - ad + ad - ac = db - ac$$

então $n \mid bd - ac$. Portanto $ac \equiv bd \mod n$.

■

Corolário 1 *Para todos $m \in \mathbb{Z}$, $a, b \in \mathbb{Z}$, se $a \equiv b \mod n$, então tem-se que $a^m \equiv b^m \mod n$.*

A demonstração vem diretamente da proposição 13, item (ii).

Proposição 14 *Sejam $a, b, c, n \in \mathbb{Z}$ com $n > 1$. Tem-se que*

$$a + c \equiv b + c \mod n \Leftrightarrow a \equiv b \mod n$$

Demonstração. Se temos que $a \equiv b \mod n$ e pela proposição 12 temos que $c \equiv c \mod n$, sendo assim, pela proposição 13, item (i), temos que $a + c \equiv b + c \mod n$. Para a volta, se $a + c \equiv b + c \mod n$ temos então que $n \mid (b + c) - (a + c)$, e $(b + c) - (a + c) = b - a + c - c = b - a$ então $n \mid b - a$, consequentemente, $a \equiv b \mod n$ ■

Proposição 15 *Sejam $a, b, c, n \in \mathbb{Z}$, com $n > 1$. Temos que*

$$ac \equiv bc \mod n \Leftrightarrow a \equiv b \mod \tfrac{n}{(c,n)}, \text{ com } (c, n) \text{ sendo mdc de } c \text{ e } n$$

Demonstração. Se $ac \equiv bc \mod n \Rightarrow n \mid bc - ac \Rightarrow n \mid (a - b)c \Rightarrow (a - b)c = nq \Rightarrow (a - b)\frac{c}{(c,n)} = \frac{n}{(c,n)}q$, pois $(c, n) \neq 0$, logo $\frac{n}{(c,n)} \mid (a - b)\frac{c}{(c,n)}$, como $\frac{n}{(c,n)}$ e $\frac{c}{(c,n)}$ são primos entre si, então $\frac{n}{(c,n)} \mid (a - b)$ e, portanto, $a \equiv b \mod \frac{n}{(c,n)}$.

A volta da implicação é análoga. ■

Corolário 2 *Sejam $a, b, c, n \in \mathbb{Z}$ com $n > 1$. Tem-se $a \equiv b \mod n \Rightarrow ac \equiv bc \pmod n$. Mas ainda, se $(c, n) = 1$, também vale $ac \equiv bc \mod n \Rightarrow a \equiv b \mod n$.*

Demonstração. Se $a \equiv b \mod n$, então $n \mid (a - b)$, isto é, $(a - b) = nq \Rightarrow (a - b)c = nqc \Rightarrow ac - bc = nq'$, com $q' = qc$. Logo $n \mid (ac - bc)$ e, portanto, $ac \equiv bc \mod n$. Para a volta da implicação, por hipotese temos que, $(c, n) = 1$ e $ac \equiv bc \mod n$, isto é, $n \mid (ac - bc) \Rightarrow n \mid (a - b)c$, como $n \nmid c$ então $n \mid (a - b) \Rightarrow a \equiv b \mod n$. ■

Proposição 16 *Sejam $a, b \in \mathbb{Z}$ e $n, m, n_1, ..., n_r$ inteiros maiores que 1. Temos que*

(i) se $a \equiv b \mod n$ e $m \mid n$, então $a \equiv b \mod m$;

(ii) $a \equiv b \mod n_i$, *para todo* $i = 1, ..., r \Leftrightarrow a \equiv b \mod [n_1, n_2, ..., n_r]$ *com* $[n_1, n_2, ..., n_r]$ *sendo o mmc de* $n_1, n_2, ..., n_r$*;*

(iii) se $a \equiv b \mod n$, *então* $(a, n) = (b, n)$.

Demonstração.

(i) Se $a \equiv b \mod n$, então $n \mid b - a$. Como $m \mid n$, segue que $m \mid b - a$. Logo $a \equiv b \mod m$.

(ii) Se $a \equiv b \mod n_i$ com $i = 1, ..., r$, então $n_i \mid b - a$, para todo i. Sendo $b - a$ um múltiplo de cada n_i, seque que $[n_1, n_2, ..., n_r] \mid b - a$, o que deixa provado então que $a \equiv b \mod [n_1, ...n_r]$.

(iii) Se $a \equiv b \mod n$, então $n \mid b - a$, isto é, $b - a = m \cdot q \Rightarrow b = m \cdot q + a$ com $q \in \mathbb{Z}$. Logo, temos que

$$(a, m) = (mq + a, m) = (b, m)$$

■

5.1 Exemplos

Exemplo 5.1 *Sejam* $a, p \in \mathbb{N}$ *com* p *primo. Mostre que, se* $a^2 \equiv 1 \pmod{p}$, *então* $a \equiv 1 \mod p$ *ou* $a \equiv -1 \mod p$.

Como $a^2 \equiv 1 \mod p$, temos que $p \mid a^2 - 1$. Sabe-se que $a^2 - 1 = (a - 1) \cdot (a + 1)$, como p é primo, ou então $p \mid (a - 1)$ ou $\mid (a + 1)$, isto é, $a \equiv 1 \mod p$ ou $a \equiv -1 \mod p$.

Exemplo 5.2 *Ache o resto da divisão de* 7^{10} *por* 51

Sabe-se que $7^2 = 49$ e que $49 + 2 \equiv 0 \mod 51$. Então $7^2 + 2 \equiv 0 \mod 51 \Rightarrow 7^2 + 2 - 2 \equiv 0 - 2 \pmod{51} \Rightarrow 7^2 \equiv -2 \mod 51$ pela proposição 13, e pelo corolário 1 tem-se que $(7^2)^5 \equiv (-2)^5 \mod 51 \Rightarrow 7^{10} \equiv -32 \mod 51$ e na divisão euclidiana de

-32 por 51, temos $-32 = 51 \cdot (-1) + 19$, isto é, $-32 \equiv 19 \mod 51$ e, portanto, $7^{10} \equiv 19 \mod 51$.

Exemplo 5.3 *Para todo* $n \in \mathbb{N}$ *mostre que* $19^{8n} - 1$ *é divisível por* 17

Temos que $19 \equiv 2 \mod 17$ e pelo corolário 1, $19^8 \equiv 2^8 \mod 17$ e como $2^8 = 256 \equiv 1 \pmod{17}$, então $19^8 \equiv 1 \mod 17$ e ainda pelo corolário 1, $(19^8)^n \equiv 1^n \mod 17 \Rightarrow 19^{8n} \equiv 1 \mod 17$ e, portanto, $17 \mid 19^{8n} - 1$ para qualquer $n \in \mathbb{N}$.

Capítulo 6

APLICAÇÕES

Algumas das aplicações de divisibilidade ou congruência é nas demonstrações dos critérios de divisibilidades usados nas escolas de ensino básico. Iremos mostrar algumas destas demonstrações nos critérios clássicos, e alguns não clássicos.

6.1 Critério de divisibilidade por 2

O critério de divisibilidade por 2, é considerado um dos clássicos. Um número é divisível por 2, se o seu algarismo da unidade for divisível por 2.

Faremos a primeira demonstração usando divisibilidade. Seja $a_n a_{n-1}...a_2 a_1 a_0$ um número que, quando escrito na base 10, $a_n a_{n-1}...a_2 a_1 a_0 = 10^n a_n + 10^{n-1} a_{n-1} + ... + 10^2 a_2 + 10a_1 + a_0$.

Demonstração. Suponhamos que $2 \mid a_n a_{n-1}...a_2 a_1 a_0$, então $10^n a_n + 10^{n-1} a_{n-1} + ... + 10^2 a_2 + 10a_1 + a_0 = 2q$ com $q \in \mathbb{Z} \Leftrightarrow 10(10^{n-1} a_n + 10^{n-2} a_{n-1} + ... + 10a_2 + a_1) + a_0 = 2q$ $\Leftrightarrow a_0 = 2q - 10(10^{n-1} a_n + 10^{n-2} a_{n-1} + ... + 10a_2 + a_1) \Leftrightarrow a_0 = 2[q - 5(10^{n-1} a_n + 10^{n-2} a_{n-1} + ... + 10a_2 + a_1)] \Leftrightarrow a_0 = 2q'$, com $q' = [q - 5(10^{n-1} a_n + 10^{n-2} a_{n-1} + ... + 10a_2 + a_1)]$, demonstrando o critério. ■

Na próxima demonstração, usaremos a aritmética dos restos. Ainda usando $a_n a_{n-1}...a_2 a_1 a_0$ um número que, quando escrito na base 10, $a_n a_{n-1}...a_2 a_1 a_0 = 10^n a_n + 10^{n-1} a_{n-1} + ... + 10^2 a_2 + 10 a_1 + a_0$.

Demonstração. Vejamos os restos das divisões das potências de 10, por 2.

$10^0 \equiv 1 \mod 2$

$10^1 \equiv 0 \mod 2$ ou também $10^1 \equiv -2 \mod 2$

$10^2 \equiv 0 \mod 2$ ou também $10^2 \equiv -2 \mod 2$

$10^3 \equiv 0 \mod 2$ ou também $10^3 \equiv -2 \mod 2$

$10^4 \equiv 0 \mod 2$ ou também $10^4 \equiv -2 \mod 2$

$10^5 \equiv 0 \mod 2$ ou também $10^5 \equiv -2 \mod 2$

$10^6 \equiv 0 \mod 2$ ou também $10^6 \equiv -2 \mod 2$

$10^7 \equiv 0 \mod 2$ ou também $10^7 \equiv -2 \mod 2$

$10^8 \equiv 0 \mod 2$ ou também $10^8 \equiv -2 \mod 2$

$10^9 \equiv 0 \mod 2$ ou também $10^9 \equiv -2 \mod 2$

$10^{10} \equiv 0 \mod 2$ ou também $10^{10} \equiv -2 \mod 2$

$\vdots$

$10^n \equiv 0 \mod 2$ ou também $10^n \equiv -2 \mod 2$

Usando o corolário 2, tem-se

$a_0 \cdot 10^0 \equiv 1 \cdot a_0 \mod 2$

$a_1 \cdot 10^1 \equiv 0 \cdot a_1 \mod 2$ ou também $a_1 \cdot 10^1 \equiv -2a_1 \mod 2$

$a_2 \cdot 10^2 \equiv 0 \cdot a_2 \mod 2$ ou também $a_2 \cdot 10^2 \equiv -2a_2 \mod 2$

$a_3 \cdot 10^3 \equiv 0 \cdot a_3 \mod 2$ ou também $a_3 \cdot 10^3 \equiv -2a_3 \mod 2$

$a_4 \cdot 10^4 \equiv 0 \cdot a_4 \mod 2$ ou também $a_4 \cdot 10^4 \equiv -2a_4 \mod 2$

$a_5 \cdot 10^5 \equiv 0 \cdot a_5 \mod 2$ ou também $a_5 \cdot 10^5 \equiv -2a_5 \mod 2$

$a_6 \cdot 10^6 \equiv 0 \cdot a_6 \mod 2$ ou também $a_6 \cdot 10^6 \equiv -2a_6 \mod 2$

$a_7 \cdot 10^7 \equiv 0 \cdot a_7 \mod 2$ ou também $a_7 \cdot 10^7 \equiv -2a_7 \mod 2$

$a_8 \cdot 10^8 \equiv 0 \cdot a_8 \mod 2$ ou também $a_8 \cdot 10^8 \equiv -2a_8 \mod 2$

$a_9 \cdot 10^9 \equiv 0 \cdot a_9 \mod 2$ ou também $a_9 \cdot 10^9 \equiv -2a_9 \mod 2$

$a_{10} \cdot 10^{10} \equiv 0 \cdot a_{10} \mod 2$ ou também $a_{10} \cdot 10^{10} \equiv -2a_{10} \mod 2$

$\vdots$

$a_n \cdot 10^n \equiv 0 \cdot a_n \mod 2$ ou também $a_n \cdot 10^n \equiv -2a_n \mod 2$

Logo, pela proposição 13 $a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + ... + a_n \cdot 10^n \equiv a_0 \mod 2 \Rightarrow a_n a_{n-1}...a_2 a_1 a_0 \equiv a_0 \mod 2$, ou seja, para que $a_n a_{n-1}...a_2 a_1 a_0$ ser divisível por 2, tem-se que a_0 deve ser divisível por 2.

Ou ainda, $a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + ... + a_n \cdot 10^n \equiv a_0 - 2(a_1 + a_2 + ... + a_n) \mod 2$, isto é, se o valor absoluto da diferença entre o algarismo da unidade e o dobro da soma dos outros algarismo for divisível por 2, então o número dado é divisível por 2. ■

Exemplo 6.1 *Dado 2586, verifique se é divisível por 2.*

Veja que 6 é o último algarismo do número dado, e como $6 = 2 \cdot 3$, isto é, $2 \mid 6$ então, 2586 é divisível por 2.

Ou ainda, $|6 - 2 \cdot (2 + 5 + 8)| = |6 - 30| = |-24| = 24$ e $|24| = 2 \cdot 12$, ou seja, 24 é divisível por 2, portanto 2586 também é.

Exemplo 6.2 *Dado 6259, verifique se é divisível por 2.*

Veja que 9 é o último algarismo do número dado, e como $9 = 2 \cdot 4 + 1$, isto é, $2 \nmid 9$ então, 6259 não é divisível por 2.

Ou ainda, $|9 - 2 \cdot (6 + 2 + 5)| = |9 - 26| = |-17| = 17$ e $17 = 2 \cdot 8 + 1$, isto é, 17 não é divisível por 2, portanto 6259 não é divisível por 2.

6.2 Critério de divisibilidade por 3

Um número é divisivel por 3 se, a soma do seu algarismo da unidade com o número formado pelos outros algarismos, for divisível por 3.

Seja $a_n a_{n-1}...a_2 a_1 a_0$ um número que, quando escrito na base 10, $a_n a_{n-1}...a_2 a_1 a_0 = 10^n \cdot a_n + 10^{n-1} a_{n-1} + ... + 10^2 a_2 + 10 a_1 + a_0$. Primeiro iremos provar por divisibilidade.

Demonstração. Suponhamos que $a_n a_{n-1}...a_2 a_1 a_0 = 10^n a_n + 10^{n-1} a_{n-1} + ... + 10^2 \cdot a_2 + 10 \cdot a_1 + a_0$ seja divisivel por 3, então $10^n \cdot a_n + 10^{n-1} a_{n-1} + ... + 10^2 a_2 + 10 a_1 + a_0 = 3q$. Soma-se então $9a_0$ nos dois membros da igualdade e teremos $10^n a_n + 10^{n-1} a_{n-1} + ... + 10^2 a_2 + 10 a_1 + a_0 + 9a_0 = 3q + 9a_0 \Leftrightarrow 10(10^{n-1} a_n + 10^{n-2} a_{n-1} + ... + 10 a_2 + a_1 + a_0) = 3q + 9a_0 \Leftrightarrow 10(10^{n-1} a_n + 10^{n-2} a_{n-1} + ... + 10 a_2 + a_1 + a_0) = 3(q + 3a_0)$. Como 3 é primo e $3 \nmid 10$, então para $3 \mid a_n a_{n-1}...a_2 a_1 a_0$, temos que $(10^{n-1} a_n + 10^{n-2} a_{n-1} + ... + 10 a_2 + a_1 + a_0)$ deve ser divisível por 3. Mas como $10^{n-1} a_n + 10^{n-2} a_{n-1} + ... + 10 a_2 + a_1 + a_0 = a_n a_{n-1}...a_2 a_1 + a_0$, então está provado que para o número ser divisível por 3, a soma do seu ultimo algarismo com o número formado pelos outros algarimos deve dividir 3. ■

Agora iremos mostrar por congruência.

Demonstração. Para isso, mostraremos os restos da divisão de potências de 10 por 3.

$10^0 \equiv 1 \mod 3$

$10^1 \equiv 1 \mod 3$ ou também $10^1 \equiv -2 \mod 3$

$10^2 \equiv 1 \mod 3$ ou também $10^2 \equiv -2 \mod 3$

$10^3 \equiv 1 \mod 3$ ou também $10^3 \equiv -2 \mod 3$

$10^4 \equiv 1 \mod 3$ ou também $10^4 \equiv -2 \mod 3$

$10^5 \equiv 1 \mod 3$ ou também $10^5 \equiv -2 \mod 3$

$10^6 \equiv 1 \mod 3$ ou também $10^6 \equiv -2 \mod 3$

$10^7 \equiv 1 \mod 3$ ou também $10^7 \equiv -2 \mod 3$

$10^8 \equiv 1 \mod 3$ ou também $10^8 \equiv -2 \mod 3$

$10^9 \equiv 1 \mod 3$ ou também $10^9 \equiv -2 \mod 3$

$10^{10} \equiv 1 \mod 3$ ou também $10^{10} \equiv -2 \mod 3$

$\vdots$

$10^n \equiv 1 \mod 3$ ou também $10^n \equiv -2 \mod 3$

Usando o corolário 2, temos

$a_0 \cdot 10^0 \equiv 1 \cdot a_0 \mod 3$

$a_1 \cdot 10^1 \equiv 1 \cdot a_1 \mod 3$ ou também $a_1 \cdot 10^1 \equiv -2a_1 \mod 3$

$a_2 \cdot 10^2 \equiv 1 \cdot a_2 \mod 3$ ou também $a_2 \cdot 10^2 \equiv -2a_2 \mod 3$

$a_3 \cdot 10^3 \equiv 1 \cdot a_3 \mod 3$ ou também $a_3 \cdot 10^3 \equiv -2a_3 \mod 3$

$a_4 \cdot 10^4 \equiv 1 \cdot a_4 \mod 3$ ou também $a_4 \cdot 10^4 \equiv -2a_4 \mod 3$

$a_5 \cdot 10^5 \equiv 1 \cdot a_5 \mod 3$ ou também $a_5 \cdot 10^5 \equiv -2a_5 \mod 3$

$a_6 \cdot 10^6 \equiv 1 \cdot a_6 \mod 3$ ou também $a_6 \cdot 10^6 \equiv -2a_6 \mod 3$

$a_7 \cdot 10^7 \equiv 1 \cdot a_7 \mod 3$ ou também $a_7 \cdot 10^7 \equiv -2a_7 \mod 3$

$a_8 \cdot 10^8 \equiv 1 \cdot a_8 \mod 3$ ou também $a_8 \cdot 10^8 \equiv -2a_8 \mod 3$

$a_9 \cdot 10^9 \equiv 1 \cdot a_9 \mod 3$ ou também $a_9 \cdot 10^9 \equiv -2a_9 \mod 3$

$a_{10} \cdot 10^{10} \equiv 1 \cdot a_{10} \mod 3$ ou também $a_{10} \cdot 10^{10} \equiv -2a_{10} \mod 3$

$\vdots$

$a_n \cdot 10^n \equiv 1 \cdot a_n \mod 3$ ou também $a_n \cdot 10^n \equiv -2a_n \mod 3$

Logo, pela proposição 13 $a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + ... + a_n \cdot 10^n \equiv a_0 + a_1 + a_2 + ... + a_n \mod 3$, isto é, $a_n a_{n-1} ... a_2 a_1 a_0 \equiv 0 \mod 3 \Leftrightarrow a_0 + a_1 + a_2 + ... + a_n \equiv 0 \mod 3$. Portanto, se a soma dos algarismos de um número é divisível por 3, o número também será.

Ou ainda, $a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + ... + a_n \cdot 10^n \equiv a_0 - 2(a_1 + a_2 + ... + a_n) \mod 3$, isto é, se o valor absoluto do algarismo da unidade subtraído o dobro da soma dos outros algarismo for divisível por 3, então o número dado também é. ■

Exemplo 6.3 *Dado o número 51354897, verifique se é divisível por 3.*

Veja que a soma dos algarismos do número é dada por $5+1+3+5+4+8+9+7 = 42$ e $42 = 3 \cdot 14$, ou seja, $3 \mid 42$ então, 51354897 é divisível por 3.

Ou ainda, $|7 - 2 \cdot (5+1+3+5+4+8+9)| = |7 - 2 \cdot (35)| = |7 - 70| = |-63| = 63$ e $63 = 3 \cdot 21$, logo 63 é divisível por 3. Portanto 51354897 é divisível por 3.

Exemplo 6.4 *Dado o número 97481255, verifique se é divisível por 3.*

Veja que a soma dos algarismos do número é dada por $9+7+4+8+1+2+5+5 = 41$ e $3 \nmid 41$, então 97481255 não é divisível por 3.

Ou ainda, $|5 - 2 \cdot (36)| = |5 - 72| = |-67| = 67$ e $67 \equiv 1 \mod 3$, ou seja, $3 \nmid 67$, portanto 97481255 não é divisível por 3.

6.3 Critério de divisibilidade por 5

Um número é divisível por 5 se o seu último algarismo é também divisível por 5, isto é, se for 0 ou 5.

Seja $a_n a_{n-1}...a_2a_1a_0$ um número que, quando escrito na base 10, $a_n a_{n-1}...a_2a_1a_0 = 10^n \cdot a_n + 10^{n-1}a_{n-1} + ... + 10^2a_2 + 10a_1 + a_0$. Primeiro iremos provar por divisibilidade.

Demonstração. Suponhamos que $5 \mid a_n a_{n-1}...a_2a_1a_0$, então $10^n a_n + 10^{n-1}a_{n-1} + ... + 10^2a_2 + 10a_1 + a_0 = 5q$ com $q \in \mathbb{Z} \Leftrightarrow 10(10^{n-1}a_n + 10^{n-2}a_{n-1} + ... + 10a_2 + a_1) + a_0 = 5q$ $\Leftrightarrow a_0 = 5q - 10(10^{n-1}a_n + 10^{n-2}a_{n-1} + ... + 10a_2 + a_1) \Leftrightarrow a_0 = 5[q - 2(10^{n-1}a_n + 10^{n-2}a_{n-1} + ... + 10a_2 + a_1)] \Leftrightarrow a_0 = 5q'$, com $q' = [q - 2(10^{n-1}a_n + 10^{n-2}a_{n-1} + ... + 10a_2 + a_1)]$, ou seja, para um número ser divisível por 5, o seu ultimo algarismo também deve ser divisivel por 5. ■

Na próxima demonstração, usaremos a aritmética dos restos. Ainda usando $a_n a_{n-1}...a_2a_1a_0$ um número que, quando escrito na base 10, $a_n a_{n-1}...a_2a_1a_0 = 10^n a_n + 10^{n-1}a_{n-1} + ... + 10^2a_2 + 10a_1 + a_0$.

Demonstração. Vejamos os restos das divisões das potências de 10, por 5.

$$10^0 \equiv 1 \mod 5$$

$$10^1 \equiv 0 \mod 5$$

$$10^2 \equiv 0 \mod 5$$

$$10^3 \equiv 0 \mod 5$$

$$10^4 \equiv 0 \mod 5$$

$$10^5 \equiv 0 \mod 5$$

$$10^6 \equiv 0 \mod 5$$

$$10^7 \equiv 0 \mod 5$$

$$10^8 \equiv 0 \mod 5$$

$$10^9 \equiv 0 \mod 5$$

$$10^{10} \equiv 0 \mod 5$$

$$\vdots$$

$$10^n \equiv 0 \mod 5$$

Usando o corolário 2, tem-se

$$a_0 \cdot 10^0 \equiv 1 \cdot a_0 \mod 5$$

$$a_1 \cdot 10^1 \equiv 0 \cdot a_1 \mod 5$$

$$a_2 \cdot 10^2 \equiv 0 \cdot a_2 \mod 5$$

$$a_3 \cdot 10^3 \equiv 0 \cdot a_3 \mod 5$$

$$a_4 \cdot 10^4 \equiv 0 \cdot a_4 \mod 5$$

$$a_5 \cdot 10^5 \equiv 0 \cdot a_5 \mod 5$$

$$a_6 \cdot 10^6 \equiv 0 \cdot a_6 \mod 5$$

$$a_7 \cdot 10^7 \equiv 0 \cdot a_7 \mod 5$$

$$a_8 \cdot 10^8 \equiv 0 \cdot a_8 \mod 5$$

$$a_9 \cdot 10^9 \equiv 0 \cdot a_9 \mod 5$$

$$a_{10} \cdot 10^{10} \equiv 0 \cdot a_{10} \mod 5$$

$$\vdots$$

$$a_n \cdot 10^n \equiv 0 \cdot a_n \mod 5$$

Logo, $a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + ... + a_n \cdot 10^n \equiv a_0 \mod 5 \Rightarrow a_n a_{n-1}...a_2 a_1 a_0 \equiv a_0 \mod 5$, ou seja, para que $a_n a_{n-1}...a_2 a_1 a_0$ ser divisível por 5, tem-se que $a_0 = 0$ ou $a_0 = 5$. ■

Exemplo 6.5 *Seja 859302 um número na base 10, verifique se é divisível por 5.*

Seguindo o critério de divisibilidade, olhando para o algarismos da unidade, vemos que ele não é divisível por 5. Portanto $5 \nmid 859302$.

Exemplo 6.6 *Seja 7648310 um número na base 10, verifique se é divisível por 5.*

Segundo o critério de divisibilidade, se o algarismo da unidade for divisível por 5, então o número é divisível por 5. Como $5 \mid 0$, então $5 \mid 7648310$, ou seja, 7648310 é divisível por 5.

6.4 Critério de divisibilidade por 7

Um número é divisível por 7, se o quintúplo do seu algarismo da unidade somado com o número formado pelos outros algarismos for divisível por 7.

Seguindo a ordem, primeiro demonstraremos por divisibilidade.

Demonstração. Suponhamos um $a_n a_{n-1}...a_2 a_1 a_0$ que seja divisível por 7, isto é $a_n a_{n-1}...a_2 a_1 a_0 = 7q$ com $q \in \mathbb{Z}$. Escrevendo este número em potência de 10, temos $10^n a_n + 10^{n-1} a_{n-1} + ... + 10^2 a_2 + 10a_1 + a_0 = 7q \Rightarrow 10^n a_n + 10^{n-1} a_{n-1} + ... + 10^2 a_2 + 10a_1 + 50a_0 = 7q + 49a_0 \Rightarrow 10(10^{n-1} a_n + 10^{n-2} a_{n-1} + ... + 10a_2 + a_1 + 5a_0) = 7(q + 7a_0)$. Sabemos que $10^{n-1} a_n + 10^{n-2} a_{n-1} + ... + 10a_2 + a_1 + 5a_0 = a_n a_{n-1}...a_3 a_2 a_1 + 5a_0$. Como $7 \nmid 10$ então $7 \mid a_n a_{n-1}...a_3 a_2 a_1 + 5a_0$, provando o critério. ■

Agora usaremos a Aritmética dos Restos, para demonstrar outro critério.

Demonstração. Vejamos os restos da divisão das potências de 10 por 7.

$10^0 \equiv 1 \mod 7$

$10^1 \equiv 3 \mod 7$ ou também $10^1 \equiv -4 \mod 7$

$10^2 \equiv 2 \mod 7$ ou também $10^2 \equiv -5 \mod 7$

$10^3 \equiv 6 \mod 7$ ou também $10^3 \equiv -1 \mod 7$

$10^4 \equiv 4 \mod 7$ ou também $10^4 \equiv -3 \mod 7$

$10^5 \equiv 5 \mod 7$ ou também $10^5 \equiv -2 \mod 7$

$10^6 \equiv 1 \mod 7$ ou também $10^6 \equiv -6 \mod 7$

$10^7 \equiv 3 \mod 7$ ou também $10^7 \equiv -4 \mod 7$

$10^8 \equiv 2 \mod 7$ ou também $10^8 \equiv -5 \mod 7$

$10^9 \equiv 6 \mod 7$ ou também $10^9 \equiv -1 \mod 7$

$10^{10} \equiv 4 \mod 7$ ou também $10^{10} \equiv -3 \mod 7$

$\vdots$

Assim por diante, até 10^n.

$a_0 \cdot 10^0 \equiv a_0 \mod 7$

$a_1 \cdot 10^1 \equiv 3a_1 \mod 7$ ou também $a_1 \cdot 10^1 \equiv -4a_1 \mod 7$

$a_2 \cdot 10^2 \equiv 2a_2 \mod 7$ ou também $a_2 \cdot 10^2 \equiv -5a_2 \mod 7$

$a_3 \cdot 10^3 \equiv 6a_3 \mod 7$ ou também $a_3 \cdot 10^3 \equiv -a_3 \mod 7$

$a_4 \cdot 10^4 \equiv 4a_4 \mod 7$ ou também $a_4 \cdot 10^4 \equiv -3a_4 \mod 7$

$a_5 \cdot 10^5 \equiv 5a_5 \mod 7$ ou também $a_5 \cdot 10^5 \equiv -2a_5 \mod 7$

$a_6 \cdot 10^6 \equiv a_6 \mod 7$ ou também $a_6 \cdot 10^6 \equiv -6a_6 \mod 7$

$a_7 \cdot 10^7 \equiv 3a_7 \mod 7$ ou também $a_7 \cdot 10^7 \equiv -4a_7 \mod 7$

$a_8 \cdot 10^8 \equiv 2a_8 \mod 7$ ou também $a_8 \cdot 10^8 \equiv -5a_8 \mod 7$

$a_9 \cdot 10^9 \equiv 6a_9 \mod 7$ ou também $a_9 \cdot 10^9 \equiv -a_9 \mod 7$

$a_{10} \cdot 10^{10} \equiv 4a_{10} \mod 7$ ou também $a_{10} \cdot 10^{10} \equiv -3a_{10} \mod 7$

$\vdots$

Assim por diante, até 10^n.

Então $a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + ... + a_n \cdot 10^n \equiv (a_0 + 3a_1 + 2a_2) - (a_3 + 3a_4 + 2a_5) + (a_6 + 3a_7 + 2a_8) - (a_9 + 3a_{10} + 2a_{11})... \mod 7$.

Logo $a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + ... + a_n \cdot 10^n \equiv 0 \mod 7 \Leftrightarrow (a_0 + 3a_1 + 2a_2) - (a_3 + 3a_4 + 2a_5) + (a_6 + 3a_7 + 2a_8) - (a_9 + 3a_{10} + 2a_{11})... \equiv 0 \mod 7$. ■

Exemplo 6.7 *Dado o número 18179, verifique se é divisível por 7.*

Usando o primeiro critério temos, $1817 + 5 \cdot 9 = 1862$, ainda está dificil de saber, aplicaremos de novo o critério e teremos $186 + 5 \cdot 2 = 196$, aplicando novamente $19 + 5 \cdot 6 = 49$ e $7 \mid 49$, portanto 18179 é divisível por 7.

Ou usando o segundo critério, $(9 + 3 \cdot 7 + 2 \cdot 1) - (8 + 3 \cdot 1) = (9 + 21 + 2) - (8 + 3) = 32 - 11 = 21$ e $7 \mid 21$, portanto 18179 é divisível por 7.

Exemplo 6.8 *Dado o número 429269, verifique se é divisível por 7.*

Usando o segundo critério, temos então $(9 + 3 \cdot 6 + 2 \cdot 2) - (9 + 3 \cdot 2 + 2 \cdot 4) = 31 - 23 = 8$ e $7 \nmid 8$, portanto 429269 não é divisível por 7.

Ou ainda, usando o primeiro critério, temos $42926 + 5 \cdot 9 = 43014$ que ainda é um número muito grande, aplicamos novamente o critério até o número ficar facil decidir se é ou não divisível por 7, então $4301 + 5 \cdot 4 = 4321$; $432 + 5 = 437$; $43 + 5 \cdot 7 = 88$ e $7 \nmid 88$ pois $88 = 7 \cdot 12 + 4$, isto é 429269 não é divisível por 7.

6.5 Critério de divisibilidade por 11

Um número é divisível por 11, se o número formado pelos algarismos excluindo o algarismo da unidade, subtraído pelo mesmo, for divisível por 11.

Exemplo 6.9 *Verifique se 22737 é divisivel por 11.*

Aplicando o critério, temos então $2273 - 7 = 2266$, só olhando para o número não conseguimos, ainda, saber se ele é ou não divisível por 11. Então aplicaremos o critério até o número resultante ser suficiente para sabermos se é ou não divisível por 11. Logo, $226 - 6 = 220$; $22 - 0 = 22$ e $11 \mid 22$. Portanto, 22737 é divisivel por 11.

Para demonstrar o critério, usaremos divisibilidade.

Demonstração. Suponhamos um $a_n a_{n-1}...a_2 a_1 a_0$ que seja divisível por 11, isto é $a_n a_{n-1}...a_2 a_1 a_0 = 11q$ com $q \in \mathbb{Z}$. Escrevendo este número em potência de 10, temos $10^n a_n + 10^{n-1} a_{n-1} + ... + 10^2 a_2 + 10a_1 + a_0 = 11q \Rightarrow 10^n a_n + 10^{n-1} a_{n-1} + ... + 10^2 a_2 + 10a_1 - 10a_0 = 11q - 11a_0 \Rightarrow 10(10^{n-1} a_n + 10^{n-2} a_{n-1} + ... + 10a_2 + a_1 - a_0) = 11(q - a_0)$. Sabemos que $10^{n-1} a_n + 10^{n-2} a_{n-1} + ... + 10a_2 + a_1 - a_0 = a_n a_{n-1}...a_3 a_2 a_1 - a_0$. Como $11 \nmid 10$ então $11 \mid a_n a_{n-1}...a_3 a_2 a_1 - a_0$, provando o critério. ■

Usando aritmética modular, começaremos analisando os restos das potências de dez, por onze, no final chegaremos ao um outro critério.

Demonstração. $10^0 \equiv 1 \mod 11$

$10^1 \equiv 10 \mod 11$ ou também $10^1 \equiv -1 \mod 11$

$10^2 \equiv 1 \mod 11$ ou também $10^2 \equiv -10 \mod 11$

$10^3 \equiv 10 \mod 11$ ou também $10^3 \equiv -1 \mod 11$

$10^4 \equiv 1 \mod 11$ ou também $10^4 \equiv -10 \mod 11$

$10^5 \equiv 10 \mod 11$ ou também $10^5 \equiv -1 \mod 11$

$10^6 \equiv 1 \mod 11$ ou também $10^6 \equiv -10 \mod 11$

$10^7 \equiv 10 \mod 11$ ou também $10^7 \equiv -1 \mod 11$

$10^8 \equiv 1 \mod 11$ ou também $10^8 \equiv -10 \mod 11$

$10^9 \equiv 10 \mod 11$ ou também $10^9 \equiv -1 \mod 11$

$10^{10} \equiv 1 \mod 11$ ou também $10^{10} \equiv -10 \mod 11$

$\vdots$

Assim por diante, até 10^n.

$a_0 \cdot 10^0 \equiv a_0 \mod 11$

$a_1 \cdot 10^1 \equiv 10a_1 \mod 11$ ou também $a_1 \cdot 10^1 \equiv -a_1 \mod 11$

$a_2 \cdot 10^2 \equiv a_2 \mod 11$ ou também $a_2 \cdot 10^2 \equiv -10a_2 \mod 11$

$a_3 \cdot 10^3 \equiv 10a_3 \mod 11$ ou também $a_3 \cdot 10^3 \equiv -a_3 \mod 11$

$a_4 \cdot 10^4 \equiv a_4 \mod 11$ ou também $a_4 \cdot 10^4 \equiv -10a_4 \mod 11$

$a_5 \cdot 10^5 \equiv 10a_5 \mod 11$ ou também $a_5 \cdot 10^5 \equiv -a_5 \mod 11$

$a_6 \cdot 10^6 \equiv a_6 \mod 11$ ou também $a_6 \cdot 10^6 \equiv -10a_6 \mod 11$

$a_7 \cdot 10^7 \equiv 10a_7 \mod 11$ ou também $a_7 \cdot 10^7 \equiv -a_7 \mod 11$

$a_8 \cdot 10^8 \equiv a_8 \mod 11$ ou também $a_8 \cdot 10^8 \equiv -10a_8 \mod 11$

$a_9 \cdot 10^9 \equiv 10a_9 \mod 11$ ou também $a_9 \cdot 10^9 \equiv -a_9 \mod 11$

$a_{10} \cdot 10^{10} \equiv a_{10} \mod 11$ ou também $a_{10} \cdot 10^{10} \equiv -10a_{10} \mod 11$

$\vdots$

Assim por diante, até 10^n.

Ou seja, $a_n a_{n-1}...a_2 a_1 a_0$ é divisível por 11, se:

i) o algarismo da unidade somado ao décimo da soma dos algarismos da ordem par, somado com a soma dos algarismos da ordem ímpar o for;

ii) o algarismo da unidade subtraído da soma dos algarismos de ordem par, subtraído do décimo da soma dos algarismos da ordem ímpar o for.

■

Exemplo 6.10 *Verifique se 22737 é divisivel por 11.*

Já mostramos que pelo critério demonstrado por divisibilidade que 22737 é divisível por 11. Agora mostraremos usando este outro critério.

Repare que:

o algarismo da unidade é 7,

os algarismos da ordem par são 3 e 2,

os algarismos da ordem ímpar são 7 e 2.

Logo, temos:

i) $7 + 10(3 + 2) + (7 + 2) = 7 + 50 + 9 = 66$ e $66 \equiv 0 \mod 11$;

ii) $7 - (3 + 2) - 10(7 + 2) = 7 - 5 - 90 = -88$ e $-88 \equiv 0 \mod 11$.

Portanto, 22737 é divisível por 11.

6.6 Critério de divisibilidade por 13

Um número é divisível por 13 se a soma do quadruplo do algarismo da unidade somado com o número formado pelos outros algarismos, for divisível por 13.

Demonstração. Suponhamos um $a_n a_{n-1}...a_2 a_1 a_0$ que seja divisível por 13, isto é $a_n a_{n-1}...a_2 a_1 a_0 = 13q$ com $q \in \mathbb{Z}$. Escrevendo este número em potência de 10, temos $10^n a_n + 10^{n-1} a_{n-1} + ... + 10^2 a_2 + 10a_1 + a_0 = 13q \Rightarrow 10^n a_n + 10^{n-1} a_{n-1} + ... + 10^2 a_2 + 10a_1 + 40a_0 = 13q + 39a_0 \Rightarrow 10(10^{n-1} a_n + 10^{n-2} a_{n-1} + ... + 10a_2 + a_1 + 4a_0) = 13(q + 3a_0)$. Sabemos que $10^{n-1} a_n + 10^{n-2} a_{n-1} + ... + 10a_2 + a_1 + 4a_0 = a_n a_{n-1}...a_3 a_2 a_1 + 4a_0$. Como $13 \nmid 10$ então $13 \mid a_n a_{n-1}...a_3 a_2 a_1 + 4a_0$, provando o critério. ■

Agora usaremos a Aritmética dos Restos, para demonstrar outro critério.

Demonstração. Vejamos os restos da divisão das potências de 10 por 13.

$10^0 \equiv 1 \mod 13$

$10^1 \equiv 10 \mod 13$ ou também $10^1 \equiv -3 \mod 13$

$10^2 \equiv 9 \mod 13$ ou também $10^2 \equiv -4 \mod 13$

$10^3 \equiv 12 \mod 13$ ou também $10^3 \equiv -1 \mod 13$

$10^4 \equiv 3 \mod 13$ ou também $10^4 \equiv -10 \mod 13$

$10^5 \equiv 4 \mod 13$ ou também $10^5 \equiv -9 \mod 13$

$10^6 \equiv 1 \mod 13$ ou também $10^6 \equiv -12 \mod 13$

$10^7 \equiv 10 \mod 13$ ou também $10^7 \equiv -3 \mod 13$

$10^8 \equiv 9 \mod 13$ ou também $10^8 \equiv -4 \mod 13$

$10^9 \equiv 2 \mod 13$ ou também $10^9 \equiv -1 \mod 13$

$10^{10} \equiv 3 \mod 13$ ou também $10^{10} \equiv -10 \mod 13$

$\vdots$

Assim por diante, até 10^n.

$a_0 \cdot 10^0 \equiv a_0 \mod 13$

$a_1 \cdot 10^1 \equiv 10a_1 \mod 13$ ou também $a_1 \cdot 10^1 \equiv -3a_1 \mod 13$

$a_2 \cdot 10^2 \equiv 9a_2 \mod 13$ ou também $a_2 \cdot 10^2 \equiv -4a_2 \mod 13$

$a_3 \cdot 10^3 \equiv 12a_3 \mod 13$ ou também $a_3 \cdot 10^3 \equiv -a_3 \mod 13$

$a_4 \cdot 10^4 \equiv 3a_4 \mod 13$ ou também $a_4 \cdot 10^4 \equiv -10a_4 \mod 13$

$a_5 \cdot 10^5 \equiv 4a_5 \mod 13$ ou também $a_5 \cdot 10^5 \equiv -9a_5 \mod 13$

$a_6 \cdot 10^6 \equiv a_6 \mod 13$ ou também $a_6 \cdot 10^6 \equiv -12a_6 \mod 13$

$a_7 \cdot 10^7 \equiv 10a_7 \mod 13$ ou também $a_7 \cdot 10^7 \equiv -3a_7 \mod 13$

$a_8 \cdot 10^8 \equiv 9a_8 \mod 13$ ou também $a_8 \cdot 10^8 \equiv -4a_8 \mod 13$

$a_9 \cdot 10^9 \equiv 2a_9 \mod 13$ ou também $a_9 \cdot 10^9 \equiv -a_9 \mod 13$

$a_{10} \cdot 10^{10} \equiv 3a_{10} \mod 13$ ou também $a_{10} \cdot 10^{10} \equiv -10a_{10} \mod 13$

$\vdots$

Assim por diante, até 10^n.

Ou seja, $a_n a_{n-1}...a_2 a_1 a_0$ é divisível por 13, se:

i) $(a_0 + 10a_1 + 9a_2) - (a_3 + 10a_4 + 9a_5) + (a_6 + 10a_7 + 9a_8) - ...$ for divisível por 13;

ii) $(a_0 + 10a_1 + 9a_2 + 12a_3 + 3a_4 + 4a_5 + a_6 + 10a_7 + 9a_8 + ...$ for divisível por 13.

■

Exemplo 6.11 *Dado o número 46787, verifique se é divisível por 13.*

Usando o primeiro critério, temos: $4678 + 7 \cdot 4 = 4706$, aplicamos novamente o critério, $470 + 6 \cdot 4 = 494$; $49 + 4 \cdot 4 = 65$; $6 + 5 \cdot 4 = 26$ e $13 \mid 26$, portanto 46787 é divisível por 13.

Ou ainda, usando os outros critério, temos:

i) $(7 + 10 \cdot 8 + 9 \cdot 7) - (6 + 10 \cdot 4) = (7 + 80 + 63) - (6 + 40) = 150 - 46 = 104$ e $104 \equiv 0 \mod 13$, ou seja, $13 \mid 46787$.

ii) $(7 + 10 \cdot 8 + 9 \cdot 7 + 12 \cdot 6 + 3 \cdot 4) = 7 + 80 + 63 + 72 + 12 = 234$ e $13 \mid 234$, portanto 46787 é divisivel por 13.

6.7 Critério de divisibilidade por 17

Para saber se um número é divisível por 17, separe o número do seu algarismo da unidade. Se o 1° grupo de algarismos separados subtraído o quíntuplo do algarismo da unidade for múltiplo de 17, então o número original é divisível por 17

Demonstração. Suponhamos um $a_n a_{n-1}...a_2a_1a_0$ que seja divisível por 17, isto é, $a_n a_{n-1}...a_2a_1a_0 = 17q$ com $q \in \mathbb{Z}$. Escrevendo este número em potência de 10, temos $10^n a_n + 10^{n-1}a_{n-1} + ... + 10^2a_2 + 10a_1 + a_0 = 17q \Rightarrow 10^n a_n + 10^{n-1}a_{n-1} + ... + 10^2a_2 + 10a_1 - 50a_0 = 17q - 51a_0 \Rightarrow 10(10^{n-1}a_n + 10^{n-2}a_{n-1} + ... + 10a_2 + a_1 - 5a_0) = 17(q - 3a_0)$. Sabemos que $10^{n-1}a_n + 10^{n-2}a_{n-1} + ... + 10a_2 + a_1 - 5a_0 = a_n a_{n-1}...a_3a_2a_1 - 5a_0$. Como $17 \nmid 10$ então $17 \mid a_n a_{n-1}...a_3a_2a_1 - 5a_0$, provando o critério. ■

A próxima demonstração, de um novo critério, será por congruência.

Demonstração. Vejamos os restos da divisão das potências de 10 por 17.

$10^0 \equiv 1 \mod 17$

$10^1 \equiv 10 \mod 17$ ou também $10^1 \equiv -7 \mod 17$

$10^2 \equiv 15 \mod 17$ ou também $10^2 \equiv -2 \mod 17$

$10^3 \equiv 14 \mod 17$ ou também $10^3 \equiv -3 \mod 17$

$10^4 \equiv 4 \mod 17$ ou também $10^4 \equiv -13 \mod 17$

$10^5 \equiv 6 \mod 17$ ou também $10^5 \equiv -11 \mod 17$

$10^6 \equiv 9 \mod 17$ ou também $10^6 \equiv -8 \mod 17$

$10^7 \equiv 5 \mod 17$ ou também $10^7 \equiv -12 \mod 17$

$10^8 \equiv 16 \mod 17$ ou também $10^8 \equiv -1 \mod 17$

$10^9 \equiv 7 \mod 17$ ou também $10^9 \equiv -10 \mod 17$

$10^{10} \equiv 2 \mod 17$ ou também $10^{10} \equiv -15 \mod 17$

$\vdots$

Assim por diante, até 10^n.

$a_0 \cdot 10^0 \equiv a_0 \mod 17$

$a_1 \cdot 10^1 \equiv 10a_1 \mod 17$ ou também $a_1 \cdot 10^1 \equiv -7a_1 \mod 17$

$a_2 \cdot 10^2 \equiv 15a_2 \mod 17$ ou também $a_2 \cdot 10^2 \equiv -2a_2 \mod 17$

$a_3 \cdot 10^3 \equiv 14a_3 \mod 17$ ou também $_3 \cdot 10^3 \equiv -3a_3 \mod 17$

$a_4 \cdot 10^4 \equiv 4a_4 \mod 17$ ou também $a_4 \cdot 10^4 \equiv -13a_4 \mod 17$

$a_5 \cdot 10^5 \equiv 6a_5 \mod 17$ ou também $a_5 \cdot 10^5 \equiv -11a_5 \mod 17$

$a_6 \cdot 10^6 \equiv 9a_6 \mod 17$ ou também $a_6 \cdot 10^6 \equiv -8a_6 \mod 17$

$a_7 \cdot 10^7 \equiv 5a_7 \mod 17$ ou também $a_7 \cdot 10^7 \equiv -12a_7 \mod 17$

$a_8 \cdot 10^8 \equiv 16a_8 \mod 17$ ou também $a_8 \cdot 10^8 \equiv -a_8 \mod 17$

$a_9 \cdot 10^9 \equiv 7a_9 \mod 17$ ou também $a_9 \cdot 10^9 \equiv -10a_9 \mod 17$

$a_{10} \cdot 10^{10} \equiv 2a_{10} \mod 17$ ou também $a_{10} \cdot 10^{10} \equiv -15a_{10} \mod 17$

$\vdots$

Assim por diante, até 10^n, sendo assim, para um número ser divísivel por 17, $(a_0 + 10a_1 + 15a_2 + 14a_3 + 4a_4 + 6a_5 + 9a_6 + 5a_7) - (a_8 + 10a_9 + 15a_{10} + 14a_{11} + 4a_{12} + 6a_{13} + 9a_{14} + 5a_{15}) + ...$ deverá ser divisível por 17. ■

Exemplo 6.12 *Dado o número 25296, verifique se é divisível por 17.*

Usando o primeiro critério, temos $2529 - 5 \cdot 6 = 2499$, aplicamos o critério até ficar fácil de verificar, então $249 - 5 \cdot 9 = 204$; $20 - 5 \cdot 4 = 0$ e $17 \mid 0$, isto é, 25296 é divisível por 17.

Exemplo 6.13 *Seja o número 2513490285597, verifique se é divisível por 17.*

Perceba que $a_0 = 7$, $a_1 = 9$, $a_2 = 5$, $a_3 = 5$, $a_4 = 8$, $a_5 = 2$, $a_6 = 0$, $a_7 = 9$, $a_8 = 4$, $a_9 = 3$, $a_{10} = 1$, $a_{11} = 5$ e por fim $a_{12} = 2$, aplicando no segundo critério, temos $(7 + 10 \cdot 9 + 15 \cdot 5 + 14 \cdot 5 + 4 \cdot 8 + 6 \cdot 2 + 9 \cdot 0 + 5 \cdot 9) - (4 + 10 \cdot 3 + 15 \cdot 1 + 14 \cdot 5 + 4 \cdot 2) = (7 + 90 + 75 + 70 + 32 + 12 + 0 + 45) - (4 + 30 + 15 + 70 + 8) = 331 - 127 = 204$, como vimos acima $17 \mid 204$, portanto 2513490285597 é divisível por 17.

6.8 Critério de divisibilidade por 19

Um número é divisível por 19 quando o dobro do algarismo da unidade, somado ao número formado pelos outros algarismos, formar um número divisível por 19.

Demonstraremos isto por divisibilidade.

Demonstração. Suponhamos um $a_n a_{n-1}...a_2a_1a_0$ que seja divisível por 19, isto é, $a_n a_{n-1}...a_2a_1a_0 = 19q$ com $q \in \mathbb{Z}$. Escrevendo este número em potência de 10, temos $10^n a_n + 10^{n-1}a_{n-1} + ... + 10^2a_2 + 10a_1 + a_0 = 19q \Rightarrow 10^n a_n + 10^{n-1}a_{n-1} + ... + 10^2a_2 + 10a_1 + 20a_0 = 19q + 19a_0 \Rightarrow 10(10^{n-1}a_n + 10^{n-2}a_{n-1} + ... + 10a_2 + a_1 + 2a_0) = 19(q + a_0)$. Sabemos que $10^{n-1}a_n + 10^{n-2}a_{n-1} + ... + 10a_2 + a_1 + 2a_0 = a_n a_{n-1}...a_3a_2a_1 + 2a_0$. Como $19 \nmid 10$ então $19 \mid a_n a_{n-1}...a_3a_2a_1 + 2a_0$, provando o critério. ■

A próxima demonstração, de um novo critério, será por congruência.

Demonstração. Vejamos os restos da divisão das potências de 10 por 19.

$10^0 \equiv 1 \mod 19$

$10^1 \equiv 10 \mod 19$ ou também $10^1 \equiv -9 \mod 19$

$10^2 \equiv 5 \mod 19$ ou também $10^2 \equiv -14 \mod 19$

$10^3 \equiv 12 \mod 19$ ou também $10^3 \equiv -7 \mod 19$

$10^4 \equiv 6 \mod 19$ ou também $10^4 \equiv -13 \mod 19$

$10^5 \equiv 3 \mod 19$ ou também $10^5 \equiv -16 \mod 19$

$10^6 \equiv 11 \mod 19$ ou também $10^6 \equiv -8 \mod 19$

$10^7 \equiv 15 \mod 19$ ou também $10^7 \equiv -4 \mod 19$

$10^8 \equiv 17 \mod 19$ ou também $10^8 \equiv -3 \mod 19$

$10^9 \equiv 8 \mod 19$ ou também $10^9 \equiv -1 \mod 19$

$10^{10} \equiv 9 \mod 19$ ou também $10^{10} \equiv -10 \mod 19$

$\vdots$

Assim por diante, até 10^n.

$a_0 \cdot 10^0 \equiv a_0 \mod 19$

$a_1 \cdot 10^1 \equiv 10a_1 \mod 19$ ou também $a_1 \cdot 10^1 \equiv -9a_1 \mod 19$

$a_2 \cdot 10^2 \equiv 5a_2 \mod 19$ ou também $a_2 \cdot 10^2 \equiv -14a_2 \mod 19$

$a_3 \cdot 10^3 \equiv 12a_3 \mod 19$ ou também $a_3 \cdot 10^3 \equiv -7a_3 \mod 19$

$a_4 \cdot 10^4 \equiv 6a_4 \mod 19$ ou também $a_4 \cdot 10^4 \equiv -13a_4 \mod 19$

$a_5 \cdot 10^5 \equiv 3a_5 \mod 19$ ou também $a_5 \cdot 10^5 \equiv -16a_5 \mod 19$

$a_6 \cdot 10^6 \equiv 11a_6 \mod 19$ ou também $a_6 \cdot 10^6 \equiv -8a_6 \mod 19$

$a_7 \cdot 10^7 \equiv 15a_7 \mod 19$ ou também $a_7 \cdot 10^7 \equiv -4a_7 \mod 19$

$a_8 \cdot 10^8 \equiv 17a_8 \mod 19$ ou também $a_8 \cdot 10^8 \equiv -2a_8 \mod 19$

$a_9 \cdot 10^9 \equiv 8a_9 \mod 19$ ou também $a_9 \cdot 10^9 \equiv -1a_9 \mod 19$

$a_{10} \cdot 10^{10} \equiv 9a_{10} \mod 19$ ou também $a_{10} \cdot 10^{10} \equiv -10a_{10} \mod 19$

$\vdots$

Assim por diante, até 10^n.

Assim um número é divisível por 19, quando $(a_0 + 10a_1 + 5a_2 + 12a_3 + 6a_4 + 3a_5 + 11a_6 + 15a_7 + 17a_8) - (a_9 + 10a_10 + 5a_11 + 12a_12 + 6a_13 + 3a_14 + 11a_15 + 15a_16 + 17a_17) +$ ... for divisível por 19. ■

Exemplo 6.14 *Dado 4826, verifique se é divisível por 19.*

Usando o primeiro critério de divisibilidade por 19, temos $482 + 2 \cdot 6 = 494$, aplicando o critério neste novo número, $49 + 2 \cdot 4 = 57$, $5 + 2 \cdot 7 = 19$ e $19 \mid 19$, portanto 4826 é divisível por 19.

Exemplo 6.15 *Dado o número 9348570798, verifique se é divisível por 19.*

Usando o segundo critério, temos $(8 + 10 \cdot 9 + 5 \cdot 7 + 12 \cdot 0 + 6 \cdot 7 + 3 \cdot 5 + 11 \cdot 8 + 15 \cdot 4 + 17 \cdot 3) - (9) = (8 + 90 + 35 + 0 + 42 + 15 + 88 + 60 + 51) - (9) = 389 - 9 = 380$. Aplicando o primeiro critério em 380 e, obtemos $38 + 2 \cdot 0 = 38 = 19 \cdot 2$, isto é, 380 é divisível por 19 e, portanto, 9348570798 é divisível por 19.

6.9 Critério de divisibilidade por 23

Um número é divisível por 23 quando o héptuplo (7 vezes) o algarismo da unidade somado ao número formado pelos outros algarismos, for um número divisível por 23.

Iremos demonstrar usando divisibilidade.

Demonstração. Suponhamos um $a_n a_{n-1} ... a_2 a_1 a_0$ que seja divisível por 23, isto é, $a_n a_{n-1} ... a_2 a_1 a_0 = 23q$ com $q \in \mathbb{Z}$. Escrevendo este número em potência de 10, temos $10^n a_n + 10^{n-1} a_{n-1} + ... + 10^2 a_2 + 10a_1 + a_0 = 23q \Rightarrow 10^n a_n + 10^{n-1} a_{n-1} + ... + 10^2 a_2 + 10a_1 + 70a_0 =$

$23q + 69a_0 \Rightarrow 10(10^{n-1}a_n + 10^{n-2}a_{n-1} + ... + 10a_2 + a_1 + 7a_0) = 23(q + 7a_0)$. Sabemos que $10^{n-1}a_n + 10^{n-2}a_{n-1} + ... + 10a_2 + a_1 + 7a_0 = a_n a_{n-1}...a_3 a_2 a_1 + 7a_0$. Como $23 \nmid 10$ então $23 \mid a_n a_{n-1}...a_3 a_2 a_1 + 7a_0$, provando o critério. ■

Agora, usando aritmética dos restos, teremos um outro critério de divisibilidade por 23.

Demonstração. Vejamos o resto da divisão das potências de 10, por 23.

$10^0 \equiv 1 \mod 23$

$10^1 \equiv 10 \mod 23$ ou também $10^1 \equiv -13 \mod 23$

$10^2 \equiv 8 \mod 23$ ou também $10^2 \equiv -15 \mod 23$

$10^3 \equiv 11 \mod 23$ ou também $10^3 \equiv -12 \mod 23$

$10^4 \equiv 18 \mod 23$ ou também $10^4 \equiv -5 \mod 23$

$10^5 \equiv 19 \mod 23$ ou também $10^5 \equiv -4 \mod 23$

$10^6 \equiv 6 \mod 23$ ou também $10^6 \equiv -17 \mod 23$

$10^7 \equiv 14 \mod 23$ ou também $10^7 \equiv -9 \mod 23$

$10^8 \equiv 2 \mod 23$ ou também $10^8 \equiv -21 \mod 23$

$10^9 \equiv 20 \mod 23$ ou também $10^9 \equiv -3 \mod 23$

$10^{10} \equiv 16 \mod 23$ ou também $10^{10} \equiv -7 \mod 23$

$10^{11} \equiv 22 \mod 23$ ou também $10^{11} \equiv -1 \mod 23$

$10^{12} \equiv 13 \mod 23$ ou também $10^{12} \equiv -10 \mod 23$

$\vdots$

Assim por diante, até 10^n.

$a_0 \cdot 10^0 \equiv a_0 \mod 23$

$a_1 \cdot 10^1 \equiv 10a_1 \mod 23$ ou também $a_1 \cdot 10^1 \equiv -13a_1 \mod 23$

$a_2 \cdot 10^2 \equiv 8a_2 \mod 23$ ou também $a_2 \cdot 10^2 \equiv -15a_2 \mod 23$

$a_3 \cdot 10^3 \equiv 11a_3 \mod 23$ ou também $a_3 \cdot 10^3 \equiv -12a_3 \mod 23$

$a_4 \cdot 10^4 \equiv 18a_4 \mod 23$ ou também $a_4 \cdot 10^4 \equiv -5a_4 \mod 23$

$a_5 \cdot 10^5 \equiv 19a_5 \mod 23$ ou também $a_5 \cdot 10^5 \equiv -4a_5 \mod 23$

$a_6 \cdot 10^6 \equiv 6a_6 \mod 23$ ou também $a_6 \cdot 10^6 \equiv -17a_6 \mod 23$

$a_7 \cdot 10^7 \equiv 14a_7 \mod 23$ ou também $a_7 \cdot 10^7 \equiv -9a_7 \mod 23$

$a_8 \cdot 10^8 \equiv 2a_8 \mod 23$ ou também $a_8 \cdot 10^8 \equiv -21a_8 \mod 23$

$a_9 \cdot 10^9 \equiv 20a_9 \mod 23$ ou também $a_9 \cdot 10^9 \equiv -3a_9 \mod 23$

$a_{10} \cdot 10^{10} \equiv 16a_{10} \mod 23$ ou também $a_{10} \cdot 10^{10} \equiv -7a_{10} \mod 23$

$a_{11} \cdot 10^{11} \equiv 22a_{11} \mod 23$ ou também $a_{11} \cdot 10^{11} \equiv -a_{11} \mod 23$

$a_{12} \cdot 10^{12} \equiv 13a_{12} \mod 23$ ou também $a_{12} \cdot 10^{12} \equiv -10a_{12} \mod 23$

$\vdots$

Assim por diante, até 10^n.

Sendo assim, um número é divisível por 23 quando $(a_0 + 10a_1 + 8a_2 + 11a_3 + 18a_4 + 19a_5 + 6a_6 + 14a_7 + 2a_8 + 20a_9 + 16a_{10}) - (a_{11} + 10a_{12} + 8a_{13} + 11a_{14} + 18a_{15} + 19a_{16} + 6a_{17} + 14a_{18} + 2a_{19} + 20a_{20} + 16a_{21}) + ...$ for divisível por 23. ■

Exemplo 6.16 *Mostre que 2829 é divisível por 23.*

Usando o primeiro critério temos $282 + 7 \cdot 9 = 345$; $34 + 7 \cdot 5 = 69$ e $69 = 23 \cdot 3$, isto é, $23 \mid 69$ e, portanto 2829 é divisível por 23.

Exemplo 6.17 *Mostre que o número 136876471597 é divisível por 23.*

Usando o segundo critério de divisibilidade, temos $(7+10\cdot9+8\cdot5+11\cdot1+18\cdot7+19\cdot4+6\cdot6+14\cdot7+2\cdot8+20\cdot6+16\cdot3)-(1) = (7+90+40+11+126+76+36+98+16+120+48)-1 = 668-1 = 667$, aí aplicando o primeiro critério, temos $66+7\cdot7 = 115$, aplicamos novamente, $11 + 7 \cdot 5 = 46$, como $23 \mid 46$, $23 \mid 667$ e, portanto, 136876471597 é divisível por 23.

6.10 Critério de divisibilidade por 29

Um número é divisível por 29 quando o tripo do algarismo da unidade somado ao número formado pelos outros algarismos, for um número divisível por 29.

Iremos demonstrar usando divisibilidade.

Demonstração. Suponhamos um $a_n a_{n-1}...a_2a_1a_0$ que seja divisível por 29, isto é, $a_n a_{n-1}...a_2a_1a_0 = 29q$ com $q \in \mathbb{Z}$. Escrevendo este número em potência de 10, temos $10^n a_n + 10^{n-1}a_{n-1} +$

$... + 10^2a_2 + 10a_1 + a_0 = 29q \Rightarrow 10^n a_n + 10^{n-1}a_{n-1} + ... + 10^2a_2 + 10a_1 + 30a_0 = 29q + 29a_0 \Rightarrow 10(10^{n-1}a_n + 10^{n-2}a_{n-1} + ... + 10a_2 + a_1 + 3a_0) = 29(q + a_0)$. Sabemos que $10^{n-1}a_n + 10^{n-2}a_{n-1} + ... + 10a_2 + a_1 + 3a_0 = a_n a_{n-1}...a_3a_2a_1 + 3a_0$. Como $29 \nmid 10$ então $29 \mid a_n a_{n-1}...a_3a_2a_1 + 3a_0$, provando o critério. ■

Agora, usando aritmética dos restos, teremos um outro critério de divisibilidade por 29.

Demonstração. Vejamos o resto da divisão das potências de 10, por 29.

$10^0 \equiv 1 \mod 29$

$10^1 \equiv 10 \mod 29$ ou também $10^1 \equiv -19 \mod 29$

$10^2 \equiv 13 \mod 29$ ou também $10^2 \equiv -16 \mod 29$

$10^3 \equiv 14 \mod 29$ ou também $10^3 \equiv -15 \mod 29$

$10^4 \equiv 24 \mod 29$ ou também $10^4 \equiv -5 \mod 29$

$10^5 \equiv 8 \mod 29$ ou também $10^5 \equiv -21 \mod 29$

$10^6 \equiv 22 \mod 29$ ou também $10^6 \equiv -7 \mod 29$

$10^7 \equiv 17 \mod 29$ ou também $10^7 \equiv -12 \mod 29$

$10^8 \equiv 25 \mod 29$ ou também $10^8 \equiv -4 \mod 29$

$10^9 \equiv 18 \mod 29$ ou também $10^9 \equiv -11 \mod 29$

$10^{10} \equiv 6 \mod 29$ ou também $10^{10} \equiv -23 \mod 29$

$10^{11} \equiv 2 \mod 29$ ou também $10^{11} \equiv -27 \mod 29$

$10^{12} \equiv 20 \mod 29$ ou também $10^{12} \equiv -9 \mod 29$

$10^{13} \equiv 26 \mod 29$ ou também $10^{13} \equiv -3 \mod 29$

$10^{14} \equiv 28 \mod 29$ ou também $10^{14} \equiv -1 \mod 29$

$10^{15} \equiv 19 \mod 29$ ou também $10^{15} \equiv -10 \mod 29$

$\vdots$

Assim por diante, até 10^n.

$a_0 \cdot 10^0 \equiv a_0 \mod 29$

$a_1 \cdot 10^1 \equiv 10a_1 \mod 29$ ou também $a_1 \cdot 10^1 \equiv -19a_1 \mod 29$

$a_2 \cdot 10^2 \equiv 13a_2 \mod 29$ ou também $a_2 \cdot 10^2 \equiv -16a_2 \mod 29$

$a_3 \cdot 10^3 \equiv 14a_3 \mod 29$ ou também $a_3 \cdot 10^3 \equiv -15a_3 \mod 29$

$a_4 \cdot 10^4 \equiv 24a_4 \mod 29$ ou também $a_4 \cdot 10^4 \equiv -5a_4 \mod 29$

$a_5 \cdot 10^5 \equiv 8a_5 \mod 29$ ou também $a_5 \cdot 10^5 \equiv -21a_5 \mod 29$

$a_6 \cdot 10^6 \equiv 22a_6 \mod 29$ ou também $a_6 \cdot 10^6 \equiv -7a_6 \mod 29$

$a_7 \cdot 10^7 \equiv 17a_7 \mod 29$ ou também $a_7 \cdot 10^7 \equiv -12a_7 \mod 29$

$a_8 \cdot 10^8 \equiv 25a_8 \mod 29$ ou também $a_8 \cdot 10^8 \equiv -4a_8 \mod 29$

$a_9 \cdot 10^9 \equiv 18a_9 \mod 29$ ou também $a_9 \cdot 10^9 \equiv -11a_9 \mod 29$

$a_{10} \cdot 10^{10} \equiv 6a_{10} \mod 29$ ou também $a_{10} \cdot 10^{10} \equiv -23a_{10} \mod 29$

$a_{11} \cdot 10^{11} \equiv 2a_{11} \mod 29$ ou também $a_{11} \cdot 10^{11} \equiv -27a_{11} \mod 29$

$a_{12} \cdot 10^{12} \equiv 20a_{12} \mod 29$ ou também $a_{12} \cdot 10^{12} \equiv -9a_{12} \mod 29$

$a_{13} \cdot 10^{13} \equiv 26a_{13} \mod 29$ ou também $a_{13} \cdot 10^{13} \equiv -3a_{13} \mod 29$

$a_{14} \cdot 10^{14} \equiv 28a_{14} \mod 29$ ou também $a_{14} \cdot 10^{14} \equiv -a_{14} \mod 29$

$a_{15} \cdot 10^{15} \equiv 19a_{15} \mod 29$ ou também $a_{15} \cdot 10^{15} \equiv -10a_{15} \mod 29$

$\vdots$

Assim por diante, até 10^n.

Sendo assim, um número é divisível por 29 quando, $(a_0+10a_1+13a_2+14a_3+24a_4+8a_5+22a_6+17a_7+25a_8+18a_9+6a_{10}+2a_{11}+20a_{12}+26a_{13})-(a_{14}+10a_{15}+13a_{16}+14a_{17}+24a_{18}+8a_{19}+22a_{20}+17a_{21}+25a_{22}+18a_{23}+6a_{24}+2a_{25}+20a_{26}+26a_{27})+...-$ for divisível por 29. ■

Exemplo 6.18 *Mostre que 54195620176650 é divisível por 29.*

Usando o segundo critério, temos $(0+10\cdot5+13\cdot6+14\cdot6+24\cdot7+8\cdot1+22\cdot0+17\cdot2+25\cdot6+18\cdot5+6\cdot9+2\cdot1+20\cdot4+26\cdot5) = (0+50+78+84+168+8+0+34+150+90+54+2+80+130) = 928$, usando o primeiro critério, obtemos $92+3\cdot8 = 116$, aplicando novamente $11+3\cdot6 = 29$ então $29 \mid 928$ e, portando, 54195620176650 é divisível por 29.

6.11 Critério de divisibilidade por 31

Um número é divisível por 31 quando o tripo do algarismo da unidade subtraído do

número formado pelos outros algarismos, for um número divisível por 31.

Iremos demonstrar usando divisibilidade.

Demonstração. Suponhamos um $a_n a_{n-1}...a_2 a_1 a_0$ que seja divisível por 31, isto é, $a_n a_{n-1}...a_2 a_1 a_0 = 31q$ com $q \in \mathbb{Z}$. Escrevendo este número em potência de 10, temos $10^n a_n + 10^{n-1} a_{n-1} + ... + 10^2 a_2 + 10a_1 + a_0 = 31q \Rightarrow 10^n a_n + 10^{n-1} a_{n-1} + ... + 10^2 a_2 + 10a_1 - 30a_0 = 31q - 31a_0 \Rightarrow 10(10^{n-1} a_n + 10^{n-2} a_{n-1} + ... + 10a_2 + a_1 - 3a_0) = 31(q - a_0)$. Sabemos que $10^{n-1} a_n + 10^{n-2} a_{n-1} + ... + 10a_2 + a_1 - 3a_0 = a_n a_{n-1}...a_3 a_2 a_1 - 3a_0$. Como $31 \nmid 10$ então $31 \mid a_n a_{n-1}...a_3 a_2 a_1 - 3a_0$, provando o critério. ■

Agora, usando aritmética dos restos, teremos um outro critério de divisibilidade por 31.

Demonstração. Vejamos o resto da divisão das potências de 10, por 31.

$10^0 \equiv 1 \mod 31$

$10^1 \equiv 10 \mod 31$ ou também $10^1 \equiv -21 \mod 31$

$10^2 \equiv 7 \mod 31$ ou também $10^2 \equiv -24 \mod 31$

$10^3 \equiv 8 \mod 31$ ou também $10^3 \equiv -23 \mod 31$

$10^4 \equiv 18 \mod 31$ ou também $10^4 \equiv -13 \mod 31$

$10^5 \equiv 25 \mod 31$ ou também $10^5 \equiv -6 \mod 31$

$10^6 \equiv 2 \mod 31$ ou também $10^6 \equiv -29 \mod 31$

$10^7 \equiv 20 \mod 31$ ou também $10^7 \equiv -11 \mod 31$

$10^8 \equiv 14 \mod 31$ ou também $10^8 \equiv -17 \mod 31$

$10^9 \equiv 16 \mod 31$ ou também $10^9 \equiv -15 \mod 31$

$10^{10} \equiv 5 \mod 31$ ou também $10^{10} \equiv -26 \mod 31$

$10^{11} \equiv 19 \mod 31$ ou também $10^{11} \equiv -12 \mod 31$

$10^{12} \equiv 4 \mod 31$ ou também $10^{12} \equiv -27 \mod 31$

$10^{13} \equiv 9 \mod 31$ ou também $10^{13} \equiv -22 \mod 31$

$10^{14} \equiv 18 \mod 31$ ou também $10^{14} \equiv -13 \mod 31$

$10^{15} \equiv 1 \mod 31$ ou também $10^{15} \equiv -30 \mod 31$

$10^{16} \equiv 10 \mod 31$ ou também $10^{16} \equiv -21 \mod 31$

$10^{17} \equiv 7 \mod 31$ ou também $10^{17} \equiv -24 \mod 31$

$\vdots$

Assim por diante, até 10^n.

$a_0 \cdot 10^0 \equiv a_0 \mod 31$

$a_1 \cdot 10^1 \equiv 10a_1 \mod 31$ ou também $a_1 \cdot 10^1 \equiv -21a_1 \mod 31$

$a_2 \cdot 10^2 \equiv 7a_2 \mod 31$ ou também $a_2 \cdot 10^2 \equiv -24a_2 \mod 31$

$a_3 \cdot 10^3 \equiv 8a_3 \mod 31$ ou também $a_3 \cdot 10^3 \equiv -23a_3 \mod 31$

$a_4 \cdot 10^4 \equiv 18a_4 \mod 31$ ou também $a_4 \cdot 10^4 \equiv -13a_4 \mod 31$

$a_5 \cdot 10^5 \equiv 25a_5 \mod 31$ ou também $a_5 \cdot 10^5 \equiv -6a_5 \mod 31$

$a_6 \cdot 10^6 \equiv 2a_6 \mod 31$ ou também $a_6 \cdot 10^6 \equiv -29a_6 \mod 31$

$a_7 \cdot 10^7 \equiv 20a_7 \mod 31$ ou também $a_7 \cdot 10^7 \equiv -11a_7 \mod 31$

$a_8 \cdot 10^8 \equiv 14a_8 \mod 31$ ou também $a_8 \cdot 10^8 \equiv -17a_8 \mod 31$

$a_9 \cdot 10^9 \equiv 16a_9 \mod 31$ ou também $a_9 \cdot 10^9 \equiv -15a_9 \mod 31$

$a_{10} \cdot 10^{10} \equiv 5a_{10} \mod 31$ ou também $a_{10} \cdot 10^{10} \equiv -26a_{10} \mod 31$

$a_{11} \cdot 10^{11} \equiv 19a_{11} \mod 31$ ou também $a_{11} \cdot 10^{11} \equiv -12a_{11} \mod 31$

$a_{12} \cdot 10^{12} \equiv 4a_{12} \mod 31$ ou também $a_{12} \cdot 10^{12} \equiv -27a_{12} \mod 31$

$a_{13} \cdot 10^{13} \equiv 96a_{13} \mod 31$ ou também $a_{13} \cdot 10^{13} \equiv -22a_{13} \mod 31$

$a_{14} \cdot 10^{14} \equiv 18a_{14} \mod 31$ ou também $a_{14} \cdot 10^{14} \equiv -13a_{14} \mod 31$

$a_{15} \cdot 10^{15} \equiv a_{15} \mod 31$ ou também $a_{15} \cdot 10^{15} \equiv -31a_{15} \mod 31$

$a_{16} \cdot 10^{16} \equiv 10a_{16} \mod 31$ ou também $a_{16} \cdot 10^{16} \equiv -21a_{16} \mod 31$

$a_{17} \cdot 10^{17} \equiv 7a_{17} \mod 31$ ou também $a_{17} \cdot 10^{17} \equiv -24a_{17} \mod 31$

$\vdots$

Assim por diante, até 10^n.

Isto é, um número é divisível por 31, quando $a_0 + 10a_1 + 7a_2 + 8a_3 + 18a_4 + 25a_5 + 2a_6 + 20a_7 + 14a_8 + 16a_9 + 5a_{10} + 19a_{11} + 4a_{12} + 9a_{13} + 18a_{14} + a_{15} + 10a_{16} + 7a_{17} + ...$ for divisível por 31. ■

Exemplo 6.19 *Mostre que 38274397538751 é divisível por 31.*

Usaremos, primeiramente, o segundo critério. Então $31 \mid 38274397538751$ se $1 + 10 \cdot 5 + 7 \cdot 7 + 8 \cdot 8 + 18 \cdot 3 + 25 \cdot 5 + 2 \cdot 7 + 20 \cdot 9 + 14 \cdot 3 + 16 \cdot 4 + 5 \cdot 7 + 19 \cdot 2 + 4 \cdot 8 + 9 \cdot 3 =$

$1+50+49+64+54+125+14+180+42+64+35+38+32+27 = 775$, aplicando o primeiro critério, temos $77 - 3 \cdot 5 = 62$ como $31 \mid 62$ então $31 \mid 775$ e, portanto 38274397538751 é divisível por 31.

6.12 Critério de divisibilidade por 37

Um número é divisível por 37 quando o algarismo da unidade multiplicado por 11 subtraído do número formado pelos outros algarismos, for um número divisível por 37.

Iremos demonstrar usando divisibilidade.

Demonstração. Suponhamos um $a_n a_{n-1}...a_2 a_1 a_0$ que seja divisível por 37, isto é, $a_n a_{n-1}...a_2 a_1 a_0 = 37q$ com $q \in \mathbb{Z}$. Escrevendo este número em potência de 10, temos $10^n a_n + 10^{n-1} a_{n-1} + ... + 10^2 a_2 + 10a_1 + a_0 = 37q \Rightarrow 10^n a_n + 10^{n-1} a_{n-1} + ... + 10^2 a_2 + 10a_1 - 110a_0 = 37q - 111a_0 \Rightarrow 10(10^{n-1} a_n + 10^{n-2} a_{n-1} + ... + 10a_2 + a_1 - 11a_0) = 37(q - 11a_0)$. Sabemos que $10^{n-1} a_n + 10^{n-2} a_{n-1} + ... + 10a_2 + a_1 - 11a_0 = a_n a_{n-1}...a_3 a_2 a_1 - 11a_0$. Como $37 \nmid 10$ então $37 \mid a_n a_{n-1}...a_3 a_2 a_1 - 11a_0$, provando o critério. ■

Agora, usando aritmética dos restos, teremos um outro critério de divisibilidade por 37.

Demonstração. Vejamos o resto da divisão das potências de 10, por 37.

$10^0 \equiv 1 \mod 37$

$10^1 \equiv 10 \mod 37$ ou também $10^1 \equiv -27 \mod 37$

$10^2 \equiv 26 \mod 37$ ou também $10^2 \equiv -11 \mod 37$

$10^3 \equiv 1 \mod 37$ ou também $10^3 \equiv -36 \mod 37$

$10^4 \equiv 10 \mod 37$ ou também $10^4 \equiv -27 \mod 37$

$10^5 \equiv 26 \mod 37$ ou também $10^5 \equiv -11 \mod 37$

$10^6 \equiv 1 \mod 37$ ou também $10^6 \equiv -36 \mod 37$

Assim por diante, até 10^n.

$a_0 \cdot 10^0 \equiv a_0 \mod 37$

$a_1 \cdot 10^1 \equiv 10a_1 \mod 37$ ou também $a_1 \cdot 10^1 \equiv -27a_1 \mod 37$

$a_2 \cdot 10^2 \equiv 26a_2 \mod 37$ ou também $a_2 \cdot 10^2 \equiv -11a_2 \mod 37$

$a_3 \cdot 10^3 \equiv a_3 \mod 37$ ou também $a_3 \cdot 10^3 \equiv -36a_3 \mod 37$

$a_4 \cdot 10^4 \equiv 10a_4 \mod 37$ ou também $a_4 \cdot 10^4 \equiv -27a_4 \mod 37$

$a_5 \cdot 10^5 \equiv 26a_5 \mod 37$ ou também $a_5 \cdot 10^5 \equiv -11a_5 \mod 37$

$a_6 \cdot 10^6 \equiv a_6 \mod 37$ ou também $a_6 \cdot 10^6 \equiv -36a_6 \mod 37$

$\vdots$Assim por diante, até 10^n.

Ou seja, um número é divisível por 37, quando: $(a_0 + a_3 + a_6 + ...) + 10(a_1 + a_4 + a_7 + ...) + 26(a_2 + a_5 + a_8 + ...)$ for divisível por divisível por 37. ■

Exemplo 6.20 *Mostre que 464272152 é divisível por 37.*

Usando o segundo critério, temos $(2 + 2 + 4) + 10 \cdot (5 + 7 + 6) + 26 \cdot (1 + 2 + 4) = 8 + 180 + 182 = 370$, e assim, usando o primeiro critério, obtemos $37 - 11 \cdot 0 = 37$ e $37 \mid 37$, logo $37 \mid 370$ e, portanto, 464272152 é divisível por 37.

6.13 Critério de divisibilidade por 41

Um número é divisível por 41 quando o algarismo da unidade multiplicado por 4 e subtraído do número formado pelos outros algarismos, for um número divisível por 41.

Iremos demonstrar usando divisibilidade.

Demonstração. Suponhamos um $a_n a_{n-1}...a_2 a_1 a_0$ que seja divisível por 41, isto é, $a_n a_{n-1}...a_2 a_1 a_0 = 41q$ com $q \in \mathbb{Z}$. Escrevendo este número em potência de 10, temos $10^n a_n + 10^{n-1} a_{n-1} + ... + 10^2 a_2 + 10a_1 + a_0 = 41q \Rightarrow 10^n a_n + 10^{n-1} a_{n-1} + ... + 10^2 a_2 + 10a_1 - 40a_0 = 41q - 41a_0 \Rightarrow 10(10^{n-1} a_n + 10^{n-2} a_{n-1} + ... + 10a_2 + a_1 - 4a_0) = 41(q - a_0)$. Sabemos que $10^{n-1} a_n + 10^{n-2} a_{n-1} + ... + 10a_2 + a_1 - 4a_0 = a_n a_{n-1}...a_3 a_2 a_1 - 4a_0$. Como $41 \nmid 10$ então $41 \mid a_n a_{n-1}...a_3 a_2 a_1 - 4a_0$, provando o critério. ■

Agora, usando aritmética dos restos, teremos um outro critério de divisibilidade por 41.

Demonstração. Veja os restos da divisão das potência de 10 por 41.

$10^0 \equiv 1 \mod 41$

$10^1 \equiv 10 \mod 41$ ou também $10^1 \equiv -31 \mod 41$

$10^2 \equiv 18 \mod 41$ ou também $10^2 \equiv -23 \mod 41$

$10^3 \equiv 16 \mod 41$ ou também $10^3 \equiv -25 \mod 41$

$10^4 \equiv 37 \mod 41$ ou também $10^4 \equiv -4 \mod 41$

$10^5 \equiv 1 \mod 41$ ou também $10^5 \equiv -40 \mod 41$

$10^6 \equiv 10 \mod 41$ ou também $10^6 \equiv -31 \mod 41$

$10^7 \equiv 18 \mod 41$ ou também $10^7 \equiv -23 \mod 41$

$10^8 \equiv 16 \mod 41$ ou também $10^8 \equiv -25 \mod 41$

Assim por diante, até 10^n.

$a_0 \cdot 10^0 \equiv a_0 \mod 41$

$a_1 \cdot 10^1 \equiv 10a_1 \mod 41$ ou também $a_1 \cdot 10^1 \equiv -31a_1 \mod 41$

$a_2 \cdot 10^2 \equiv 18a_2 \mod 41$ ou também $a_2 \cdot 10^2 \equiv -23a_2 \mod 41$

$a_3 \cdot 10^3 \equiv 16a_3 \mod 41$ ou também $a_3 \cdot 10^3 \equiv -25a_3 \mod 41$

$a_4 \cdot 10^4 \equiv 37a_4 \mod 41$ ou também $a_4 \cdot 10^4 \equiv -4a_4 \mod 41$

$a_5 \cdot 10^5 \equiv a_5 \mod 41$ ou também $a_5 \cdot 10^5 \equiv -40a_5 \mod 41$

$a_6 \cdot 10^6 \equiv 10a_6 \mod 41$ ou também $a_6 \cdot 10^6 \equiv -31a_6 \mod 41$

$a_7 \cdot 10^7 \equiv 18a_7 \mod 41$ ou também $a_7 \cdot 10^7 \equiv -23a_7 \mod 41$

$a_8 \cdot 10^8 \equiv 16a_8 \mod 41$ ou também $a_8 \cdot 10^8 \equiv -25a_8 \mod 41$

Assim por diante, até 10^n.

Ou seja, um número é divisível por 41 quando $(a_0 + a_5 + a_{10} + ...) + 10(a_1 + a_6 + a_{11} + ...) + 18(a_2 + a_7 + a_{12} + ...) + 16(a_3 + a_8 + a_{13} + ...) + 37(a_4 + a_9 + a_{14} + ...)$ for divisível por 41. ■

Exemplo 6.21 *Mostre que o número 506985080242 é divisível por 41.*

Usando o segundo critério de divisibilidade, temos $(2+0+0)+10(4+5+5)+18(2+8)+16(0+9)+37(8+6) = 2+140+180+144+518 = 984$, usando agora o segundo critério, obtemos $98 - 4 \cdot 4 = 82$ e, $41 \mid 82$, logo $41 \mid 984$ e, portanto, 506985080242 é divisível por 41.

Capítulo 7

CURIOSIDADES

Não se consegue contar as inúmeras aplicações de aritmética modular que existem em nosso dia-a-dia. Os Sistemas de Identificação, onde mais se encontra aritmética modular, é um processo que atende desde produtos até documentos.

Um dos casos do cotidiano a ser apresentado, é o próprio documento pessoal que todos carregamos, o CPF (Cadastro de Pessoa Física). Este documento contém um número de 11 dígitos, sendo os dois últimos chamados de dígitos de controle ou verificação. Eles têm a função de evitar fraudes e enganos. São encontrados em função dos 9 primeiros, seguindo a seguinte regra:

Sejam os x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 e x_9 os primeiros dígitos. Para encontrar os dígitos de controle devemos multiplicar todos estes nove primeiros dígitos respectivamente por 1, 2, 3, 4, 5, 6, 7, 8 e 9, e somar os resultados (a). O décimo dígito, primeiro de controle, x_{10} será o resto da divisão de a por 11. Caso o resto seja 10, usará o dígito 0 em x_{10}. Repita os passos para encontrar o próximo dígito de controle, mas agora, usando os 10 dígitos que se tem, isto é, fazer o produto dos x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9 e x_{10}, respectivamente por 0, 1, 2, 3, 4, 5, 6, 7, 8 e 9 e soma os resultados (a_1), sendo assim, o décimo primeiro dígito x_{11} será o resto da divisão de a_1 por 11, no caso particular de o resto ser 10, $x_{11} = 0$.

Resumindo, os dígitos de controle do CPF, são encontrados por congruência $mod 11$.

Onde estas congruências, são especificadas por $a \equiv x_{10} mod 11$ e $a_1 \equiv x_{11} mod 11$, lembrando das execões citadas.

Existem outras aplicações nos Sistemas de Identificação, que utilizam da Aritmética Modular: *os códigos de barras* é um exemplo que cria um sistema simples e preciso, independente da língua, utilizando apenas números e matemática.

Há outras aplicações, que não necessariamente esteja dentro do campo de Sistema de Identificação, um deles é a Criptografia. A Criptografia tem um propósito de enviar mensagens a um destinatário final, sem que intermediários consigam interpretá-las. Há vários níveis de complexidade para produzir mensagens criptografadas, mas mostraremos um caso simples que aplica Aritmética Modular. Por exemplo, consegue ler o que está escrito abaixo?

PDXHPDXLFD QD FULSXRJUDILD

Sem uma chave/senha que faça a correspondências das letras escritas com as letras corretas, fica difícil (quase impossível) de descobrir. Poderíamos tentar até conseguir, mas seria uma tarefa cansativa. Portanto, conhecendo a chave de acesso e o alfabeto, torna-se muito simples ler a mensagem. A senha de acesso para a mensagem acima é dada por:

posição da letra utilizada = posição da letra inicial + 3 posições

Posição das letras	Letras
1º	A
2º	B
3º	C
4º	D
5º	E
6º	F
7º	G
8º	H
9º	I
10º	J
11º	K
12º	L
13º	M
14º	N
15º	O
16º	P
17º	Q
18º	R
19º	S
20º	T
21º	U
22º	V
23º	X
24º	W
25º	Y
26º	Z

Portanto, a mensagem correta é:

MATEMATICA NA CRIPTOGRAFIA

Aonde está a aplicação de Aritmética Modular? O processo acima, consiste em transformar a letra apresentada pela letra real da mensagem, isto é

$L - 3 \equiv L_R \mod 26$, onde L é a letra apresentada e L_R é a letra real

Capítulo 8

CONCLUSÃO

Na matemática, como em qualquer outra coisa na vida, devemos ser claros ao mostrar novidades à alguém. Por isto, ao desenvolvermos este trabalho trouxemos uma bagagem considerável, de conceitos e definições, para tonar o mais claro possível a leitura do mesmo. O resultado alcançado pode não ser tão simples quanto os ensinados nas escolas básicas, mas é uma forma nova de apresenta-los, explorando por outra área do conteúdo. Além do trabalho, atingir a proposta de ser uma possível ferramenta de estudos para trabalhos futuros, melhorou meu conhecimento na área.

Referências Bibliográficas

[1] HEFEZ, A. **Aritmética**. SBM. Rio de Janeiro, 2013.

[2] KLEIN, F. **Critérios não clássicos de divisibilidade**. Florianópolis, 2007.

[3] DOMINGUES, Hygino H. **Algebra Moderna**. Editora Atual Ltda. 4ª Edição. São Paulo, 2003.

[4] KERSNOWSKY, Iury **A Aritmética Modular como Ferramenta para as Séries Finais do Ensino Fundamental**. Edição. Rio de Janeiro, 2013.

[5] SANTOS, José Plínio de O. **Introdução à Teoria dos Números**. Rio de Janeiro, 1998.