

初等数论

吴伊涛

2022 年春

- Division Algorithm

$$30 \div 11 = 2 \cdots 8$$

30: dividend(被除数)

11: divisor(除数)

2: quotient(商)

8: remainder(余数)

$$-19 \div 8 = -3 \cdots 5$$

-19: dividend(被除数)

8: divisor(除数)

-3: quotient(商)

5: remainder(余数)



Division Algorithm

Lemma: Let a be an integer, b be a **positive** integer, then there **exist unique** integers q, r , such that

$$a = qb + r$$

with $0 \leq r < b$

$(\forall a \in \mathbb{Z}, b \in \mathbb{Z}^+, \exists! q, r \in \mathbb{Z}, \text{ s.t. } a = qb + r \text{ with } 0 \leq r < b)$

Remark 1:

a : dividend

b : divisor

q : quotient

r : remainder

Remark 2: Need to prove both **Existence**(存在性) and **Uniqueness**(唯一性).

Proof of Existence:

Note that there exists a unique integer n , s.t.

$$nb \leq a < (n+1)b$$

Just let $q = n, r = a - nb$.

Clearly $q, r \in \mathbb{Z}$ and $a = qb + r$, we only need to prove $0 \leq r < b$, which follows from

$$0 \leq r = a - nb < (n+1)b - nb = b.$$

□

Another Proof of Existence:

Consider the set $\{a - xb : x \in \mathbb{Z}\}$ (i.e. the set $\{a, a - b, a + b, a - 2b, a + 2b, \dots\}$).

Clearly, there are positive integers in this set (since $\lim_{x \rightarrow +\infty} a + xb = +\infty$).

Let r be the minimal nonnegative integer in this set. (Why r exists ?)

Claim: $0 \leq r < b$.

Otherwise, $r \geq b$, then $r - b \geq 0$ is a nonnegative integer in the set $\{a - xb : x \in \mathbb{Z}\}$,

but $r - b < r$, contradicts to the minimal assumption of r .

So, by definition of r , there exists an integer q , s.t. $r = a - qb$. We get the required

q, r .

□



Proof of Uniqueness:

Suppose we have $a = q_1b + r_1 = q_2b + r_2$, both satisfy the requirements. We need to show

$$q_1 = q_2, \quad r_1 = r_2$$

In fact,

$$q_1b + r_1 = q_2b + r_2$$

which leads to

$$(q_1 - q_2)b = r_2 - r_1 \quad (*)$$

Since $0 \leq r_1, r_2 \leq b - 1$, we have

$$b \cdot (-1) < 0 - (b - 1) \leq r_2 - r_1 \leq (b - 1) - 0 < b \cdot 1$$

So the only possible solution of $(*)$ is $r_2 - r_1 = b \cdot 0 = 0$.

Thus $r_1 = r_2, q_1 = q_2$, we get the uniqueness.

□



Remark

1. Division Algorithm for all divisors: Let a be an integer, b be a **nonzero** integer, then there **exist unique** integers q, r , such that

$$a = qb + r$$

with $0 \leq r < |b|$

$(\forall a \in \mathbb{Z}, b \in \mathbb{Z}^+, \exists! q, r \in \mathbb{Z}, \text{ s.t. } a = qb + r \text{ with } 0 \leq r < |b|)$

2. Assume the remainder of a divides by b is r , note that the remainder of a divides by $-b$ is still r , NOT $-r$. e.g.

$$30 \div 11 = 2 \cdots 8$$

$$30 \div (-11) = -2 \cdots 8$$

3. Assume the remainder of a divides by b is r , note that the remainder of $-a$ divides by b is NOT $-r$. e.g.

$$30 \div 11 = 2 \cdots 8$$

$$(-30) \div 11 = -3 \cdots 3$$



Representation of Integers

Recall the "decimal representation of integers":

$$2022 = 2 \times 10^3 + 0 \times 10^2 + 2 \times 10 + 2$$

$$1235 = 1 \times 10^3 + 2 \times 10^2 + 3 \times 10 + 5$$

ALL integers have the "decimal representation"!



base b-representation of integers


Theorem: Fix b be an integer greater than 1, then every positive integer n can be written **uniquely** in the following form

$$n = c_k b^k + c_{k-1} b^{k-1} + \cdots + c_1 b + c_0 \times b^0$$

where k is a nonnegative integer, $c_0, c_1, \cdots, c_{k-1}$ are integers lie in $[0, b-1]$, c_k is an integer lie in $[1, b-1]$.

Definition: We then write $n = (c_k c_{k-1} \cdots c_1 c_0)_b$, called the **base b-expansion**(**base b-representation**) of n . c_0, c_1, \cdots, c_k are called the digits of n , c_k is called the leading digit of n .

In case $b = 10$, we just write $n = c_k c_{k-1} \cdots c_1 c_0$.



Proof of theorem:

Existence:

Use induction on n .

When $n = 1$, then $n = 1 \times b^0 = (1)_b$.

When $n = 2$, then $n = 2 \times b^0 = (2)_b$.

\dots When $n = b - 1$, then $n = (b - 1) \times b^0 = (b - 1)_b$.

When $n = b$, then $n = 1 \times b = (10)_b$.

(Why these steps?)

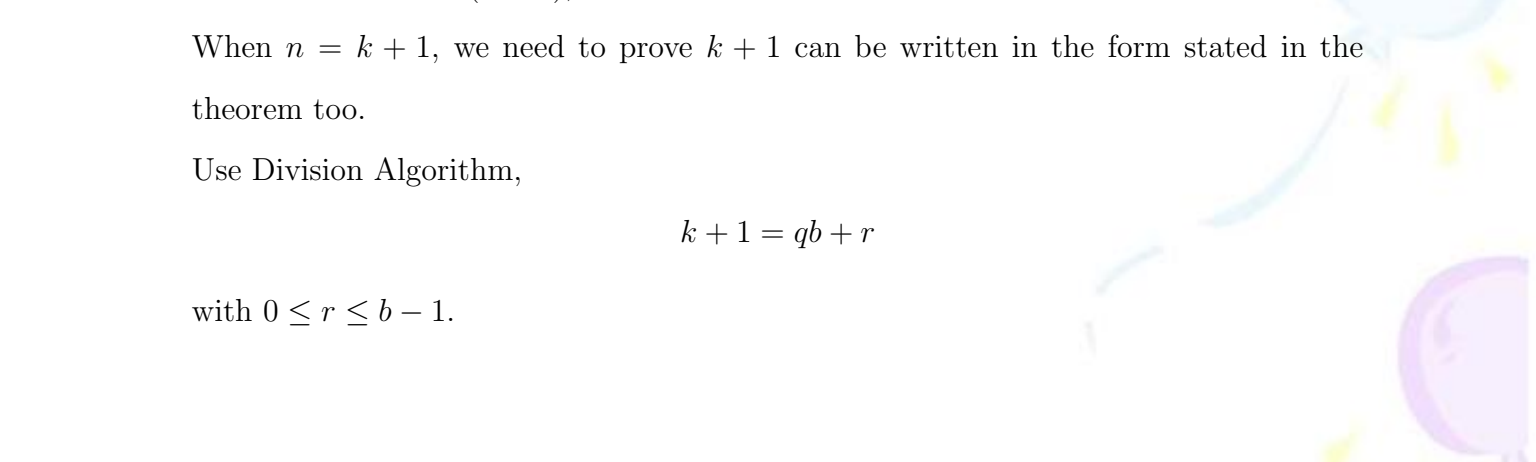
Assume when $n \leq k$ ($k \geq b$), the statement holds.

When $n = k + 1$, we need to prove $k + 1$ can be written in the form stated in the theorem too.

Use Division Algorithm,

$$k + 1 = qb + r$$

with $0 \leq r \leq b - 1$.



Clearly, q is a positive integer smaller than or equal to $k(q \leq \frac{k+1}{b} \leq \frac{k+1}{2} \leq k)$, so by induction hypothesis, $q = (a_l a_{l-1} \cdots a_1 a_0)_b$. Then $k+1 = (a_l a_{l-1} \cdots a_1 a_0 r)_b$ (Check this!).

Uniqueness:

Assume $n = (c_k c_{k-1} \cdots c_1 c_0)_b = (d_t d_{t-1} \cdots d_1 d_0)_b$, we need to show:

$$k = t, c_k = d_t, c_{k-1} = d_{t-1}, \cdots, c_1 = d_1, c_0 = d_0$$

If $k \neq t$, without loss of generality (WLOG for short), assume $k > t$, then

$$(c_k c_{k-1} \cdots c_1 c_0)_b \geq (10 \cdots 00)_b = b^k$$

$$(d_t d_{t-1} \cdots d_1 d_0)_b \leq (b-1, b-1, \cdots, b-1, b-1)_b = b^{t+1} - 1 < b^k$$

A contradiction. Thus $k = t$.

Now, assume $s = \max\{i : c_i \neq d_i\}$, WLOG, assume $c_s > d_s$, then

$$(c_k c_{k-1} \cdots c_1 c_0)_b \geq (c_k c_{k-1} \cdots c_s, 0, \cdots, 0)_b = (c_k c_{k-1} \cdots c_s - 1, b-1, \cdots, b-1)_{b+1} > (d_t d_{t-1} \cdots d_1 d_0)_b$$

A contradiction. □

base b-expansion(representation) of integers

- $b=2$: binary representation(二进制表示), BINARY
- $b=10$: decimal representation(十进制表示), DEC
- $b=16$: hexadecimal representation(十六进制表示), HEX
- $b=8$: octal representation(八进制表示), OCT
- $b=12$: duodecimal representation(十二进制表示), DUO

base change

Example 1: Convert $(2021)_3$ to decimal representation.

Solution:

$$(2022)_3 = 2 \times 3^3 + 2 \times 3 + 2 = 62$$

Example 2: Convert $(5AC)_{16}$ to decimal representation.

Solution:

(Note that, In HEX, $(A)_{16} = 10$, $(B)_{16} = 11$, $(C)_{16} = 12$, $(D)_{16} = 13$, $(E)_{16} = 14$, $(F)_{16} = 15$)

$$(5AC)_{16} = 5 \times 16^2 + 10 \times 16 + 12 = 1452$$

Eg. Convert 209 to binary representation.

Sol:

2	209	1
	104	0
	52	0
	26	0
	13	1
	6	0
	3	1
	1	1
	0	

$$209 = (11010001)_2$$

Eg. Convert 605 to HEX.

Sol:

16	605	13
	37	5
	2	2
	0	

$$\therefore 13 = (D)_{16}$$

$$\therefore 605 = (25D)_{16}$$

Eg. Convert $(2022)_9$ to base-11 representation.

Sol:

$$(2022)_9 = 2 \times 9^3 + 2 \times 9 + 2 = 1478$$

$$\begin{array}{r|l} 11 & 1478 \\ & 134 \\ & 12 \\ & 1 \\ & 0 \end{array} \begin{array}{l} 4 \\ 2 \\ 1 \\ 1 \end{array}$$

$$\therefore 1478 = (1124)_{11}$$

$$\therefore (2022)_9 = (1124)_{11}$$

Eg 4. Convert $(314)_{16}$ to binary.

(14)

Sol: Note that $16 = 2^4$, so we just need to convert each digit in the hexadecimal representation of $(314)_{16}$ to a 4-digits binary representation.

$$(3)_{16} = (0011)_2, (1)_{16} = (0001)_2, (4)_{16} = (0100)_2$$

$$\therefore (314)_{16} = (0011\ 0001\ 0100)_2 \\ = (1100010100)_2$$

Eg 5. Convert $(1100100101)_2$ to octal.

Sol: Since $8 = 2^3$, so we just need to convert every 3-digits in the octal representation (from right to left) to a digit in octal.

$$(11, 001, 001, 101)_2 = (3115)_8 \\ \begin{matrix} \text{"} & \text{"} & \text{"} & \text{"} \\ (3)_8 & (1)_8 & (1)_8 & (5)_8 \end{matrix}$$

Eg 6. Convert $(ABC)_{16}$ to octal.

$$\text{Sol: } (ABC)_{16} = (101010111100)_2 \\ = (101, 010, 111, 100)_2 \\ = (5274)_8$$

1	101
0	010
0	111
0	100

1	1
0	0
1	1
1	1
0	0

Remark

1. Similarly, we have a fast base change between base-3, base-9, base-27 representations of integers, summarize the method yourself.



Eg. $(1235)_8 + (116)_8$.

Sol:

	1	2	3	5
+		1	1	6
<hr/>				
8	1	3	5	3

$$\therefore (1235)_8 + (116)_8 = (1353)_8.$$

Eg. $(1235)_8 - (443)_8$

Sol:

	1	2	3	5
		4	4	3
8	<hr/>			
	5	7	2	

$$\therefore (1235)_8 - (443)_8 = (572)_8$$

Integers with missing digits

Recall the "probability" or "density":

If we have 3 red balls and 8 blue balls, then we can say:

then density of red balls in whole is $\frac{3}{3+8} = \frac{3}{11}$.

or

If we choose a ball randomly, then the probability of the chosen ball is a red ball is

$$\frac{3}{3+8} = \frac{3}{11}.$$

The above is a FINITE case. How about the infinite case?

It seems natural if we say that even positive numbers are just $\frac{1}{2}$ of all positive integers,

but it makes nonsense to calculate $\frac{\text{number of all positive even numbers}}{\text{number of all positive integers}}$, because it is $\frac{\infty}{\infty}$.

So, what can we say about the "density" of all even positive numbers in all positive integers?

The idea is using "Limit".

Let's consider the "density" of all even positive numbers smaller than or equal to n in all positive integers smaller than or equal to n , this is a finite case, and could be calculated as:

$$p(n) = \frac{\text{number of all positive even numbers} \leq n}{n}$$

Clearly, if $n = 2k$, then *number of all positive even numbers* $\leq n = k$;

if $n = 2k + 1$, then *number of all positive even numbers* $\leq n = k$.

So, if $n = 2k$, then $p(n) = \frac{k}{2k} = \frac{1}{2}$;

if $n = 2k + 1$, then $p(n) = \frac{k}{2k+1}$.

It's easy to get

$$\lim_{n \rightarrow \infty} p(n) = \frac{1}{2}$$

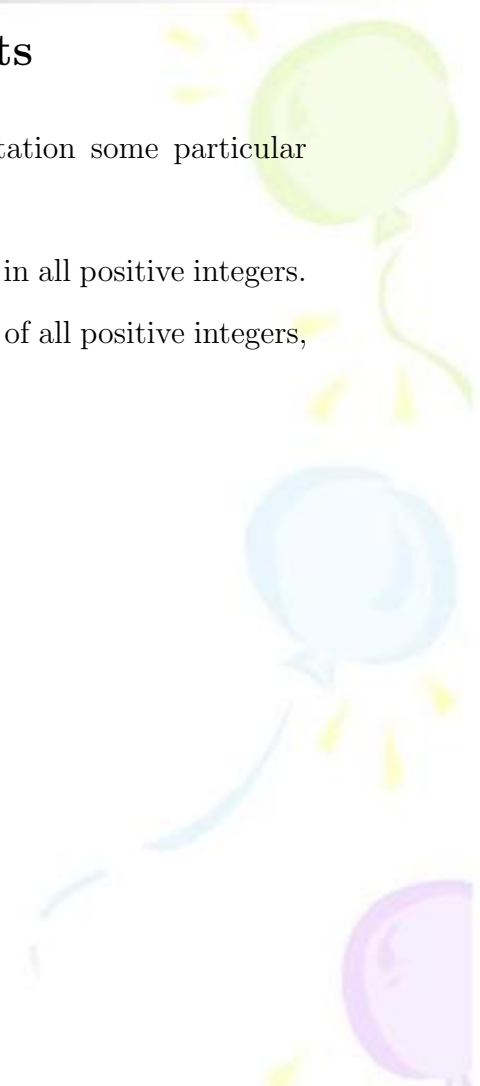
Thus it's reasonable to say that even positive numbers are just $\frac{1}{2}$ of all positive integers.

Integers with missing digits

Now, let's consider positive integers whose (decimal) representation some particular digit such as "9" is missing, e.g. 2333, 12306, 10086, ...

We want to compute the density of this kind of positive integers in all positive integers.

It might seem at first as if the restriction should only exclude $\frac{1}{10}$ of all positive integers, but this is far from the truth...



Theorem: Almost all positive integers contain the digit "9", i.e. If we let $N(n)$ be the number of positive integers $\leq n$ whose decimal expansions do not contain the digit "9", then

$$\lim_{n \rightarrow \infty} \frac{N(n)}{n} = 0$$

Proof:

Note that the number of k -digits integers without a digit 9 (in its decimal representation) is $9^{k-1} \times 8$ (Since in the decimal representation of a k -digits integers, the leading digit has 8 choices, the other digits have 9 choices).

Thus, if $10^{l-1} \leq n < 10^l$, then

$$N(n) \leq 8 + 9 \times 8 + 9^2 \times 8 + \cdots + 9^{l-1} \times 8 = 9^l - 9$$

$$0 \leq \lim_{n \rightarrow \infty} \frac{N(n)}{n} \leq \lim_{l \rightarrow \infty} \frac{9^l - 9}{10^{l-1}} = 0$$

Thus

$$\lim_{n \rightarrow \infty} \frac{N(n)}{n} = 0$$

Remark

1. You can replace the digit "9" by other digits like "0", "1", ... "8", proof is similar.
2. You can replace the decimal expansion by other base b -expansion, proof is similar.
3. You can even replace the digit "9" by a string like "2022":

Theorem: Almost all positive integers contain the chain "2022", i.e.

If we let $N(n)$ be the number of positive integers $\leq n$ whose decimal expansions do not contain the chain "2022" (e.g. 20220228 contains the chain 2022, while 20200222 does not contain the chain 2022), then

$$\lim_{n \rightarrow \infty} \frac{N(n)}{n} = 0$$

(Think how to prove it?)

Representation of Real numbers

Recall the "decimal representation of real numbers":

$$2022.38 = 2 \times 10^3 + 0 \times 10^2 + 2 \times 10 + 2 + 3 \times 10^{-1} + 8 \times 10^{-2}$$

$$2.333 = 2 + 3 \times 10^{-1} + 3 \times 10^{-2} + 3 \times 10^{-3}$$

$$2.\dot{3} = 2.333\ldots = 2 + 3 \times 10^{-1} + 3 \times 10^{-2} + 3 \times 10^{-3} + \ldots$$

ALL real numbers have the "decimal representation"!


Compare to the representation of integers, we may guess:

Every positive real number x can be written **uniquely** in the following form:

$$x = c_k b^k + c_{k-1} b^{k-1} + \cdots + c_1 b + c_0 \times b^0 + a_1 \times b^{-1} + a_2 \times b^{-2} + a_3 \times b^{-3} \cdots$$

i.e.

$$x = (c_k c_{k-1} \cdots c_1 c_0 . a_1 a_2 a_3 \cdots)_b$$



E.g. $b = 10, x = 0.99999 \dots$ Then

$$0.99999 \dots = 9 \times 10^{-1} + 9 \times 10^{-2} + 9 \times 10^{-3} + \dots = \frac{\frac{9}{10}}{1 - \frac{1}{10}} = 1$$

So 1 has two decimal representation(as a real number): $(1)_{10}$ and $(0.99999 \dots)_{10}$.

Uniqueness failed !



Representation of Real numbers

Theorem: Fix b be an integer greater than 1, then every positive real number x can be written **uniquely** in the following form

$$x = (c_k c_{k-1} \cdots c_1 c_0 . a_1 a_2 a_3 \cdots)_b = c_k b^k + c_{k-1} b^{k-1} + \cdots + c_1 b + c_0 \times b^0 + a_1 \times b^{-1} + a_2 \times b^{-2} + a_3 \times b^{-3} \cdots$$

where k is a nonnegative integer, $c_0, c_1, \cdots, c_{k-1}$ are integers lie in $[0, b-1]$, c_k is an integer lie in $[1, b-1]$, $a_1, a_2, a_3 \cdots$ are all integers lie in $[0, b-1]$, and **for infinitely many i , $a_i \leq b-2$** .

Proof: Omitted, see page 346 of textbook.

Examples: $x = \frac{1}{3}$

- decimal representation:

$$\frac{1}{3} = 0.\dot{3} = 0.333\cdots$$

- base-3 representation:


$$\frac{1}{3} = (0.1)_3$$

- binary representation:

$$\frac{1}{3} = \frac{1}{4-1} = \frac{\frac{1}{4}}{1-\frac{1}{4}} = \frac{1}{4} + \left(\frac{1}{4}\right)^2 + \left(\frac{1}{4}\right)^3 + \cdots = (0.010101\cdots)_2 = (0.\dot{0}\dot{1})_2$$

- base-5 representation:

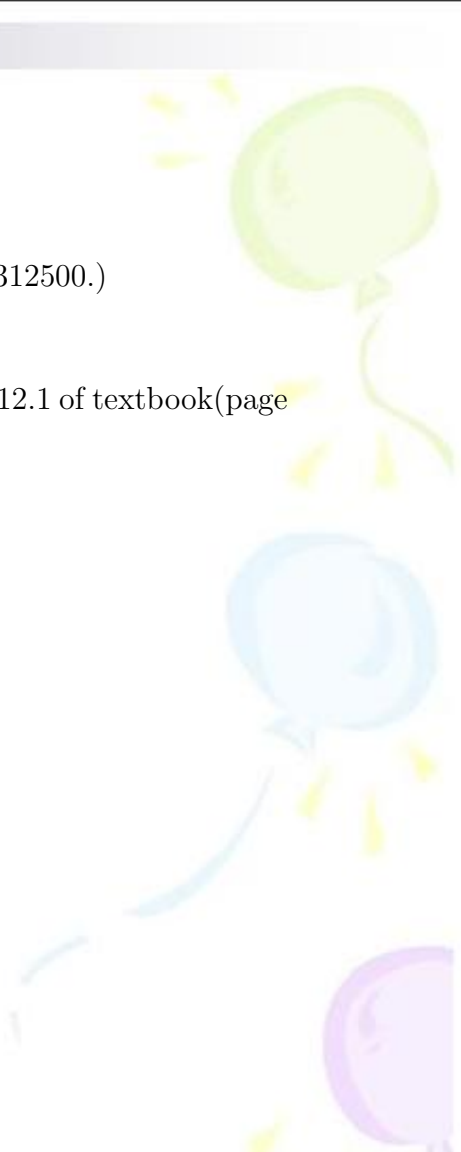
$$\frac{1}{3} = \frac{8}{25-1} = \frac{\frac{8}{25}}{1-\frac{1}{25}} = 8 \times \frac{1}{25} + 8 \times \left(\frac{1}{25}\right)^2 + 8 \times \left(\frac{1}{25}\right)^3 + \cdots = (0.131313\cdots)_5 = (0.\dot{1}\dot{3})_5$$



Exercise: Convert 0.20220301 to binary representation.

(the period length of the binary representation of 0.20220301 is 312500.)

For more materials of the representation of real numbers, see chap12.1 of textbook (page 346-355).



谢谢！

