Remainder

In mathematics, the **remainder** is the amount "left over" after performing some computation. In arithmetic, the remainder is the integer "left over" after dividing one integer by another to produce an integer quotient (integer division). In algebra of polynomials, the remainder is the polynomial "left over" after dividing one polynomial by another. The *modulo operation* is the operation that produces such a remainder when given a dividend and divisor.

Alternatively, a remainder is also what is left after subtracting one number from another, although this is more precisely called the *difference*. This usage can be found in some elementary textbooks; colloquially it is replaced by the expression "the rest" as in "Give me two dollars back and keep the rest."[1] However, the term "remainder" is still used in this sense when a function is approximated by a series expansion, where the error expression ("the rest") is referred to as the remainder term.

Integer division

Given an integer a and a non-zero integer d, it can be shown that there exist unique integers q and r, such that $a = qd + r$ and $0 \leq r < |d|$. The number q is called the *quotient*, while r is called the *remainder*.

(For a proof of this result, see Euclidean division. For algorithms describing how to calculate the remainder, see division algorithm.)

The remainder, as defined above, is called the *least positive remainder* or simply the *remainder*.[2] The integer a is either a multiple of d, or lies in the interval between consecutive multiples of d, namely, $q \cdot d$ and $(q + 1)d$ (for positive q).

In some occasions, it is convenient to carry out the division so that a is as close to an integral multiple of d as possible, that is, we can write

$$a = k \cdot d + s, \text{ with } |s| \leq |d/2| \text{ for some integer } k.$$

In this case, s is called the *least absolute remainder*.[3] As with the quotient and remainder, k and s are uniquely determined, except in the case where $d = 2n$ and $s = \pm n$. For this exception, we have:

$$a = k \cdot d + n = (k + 1)d - n.$$

A unique remainder can be obtained in this case by some convention—such as always taking the positive value of s.

Examples

In the division of 43 by 5, we have:

$$43 = 8 \times 5 + 3,$$

so 3 is the least positive remainder. We also have that:

$$43 = 9 \times 5 - 2,$$

and −2 is the least absolute remainder.

These definitions are also valid if d is negative, for example, in the division of 43 by −5,

$$43 = (-8) \times (-5) + 3,$$

and 3 is the least positive remainder, while,

$$43 = (-9) \times (-5) + (-2)$$

and −2 is the least absolute remainder.

In the division of 42 by 5, we have:

$$42 = 8 \times 5 + 2,$$

and since $2 < 5/2$, 2 is both the least positive remainder and the least absolute remainder.

In these examples, the (negative) least absolute remainder is obtained from the least positive remainder by subtracting 5, which is d. This holds in general. When dividing by d, either both remainders are positive and therefore equal, or they have opposite signs. If the positive remainder is r_1, and the negative one is r_2, then

$$r_1 = r_2 + d.$$

For floating-point numbers

When a and d are floating-point numbers, with d non-zero, a can be divided by d without remainder, with the quotient being another floating-point number. If the quotient is constrained to being an integer, however, the concept of remainder is still necessary. It can be proved that there exists a unique integer quotient q and a unique floating-point remainder r such that $a = qd + r$ with $0 \le r < |d|$.

Extending the definition of remainder for floating-point numbers, as described above, is not of theoretical importance in mathematics; however, many programming languages implement this definition (see modulo operation).

In programming languages

While there are no difficulties inherent in the definitions, there are implementation issues that arise when negative numbers are involved in calculating remainders. Different programming languages have adopted different conventions. For example:

- Pascal chooses the result of the *mod* operation positive, but does not allow d to be negative or zero (so, $a = (a \text{ div } d) \times d + a \text{ mod } d$ is not always valid).[4]
- C99 chooses the remainder with the same sign as the dividend a.[5] (Before C99, the C language allowed other choices.)
- Perl, Python (only modern versions) choose the remainder with the same sign as the divisor d.[6]
- Scheme offer two functions, *remainder* and *modulo* – Ada and PL/I have *mod* and *rem*, while Fortran has *mod* and *modulo*; in each case, the former agrees in sign with the dividend, and the latter with the divisor. Common Lisp and Haskell also have *mod* and *rem*, but *mod* uses the sign of the divisor and *rem* uses the sign of the dividend.

Polynomial division

Euclidean division of polynomials is very similar to Euclidean division of integers and leads to polynomial remainders. Its existence is based on the following theorem: Given two univariate polynomials $a(x)$ and $b(x)$ (where $b(x)$ is a non-zero polynomial) defined over a field (in particular, the reals or complex numbers), there exist two polynomials $q(x)$ (the *quotient*) and $r(x)$ (the *remainder*) which satisfy:[7]

$$a(x) = b(x)q(x) + r(x)$$

where

$$\deg(r(x)) < \deg(b(x)),$$

where "deg(...)" denotes the degree of the polynomial (the degree of the constant polynomial whose value is always 0 can be defined to be negative, so that this degree condition will always be valid when this is the remainder). Moreover, $q(x)$ and $r(x)$ are uniquely determined by these relations.

This differs from the Euclidean division of integers in that, for the integers, the degree condition is replaced by the bounds on the remainder r (non-negative and less than the divisor, which insures that r is unique.) The similarity between Euclidean division for integers and that for polynomials motivates the search for the most general algebraic setting in which Euclidean division is valid. The rings for which such a theorem exists are called Euclidean domains, but in this generality, uniqueness of the quotient and remainder is not guaranteed.[8]

Polynomial division leads to a result known as the polynomial remainder theorem: If a polynomial $f(x)$ is divided by $x - k$, the remainder is the constant $r = f(k)$.[9][10]

See also

- Chinese remainder theorem

- Divisibility rule
- Egyptian multiplication and division
- Euclidean algorithm
- Long division
- Modular arithmetic
- Polynomial long division
- Synthetic division
- Ruffini's rule, a special case of synthetic division
- Taylor's theorem

Notes

1. Smith 1958, p. 97
2. Ore 1988, p. 30. But if the remainder is 0, it is not positive, even though it is called a "positive remainder".
3. Ore 1988, p. 32
4. Pascal ISO 7185:1990 (http://pascal-central.com/iso7185.html) 6.7.2.2
5. "6.5.5 Multiplicative operators". C99 specification (ISO/IEC 9899:TC2) (http://www.open-std.org/jtc1/sc22/wg14/www/docs/n1124.pdf) (PDF) (Report). 6 May 2005. Retrieved 2018-08-16.
6. "Built-in Functions — Python 3.10.7 documentation" (https://docs.python.org/3.10/library/functions.html#divmod). 9 September 2022. Retrieved 2022-09-10.
7. Larson & Hostetler 2007, p. 154
8. Rotman 2006, p. 267
9. Larson & Hostetler 2007, p. 157
10. Weisstein, Eric W. "Polynomial Remainder Theorem" (https://mathworld.wolfram.com/PolynomialRemainderTheorem.html). *mathworld.wolfram.com*. Retrieved 2020-08-27.

References

- Larson, Ron; Hostetler, Robert (2007), *Precalculus:A Concise Course* (https://archive.org/details/precalculusconci00lars), Houghton Mifflin, ISBN 978-0-618-62719-6
- Ore, Oystein (1988) [1948], *Number Theory and Its History* (https://archive.org/details/numbertheoryitsh0000orey), Dover, ISBN 978-0-486-65620-5
- Rotman, Joseph J. (2006), *A First Course in Abstract Algebra with Applications* (3rd ed.), Prentice-Hall, ISBN 978-0-13-186267-8
- Smith, David Eugene (1958) [1925], *History of Mathematics, Volume 2*, New York: Dover, ISBN 0486204308

Further reading

- Davenport, Harold (1999). *The higher arithmetic: an introduction to the theory of numbers*. Cambridge, UK: Cambridge University Press. p. 25. ISBN 0-521-63446-6.
- Katz, Victor, ed. (2007). *The mathematics of Egypt, Mesopotamia, China, India, and Islam : a*

sourcebook. Princeton: Princeton University Press. ISBN 9780691114859.

- Schwartzman, Steven (1994). "remainder (noun)" (https://archive.org/details/wordsofmathemati0000schw). *The words of mathematics : an etymological dictionary of mathematical terms used in english*. Washington: Mathematical Association of America. ISBN 9780883855119.
- Zuckerman, Martin M (December 1998). *Arithmetic: A Straightforward Approach*. Lanham, Md: Rowman & Littlefield Publishers, Inc. ISBN 0-912675-07-1.
