INSTITUTO DE MATEMÁTICA PURA E APLICADA
MESTRADO PROFISSIONAL EM MATEMÁTICA
PROFMAT-SBM

RINALDO DINIZ COSTA

CRITÉRIO DE DIVISIBILIDADE NO ENSINO BÁSICO

RIO DE JANEIRO
2014

RINALDO DINIZ COSTA

CRITÉRIO DE DIVISIBILIDADE
NO ENSINO BÁSICO

Trabalho de conclusão de curso apresentado ao Programa de Mestrado Profissional em Matemática do Instituto de Matemática Pura e Aplicada (PROFMAT-SBM) para obtenção do grau de Mestre em Matemática.

Orientador: Carlos Gustavo Moreira

RIO DE JANEIRO
2014

AGRADECIMENTO

Agradeço a **Jesus de Nazaré** pela **Sua Presença** em minha vida trazendo todo estímulo suficiente para apresentação deste trabalho.

Agradeço a minha esposa **Marize Fernandes Costa** pela **minha matrícula** no **Impa** que deu origem a este trabalho.

Agradeço aos **Professores do Impa** sempre pacientes e dedicados comigo e com meus colegas.

Agradeço ao **Professor Carlos Gustavo Moreira (Gugu)** pela orientação eficaz e estimuladora que recebi.

Agradeço aos **meus colegas**, sempre dispostos para ajudar.

Agradeço a cada **aluno** que sempre reage muito bem toda vez que apresento este "**Critério Único de Divisibilidade**".

Muito obrigado!

SUMÁRIO

1. Resumo

2 **Introdução.**

2.1 **Por que ensinar Matemática?**

2.2 **Motivação para a escolha deste trabalho.**

2 E**xperiência com este trabalho em sala de aula.**

3 **Objetivos**

4 **Metodologia/Fundamentação Teórica**

5 **Bibliografia**

1. Resumo

Neste trabalho apresentamos um critério de divisibilidade geral, que fornece de um modo prático o resto da divisão de qualquer inteiro positivo por um dado inteiro positivo n, baseado nos restos das divisões das potências consecutivas de 10 por n. Discutimos também a periodicidade dessa sequência de restos das divisões das potências consecutivas de 10 por n.

Apresentamos ainda diversos exercícios e problemas resolvidos que usam as ideias e métodos deste trabalho.

Abstract.

We present a general criterion of divisibility, which provides in a practical way the remainder of the division of any positive integer for a given positive integer n, based on the remainders of the divisions of the consecutive powers of 10 by n. We also discuss the periodicity of this sequence of remainders of the divisions of the consecutive powers of 10 by n. We also present several exercises and problems solved using the ideas and methods of this work.

2. **Introdução**

Com frequência nas turmas preparatórias visando concursos públicos há alunos que perguntam se há algum critério que verifique se um número é ou não múltiplo, por exemplo, de 17; 19; 23; 29; etc. Também perguntam, caso não seja múltiplo qual é o resto apresentado nesta divisão.

Na verdade, o que o aluno está perguntando é “existe algum critério de divisibilidade por 17; 19; 23; 73; etc.”? . Nesta hora se vê em geral a falta de resposta por parte do professor, mesmo que tenha muitos anos de experiência no magistério e podendo até ser um especialista em Aritmética.

Por falta de resposta, o aluno deste segmento, que costuma ser muito interessado, recorre ao “Dr. Google”. Nesta pesquisa encontra algum tipo de resposta

“Um número é divisível por 17 quando o quíntuplo (5 vezes) do último algarismo, subtraído do número que não contém este último algarismo, proporcionar um número divisível por 17. Se o número obtido ainda for grande, repete-se o processo até que se possa verificar a divisão por 17.”

‘’ Um número é divisível por 19 quando (2 vezes) do último algarismo, somado ao número que não contém este último algarismo, proporcionar um número divisível por 19. Se o número obtido ainda for grande, repete-se o processo até que se possa verificar a divisão por 19.”

‘’ Um número é divisível por 23 quando o sétuplo (7 vezes) do último algarismo, somado ao número que não contém este último algarismo, proporcionar um número divisível por 23.Se o número obtido ainda for grande, repete-se o processo até que se possa verificar a divisão por 23.”

“Um número é divisível por 29 quando o triplo (3 vezes) do último algarismo, subtraído do número que não contém este último algarismo, proporcionar um número divisível por 29. Se o número obtido ainda for grande, repete-se o processo até que se possa verificar a divisão por 29.”

Pode-se verificar se o número tivesse grande quantidade de algarismos então haveria necessidade de repetir este processo tantas vezes que este método apresentado talvez se tornasse pouco interessante.

2.1 Por que ensinar Matemática?

Ensinar traz na origem de sua palavra: “insignare; sinal, marcar”. Quem ensina marca. O Magistério é marcante. Para ser ensinado é preciso deixar-se marcar, é preciso querer, pois a mente não alcança aquilo que o coração não deseja.

Dentre as disciplinas apresentadas “*a Matemática é a única em que a geração que chega não desmente o que foi dito pela geração anterior*.”

A Matemática “afina o ouvido” do aluno. Normalmente, ouvem-se coisas que não foram ditas e não se considera aquelas mencionadas, por mais ênfase que se dê ao texto. A Matemática torna o aluno mais atento. É bastante frequente um bom aluno em Matemática ser bom nas outras disciplinas. Porém a recíproca não é verdadeira com a mesma frequência.

Vê-se, muitas vezes, que na reunião de professores de Matemática, em algum momento, surgirá alguém apresentado “um probleminha”, mesmo não sendo a hora e o lugar apropriados. Os parentes dos professores podem testemunhar isto.

Muitos professores de Matemática são inspiração para que seus alunos façam Licenciatura em Matemática. É muito bom ver alguém fazendo aquilo que gosta. Normalmente o aluno verá, na maioria das vezes, pessoas usando a profissão com o propósito maior de levar vantagem e obter vantagens econômicas. Ser professor é privilégio.

“A Matemática oferece-nos um conjunto singular de ferramentas poderosas para compreender e mudar o mundo. Estas ferramentas incluem o raciocínio lógico, técnicas de resolução de problemas, e a capacidade de pensar em termos abstratos.”

A Matemática ensina ao aluno a arte: de argumentar, de contra-argumentar, de buscar e exemplos e contra exemplos, de usar os conectivos de forma certa e oportuna.

2.2 Motivação para escolha deste trabalho.

Um dos objetivos do Ensino Matemático é gerar um cidadão que consiga ser um crítico responsável, então à medida que se possa, deve-se apresentar resposta às perguntas feitas em sala de aula e a existência de critérios de divisibilidade para determinados números, principalmente números primos, é uma destas perguntas frequentes que acabam ficando sem respostas.

As soluções apresentadas pelo "Dr. Google" embora costumem vir sem demonstração e sejam pouco práticas para diversas situações, acabam sendo utilizadas pelo professor, devido à falta de resposta para as perguntas apresentadas em sala de aula quando o assunto é divisibilidade por números não encontrados nos livros didáticos que tratam da matéria.

A falta de um critério que alcance outros números só não é sentida com maior intensidade por não haver exercícios relacionados ao tema propostos nos livros cujos autores não apresentam base teórica para resolvê-los.

Muitas vezes para resolver algum exercício cuja base teórica não é suficiente, é fornecida alguma informação auxiliar, sem a qual o problema não seria resolvido.

A escolha deste trabalho tornará este novo olhar sobre a Divisibilidade mais conhecido, embora já venha sendo feito em sala de aula há algumas décadas.

2. **Experiência com este trabalho em sala de aula.**

Problemas apresentados em sala de aula, cuja solução não surge através dos critérios vistos nos livros didáticos.

Problema 1

O número 111... 111 com o algarismo 1 aparecendo 6n vezes é divisível por 91 ?

Problema 2

O número 111... 111 com o algarismo 1 aparecendo 5n vezes é divisível por 41?

O número 111 ... 111 com o algarismo 1 aparecendo 3n vezes é divisível por 37?

(Extraídos do Livro Problemas Selecionados de Matemática, pag.377. Autor Antonio Luiz Santos, (**Gandhi**))

Problema 4

Qual o valor de n de modo que o número 12345n789 seja divisível por 91?

(Extraído do livro Praticando a Aritmética, pag. 154. Autor: Jose Carlos Admo Lacerda, (**Lacerda**))

Estes exercícios foram propostos em sala, pois estes dois livros fazem parte da biblioteca obrigatória de qualquer aluno que esteja se preparando para os concursos militares. Estes problemas surgiram juntos como um desafio, não só para alunos como também para professores independente da experiência no magistério que cada um possa ter.

Resolução em sala, sob o ponto de vista prático, *como fazer* sem a preocupação teórica que o assunto exige apenas na perspectiva da realização de uma prova de múltipla escolha; mais adiante todo o embasamento matemático será apresentado:

Problema 1

N =	...	1	1	1	1	1	1	1	1	1	1	1	1
r_{91}	...	-9	-10	-1	9	10	1	-9	-10	-1	9	10	1
R_{91}^{N}	...	-9	-10	-1	9	10	1	-9	-10	-1	9	10	1

2ª linha: r_{91} = os restos de $10^{n} \div 91$

3ª linha: os algarismos de N multiplicados pelo número abaixo

R_{91}^{N} = a soma dos valores da 3ª linha, com 6n parcelas = ZERO.

Se soma for igual a algum múltiplo de 91então o número N será múltiplo de 91.

Visivelmente de 6 em 6 a soma vale ZERO logo N é divisível por 91.

Problema 2

N =	...	1	1	1	1	1	1	1	1	1	1	1	1
r_{41}	...	18	10	-4	16	18	10	1	-4	16	18	10	1
R_{41}^{N}									-4	16	18	10	1

Visivelmente de 5 em 5 a soma, com 5n parcelas, vale ZERO logo N é divisível por 41.

Problema 3

N =	...	1	1	1	1	1	1	1	1	1	1	1	1
r_{37}	...	-11	10	1	-11	10	1	-11	10	1	-11	10	1
	...										-11	10	1

Visivelmente de 3 em 3 a soma vale ZERO, e como apresenta 3n parcelas é divisível por 37.

Problema 4

N =					1	2	3	4	5	n	7	8	9
r_{91}					9	10	1	-9	-10	-1	9	10	1
R_{91}^{N}					9	20	3	-36	-50	-n	63	80	9

$$R_{91}^{N} = 184 - 86 - n = M(7) = 0, \pm 91, \pm 182, \ldots$$

$$184 - 86 - n = 91$$

$$98 - n = 91$$

$$n = 7$$

3. Objetivos

Estabelecer de forma bastante clara tanto para alunos como para professores um **Critério Único de Divisibilidade** que possa ser usado para no Ensino Básico, particularmente para os candidatos aos concursos militares no nível de 9º ano.

Para que seja possível estabelecer esta forma de ver a divisibilidade, tanto na prática quanto academicamente, será apresentada base matemática, que tornará este trabalho em uma tese matemática.

No desenvolvimento deste novo olhar surgirá uma maneira bastante simples para provar os critérios já existentes, visto que este trabalho não nega nenhuma afirmação publicada na literatura que trata do tema.

A fundamentação teórica pode ser encontrada no livro **TÓPICOS DE TEORIA DOS NÚMEROS** dos autores **Carlos Gustavo T. de A. Moreira (Gugu), Fabio E. Brochero Martinez** e **Nicolau C. Saldanha. Coleção PROFMAT. Sociedade Brasileira de Matemática.**

4. Metodologia e demonstrações

Para que haja uma base sólida e suficientemente capaz de sustentar os fundamentos necessários para a apresentação deste trabalho, serão abordados os seguintes tópicos.

4.1 Sejam $a, b, n \in \mathbb{Z}$ com $n > 0$. Diz-se que ***a é congruente a b módulo n*** e escreve-se $a \equiv b \pmod n$ se $n \mid a-b$,ou seja, **a e b deixam o mesmo resto quando divididos por n**. De fato, note que se $a = nq_1 + r$, $b = nq_2 + r$, com $q_1, q_2, r \in \mathbb{Z}$ então $a-b = n(q_1 - q_2)$ é múltiplo de *n*; por outro lado, se $a = nq_1 + r_1$, $b = nq_2 + r_2$, com $q_1, q_2, r_1, r_2 \in \mathbb{Z}, 0 \le r_1, r_2 < n$ e $n \mid a-b$ então $n \mid n(q_1 - q_2) + r_1 - r_2$, donde $n \mid r_1 - r_2$, e logo $r_1 = r_2$.

Exemplos: $17 \equiv 3 \pmod 7$, $10 \equiv -5 \pmod 3$.

Dados $a, b, c, d, x, y, q_1, q_2, q \in \mathbb{Z}$, $d \ne 0$, $q \ne 0$ tem-se:

4.2 $d \mid a$, $d \mid b \Rightarrow d \mid ax + by$

Demonstração

Se $d \mid a$, $d \mid b \Rightarrow a = dq_1$, $b = dq_2$

$\Rightarrow ax = dxq_1$, $by = dyq_2 \Rightarrow ax + by = d(xq_1 + yq_2)$

como $(xq_1 + yq_2) \in \mathbb{Z} \Rightarrow (ax + by)$ é múltiplo de "d" $\Rightarrow d \mid ax + by$.

4.3 $d \mid a \Rightarrow a = 0 \vee |d| \le |a|$

Demonstração

Se $a = 0 \Rightarrow d \mid a$, pois zero é múltiplo de qualquer inteiro.

Se $a \ne 0$, $a = dq$ como $q \ne 0$ então $|q| \ge 1$ e $|a| = |d||q| \ge |d| \Rightarrow |d| \le |a|$.

4.5 $a \mid b,\ b \mid c \Rightarrow a \mid c$

Demonstração

Se $a \mid b$ e $b \mid c$ então $\exists\, q_1, q_2 \in \mathbb{Z}$ tais que $b = aq_1$ e $c = bq_2$
logo $c = aq_1q_2$ *então* $a \mid c$.

4.6 Se $a \equiv b \pmod n, c \equiv d \pmod n$ então $a + c \equiv b + d \pmod n$.

Demonstração

De fato, se $a = nq_1 + r$, $b = nq_2 + r$, $c = nq_3 + r'$, $d = nq_4 + r'$ com $q_1, q_2, q_3, q_4, r, r' \in \mathbb{Z}$, então $a - b = n(q_1 - q_2)$, e logo $a - b$ é múltiplo de *n*. Da mesma forma, $c - d = n(q_3 - q_4)$ e $c - d$ é multiplo de n.

Concluímos que $(a-b)+(c-d)$ é múltiplo de n ,porém $(a-b)+(c-d) = (a+c)-(b+d)$.

Portanto $(a+c)-(b+d)$ é múltiplo de n , ou seja, $a + c \equiv b + d \pmod n$.

Finalmente... $\boxed{\text{Se } a \equiv b \pmod n,\ c \equiv d \pmod n \quad \text{então} \quad a + c \equiv b + d \pmod n}$

4.7 Se $a \equiv b \pmod n \Rightarrow ac \equiv bc \pmod n$

Demonstração

Temos que $a = nq_1 + r$, $b = nq_2 + r$

logo $ac = c(nq_1 + r)$, $bc = c(nq_2 + r)$

então $ac - bc = cn(q_1 - q_2)$

ou seja $ac - bd$ é múliplo de n logo

$ac \equiv bc \pmod n$

Finalmente... $\boxed{\textit{Se } a \equiv b \pmod n \text{ então } ac \equiv bc \pmod n}$.

Além disso, $\boxed{\text{se } a \equiv b \pmod n,\ c \equiv d \pmod n \quad \text{então} \quad ac \equiv bd \pmod n}$

De fato, pelo que provamos acima, temos $ac \equiv bc \equiv bd \pmod n$.

(as demonstrações de 4.2 até 4.7 foram extraídas da pag.40, **Gugu**)

4.8 Seja $N = (a_n a_{n-1} \ldots a_1 a_0)_{10} = \sum_{0 \le k \le n} a_k 10^k$,ou seja, N é um número de (n+1) algarismos, na base 10.

4.9 Se $10^k \equiv r_k \pmod p \Rightarrow a_k 10^k \equiv a_k r_k \pmod p$ sendo $r_k =$ o resto da divisão $(10^k \div p)$

então $\left(\sum_{0 \le k \le n} a_k 10^k\right) \equiv \left(\sum_{0 \le k \le n} a_k r_k\right) \pmod p$

Finalmente...

$$N = (a_n a_{n-1} \ldots a_1 a_o) = (\sum_{0 \le k \le n} a_k 10^k) \equiv (\sum_{0 \le k \le n} a_k r_k) \text{ onde } r_k \text{ é o resto da divisão } (10^k \div p)$$

4.10 Análise dos períodos das sequências dos restos das divisões das potências sucessivas de 10 por um dado inteiro positivo.

Começaremos com uma definição importante para estudar potências de um dado inteiro *a* (no nosso caso estamos particularmente interessados no caso *a*=10) módulo um dado inteiro positivo *n*:

Dados $n \in \mathbb{N}^*$ e $a \in \mathbb{Z}$ com *mcd* (*a, n*) = 1, definimos **a ordem de *a* módulo *n***, $ord_n\, a$ como sendo o menor inteiro positivo t tal que $a^t \equiv 1$(módulo *n*).

Proposição: $\{t \in \mathbb{N}^* \mid a^t \equiv 1(\text{módulo } n)\} = \{k.ord_n\, a,\ k \in \mathbb{N}^*\}$.

Demonstração: Como $a^{ord_n a} \equiv 1$ (módulo *n*), para todo $k \in \mathbb{N}$ tem-se $a^{k.ord_n a} = (a^{ord_n a})^k \equiv 1^k = 1$ (módulo *n*). Por outro lado, se $t \in N$, $a^t \equiv 1$ (módulo *n*), existe $k \in \mathbb{N}$ com $t = k \cdot ord_n a + r, 0 \le r < ord_n a \Rightarrow a^t = a^{k.ord_n a} \cdot a^r \equiv 1.a^r \equiv a^r$ (módulo *n*) $\Rightarrow$ $a^r \equiv 1$ (módulo *n*), portanto $r = 0$ (pois $0 < r < ord_n a$ contradiria a minimalidade de $ord_n a$), e $t = k.\ ord_n a$ □

Proposição: O número de restos distintos na divisão por *n* dos números a^t, com *t* natural coincide com o período da sequência desses restos, e é igual a $ord_n\, a$.

Demonstração: Para todo *a* inteiro com *mdc* (*a, n*) = 1 temos que os $ord_n\, a$ números $1, a, a^2, \ldots, a^{ord_n a - 1}$ são distintos (módulo *n*) pois $a^i \equiv a^j$ (módulo *n*), com $0 \le i < j < ord_n\, a \Rightarrow$ $a^{j-i} \equiv 1$ (módulo *n*) com $0 < j - i < ord_n a$, absurdo. Como, para *k* inteiro e $0 \le r < ord_n a$, $a^{k.ord_n a + r} = a^{k.ord_n a} \cdot a^r \equiv 1 \cdot a^r = a^r$ (módulo *n*), o resultado segue.□

Note que se *n* é primo com 10, isto é, se não é múltiplo de 2 nem de 5 então a sequência dos restos das divisões das potências sucessivas de 10 por *n* é periódica e o tamanho de seu período é $ord_n\, 10$.

4.11 Seja p um número primo. Há p-1 números primos com p e menores que p.

Seja p≠2 e p≠5. Tem-se que 10 e p são primos entre si. Nestas circunstâncias $(10^{p-1} \div \text{p})$ deixa resto 1 (pelo Pequeno Teorema de Fermat).

Portanto, se $k = \text{ord}_n(a)$ então $(10^k \div \text{p})$ deixa resto 1 e k é um divisor de p-1.

Exemplos: r_k representa o resto da divisão $(10^k \div p)$

10^k	...	10^{11}	10^{10}	10^9	10^8	10^7	10^6	10^5	10^4	10^3	10^2	10^1	10^0
r_k	...	r_{11}	r_{10}	r_9	r_8	r_7	r_6	r_5	r_4	r_3	r_2	r_1	r_0

Exemplo 1: para p=13

Múltiplos de p: (13, 26, 39, 52, 65, 78, 91, 104, 117, 130,...)

10^k		10^{11}	10^{10}	10^9	10^8	10^7	10^6	10^5	10^4	10^3	10^2	10^1	10^0
r_k	...	4	3	-1	-4	-3	1	4	3	-1	-4	-3	1

$(10^{12} \div p)$ deixou resto 1 assim como $(10^6 \div p)$ *também deixou resto* 1

Ou seja $10^{12} \equiv 1 \pmod{13}$, $10^6 \equiv 1 \pmod{13}$

O período dos restos, r_k, para p=13 vale 6 sendo este um divisor de 12, visto que há 12 números primos com 13 e menores que 13.

Exemplo 2: para p=37

Múltiplos de p: (37, 74, 111, 148, 185, 222, 259, 296, 333, 370,...)

10^k	...	10^{11}	10^{10}	10^9	10^8	10^7	10^6	10^5	10^4	10^3	10^2	10^1	10^0
r_k	...				**-11**	**10**	**1**	**-11**	**10**	**1**	-11	10	1

Há 36 números primos com 37 sendo menores que 37. O período dos restos é igual a 3, sendo 3 um divisor de 36.

Exemplo 3: para p=41

Múltiplos de p: (41, 82, 123, 164, 205, 246, 287, 328, 369, 410,...)

10^k	...	10^{11}	10^{10}	10^9	10^8	10^7	10^6	10^5	10^4	10^3	10^2	10^1	10^0
r_k	...	10	1	-4	16	18	10	1	-4	16	18	10	1

Há 40 primos com o 41, menores que 41, e o período dos restos é 5, sendo 5 um divisor de 40.

4.12 Se p_1 , p_2 , p_3, ..., p_k são primos diferentes de 2 e 5 e α_1 , α_2 , α_3, ..., α_k são naturais então 10^k é congruente a 1 módulo $p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}...p_k^{\alpha_k}$ se, e somente se 10^k é congruente a 1 módulo $p_j^{\alpha_j}$ para todo $j \le k$. Isso nos leva à seguinte conclusão:

O período da sequência dos restos da divisão $(10^k \div p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}...p_k^{\alpha_k})$**,**
que é sempre igual a $\mathrm{ord}_{p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}...p_k^{\alpha_k}} 10$**, é igual ao mmc entre os períodos nas divisões por** $p_1^{\alpha_1}$, $p_2^{\alpha_2}$, $p_3^{\alpha_3}$, ..., $p_k^{\alpha_k}$ **.**

Exemplo 4:

Para p=119=7×17, o período dos restos de 10^k por 7 tem 6 termos , o período por 17 tem 16 termos e portanto o período por 119 é $mmc(6;16) = 48$. Vejamos:

(7, 14, 21, 28, 35, 42, 49, 56, 63, 70,...)

congruência (mod 7)

$10^0 \equiv 1$	$10^1 \equiv 3$
$10^2 \equiv 30 \equiv 2$	$10^3 \equiv 20 \equiv -1$
$10^4 \equiv -10 \equiv -3$	$10^5 \equiv -30 \equiv -2$
$10^6 \equiv -20 \equiv 1$	

O período apresentou 6 termos .

Para determinar o período nas divisões por 17 o seguinte fato será útil:

Se alguma potência de 10 for congruente a -1 módulo n então a quantidade de termos do período dos restos será igual a 2*m*, onde *m* é tal que $10^m \equiv -1$ pela primeira na sequências das divisões.

(17, 34, 51, 68, 85, 102, 119, 136, 153, 170,...)

congruência (mod 17)

$10^0 \equiv 1$ $10^1 \equiv 10$

$10^2 \equiv -2$ $10^3 \equiv -20 \equiv -3$

$10^4 \equiv -30 \equiv 4$ $10^5 \equiv 40 \equiv 6$

$10^6 \equiv 60 \equiv -8$ $10^7 \equiv -80 \equiv 5$

$10^8 \equiv 50 \equiv -1$

O período vale apresentou 8×2=16 valores.

(119, 238, 357, 476, 595, 714, 833, 952, 1071, 1190,...)

congruência (mod 119)

$10^0 \equiv 1$ $10^1 \equiv 10$ $10^2 \equiv 100 \equiv -19$

$10^3 \equiv -190 \equiv 48$ $10^4 \equiv 480 \equiv 4$ $10^5 \equiv 40$

$10^6 \equiv 400 \equiv 43$ $10^7 \equiv 430 \equiv -46$ $10^8 \equiv -460 \equiv 16$

$10^9 \equiv 160 \equiv 41$ $10^{10} \equiv 410 \equiv 53$ $10^{11} \equiv 530 \equiv 54$

$10^{12} \equiv 540 \equiv -55$ $10^{13} \equiv -550 \equiv 45$ $10^{14} \equiv 450 \equiv -26$

$10^{15} \equiv -260 \equiv -22$ $10^{16} \equiv -220 \equiv 18$ $10^{17} \equiv 180 \equiv 61$

$10^{18} \equiv 610 \equiv 15$ $10^{19} \equiv 150 \equiv 31$ $10^{20} \equiv 310 \equiv -47$

$10^{21} \equiv -470 \equiv 6$ $10^{22} \equiv 60$ $10^{23} \equiv 600 \equiv 5$

$10^{24} \equiv 50$ $10^{25} \equiv 500 \equiv 24$ $10^{26} \equiv 240 \equiv 2$

$10^{27} \equiv 20$ $10^{28} \equiv 200 \equiv -38$ $10^{29} \equiv -380 \equiv -23$

$10^{30} \equiv -230 \equiv 8$ $10^{31} \equiv 80 \equiv -39$ $10^{32} \equiv -390 \equiv -33$

$10^{33} \equiv -330 \equiv 27$ $10^{34} \equiv 270 \equiv 32$ $10^{35} \equiv 320 \equiv -37$

$10^{36} \equiv -370 \equiv -13$ $10^{37} \equiv -130 \equiv -11$ $10^{38} \equiv -110 \equiv 9$

$10^{39} \equiv 90 \equiv -29$ $10^{40} \equiv -290 \equiv -52$ $10^{41} \equiv -520 \equiv -44$

$10^{42} \equiv -440 \equiv 36$ $10^{43} \equiv 360 \equiv 3$ $10^{44} \equiv 30$

$10^{45} \equiv 300 \equiv -57$ $10^{46} \equiv -570 \equiv 25$ $10^{47} \equiv 250 \equiv 12$

$10^{48} \equiv 120 \equiv 1$

4.13 Período e pré-período

Se na decomposição em fatores primos do número n pelo qual vamos dividir as potências 10^k aparecer os números 2 ou 5 , então existirá um pré-período e quantidade de termos deste pré-período será igual ao maior dos expoentes de 2 e 5.

De fato, se $n = 2^{\alpha}5^{\beta}m$, com mdc(m,10)=1, então $10^k \equiv 0 \pmod{2^{\alpha}}$ para todo $k \geq \alpha$ e $10^k \equiv 0 \pmod{5^{\beta}}$ para todo $k \geq \beta$. Após esse pré-período, a sequência dos restos ficará periódica, e o período terá $\text{ord}_m 10$ termos.

Exemplo: $10^k \div (2^3.5^2.7)$, ou seja, $10^k \div 1400$

(1400, 2800, 4200, 5600, 7000, 8400, 9800, 11200, 12600, 14000,...)

congruência (mod 1400)

$10^0 \equiv 1$ $\quad 10^1 \equiv 10$ $\quad 10^2 \equiv 100$

$10^3 \equiv 1000 \equiv -400$ $\quad 10^4 \equiv -4000 \equiv 200$ $\quad 10^5 \equiv 2000 \equiv 600$

$10^6 \equiv 6000 \equiv 400$ $\quad 10^7 \equiv 4000 \equiv -200$ $\quad 10^8 \equiv -2000 \equiv -600$

$10^9 \equiv -6000 \equiv -400$

Pré-Período: (100;10;1) Período: (−600; −200; 400; 600; 200; -400)

Aplicação: Seja o número N=5555... 5678 formado por 100 algarismos 5 seguidos por 6,7, e 8, quando dividido por 72 deixa qual resto?

(72, 144,216, 288, 360, 432, 504, 576, 648, 720,792,864,936,1008,1080)

N	...	5	5	5	5	5	5	5	5	5	6	7	8
r_k								−8	−8	−8	28	10	1
R_{72}^N								−40	−40	−40	168	70	8

$$72 = 8 \times 9 = 2^3.9$$

Pré-período: 3 números Período : 1 número pois este é o período do 9

congruências (mod 72)

$R_{72}^N = 100.(-40) + 168 + 70 + 8$ $\quad 100 \equiv 28 \quad 168 \equiv 24 \quad 70 + 8 \equiv 6$

$R_{72}^N = 28.(-40) + 24 + 6 = -1090 \equiv -10 \equiv 62 \pmod{72}$

Resposta: N ÷72 deixa resto 62

4.14 A quantidade de números primos com um número natural N e menores que N é representada por $\varphi(N)$. Seja $N = p_1^{\alpha_1}.p_2^{\alpha_2}...p_k^{\alpha_k}$. Temos

$$\boxed{\varphi(N) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}).(p_2^{\alpha_2} - p_2^{\alpha_2 - 1})...(p_k^{\alpha_k} - p_k^{\alpha_k - 1})}$$

O Teorema de Euler diz que, para todo natural N e todo inteiro a primo com N, temos

$$a^{\varphi(N)} \equiv 1 \pmod{N}.$$

Uma consequência desse teorema é que se mdc(a,N)=1 sempre temos $\mathrm{ord}_n a \mid \varphi(N)$.

Podemos melhorar um pouco este resultado: pelo que vimos anteriormente, temos sempre

$$\mathrm{ord}_n a \mid \mathrm{mmc}(\mathrm{ord}_{p_1^{\alpha_1}} a, \mathrm{ord}_{p_2^{\alpha_2}} a, ..., \mathrm{ord}_{p_k^{\alpha_k}} a) \mid \mathrm{mmc}(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}, p_2^{\alpha_2} - p_2^{\alpha_2 - 1}, ..., p_k^{\alpha_k} - p_k^{\alpha_k - 1}).$$

Note que $\mathrm{mmc}(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}, p_2^{\alpha_2} - p_2^{\alpha_2 - 1}, ..., p_k^{\alpha_k} - p_k^{\alpha_k - 1})$ é sempre um divisor de $\varphi(N)$, e na maior parte das vezes é um divisor próprio de $\varphi(N)$.

Exemplos:

Primos com N, menores que N.

Com 30, $\varphi(30) = |\{1,29,7,23,11,19,13.17\}| = 8$.

Por outro lado, $30 = 2^1.3^1.5^1$ e $(2^1 - 2^0).(3^1 - 3^0).(5^1 - 5^0) = 1.2.4 = 8$.

Primos com 360, menores que 360.

$360 = 2^3.3^2.5^1$

$\varphi(360) = (2^3 - 2^2).(3^2 - 3^1).(5^1 - 5^0) = 4.6.4 = 96$

Quando N=p é primo, temos: $\varphi(p) = (p^1 - p^0) = p - 1$

Uma aplicação da noção de $\varphi(N)$:

Qual o resto de $(3^{98} \div 10)$?

$\varphi(10)=\varphi(2\cdot 5)=\varphi(2)\varphi(5)=(2-1)(5-1)=4;\ D(4)=\{1,2,4\}$

$3^1 \equiv 3 \pmod{10}$ $\quad 3^2 \equiv 9 \pmod{10}$ $\quad 3^4 \equiv 1 \pmod{10}$

logo $3^{98} \pmod{10} = \left(3^4\right)^{24} . 3^2 = 1^{24} \pmod{10} . 3^2 \pmod{10} = 1.9 = 9$

Resposta: O resto é 9.

4.11 Exercícios resolvidos:

Ex: O número N= xxx...x é formado por 1000 algarismos todos iguais a x e quando dividido por 17 deixa resto 5 e o número M=yyy...y formado por 1000 algarismos todos iguais a y e quando dividido por 17 deixa resto 2. Qual o valor de y−x?

x	x	x	x	x	x	x	x	x	x	x	X	x	x	x	x
−5	−9	−6	−4	3	2	−10	−1	5	9	6	4	−3	−2	10	1
−5x	−9x	−6x	−4x	2x	2x	−10x	−1x	5x	9x	6x	4x	−3x	−2x	10x	1x

Vê-se que a soma dos 16 elementos da 3ª linha vale zero, ou seja, o número formado por 16 algarismos iguais a 1 representa um múltiplo de 17, da mesma forma um número formado por 32 algarismos x, por 48 algarismos x,..., por 992 algarismos x, representa um múltiplo de 17.
O número N é formado por 8 algarismos x, seguidos de 992 algarismos x, logo N dividido por 17 deixa o mesmo resto que (5x+9x+6x+4x−3x−2x+10x+1x) deixará quando dividido por17 , ou seja, deixa resto 30x÷17, e portanto deixa resto13x.
Deseja-se que N quando dividido por 17 deixe resto 5, então 13x deverá ser um múltiplo de 17 mais 5 unidades, ou seja: 13x=17k+5 ($1 \le x \le 9$ e $k \in \mathbb{N}$) o único valor para x é 3.
Deseja-se que M quando dividido por 17 deixe resto 2, então 13x deverá ser um múltiplo de 17 mais 2 unidades, ou seja: 13y=17k+2 ($1 \le y \le 9$ e $k \in \mathbb{N}$) o único valor para y é 8.
Finalmente y−x=8−3=5.

Ex: Qual o resto da divisão de 15051952 por 13?

1	5	0	5	1	9	5	2
−3	1	4	3	−1	−4	−3	1(sempre)
−3	5	0	15(ou2)	−1	−36(ou3)	−15(ou−2)	2

10÷13 deixa resto 10 ou resto −3 (linha seguinte: colocar 1 zero à direita de −3)

−30 ÷ 13 deixa resto −4 (linha seguinte: colocar 1 zero à direita de −4)

−40 ÷ 13 deixa resto −1 (linha seguinte: colocar 1 zero à direita de −1)

−10÷13 deixa resto −10 ou resto 3 (linha seguinte: colocar 1 zero à direita de 3)

30÷13 deixa resto 4 (linha seguinte: colocar 1 zero à direita de 4)

40÷13 deixa resto 1 (linha seguinte: colocar 1 zero à direita de 1)

10÷13 deixa resto 10 ou resto −3.

Quando o módulo do número da 3ª linha da tabela for maior que 13 então se substitui este número pelo resto da divisão dele por 13.

15÷13 deixa resto 2; −36÷13 deixa resto −10 ou 3; −15÷13 deixa resto −2.

Resp.: −3+5+0+2−1+3−2+2=6

(verificação:15051952÷13=1157842 e deixa resto 6)

4.12 Este algoritmo para verificar a divisibilidade implica os critérios existentes nos livros didáticos de uma forma muito simples.

Exemplo: o número abcdefgh é múltiplo, por exemplo, de 3 quando a soma for múltipla

	a	b	c	d	e	f	g	h
	10→1	10→1	10→1	10→1	10→1	10→1	10→1	1(sempre)
Soma	+a	+b	+c	+d	+e	+f	+g	+h

“Um número é múltiplo de 3 quando a soma dos seus algarismos for múltipla de 3” , como mostra a tabela acima.

Exemplo: o número abcdefgh é múltiplo, por exemplo, de 11 quando a soma for múltipla

	a	b	c	d	e	f	g	h
	−10→−1	10→1	−10→−1	10→1	10→−1	−10→1	10→−1	1(sempre)
Soma	−a	+b	−c	+d	−e	+f	−g	+h

“Um número é divisível por 11 quando a diferença entre a soma dos algarismos de ordem impar e a soma dos algarismos de ordem par formar um número múltiplo de 11”, ou seja, como mostra a tabela acima.

Exemplo: o número abcdefgh é múltiplo, por exemplo, de 5 quando a soma for múltipla

	a	b	c	d	e	f	g	h
	0	0	0	0	0	0	10→0	1(sempre)
Soma	0	0	0	0	0	0	0	+h

"Um número é múltiplo de 5 quando terminar em zero ou 5", ou seja depende apenas do ultimo algarismos, este deverá ser múltiplo de 5, isto é, deverá ser zero ou 5, como mostra a tabela acima.

Exemplo: o número abcdef é múltiplo, por exemplo, de 7 quando a soma for múltipla

			a	b	c	d	e	f
			−30 (−2)	−10 (−3)	20 (−1)	30 (2)	10 (3)	1(sempre)
soma			−2a	−3b	−1c	+2d	+3e	+1f

Se a soma: −2a−3b−1c+2d+3e+1f é múltipla de 7, então −2a – (*98a*) −3b – (*7b*) −1c + 2d + (*98d*) + 3e+ (*7e*) + 1f permanecerá múltipla de 7, pois somou-se apenas múltiplo de 7, porém a nova soma será (100d+10e+1f) – (100a+10b+c), ou seja, a diferença: def−abc deverá ser múltipla de 7, resultando na conclusão de que o seu resto na divisão por 7 é igual ao resto da diferença entre sua classe ímpar e sua classe par, como é apresentado em alguns livros didáticos.

4.13 Resumindo, o critério geral de divisibilidade funciona da seguinte forma:

Este critério único, ou seja, o critério de divisibilidade pelo número inteiro n depende fundamentalmente da 2ª linha da tabela elaborada que se determina durante a resolução do exercício, não havendo necessidade de memorizá-la.

Destaca-se que abaixo do algarismo das unidades simples sempre estará o 1. Abaixo das dezenas simples sempre estará o resto r_1 da divisão de 10 por n. Abaixo das centenas simples estará o resto r_2 da divisão de (10.r_1÷n, deixando resto r_2). Abaixo das unidades de milhar estará o resto r_3 da divisão de (10r_2÷n, deixando resto $r_{3)}$ e assim sucessivamente.

Dado um inteiro positivo qualquer, ele deixará o mesmo resto na divisão por n que a soma de seu algarismo das unidades com o produto do seu algarismo das dezenas multiplicado por $r_{1,}$ com o produto de seu algarismo das dezenas por r_2, e assim sucessivamente.

A tabela abaixo reúne as informações desta conclusão.

O número... gfedcba dividido por n:

		g	f	e	d	c	b	a
Por 2		0	0	0	0	0	10→0	1
Por 3		1	1	1	1	10→1	10→1	1
Por 4		0	0	0	0	20→0	10→2	1
Por 5		0	0	0	0	0	10→0	1
Por 6		4	4	4	4	40→4	10→4	1
Por 7		−20→1	−30→−2	−10→−3	20→−1	30→2	10→3	1
Por 8		0	0	0	40→0	20→4	10→2	1
Por 9		1	1	1	1	10→1	10→1	1
Por 1 1		1	−1	1	10→−1	−10→1	10→−1	1
Por 12		4	4	4	40→4	−20→4	10→−2	1
Por 13		1	4	3	−40→−1	−30→−4	10→−3	1
Por 17		60→−8	40→6	−30→4	−20→−3	−70→−2	10→−7	1
Por 19		30→−8	60→3	−70→6	50→−7	−90→5	10→−9	1

5. Bibliografia

Carlos Gustavo T. de A. Moreira (**Gugu**), Fabio Martinez, Nicolau Saldanha. **Tópicos de Teoria dos Números**. Coleção PROFMAT. Editora SBM. Rio de Janeiro.

Bezerra, Manoel Jairo. **Questões de Matemática**. Companhia Editora Nacional.,1976. São Paulo.

Santos, Antonio Luiz. (**Gandy**) **Problemas Selecionados de Matemática**. Editora Moderna Ltda. 2006. Rio de Janeiro.

Lacerda, José Carlos Admo**. Praticando a Aritmética**. Editora: Dissonnarte 4ª edição, 2010. Rio de Janeiro.