British Journal of Mathematics & Computer Science
13(3): 1-5, 2016, Article no.BJMCS.18354
ISSN: 2231-0851

SCIENCEDOMAIN *international*
www.sciencedomain.org

Finding Remainder on Dividing Numbers

Kritsana Sokhuma[1*], Anurak Thanyacharoen[1] and Chatchai Jaisin[1]

[1] *Department of Mathematics, Faculty of Science and Technology, Muban Chom Bueng Rajabhat University, Ratchaburi 70150, Thailand.*

Article Information

DOI: 10.9734/BJMCS/2016/18354
Editor(s):
(1) Nikolaos Dimitriou Bagis, Department of Informatics and Mathematics, Aristotelian University of Thessaloniki, Greece.
Reviewers:
(1) Anonymous, Norfolk State University, USA.
(2) Francisco Bulnes, Tecnologico de Estudios Superiores de Chalco, Chalco, Mexico.
(3) Grienggrai Rajchakit, Maejo University, Thailand.
(4) Anonymous, Xi'an Jiaotong University, Xi'an, China.
(5) Rajesh Pereira, University of Guelph, Guelph, Canada.
Complete Peer review History: http://sciencedomain.org/review-history/12654

Original Research Article

Received: 16 April 2015
Accepted: 02 December 2015
Published: 12 December 2015

Abstract

In this paper, we also prove an interesting in the case of dividing numbers by a prime number p.

Keywords: Divisibility; congruence.

2010 Mathematics Subject Classification: Primary 11A07,11A99.

1 Introduction

Fact 1. Let p be a prime number. Then there is a ring homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$, where $\phi(a) = \bar{a}$ is the congruent class modulo p. If $f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_0$ with $x, a_m, \cdots, a_0 \in \mathbb{Z}$, then

$$\overline{f(x)} = \overline{a_m} \cdot \bar{x}^m + \overline{a_{m-1}} \cdot \bar{x}^{m-1} + \overline{a_{m-2}} \cdot \bar{x}^{m-2} + \cdots + \overline{a_0}.$$

Fact 2. Let $a \in \mathbb{Z}$ and p be a prime number. Fermat's Little Theorem says that if $gcd(a, p) = 1$, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

**Corresponding author: E-mail: k_sokhuma@yahoo.co.th*

Fact 3. Let p be a prime number and $gcd(a,p)=1$. Then the order d of $\bar{a}$ in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^{\times}=\{\overline{1},\overline{2},\cdots,\overline{p-1}\}$ satisfies $d \mid p-1$ by Fact 2 and Lagrange's Theorem.

The aim of this paper is to prove an interesting method of divisibility by $7, 13, 17$ and 19. In Section 2, we will review some basic properties of congruence. In Section 3, we show the main result for special method divisibility. In Section 4, we show an application for the main results. A conclusion is the last section of the paper.

2 Basic Properties of Congruence and Special Divisibility Tests

In this section, we review some basic properties of congruence and special divisibility tests, contained in [1], [2], [3] and [4]. Putting this into the form of a definition, we have Definition 2.1.

2.1 Basic properties of congruence

Definition 2.1. *Let n be a fixed positive integer. Two integers a and b are said to be congruent modulo n, symbolized by $a \equiv b \pmod{n}$. If n divides the difference $a-b$; that is, provided that $a-b=kn$ for some integer k.*

Theorem 2.1. For arbitrary integers a and b, $a \equiv b \pmod{n}$ if and only if a and b leave the same nonnegative remainder when divided by n.

Theorem 2.2. Let $n>1$ be fixed and a, b, c, d be arbitrary integers. Then the following properties hold:

(a) $a \equiv a \pmod{n}$
(b) If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$
(c) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$
(d) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a+c \equiv b+d \pmod{n}$
(e) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$
(f) If $a \equiv b \pmod{n}$, then $a+c \equiv b+c \pmod{n}$
(g) If $a \equiv b \pmod{n}$, then $ac \equiv bc \pmod{n}$
(h) If $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$ for any positive integer k.

In Theorem 2.2 we saw that if $a \equiv b \pmod{n}$, then $ca \equiv cb \pmod{n}$ for any integer c. The converse, however, fails to hold. With suitable precautions, cancellation can be allowed; one step in this direction, and an important one, is provided by the following theorem.

Theorem 2.3. *If $ca \equiv cb \pmod{n}$, then $a \equiv b \pmod{\frac{n}{d}}$, where $d=gcd(c,n)$.*

Theorem 2.3 get its maximum force when the requirement that $gcd(c,n)=1$ is added, for then the cancellation may be accomplished without a change in modulus.

Corollary 2.4. *If $ca \equiv cb \pmod{n}$ and $gcd(c,n)=1$, then $a \equiv b \pmod{n}$.*

We take the moment to record a special case of Corollary 2.4 which we shall have frequent occation to use, namely, Corollary 2.5.

Corollary 2.5. *If $ca \equiv cb \pmod{p}$ and $p \nmid c$, where p is a prime number, then $a \equiv b \pmod{p}$.*

Definition 2.2. Let p be a prime not equal to 2 or 5. Let d be the order of $\alpha := \overline{10}$ in $(\mathbb{Z}/p\mathbb{Z})^{\times}$. Then by Fact 3, one has $\alpha^{i+d}=\alpha$. This shows that the powers $\overline{10}^i$ exhibit periodic pattern of period d. If one writes $\overline{10}^i := \mu_i$, then $\mu_{i+d}=\mu_i$ (for convenience, we always represents μ_0 by 1).

Example 2.6. *(1) For $p = 3$, one has $d = 1$: namely $\overline{10}^i, i \geq 0$ has the pattern $(\mu_0) = (1)$.*
(2) For $p = 7$,$d = 6$: and $(\mu_0, \mu_1, \mu_2, \cdots, \mu_5) = (1, -4, 2, -1, 4, -2)$.
(3) For $p = 11$, $d = 2$: and $(\mu_0, \mu_1) = (1, -1)$.
(4) For $p = 13$, $d = 6$: and $(\mu_0, \mu_1, \mu_2, \cdots, \mu_5) = (1, -3, 9, -1, 3, -9)$.

Example 2.7. *Since $10 = 2 \cdot 5$, the divisibility by $p = 2$ or $p = 5$ is very obvious. It is easy to see that the remainder for dividing N by 2 or by 5 is given by the last digit (i.e. a_0) of N.*

2.2 Special divisibility tests

The number

$$N = a_m \cdot b^m + a_{m-1} \cdot b^{m-1} + a_{m-2} \cdot b^{m-2} + \cdots + a_2 \cdot b^2 + a_1 \cdot b + a_0$$

may be replaced by the simpler symbol

$$N = (a_m a_{m-1} a_{m-2} \cdots a_2 a_1 a_0)_b \text{ (see [5])}.$$

We ordinarily record numbers in the decimal system of notation, where $b = 10$, omitting the 10-subscript which specifies the base. For instance, the symbol 1785 stands for the more awkward expression

$$1785 = 1 \cdot 10^3 + 7 \cdot 10^2 + 8 \cdot 10 + 5.$$

We are about ready to derive criteria for determining whether an integer is divisible by 9 or 11, without performing the actual division. For this, we need a result having to do with congruences involving polynomials with integral coefficients.

Theorem 2.8. *Let $P(x) = \sum_{k=0}^{m} c_k x^k$ be a polynomial function of x with integral coefficients c_k. If $a \equiv b \pmod{n}$, then $P(a) \equiv P(b) \pmod{n}$.*

One divisibility test that we have in mind is this. A positive integer is divisible by 9 if and only if the sum of the digits in its decimal representation is divisible by 9.

Theorem 2.9. *Let $N = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + a_{m-2} \cdot 10^{m-2} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$ be the decimal expansion of the positive integer $N, 0 \leq a_k < 10$, and let $A = a_0 + a_1 + a_2 + \cdots + a_m$. Then $9 \mid N$ if and only if $9 \mid A$.*

Theorem 2.8 also serves as the basis for a well-known test for divisibility by 11. We state this more precisely by Theorem 2.10 and Theorem 2.11.

Theorem 2.10. *Let $N = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + a_{m-2} \cdot 10^{m-2} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$ be the decimal expansion of the positive integer $N, 0 \leq a_k < 10$, and let $B = a_0 - a_1 + a_2 - \cdots + (-1)^m a_m$. Then $11 \mid N$ if and only if $11 \mid B$.*

Theorem 2.11. *Let $N = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + a_{m-2} \cdot 10^{m-2} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$ be the decimal expansion of the positive integer $N, 0 \leq a_k < 10$, and let*

$$M = (100a_2 + 10a_1 + a_0) - (100a_5 + 10a_4 + a_3) + (100a_8 + 10a_7 + a_6) - \cdots .$$

Then $7, 11$, and 13 divide N if and only if $7, 11$, and 13 divide M.

3 Main Results

Now we state the main results of this section.

Theorem 3.1. *Let $p \neq 2, 5$ be a prime number and $N = a_m a_{m-1} a_{m-2} \cdots a_2 a_1 a_0$ be a positive integer in the decimal system , i.e.*

$$N = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \cdots + a_0.$$

where $0 \leq a_0, a_1, a_2 \cdots, a_m \leq 9$ are integers. Then the remainder for dividing N by p is the same as that of dividing

$$\sum_{i=0}^{m} \mu_i \cdot a_i = a_0 + \mu_1 a_1 + \cdots + \mu_m a_m,$$

where μ_i has periodic pattern which is defined and explained above.

Proof. Writing

$$N = 10^0 \cdot a_0 + 10^1 \cdot a_1 + \cdots + 10^{m-1} \cdot a_{m-1} + 10^m \cdot a_m.$$

and taking congruence modulo p, it follows from Fact 1 that

$$\begin{aligned} \overline{N} &= \overline{10}^0 \cdot a_0 + \overline{10}^1 \cdot a_1 + \cdots + \overline{10}^{m-1} \cdot a_{m-1} + \overline{10}^m \cdot a_m \\ &\equiv a_0 + \mu_1 a_1 + \cdots + \mu_{m-1} a_{m-1} + \mu_m a_m \pmod{p}. \end{aligned}$$

□

Corollary 3.2. *Let p and N be given as in the above theorem. Then p divides N if and only if p divides*

$$a_0 + \mu_1 a_1 + \cdots + \mu_{m-1} a_{m-1} + \mu_m a_m.$$

Proof. Immediately. □

4 Applications

In this section, we shall utilize Corollary 3.2 to show some example.

Example 4.1. *To see an illustration of Corollary 3.2, take the integer*

$$N = 6496847279 = 13 \cdot 17 \cdot 37 \cdot 97 \cdot 8191.$$

Let $p = 13$, by direct computation, 10 is of order $d = 6$ in $(\mathbb{Z}/p\mathbb{Z})^\times$,thus $(\mu_0, \mu_1, \cdots, \mu_5) = (1, -3, 9, -1, 3, -9)$. Then the number $9 \cdot (1) + 7 \cdot (-3) + 2 \cdot (9) + 7 \cdot (-1) + 4 \cdot (3) + 8 \cdot (-9) + 6 \cdot (1) + 9 \cdot (-3) + 4 \cdot (9) + 6 \cdot (-1) = -52$, must be divisible by 13.This is true, since $-52 = (-4) \cdot 13$.

Let $p = 37$, by direct computation, 10 is of order $d = 3$ in $(\mathbb{Z}/p\mathbb{Z})^\times$, thus $(\mu_0, \mu_1, \mu_2) = (1, 10, -11)$. Then the number $9 \cdot 1 + 7 \cdot 10 + 2 \cdot (-11) + 7 \cdot 1 + 4 \cdot 10 + 8 \cdot (-11) + 6 \cdot 1 + 9 \cdot 10 + 4 \cdot (-11) + 6 \cdot 1 = 74$, must be divisible by 37. This is true, since $74 = 2 \cdot 37$.

5 Conclusion

In this paper, we showed the method to deviding numbers by a prime number p. Let $p \neq 2, 5$ be a prime number and $N = a_m a_{m-1} a_{m-2} \cdots a_2 a_1 a_0$ be a positive integer in the decimal system, where $0 \leq a_0, a_1, a_2 \cdots, a_m \leq 9$ are integers. Then p divides N if and only if p divides

$$\sum_{i=0}^{m} \mu_i \cdot a_i = a_0 + \mu_1 a_1 + \cdots + \mu_m a_m,$$

where μ_i has periodic pattern.

Competing Interests

Authors have declared that no competing interests exist.

References

[1] Burton DM. Elementary number theory, 5th ed. New York: McGraw Hill; 2002.

[2] Stillwell J. Elements of number theory, New York: Springer; 2003.

[3] Robbins N. Beginning number theory, second ed. Massachusetts: Jones and Bartlett; 2006.

[4] Koshy T. Discrete mathematics with applications, London: Elsevier; 2004.

[5] Brannan D. A first course in mathematical analysis, New York: Cambridge University; 2006.

Peer-review history:
The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)
http://sciencedomain.org/review-history/12654