УДК 511.172

Thiha Bo
Mandalar University (Myanmar)

THE VISUALIZE FORMULATION OF DIVISIBILITY

For the purposes of cryptography it is necessary to develop effective methods and algorithms: to check the simplicity of integers; to find large prime numbers; to factorize integers.

This paper studies a generalized method for constructing algorithms to check the divisibility of integers by a given number b in various number systems by analyzing the sets of divisors of base (a given number b), prebase (number $b - 1$), and postbase (number $b + 1$). It is indicated that the rules for testing divisibility by a given number may have different complexity depending on the number system used.

The paper introduces the formulations of some theorems with proofs. The theorems are supported by concrete examples.

These theorems can formulate for many divisibility rules for any number over the any base. Some numbers are although difficult over base 10, they are easy over another base. Some numbers, such as primes, have direct rules, but some composites have combined rules.

Key words: base factors, prebase factors, postbase factors, rise, visualize array.

For citation: Thina Bo. The visualize formulation of divisibility. *Proceedings of BSTU, issue 3, Physics and Mathematics. Informatics*, 2022, no. 1 (254), pp. 15–18.

Тиха Бо
Университет Мандалая (Мьянма)

ВИЗУАЛИЗИРУЕМАЯ ФОРМУЛИРОВКА ДЕЛИМОСТИ

Для целей криптографии необходимо разрабатывать эффективные методы и алгоритмы: проверки простоты целых чисел; поиска больших простых чисел; факторизации целых чисел.

В данной статье изучается обобщенный способ построения алгоритмов проверки делимости целых чисел на заданное число b в различных системах счисления путем анализа множеств делителей базы (заданного числа b), предбазы (числа $b - 1$) и постбазы (числа $b + 1$). Указано, что правила проверки делимости на данное число могут иметь разную сложность в зависимости от используемой системы счисления.

В статье приводятся формулировки некоторых теорем с доказательствами. Теоремы подкреплены конкретными примерами. Эти теоремы позволяют сформулировать множество правил делимости для любого числа в любой системе счисления. Некоторые числа, хотя и являются сложными при делении в системе счисления по основанию 10, легко делятся в системе счисления по другому основанию.

Ключевые слова: делители базы, делители предбазы, делители постбазы, рост, визуализация массива.

Для цитирования: Тиха Бо. Визуализируемая формулировка делимости // Труды БГТУ. Сер. 3, Физико-математические науки и информатика. 2022. № 1 (254). С. 15–18.

Introduction. In number theory, the properties of integers are studied. In this paper, a shorthand way of determining whether a given integer is divisible by a fixed divisor without performing the division, usually by examining its digits, were developed generally. For base 10 (decimal system), Martin Gardner explained and popularized these rules in his September 1962 “Mathematical Games” column in Scientific American. In this paper, the divisibility rules for any number, any base and the best formulae are derived by visualization. Today, all of the calculations are calculated by electronic devices. But these devices are made by human. If the algorithms of the calculation of the devices are reduced to simplest way by using the theorems in this paper, it will be great benefit for us [1–3].

Main part. To get the sense of divisibility, some definitions and notations are defined and introduced. The properties of numbers over any base are characterized.

The prime divisors or the power of prime divisors of a base b is called the *base factors of b*.

B_b is the notation of the set of all base factors of b. For examples: $B_{10} = \{2, 5\}$.

Suppose the digit of base 8 are order triple pair of zero and one, i. e.

$$0 = 000,\ 1 = 001,\ 2 = 010,\ 3 = 011,\ 4 = 100,$$

$$5 = 101,\ 6 = 110,\ 7 = 111,\ 8 = 1000,$$

$$B_8 = \{010, 100, 1000\} = \{2, 4, 8\}.$$

The divisors of $b - 1$ is called the *prebase factors of b*. P_b is the notation of the set of all prebase factors of b. For examples:

$$P_{10} = \{3, 9\},\ P_8 = \{111\} = \{7\}.$$

The divisors of $b + 1$ is called the *postbase factors of b*. Q_b is the notation of the set of all postbase factors of b. For examples:

$$Q_{10} = \{11\},\ Q_8 = \{011, 1001\} = \{3, 9\}.$$

The different form one's digit of a multiply of number n to one's digit of another multiply n is called *run of n* over base b. The different between ten's digit of a multiply of number n and ten's digit of another multiply n is called *rise of n* over base b. $r_b(p, q)_n = y : x$ is the notation of the simplest integral ratio of rise y and run x of pn and qn over base b, where $x \neq 0$ and $y \neq 0$. $R_b(n)$ is the notation of the set of all ratios $r_b(p, q)_n$ for n and base b. For examples:

For 7 and 14 over base 10, run is –3 and rise is 1, i. e., $r_{10}(1, 2)_7 = 1 : -3$.

For 7 and 21 over base 10, run is –6 and rise is 2, i. e., $r_{10}(1, 3)_7 = 1 : -3$.

For 7 and 28 over base 10, run is 1 and rise is 2, i. e., $r_{10}(1, 4)_7 = 2 : 1$.

For 7 and 35 over base 10, run is –2 and rise is 3, i. e., $r_{10}(1, 5)_7 = 3 : -2$.

Then

$$R_{10}(7) = \{-1 : 3, 2 : 1, -3 : 2, -4 : 5, 1 : 4, -6 : 1, \ldots\}.$$

Similarity

$$R_{10}(9) = \{-1 : 1, -10 : 1, 8 : 1, 7 : 2, \ldots\},$$

$$R_{10}(11) = \{1 : 1, 12 : 1, -10 : 1, -9 : 2, \ldots\},$$

$$R_{10}(3) = \{-1 : 1, -10 : 1, 8 : 1, 7 : 2, \ldots\}.$$

The element of $R_b(n)$ is defined as the best coefficient or best ratio of n over base b, if its denominator 1 and the modulus of numerator is minimum. For examples: 2 : 1 is the best coefficient of 7 over base 10. 1 : 1 is the best coefficient of 11 over base 10. –1 : 1 is the best coefficient of 3 and 9 over base 10.

The best coefficient of a prebase factor of a base b is always –1 : 1 and the best coefficient of a postbase factor of a base b is always 1 : 1.

Lemma. If $y : x \in R_b(n)$, then $n \mid x + by$.

Proof. By definition, $y : x = r_b(p, q)_n$.

Let $pn = \alpha b + \beta$ and $qn = \gamma b + \delta$.

So, $x = \delta - \beta$ and $y = \gamma - \alpha$.

$$x + by = \delta - \beta + b(\gamma - \alpha) =$$

$$= \gamma b + \delta - (\alpha b + \beta) = = qn - - pn = (q - p)n.$$

Depend on the characteristics of a number over a given base, the divisibility rules were different each other. But we need only four theorems which are developed generally as follow.

Base Factor Theorem. If n is a base factor of b and $m = \sum_{i=0}^{p} a_i b_i = a_0 b_0 + a_1 b_1 + \ldots + a_p b_p$, then $n \mid m$ if and only if $n \mid a_0$.

Proof. Since n is a base factor of b, $n \mid b$. The result is obviously.

Prebase Factor Theorem. If n is a prebase factor of b and $m = \sum_{i=0}^{p} a_i b^i = a_0 + a_1 b + \ldots + a_p b^p$, then $n \mid m$ if and only if $n \mid \sum_{i=0}^{p} a_i$.

Proof. Since n is a prebase factor, $n \mid b - 1$.

Since $b - 1 \mid 1 - b^i$, for $i = 1, 2, 3, \ldots$.

So, $n \mid (1 - b)a_1 + \ldots + (1 - b^p)a_p$ and let $(1 - b)a_1 + \ldots + (1 - b^p)a_p = sn$.

Suppose $n \mid m$. Let $m = kn$.

$$\sum_{i=0}^{p} a_i = a_0 + a_1 + \ldots + a_p =$$

$$= a_0 + a_1 + \ldots + a_p + a_1 b + \ldots + a_p b^p - a_1 b - \ldots -$$

$$- a_p b^p = a_0 + a_1 b + \ldots + a_p b^p + (1 - b)a_1 + \ldots +$$

$$+ (1 - b^p)a_p = kn + sn = (k + s)n.$$

$$m = \sum_{i=0}^{p} a_i b^i = a_0 + a_1 b + \ldots + a_p b^p =$$

$$= a_0 + a_1 b + \ldots + a_p b^p - a_1 - \ldots - a_p + a_1 + \ldots + a_p =$$

$$= a_1(b - 1) + \ldots + a_p(b^p - 1) + a_0 + a_1 + \ldots + a_p =$$

$$= -sn + tn = (t - s)n.$$

Postbase Factor Theorem. If n is a postbase factor of b and $m = \sum_{i=0}^{p} a_i b^i = a_0 + a_1 b + \ldots + a_p b^p$, then $n \mid m$ if and only if $n \mid \sum_{i=0}^{p} (-1)^i a_i$.

Proof. Since n is a postbase factor, $n \mid b + 1$.

Since $b + 1 \mid 1 + b^i$, for $i = 1, 3, 5, \ldots$ and $b + 1 \mid 1 - b^i$, for $i = 2, 4, 6, \ldots$.

So, $n \mid -a_1(1 + b) + a_2(1 - b^2) - a_3(1 + b^3) + \ldots + a_p((-1)^p - b^p) = sn$.

Suppose $n \mid m$. Let $m = kn$.

$$\sum_{i=0}^{p} (-1)^i a_i = a_0 - a_1 + \ldots + (-1)^p a_p =$$

$$= a_0 - a_1 + a_2 - a_3 + \ldots + (-1)^p a_p + a_1 b + a_2 b^2 \ldots +$$

$$+ a_p b^p - a_1 b - \ldots - a_p b^p = -a_1(1 + b) +$$

$$+ a_2(1 - b^2) - a_3(1 + b^3) + \ldots + a_p((-1)^p - b^p) =$$

$$= kn + sn = (k + s)n.$$

Conversely, suppose $n \mid \sum_{i=0}^{p} (-1)^i a_i$. Let $\sum_{i=0}^{p} (-1)^i a_i = tn$.

$$m = \sum_{i=0}^{p} a_i b^i = a_0 + a_1 b + ... + a_p b^p = a_0 + a_1 b +$$

$$+ ... + a_p b^p - a_1 + a_2 - a_3 + ... + (-1)^p a_p + a_1 - a_2 +$$

$$+ a_3 - ... - (-1)^p a_p = a_0 - a_1 + a_2 - a_3 + ... +$$

$$+ (-1)^p a_p + a_1(b+1) - a_2(1-b^2) + a_1(1+b^3) +$$

$$+ ... - a_p((-1)^p - b^p) = tn - sn = (t-s)n.$$

Visualize Divisibility Theorem. If $y : x \in R_b(n)$, $(n, y) = 1$, $(n, b) = 1$, $m = bp + q$, then $n \mid m$ if and only if $n \mid qy - xp$.

Proof. Let, by Lemma, $x + by = \mu n$, for some integer μ.

Suppose $n \mid m$, i. e., $bp + q = \lambda n$, for some integer λ.

$$bpy + qy = \lambda ny;$$

$$bpy + xp - xp + qy = \lambda ny;$$

$$(x + by)p + (qy - xp) = \lambda ny;$$

$$\mu np + (qy - xp) = \lambda ny;$$

$$qy - xp = (\lambda y - \mu p)n.$$

Conversely, suppose $n \mid qy - xp$, i. e., $qy - xp = kn$, for some integer k.

$$\mu np + qy - xp = \mu np + kn;$$

$$(x + by)p + qy - xp = (\mu p + k)n;$$

$$xp + byp + qy - xp = (\mu p + k)n;$$

$$(bp + q)y = (\mu p + k)n.$$

Since $(n, y) = 1$, $n \mid bp + q$, i. e. $n \mid m$.

Convergence of Formulae. Using the best coefficient of a number n of a base b, and using the Visualize Divisibility Theorem, we will have a convergence formula for divisibility of the number n. For a number n belong to none of the set B_b, P_b or Q_b and $(n, b) \neq 1$, using combination formula of the formulae of its prime and power of prime factors.

Some Visualize Array and Some Examples.

1) *Finding ratio of 7 over base 10 on visualize array of base 10.*

Table 1

The visualize array of $R_{10}(7) = \{2 : 1, \ldots\}$

101	102	103	104	105	106	107	…	…	…
91	92	93	94	95	96	97	98	99	100
81	82	83	84	85	86	87	88	89	90
71	72	73	74	75	76	77	78	79	80
61	62	63	64	65	66	67	68	69	70
51	52	53	54	55	56	57	58	59	60
41	42	43	44	45	46	47	48	49	50
31	32	33	34	35	36	37	38	39	40
21	22	23	24	25	26	27	28	29	30
11	12	13	14	15	16	17	18	19	20
1	2	3	4	5	6	7	8	9	10

Note. Negative (gray) and positive (boundary).

2) *Some formulae of 7 over base 10.*

There were many convergence formulae of 7.

The best formula is using 2 : 1.

By Visualize Divisibility Theorem, $x = 1$, $y = 2$, $n = 7$, $b = 10$, $(7, 2) = 1$, $(7, 10) = 1$ and let $m = 10p + q$. Then 7 divides $p - 2q$ if and only if 7 divides m.

Another convergence formula is using –5 : 1.

By Visualize Divisibility Theorem, $x = 1$, $y = -5$, $n = 7$, $b = 10$, $(7, -5) = 1$, $(7, 10) = 1$ and let $m = 10p + q$. Then 7 divides $p + 5q$ if and only if 7 divides m.

3) *A formula of 43 over base 300.*

Table 2

The visualize array of $R_{300}(43) = \{1 : 1, \ldots\}$

2001	2002	2003	2004	2005	2006	…	2298	2299	3000
601	602	603	604	605	606	…	898	899	900
1001	1002	1003	1004	1005	1006	…	1298	1299	2000
301	302	303	304	305	306	…	598	599	600
1	2	3	4	5	6	…	298	299	1000
1	2	3	4	5	6	…	298	299	300

Note. Base 10 (gray), base 300 (white) and the best ratio (boundary).

We easily see that $n = 43$ is the postbase factor of $b = 300$, because $43 \cdot 7 = 300 + 1$.

$271\ 818\ 611\ 107_{10} = 33\ 167\ 106\ 237\ 007_{300}$.

By Postbase Factor Theorem, we use the different of alternate sum of digit, $33 - 167 + 106 - 237 + 7 = -258 = -43 \times 6$.

So, 271 818 611 107 is divisible by 43.

4) *Some formulae of 13 over base 1 000 000 and base 10.*

Table 3

The visualize array of $R_{1000000}(13) = \{-1 : 1, \ldots\}$

1'1	1'2	1'3	1'4	1'5	1'6	…	1'999 998	1'999 999	2'0
1	2	3	4	5	6	…	999 998	999 999	1'0

Note. Best ratio (boundary).

We see that $n = 13$ is the prebase factor of $b = 1000000$, because $13 \cdot 76\,923 = 1\,000\,000 - 1$.

Consider $3\ 937\ 376\ 385\ 699\ 289_{10} = 3\ 937'376\ 385'699\ 289_{1000000}$.

By Prebase Factor Theorem, we use the sum of digit, 3 937 + 376 385 + 699 289 = 1'079 611.

$$1 + 79\ 611 = 79\ 612.$$

The best ratio is –4 : 1.

By Visualize Divisibility Theorem, $x = 1$, $y = -4$, $n = 13$, $b = 10$, $(13, 4) = 1$, $(13, 10) = 1$ and let $m = 10p + q$.

If 13 divides $p + 4q$, then 13 divides m. So,

$79612 \Rightarrow 7961 + 4(2) = 7969;$

$\Rightarrow 796 + 4(9) = 832;$

$\Rightarrow 83 + 4(2) = 91;$

$\Rightarrow 9 + 4(1) = 13.$

Table 4

The visualize array of $R_{10}(13) = \{-4 : 1, \ldots\}$

51	52	53	54	55	56	57	58	59	60
41	42	43	44	45	46	47	48	49	50
31	32	33	34	35	36	37	38	39	40
21	22	23	24	25	26	27	28	29	30
11	12	13	14	15	16	17	18	19	20
1	2	3	4	5	6	7	8	9	10

Note. Best ratio (boundary).

5) *A formula for 24 combining 8 over base 1000 and 3 over base 10.*

Since 24 is the product of prime number 3 and power of prime 8.

So the number which is divisible by 8 and 3 is also divisible by 24.

Consider the number 229986788520 is divisible by 24 or not. Since 3 is prebase factor of 10, adding all digits, the result 66 is divisible by 3. Since 8 is base factor of 1000, the last digit 520 is divisible by 8.

Therefore, 229986788520 is divisible by 24.

Conclusion. The above four theorems can formulate for many divisibility rules for any number over the any base. Some numbers are although difficult over base 10, they are easy over another base. Some numbers, such as primes, have direct rules, but some composites have combined rules. It is useful for all learners and teachers in mental calculating and in manipulate.

Список литературы

1. Davenpot H. The Higher Arithmetic. Cambridge: Cambridge University Press, 1999. 251 p.

2. Rina Zazkis. Divisibility: a problem solving approach through generalizing and specializing // Humanistic Mathematics Network Journal. Issue 21. 1999. Article 15. P. 34–38.

3. William Stein. Elementary number theory: primes, congruence, and secrets, a computational approach. Springer, 2009. 168 p.

References

1. Davenpot H. The Higher Arithmetic. Cambridge, Cambridge University Press, 1999. 251 p.

2. Zazkis Rina. Divisibility: a problem solving approach through generalizing and specializing. *Humanistic Mathematics Network Journal*, issue 21, 1999, article 15, pp. 34–38.

3. William Stein. Elementary number theory: primes, congruence, and secrets, a computational approach. Springer, 2009. 168 p.

Информация об авторе

Тиха Бо – доктор философии (математика). Университет Мандалая (Yangon-Mandalay Street, Nat Yay Kan Village, Amarapura Township Mandalay). E-mail: tbo290483@gmail.com

Information about the author

Thiha Bo − Doctor of Philosophy (Mathematics). Mandalar University (Yangon-Mandalay Street, Nat Yay Kan Village, Amarapura Township Mandalay). E-mail: tbo290483@gmail.com

Поступила после доработки 10.01.2022