Modulo Intervals: A Proposed Notation

Nachum Dershowitz* Edward M. Reingold†

April 3, 2012

> "We must admit with humility that, while number is purely
> a product of our minds, space has a reality outside our minds,
> so that we cannot completely prescribe its properties a priori."
> Carl Friedrich Gauss in a letter to Friedrich Bessel (1830)

We propose extending the standard modulus notation to take an interval as the modulus, rather than a divisor. An *interval-modulus*

$$x \bmod \mathcal{I}$$

shifts a real-valued x into the half-open real interval $\mathcal{I}$ by adding a multiple of the length of $\mathcal{I}$. As we will see, such notation would be quite useful in computer science.

Using the "double-dot" notation .. for interval ranges, as suggested by C. A. R. Hoare and L. Ramshaw (see [4, p. 73]), we define,

$$x \bmod [a\,..\,b) \stackrel{\text{def}}{=} \begin{cases} x - (b-a)\left\lfloor \dfrac{x-a}{b-a} \right\rfloor & \text{if } a \neq b, \\ x & \text{if } a = b. \end{cases} \tag{1}$$

This definition is equivalent to saying

$$x \bmod [a\,..\,b) \stackrel{\text{def}}{=} a + (x-a) \bmod (b-a),$$

where the mod operator on the right is the usual mathematical one, with the convention that $x \bmod 0 = x$, so that the definition makes sense even when $a = b$. That is, following [4, p. 82], $x \bmod y = x - y\lfloor x/y \rfloor$ for $y \neq 0$, and $x \bmod 0 = x$. We use Definition (1) because we want the usual mathematical mod (when $a = 0$) as a special case. Definition (1) works perfectly well when the interval is given backward, that is, $a > b$, yielding a modulus in the right-closed interval $(b\,..\,a]$. It follows from Definition (1) that $a \leq x \bmod [a\,..\,b) < b$ if $a < b$, but $b < x \bmod [a\,..\,b) \leq a$ when $a > b$. Definition (1) allows us to define the analogous equivalence relation,

$$x \equiv y \pmod{\mathcal{I}} \quad \text{if and only if} \quad x \bmod \mathcal{I} = y \bmod \mathcal{I}.$$

As noted, $x \bmod (b\,..\,a] = x \bmod [a\,..\,b)$ and the former may be preferable when $b < a$. Thus the year in the century is $y \bmod (0\,..\,100]$, which gives a value from 1 to 100. In such a case, where we are working purely with integers, it would be clearer to write the century year as $y \bmod [1\,..\,100]$, where we define

$$n \bmod [a\,..\,b] \stackrel{\text{def}}{=} n \bmod [a\,..\,b+1)$$

*School of Computer Science, Tel Aviv University, Tel Aviv 69978, Israel. Research done partly while on leave at INRIA-LIAMA (Sino French Lab in Computer Science, Automation and Applied Mathematics), Tsinghua University, Beijing, China. Email: nachum@tau.ac.il

†Department of Computer Science, Illinois Institute of Technology, 10 West 31st Street, Chicago, Illinois 60616-2987, USA. Email: reingold@iit.edu

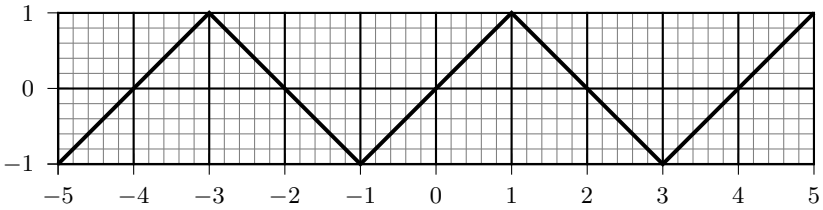

Figure 1: The triangular wave function $t(x)$ is tersely by modulus intervals in equation (2).

for integers n, a, and b. Thus, $h \bmod [1\,..\,12]$, converts an hour h, $0 \le h \le 24$, from 24-hour notation to 12-hour notation.

A different notion of "modulo interval" was suggested in [7] (see also [6]) for using interval arithmetic to analyze repetitive program constructs. It is defined by

$$[a, b]_{n(\ell)} = \{nk + \ell \colon a \le nk + \ell \le b, k \in \mathbf{Z}\},$$

where $a \le b$ are real numbers and n and ℓ are integers. This definition yields a set of integer values, all within the given closed real interval $[a\,..\,b]$. Our $\ell \bmod [a\,..\,b]$, for integers ℓ, a, and b, could be expressed as their $[a, b]_{b-a+1(\ell)}$, which gives exactly one integer in $[a\,..\,b]$. Although a bit awkward, we could use our interval-modulus to extend the notation of [6, 7] to non-integers by defining

$$[a, b)_{c(x)} \stackrel{\text{def}}{=} \{x \bmod [a + ck\,..\,a + ck + c) : k = 0\,..\,\lfloor (b - a)/c \rfloor\}\,,$$

to give the set of all $x + cj$ in $[a\,..\,b)$. Then $[a, b]_{n(\ell)} = [a, \lfloor b + 1 \rfloor)_{n(\ell)}$ for integers n and ℓ.

Note that the usual mathematical mod function does not behave like the remainder operation in most programming languages, such as $x \,\%\, y$ in C (ISO 1999), which is actually $(\operatorname{sign} x)(x \bmod y)$, and is usually defined only for integers (see [1]). This disagreement is a source of difficult-to-detect programming errors, especially in writing calendrical functions [3].

Our notation allows us to express many things concisely. For example, to convert an angle α, measured in degrees, to a standard longitude (hour angle) in the range $[-180\,..\,180]$, one can use either $\alpha \bmod [-180\,..\,180)$ or $\alpha \bmod [180\,..\,-180)$, the former giving -180 instead of the equivalent 180 of the latter. Such range reduction is critical in obtaining accurate elementary function routines; see [2].

As another example, the piecewise-linear *triangle wave* function, shown in Figure 1, is defined for an integer x as

$$t(x) = \begin{cases} 0 & \text{if } x \equiv 0 \pmod 2, \\ 1 & \text{if } x \equiv 1 \pmod 4, \\ -1 & \text{if } x \equiv -1 \pmod 4, \end{cases}$$

but is awkward to describe for non-integer real values of x. It can be neatly specified in general, for all real x, as

$$t(x) = 1 - |1 - x \bmod [-1\,..\,3)\,|. \tag{2}$$

Applying this idea allows us to convert an angle to the standard range $[-90\,..\,90]$ used for latitude or declination by writing $90 - |90 - \alpha \bmod [-90\,..\,270)\,|$, which is equivalent to $90 - |(\alpha + 180) \bmod [-180\,..\,180)\,|$ or $90 - |180 - (\alpha + 90) \bmod 360|$.

The identity

$$(-x) \bmod [-a\,..\,-b) = -\,(x \bmod [a\,..\,b))\,,$$

holds as a special case of multiplicative distributivity,

$$c\,(x \bmod [a\,..\,b)) = cx \bmod [ca\,..\,cb)\,.$$

Multiplication distributes properly for $c = 0$ because of the zero-modulus convention. Addition also distributes,

$$c + x \bmod [a\,..\,b) = (c + x) \bmod [c + a\,..\,c + b)\,.$$

Various common functions are simply and compactly defined in terms of modulus intervals:

$$\begin{array}{rcll}
x \bmod y & = & x \bmod [0\,..\,y) & \text{ordinary modulus [4, p. 82]} \\
x \operatorname{amod} y & = & x \bmod (0\,..\,y] & \text{adjusted modulus (variant) [3, p. 19]} \\
x \operatorname{mumble} y & = & -x \bmod [0\,..\,y) & \text{mumble [4, p. 97]} \\
\{x\} & = & x \bmod [0\,..\,1) & \text{fractional part [4, p. 70]} \\
\lfloor x \rfloor & = & 0 \bmod (x-1\,..\,x] & \text{integer part [5, p. 12]} \\
\lceil x \rceil & = & 0 \bmod [x\,..\,x+1) & \text{ceiling [5, p. 12]} \\
x \bmod^* y & = & x \bmod \left[y-\tfrac{1}{2}\,..\,y+\tfrac{1}{2}\right) & \text{mod-star [2, eqn. (2)]}
\end{array}$$

There are many versions of rounding (see `http://en.wikipedia.org/wiki/Rounding#Tie-breaking`), but the two most common [4, p. 95] are either always to round down to $\lfloor x \rfloor$ or always to round up to $\lceil x \rceil$ when a number x is halfway between two integers:

$$\begin{aligned}
\operatorname{round}^-(x) &= 0 \bmod \left[x-\tfrac{1}{2}\,..\,x+\tfrac{1}{2}\right) \\
\operatorname{round}^+(x) &= 0 \bmod \left(x-\tfrac{1}{2}\,..\,x+\tfrac{1}{2}\right]
\end{aligned}$$

All of the above expressions for the common functions follow easily from Definition (1).

As a final, convincing example of the utility of the modulo interval notation, we give a short, straightforward evaluation of the non-trivial sum

$$\sum_{0\le k<m} \left\lfloor \frac{nk+x}{m} \right\rfloor,$$

where $m > 0$ and n are integers and x is real. This summation is the subject of a lengthy and subtle derivation in [4, pp. 90–94]. Our derivation is straightforward because the modulo interval notation allows us to eliminate the troublesome floor functions in the summation, simplify with distributivity, and then deal only with simple instances of the mod operation.

The key step is to use the definition of the floor function in terms of an interval modulus,

$$\begin{aligned}
\sum_{0\le k<m} \left\lfloor \frac{nk+x}{m} \right\rfloor &= \sum_{0\le k<m} 0 \bmod \left(\frac{nk+x}{m} - 1\,..\,\frac{nk+x}{m} \right] \\
&= -\frac{1}{m} \sum_{0\le k<m} 0 \bmod (-nk-x+m\,..\,-nk-x] \\
&= \frac{1}{m} \sum_{0\le k<m} \big((nk+x) - (nk+x) \bmod (m\,..\,0] \big), \\
&= \frac{1}{m} \sum_{0\le k<m} (nk+x) - \frac{1}{m} \sum_{0\le k<m} (nk+x) \bmod m,
\end{aligned}$$

by two applications of distributivity, first multiplicative, then additive, and rewriting the resulting modulus interval $(m\,..\,0]$ as mod m. The first summation is easy, so we have

$$\sum_{0\le k<m} \left\lfloor \frac{nk+x}{m} \right\rfloor = x + \frac{n(m-1)}{2} - \frac{1}{m} \sum_{0\le k<m} (nk+x) \bmod m.$$

To evaluate the remaining summation, we note that for integers ℓ, m, and n, $\gcd(m,n) = 1$,

$$\sum_{0\le k<m} (nk+\ell) \bmod m = \sum_{0\le k<m} k \bmod m = \frac{m(m-1)}{2},$$

because when m and n are relatively prime, $ni \equiv nj \pmod{m}$ if and only if $i \equiv j \pmod{m}$, and hence the summation is simply over the set $\{0, 1, \ldots, m-1\}$, but reordered. Thus,

$$\begin{aligned}\sum_{0\le k<Nm} (nk+x) \bmod m &= \sum_{0\le k<Nm} \big(nk + \lfloor x\rfloor + \{x\}\big) \bmod m \\ &= \sum_{0\le k<Nm} \big[(nk+\lfloor x\rfloor) \bmod m + \{x\}\big] \\ &= N\frac{m(m-1)}{2} + Nm\{x\},\end{aligned}$$

because $\{x\}$ is less than 1 it can be moved out of the integer-valued mod function, and each time k goes from 0 through $m-1$ modulo m, $nk + \lfloor x\rfloor$ goes through each modulus of m.

Finally, when m and n are not relatively prime, that is, $d = \gcd(m,n) > 1$, we divide through by d and view the sum as d repeating segments by writing $m' = m/d$ and $n' = n/d$, so that $\gcd(m', n') = 1$, and $x' = x/d$:

$$\begin{aligned}\sum_{0\le k<m} (nk+x) \bmod m &= d\sum_{0\le k<dm'} (n'k+x') \bmod m' \\ &= \frac{d^2m'(m'-1)}{2} + d^2m'(x' \bmod 1) \\ &= \frac{m(m-d)}{2} + m(x \bmod d).\end{aligned}$$

Putting the pieces together, we find that

$$\begin{aligned}\sum_{0\le k<m} \left\lfloor \frac{nk+x}{m} \right\rfloor &= x + \frac{n(m-1)}{2} - \frac{1}{m}\sum_{0\le k<m} (nk+x) \bmod m \\ &= x + \frac{n(m-1)}{2} - \left(\frac{m-d}{2} + x \bmod d\right) \\ &= d\left\lfloor \frac{x}{d}\right\rfloor + \frac{n(m-1)}{2} + \frac{d-m}{2},\end{aligned}$$

because $x - (x \bmod d) = d(x/d - (x/d \bmod 1)) = d\lfloor x/d\rfloor$.

References

[1] Raymond T. Boute. The Euclidean definition of the functions div and mod. *ACM Trans. Program. Lang. Syst.*, 14(2):127–144, April 1992.

[2] Nicolas Brisebarre, David Defour, Peter Kornerup, Jean-Michel Muller, and Nathalie Revol. A new range-reduction algorithm. *IEEE Trans. Comput.*, 54(3):331–339, March 2005.

[3] Nachum Dershowitz and Edward M. Reingold. *Calendrical Calculations*. Cambridge University Press, New York, NY, USA, 3rd edition, 2007.

[4] Ronald L. Graham, Donald E. Knuth, and Oren Patashnik. *Concrete Mathematics*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2nd edition, 1994.

[5] Kenneth E. Iverson. *A Programming Language*. John Wiley & Sons, Inc., New York, NY, USA, 1962.

[6] Tsuneo Nakanishi and Akira Fukuda. Modulo interval arithmetic and its application to program analysis. *Transactions of Information Processing Society of Japan (Jōhō Shori Gakkai ronbun shi)*, 42(4):829–837, April 2001.

[7] Tsuneo Nakanishi, Kazuki Joe, Constantine D. Polychronopoulos, and Akira Fukuda. The modulo interval: A simple and practical representation for program analysis. In *Proceedings of the International Conference on Parallel Architectures and Compilation Techniques (PACT)*, pages 91–96, Newport Beach, CA, USA, October 1999. IEEE.