A Notation for the GCD and LCM Functions

E. E. McDonnell
IBM Corporation
1501 California Avenue
Palo Alto, CA 94304, USA

Abstract

This paper proposes a notation to be used for the greatest common divisor (gcd) and least common multiple (lcm) functions in APL. The notation proposed is that in use for the logical or and and functions: ∨ for gcd and ∧ for lcm. For this reason, special attention is paid to the cases of gcd and lcm for the arguments 0 and 1. Also, because we wish to define the functions for negative and complex rational values as well as for positive integers, we discuss the functions more generally than is the case in standard number theory texts, which usually restrict their discussions to positive integers. For this reason we give proofs of some of the basic theorems concerning gcd and lcm, written to insure that they are valid for the entire domain of values for which it is proposed the APL functions be defined. The discussion in this paper is couched in terms of integral arguments. The theoretical extension to rational arguments is an easy one, and it is assumed that the gcd and lcm functions, which depend on the residue function for their definitions, will be implemented for non-integral arguments, just as is the residue function, with all the practical difficulties which this entails.

In this paper, the terms "greatest" and "least" are taken to refer to magnitudes, and the terms "divisor" and "multiple" mean integer divisor and integer multiple.

Divisor and Multiple

If $M=D\times H$, where H is an integer, then M is a multiple of D, and D is a divisor of M. If $D=0$, H is not uniquely defined, but nonetheless 0 is a divisor of 0.

A unit is a divisor of 1. There are two real units, ¯1 and 1, and four complex units: the two real units and the square root of negative one and its negative. Multiplication or division of a number by a unit does not produce a change in its magnitude, but will produce a change in its direction, if the unit is not 1.

Numbers which differ by unit multiples are associates. Every number but zero has associates. Every number is a divisor and multiple of itself (from the identity $N=N\times 1$) and associates are divisors and multiples of each other (if A is associated with B, then $A=B\times U$ for some unit U). Associates are equal in magnitude.

Zero as Divisor and Multiple

From the identity $0=A\times 0$ we conclude that 1) the only multiple of zero is zero; 2) zero is a divisor only of zero, and no number but zero has zero as a divisor; 3) zero is the only number which is a multiple of every number; and 4) there is no unique quotient for $0\div 0$.

Common Divisors and Division

Every number which is a divisor of each of two numbers is a common divisor of them. If D is a common divisor of H and K then the associates of D are also common divisors of H and K.

If $C=A|B$, then the common divisors of A and B are also common to C. For the definition of the residue function gives us $C=B-A\times\lfloor B\div A$. If E is any common divisor of A and B, then $B\div E$ and $(A\times\lfloor B\div A)\div E$ are integers, as is their difference, to be called V. Thus we can write $C=E\times V$, showing that E is also a divisor of C. The proof shows that the expressions $C=A+B$ and $C=A-B$ may be substituted for $C=A|B$ in the statement of the theorem, and the theorem will remain true: that the common divisors of A and B are also common divisors of C.

The common divisors of 0 and H are the divisors of H. This is easily seen using the algebra of sets. If I is the set of all numbers, these are the divisors of 0. If D is the set of divisors of H, then $D=I\cap D$.

A proof for the division theorem valid for complex numbers in general is given in

[6]. The theorem states that if Z and W are arbitrary numbers, with $W \neq 0$, then there exists an integer Q, and an R such that $Z=R+Q\times W$, and $(|R)<|W$. The proof depends on the definition of the complex floor function, which provides that $1>|X-\lfloor X$ for all X. Q is determined by $\lfloor Z\div W$, and R by $W|Z$, and Q and R are thus well-defined.

If there is a non-empty set of integers closed under addition and subtraction, then the set is either zero alone or consists of all multiples of some least non-zero element. In the first case, where the set consists only of zero, then $0+0$ and $0-0$ are in the set. In the second case, choose an element $A \neq 0$. Then 0 is in the set, since $0=A-A$. Now choose among the non-zero elements least in magnitude the element B. Then all multiples of B are in the set since it is closed under addition and subtraction. Conversely, all elements in the set are multiples of B, since if A is in the set, $B|A$ is also in the set, since it is the difference of two elements in the set; but $B|A$ is less than B in magnitude by the division theorem, and so must be zero; therefore A is a multiple of B. Clearly, the other least elements are associates of B.

Greatest Common Divisor

D is a greatest common divisor of H and K if it is a common divisor of H and K and is also a multiple of every other common divisor.

It can be shown that every two integers H and K have a gcd D such that $D=(P\times H)+Q\times K$, where P and Q are integers, and $D=0$ if and only if $H=0$ and $K=0$.

In the first case, where H and K are not both zero, we see that for any two numbers of the form $(P1\times H)+Q1\times K$ and $(P2\times H)+Q2\times K$, their sum $((P1+P2)\times H)+(Q1+Q2)\times K$ and difference $((P1-P2)\times H)+(Q1-Q2)\times K$ are also of that form. Therefore the set of all such linear combinations is closed under addition and subtraction, and thus contains 0 and a non-zero element D least in magnitude. D is a divisor of each element of the set. However H and K are both elements of the set (since $H=(1\times H)+0\times K$ and $K=(0\times H)+1\times K$) and thus both have D as a divisor. For some integers P and Q, $D=(P\times H)+Q\times K$, and thus the common divisors of H and K are common divisors of D. Hence D is a greatest common divisor, for it is the greatest of the divisors of itself.

If H and K are both 0, we know that every number is a common divisor of 0 and 0. We know also that the only multiple of every number is 0. Clearly, $0=(P\times 0)+Q\times 0$ for every P and Q, and thus the gcd of 0 and 0 is 0.

The Euclidean Algorithm

For the purpose of defining a function, it is necessary to be able to specify one of the associated greatest common divisors as the greatest common divisor. This is accomplished by the Euclidean algorithm, as interpreted using the definition of the residue function current in APL. The residue function, in turn, is assumed to be using the definition of the complex floor function given in reference [6].

A version of the algorithm similar to one given in [4] is as follows: to compute the greatest common divisor of H and K, assign the values H and K to V, forming a two-element vector. If the first element of V is zero, the algorithm terminates with the second element the result. If the first element of V is not zero, form a new first element by the process $V\leftarrow(|/2\uparrow V),V$. This new element is thus the residue of the former second element, using the former first element as the modulus. The process will terminate if H and K are integers (real or complex), since the successive prefixed residues form a sequence of integers decreasing in magnitude, and thus the sequence is finite and ends in zero. The process will also terminate if H and K are rational (real or complex), but the argument is not as straightforward.

When the algorithm described above terminates, the second element of V is the greatest common divisor of H and K. This is so because each overlapping pair of elements shares the same set of common divisors. Since $V[1]=0$, the common divisors of $V[1]$ and $V[2]$ are the divisors of $V[2]$. So the divisors of $V[2]$ are the common divisors of the elements of V, and in particular of the original elements of V, namely H and K. The greatest divisor of $V[2]$ is of course $V[2]$, so the greatest common divisor of H and K (and of all the elements of V) is $V[2]$.

One is not ordinarily interested in the intermediate values developed in the course of executing the algorithm. Iterative versions of the algorithm which do not maintain the intermediate residues are given in [3] and [4]. A recursively defined function is given below:

```
D←H GCD K
D←K
→(0=H)/0
D←(H|K) GCD H
```

In a computer implementation of this function for rationals on a system like the IBM System 370, where non-terminating decimals are approximated by finite hexadecimals, the comparison $0=H$ should be replaced by a comparison of the magnitude of H with some relatively small positive number $EPSILON$, in the form $EPSILON>|H$.

A Notation for the GCD Function

The behavior of the gcd function with zero arguments has been discussed. It is evident that 0 is a left-right identity element for the function. If we tabulate the result of using all pairs of logical arguments with the function, we note that the gcd function is identical with the logical or function, denoted by ∨:

```
A   B   A GCD B
0   0       0
0   1       1
1   0       1
1   1       1
```

We adopt the ∨ notation forthwith to denote the gcd function. As is customary in APL, the gcd of a vector of numbers *V* may be found using reduction: ∨/*V*.

Least Common Multiple

Every number which is a multiple of each of two numbers is a common multiple of them. If *M* is a common multiple of *H* and *K*, then the associates of *M* are also common multiples of *H* and *K*. Among the common multiples of two numbers, other than zero, one set of associates is less than any other set of associates. This set is called the least common multiples of *H* and *K*, and any member of this set is a least common multiple of *H* and *K*.

Before investigating the lcm function, we must demonstrate several things. First we show that multiplication distributes over gcd, that is, $((M\times H)\vee M\times K)=M\times H\vee K$. If we multiply the vector *V* of the Euclidean algorithm (which contains a series of residues to the left of the original pair of arguments) by *M*, it is immediate that $((M\times H)\vee M\times K)=M\times H\vee K$.

If $1=H\vee K$, then *H* and *K* are said to be relatively prime. Now we have to show that, if we let $D\leftarrow H\vee K$, and set $H1\leftarrow H\div D$, and $K1\leftarrow K\div D$, then *H*1 and *K*1 are relatively prime. The following listing gives four equal expressions:

```
D
H∨K
(D×H1)∨D×K1
D×H1∨K1
```

and in particular the first and last expressions are equal, so that $H1\vee K1$ must equal one, and therefore *H*1 and *K*1 are relatively prime.

Now we are in a position to show that a least common multiple of two numbers *H* and *K* is given by $(H\times K)\div H\vee K$, and is 0 if and only if $0=H\times K$.

In the first case, where *H* and *K* are not both zero, we make the following assignments:

```
D←H∨K
H1←H÷D
K1←K÷D
```

Any multiple of *H* has the form $P\times H$ and thus equals $P\times H1\times D$. For $P\times H$ to be divisible by *K*, the factor $P\times H1$ must be divisible by *K*1. Because $1=H1\vee K1$, this is possible only when *P* is divisible by *K*1, so that $P=Q\times K1$. Any common multiple *M* of *H* and *K* is thus given by any of the equivalent forms:

```
M
P×H
Q×K1×H
Q×K1×H1×D
Q×H1×K1×D
Q×H1×K
Q×(H÷D)×K
Q×(H×K)÷D
Q×(H×K)÷H∨K
```

It is clear that a least common multiple is obtained when *Q* is equal to one. Therefore a least common multiple of *H* and *K* is given by $(H\times K)\div H\vee K$. The value so determined will be called the least common multiple.

In the second case, when either *H* or *K* (but not both) is equal to zero, the result must be zero, since the only multiple of 0 is 0. The formula $(H\times K)\div H\vee K$ evaluates to 0 for both these cases. When *H* and *K* are both 0, the formula becomes $(0\times 0)\div 0\vee 0$, or $0\div 0$, an indeterminate form. Since the only multiple of 0 is 0, this suggests that the value of $0\div 0$ in APL should be 0 (not 1 as is currently the case).

For integral values *N* the function $1\vee N$ gives the result 1. Thus 1 is a left identity for the lcm function, that is, $K=(1\times K)\div 1\vee K$ for all integer *K*. It is not a right identity, since any unit as a left argument of *LCM* is a left identity element. Thus $(^{-}1\times 1)\div ^{-}1\vee 1$ evaluates to $^{-}1\div ^{-}1$ or 1.

A Notation for the LCM Function

We have discussed the behavior of the lcm function with 0 arguments, and have seen that 1 is a left identity element. If we tabulate the results of all pairs of logical arguments, we note that the lcm function is identical to the logical and function, denoted by ∧:

```
A   B   A LCM B
0   0       0
0   1       0
1   0       0
1   1       1
```

We adopt the ∧ notation forthwith to denote the lcm function. As is customary

in APL, the lcm of a vector of numbers V may be found using reduction: $\wedge/V$.

Some Properties of the GCD and LCM Functions

For positive integer arguments, $\vee$ and $\wedge$ are commutative and associative functions. For integers in general, or arbitrary rational arguments, neither of these is the case, as we saw with lcm and the arguments $^{-}1$ and 1. This arises from the fact that the residue function, which is central to both the gcd and the lcm function, is defined to be affected by the signum, or more generally, by the direction of the left argument. Thus $(-H)\vee K$ and $(-H)\wedge K$ are different in general from $H\vee K$ and $H\wedge K$; the difference lies in that the results of the two different forms will be associates. If we identify associates, then we can say that gcd and lcm are commutative and associative functions, for complex rational arguments in general. The gcd and lcm functions are replete with identities. A handful are given below.

$H\vee K$	$K\vee H$
$H\wedge K$	$K\wedge H$
$H\vee K\vee L$	$(H\vee K)\vee L$
$H\wedge K\wedge L$	$(H\wedge K)\wedge L$
$M\times H\wedge K$	$(M\times H)\wedge M\times K$
$M\times H\vee K$	$(M\times H)\vee M\times K$
$(H\wedge K)\div D$	$(H\div D)\wedge K\div D$
$(H\vee K)\div D$	$(H\div D)\vee K\div D$
$(H\wedge K)\vee L$	$(H\vee L)\wedge K\vee L$
$(H\vee K)\wedge L$	$(H\wedge L)\vee K\wedge L$
H	$H\wedge H\vee K$
H	$H\vee H\wedge K$
H	$H\vee H$
H	$H\wedge H$
$\vee/(H\wedge K),(H\wedge L),K\vee L$	$\wedge/(H\vee K),(H\vee L),K\vee L$

The two columns of formulas are to be understood to be connected with the relation "is associated with," in general, and with the relation "is equal to" if the arguments are restricted to positive rationals and zero.

Conclusion

The basic idea for the notation was arrived at from a study of the properties of the functions. Subsequently, it was found that Greub, in [2] used essentially the same notation for the gcd and lcm of polynomials. Birkhoff and MacLane, in [1], use the same symbols, but interchanged. The duality between the functions, as evidenced by the identities given above, permits this when the field of discourse is restricted to the two functions. Iverson, in [5], suggested the similarly shaped symbols $\downarrow$ and $\uparrow$ to denote gcd and lcm, respectively. The most common usage in number theory texts are parentheses (H,K) for gcd and brackets $[H,K]$ for lcm. These can not be employed in a consistent system of notation because of other conflicting uses of parentheses and brackets and, more strongly, because in APL we wish to denote a scalar dyadic function by a single symbol infixed between its arguments. Extending the domain of the $\vee$ and $\wedge$ symbols accomplishes this with no additions to the notation.

Acknowledgement

Don Orth of the IBM Philadelphia Scientific Center reviewed the manuscript and made many helpful suggestions.

References

[1] Birkhoff, G., and S. MacLane, A Survey of Modern Algebra, third edition, Macmillan, New York, 1965

[2] Greub, W. H., Linear Algebra, third edition, Springer-Verlag, New York, 1967

[3] Falkoff, A. D., and K. E. Iverson, APL 360 User's Manual, Yorktown Heights, N. Y., 1968

[4] Iverson, K. E., Algebra: an Algorithmic Treatment, Addison Wesley, Menlo Park, California, 1972

[5] --, "Formalism in Programming Languages," Communications of the Association for Computing Machinery, 7, 1964

[6] McDonnell, E. E., "Complex Floor," APL Congress 73, Gjerlov et al eds., North Holland, Amsterdam, 1973

Bibliography

MacDuffee, C. C., "On the Concept of Divisor," American Mathematical Monthly, 51, 1944

Ore, O., Number Theory and its History, McGraw-Hill, N. Y., 1948

Vinogradov, I. M., Elements of Number Theory, Dover, N. Y., 1954

Note: The principal work consulted was the paper by MacDuffee, which investigated the properties of the gcd and lcm functions for zero arguments. The texts used for more conventional material were Vinogradov (especially), Ore, and the referenced work by Birkhoff and MacLane.