Very elementary number theory redone.

The natural numbers are 0,1,2 and so on; for further details, see Peano.

The positive integers are the natural numbers ≥ 1, i.e. 1,2,3 and so on.

The multiples are the natural numbers ≥ 2, i.e. 2,3,4 and so on. The product of two multiples is larger than each of those two; in formula

$$(\underline{A}\ x,y : x \geq 2, y \geq 2 : x.y > x \ \wedge\ x.y > y) \quad . \qquad (1)$$

Multiples that are the product of two multiples are called composite; multiples that are not composite are called prime; in formula

$$\text{prime } m = m \geq 2 \ \wedge\ (\underline{A}\ x,y : x \geq 2, y \geq 2 : x.y \neq m) \qquad (2)$$

$$\text{comp } m = m \geq 2 \ \wedge\ (\underline{E}\ x,y : x \geq 2, y \geq 2 : x.y = m) \qquad (3)$$

In view of (1), (3) can be rewritten

$$\text{comp } m = (\underline{E}\ x,y : 2 \leq x < m, 2 \leq y < m : x.y = m) \qquad (3')$$

From (3') it is clear that it is decidable whether a specific m is composite.

Note that we have $\neg(\text{prime } 1) \wedge \neg(\text{comp } 1)$.

With PF -for Prime Factorization- defined by

PF n = n is the product of (zero or more) multiples, all of which are prime (the empty product being defined as 1)

we can state

Theorem 0. $(\underline{A}\ n:\ n \geq 1 :\ PF\ n)$

Proof. We shall prove Theorem 0 by mathematical induction, i.e. we shall prove

$$(\underline{A}\ n:\ n \geq 1 : (PF\ n)\ V\ (\underline{E}\ i:\ 1 \leq i < n :\ \neg(PF\ i))) \qquad (4)$$

Because $(\underline{A}\ n:\ n \geq 1 :\ n=1\ V\ (\text{prime } n)\ V\ (\text{comp } n))$ and the product of one number equals that number, we deduce from the definition of PF

$$(\underline{A}\ n :\ n \geq 1 :\ (\text{comp } n)\ V\ (PF\ n)) \qquad (5)$$

Furthermore we deduce from the definition of PF

$$(\underline{A}\ x,y :\ x \geq 1, y \geq 1 :\ \neg(PF\ x)\ V\ \neg(PF\ y)\ V\ PF(x.y))$$

from which we deduce with (3')

$$(\underline{A}\ n :\ n \geq 1 :\ \neg(\text{comp } n)\ V\ (PF\ n)\ V\ (\underline{E}\ i : 1 \leq i < n : \neg(PF\ i))) \qquad (6)$$

From (5) and (6), relation (4) follows by the standard

inference rule. (End of Proof of Theorem 0.)

Theorem 1. $(\underline{A}\, p : \text{prime } p : (\underline{E}\, q : q > p : \text{prime } q))$

(This is Euclid's famous theorem that no prime is the largest one.)

Proof. Consider for arbitrary prime p the value Q defined by

Q = 1 + the product of all primes $\leq p$.

Theorem 0 allows us to conclude that Q is the product of a bag of primes, and, because $Q > 1$, that bag is not empty. By virtue of Q's construction, such a bag contains no prime $\leq p$. Hence it contains at least one prime $> p$, hence at least one prime $> p$ exists. (End of Proof of Theorem 1.)

With UPF -for Unique Prime Factorization- defined by

UPF n = the bag of prime multiples whose product equals n is unique

we can formulate

Theorem 2. $(\underline{A}\, p, x, y : p \geq 1, x \geq 1, y \geq 1 :$
$\neg(\text{prime } p) \vee \neg(p \mid (x.y)) \vee p \mid x \vee p \mid y \vee \neg(\text{UPF}(x.y)))$

(Here "a|b" should be read as "a divides b".)

Proof. When the first two terms are false, x.y is the product of a bag of primes containing p; when the next two terms are false, x.y is also the product of a bag of primes not containing p. Those two bags being different, we deduce ¬(UPF(x.y)).
(End of Proof of Theorem 2.)

We are now ready to state and prove

Theorem 3. $(\underline{A}\ n: n \geq 1: \text{UPF}\ n)$

Proof. Theorem 3 is proved by mathematical induction, i.e. by proving

$$(\underline{A} n: n \geq 1: (\text{UPF}\ n)\ V\ (\underline{E} i: 1 \leq i < n: \neg(\text{UPF}\ i))) \qquad (7)$$

Inspired by our proof of Theorem 0, we observe that (7) follows from (8) and (9), given by

$$(\underline{A} n: n \geq 1: (\text{comp}\ n)\ V\ (\text{UPF}\ n)) \qquad (8)$$

$$(\underline{A} n: n \geq 1: \neg(\text{comp}\ n)\ V\ (\text{UPF}\ n)\ V\ (\underline{E} i: 1 \leq i < n: \neg(\text{UPF}\ i))) \qquad (9)$$

Of these two, (8) follows immediately from (2), (3) and the definition of UPF. Assertion (9) requires, however, a more elaborate argument.

Consider a value of n, m say, such that the first and the last terms of (9) are false, i.e. such that

$$(\text{comp } m) \wedge (\underline{A} i : 1 \leq i < m : \text{UPF } i) \qquad (10)$$

holds. Because m is composite, it can be written as

$$m = p.P = q.Q \qquad \text{with} \qquad (11)$$

1) prime p
2) $p \leq q$
3) P standing for the product of a non-empty bag of primes all of which are $\geq p$
4) Q standing for the product of a bag of primes all of which are $\geq q$.

We obviously have $2 \leq P < m$, $1 \leq Q < m$, and $P \geq Q$.

The conclusion UPF m, required to prove (9), can then be drawn from

$$p = q \vee (\text{comp } q) \qquad (12)$$

as follows. When q is the smallest value in a bag of primes, comp q is false and from (12) we deduce $p = q$. From (11) we deduce $P = Q$, and from (10) we deduce that P and Q stand for the same bag of primes. Since $p = q$, $p.P$ and $q.Q$ then also stand for the same bag of primes,

and UPF m has been established.

Establishing (12) is now our only remaining obligation. It is trivial in the case $p=q$. In the case $p<q$ we consider the value M defined by

$$M = (q-p).Q$$

Because $1 \leq M < m$, we conclude from (10) UPF M. Because $M = q.Q - p.Q = p.P - p.Q = p.(P-Q)$, we conclude $p \mid M$. Since prime p, we now conclude from Theorem 2

$$p \mid (q-p) \;\vee\; p \mid Q \qquad (13)$$

Since $1 \leq Q < m$, we conclude from (10) UPF Q, i.e. all the primes in the unique bag of primes whose product equals Q are $\geq q$, hence $> p$. The bag being unique, we conclude $\neg(p \mid Q)$. In combination with (13) we conclude $p \mid (q-p)$; since we were considering the case $p<q$, we can conclude that q is composite. Having thus established relation (12), we have fulfilled our last proof obligation. (End of Proof of Theorem 3.)

Corollary of Theorems 2 and 3.

$$(\underline{A}\ p,x,y : p\geq 1, x\geq 1, y\geq 1 :$$
$$\neg(\text{prime } p) \vee \neg(p \mid (x.y)) \vee p \mid x \vee p \mid y\ ).$$

* * *

The above was written in reaction to the presentation in [1] of essentially the same proof of Theorem 3. I found that presentation contorted and notationally clumsy. They write (for (11))

$$m = p_1\, p_2 \cdots p_r = q_1\, q_2 \cdots q_s$$

Note the dots and the need to introduce the subscripts r and s. A little later, after having excluded $p_1 = q_1$: "Suppose $p_1 < q_1$. (If $q_1 < p_1$ we simply interchange the letters p and q in what follows (sic).)". A third of a page later they conclude that "the prime decomposition of m' must be unique, aside from the order of the factors". Theorem 2 isn't mentioned and when needed in the proof of Theorem 3 they borrow the result from a corollary of Theorem 3! (Here their argument is almost cyclic.) And it is full of reductiones ad absurdum.

[1] Courant, Richard & Robbins, Herbert, "What is mathematics?" Oxford University Press paperback, 1978.

Plataanstraat 5
5671 AL NUENEN
The Netherlands

20 October 1980

prof. dr. Edsger W. Dijkstra
Burroughs Research Fellow