PACIFIC JOURNAL OF MATHEMATICS
Vol. 112, No. 1, 1984

DIVISIBILITY OF ARITHMETIC FUNCTIONS

DAVID REARICK

Any two nonzero arithmetic functions have a greatest common divisor relative to the Dirichlet product, but the known proofs of this fact are nonconstructive. In a restricted setting, this paper develops a method for obtaining specific formulas for the greatest common divisor. It is conjectured that formulas of this type hold more generally. The method is based on properties of a certain derivative-like operator on the Dirichlet algebra of arithmetic functions. The resulting "differential calculus" is used to construct polynomial equations satisfied by the greatest common divisor of two arithmetic functions. Then the Euclidean algorithm is applied to these polynomials.

1. Units in the Dirichlet algebra. As is well known [**1**, **2**], if f and g are arithmetic functions and we define $fg(n) = \sum_{d|n} f(d)g(n/d)$ and $(f + g)(n) = f(n) + g(n)$, the resulting system forms an integral domain D called the Dirichlet algebra. The multiplicative identity δ is defined by $\delta(1) = 1$, $\delta(n) = 0$ if $n > 1$. Every nonzero function f has a norm Nf, defined to be the smallest n such that $f(n) \neq 0$; it follows that $N(fg) = NfNg$. There are infinitely many units in D, namely the functions of norm 1. The set of nonunits forms an ideal which is not principal, so D is not a principal ideal domain or a Euclidean domain. However, D has the unique prime factorization property, as was first shown by Cashwell and Everett [**1**], and it follows that any two arithmetic functions, not both zero, have a greatest common divisor (GCD), unique to within multiplication by a unit.

To simplify the treatment of units in this paper, we identify a standard form such that each nonzero associate class of arithmetic functions contains exactly one in standard form. Namely, if $Nf = a$, we say that f is in standard form if $f(na) = \delta(n)$ for all n.

LEMMA 1. *Let f be any nonzero arithmetic function (i.e., not identically zero). There is a unique unit u such that uf is in standard form.*

Proof. Let $Nf = a$. The condition $\sum_{d|na} u(d)f(na/d) = \delta(n)$ gives a recursive formula for u, starting with $u(1) = 1/f(a)$, and $u(n)$ is then determined uniquely in terms of values $u(k)$, $k < n$.

We shall denote by L the GCD, in standard form, of two nonzero arithmetic functions h_0 and h_1. Thus L is that unique common divisor of h_0 and h_1 which is in standard form and has maximum norm.

2. A derivative-like operator. Throughout the rest of the paper, let p denote a fixed prime number. Let r be the fixed arithmetic function defined by

$$r(n) = \begin{cases} 1 & \text{if } n = p, \\ 0 & \text{if } n \neq p. \end{cases}$$

Consider the mapping $f \to f'$ of D into D defined by $f'(n) = f(np)$ for all n.

It follows from the definition of norm that

$$pNf' \geq Nf, \tag{1}$$

with equality holding if and only if $p \mid Nf$.

Clearly $(f + g)' = f' + g'$ for all $f, g \in D$. We also verify readily that

$$(fg)' = f'g + fg' - rf'g'. \tag{2}$$

Since the product rule (2) is suggestive of that for a derivation, we shall refer to f' as the *derivative* of f. It follows from (2) that

$$(rf)' = f, \tag{3}$$

so, in this kind of calculus, integration is equivalent to multiplication by r. For use later in this paper, several further principles of this calculus must be developed.

Denoting the kth derivative of f by $f^{(k)}$, we have the following Leibniz-like formula for higher derivatives of a product:

$$(fg)^{(k)} = \sum_{j=0}^{k} f^{(j)}g^{(k-j)} - r\sum_{j=1}^{k} f^{(j)}g^{(k+1-j)}. \tag{4}$$

This is proved by induction, making use of (3). Also by induction we establish a formula for the first derivative of a kth power,

$$r(f^k)' = f^k - (f - rf')^k,$$

and, applying the binomial theorem,

$$(f^k)' = rf' \sum_{j=0}^{k-1} \binom{k}{j} (-1)^{k-j+1} f^j (rf')^{k-j-1}. \tag{5}$$

Now suppose $f' \neq 0$ (0 being the zero element of D). From (5) we find that if we start with a power f^k, differentiate it and then divide by rf', and

repeat this process successively, a total of k times, the result is δ. This leads to the following principle.

LEMMA 2. *Let $P(f)$ be a polynomial in f, of positive degree k, each coefficient being an arithmetic function with zero derivative. Assume $P(f) = 0$. Then $f' = 0$.*

Proof. Suppose $f' \neq 0$. Apply k successive operations, of the type just described, to both sides of the equation $P(f) = 0$. On the right side we obtain 0, and on the left side the leading coefficient of P, which is not zero.

3. Functions of prime-power norm. From now on we shall restrict our attention to functions whose norms are powers of p, the prime number fixed earlier. If $Nf = p^a$, then $Nf' = p^{a-1}$; and if f is in standard form then so is f'. Note that such a function f is in standard form if and only if $f^{(a)} = \delta$. We also have the following principle, which is essential in the remainder of the paper, and which breaks down for functions whose norms are other than powers of the same prime.

LEMMA 3. *Let $h = fg$, where $Nf = p^a$ and $Ng = p^b$. If two of these three functions are in standard form, then the third is also in standard form.*

Proof. First assume f and g are in standard form. By (4),

$$h^{(a+b)} = \sum_{j=0}^{a+b} f^{(j)} g^{(a+b-j)} - r \sum_{j=1}^{a+b} f^{(j)} g^{(a+b+1-j)}. \tag{6}$$

In the first sum, the summand is zero if $j < a$ or $j > a$, so the only contributing term is $f^{(a)}g^{(b)} = \delta$. In the second sum, the summand is always zero. Thus $h^{(a+b)} = \delta$, so h is in standard form.

Now suppose g and h are in standard form. The left side of (6) is δ, and we may rewrite (6) in the form

$$\delta - f^{(a)} = \sum_{j=1}^{b} f^{(j+a)} \left(g^{(b-j)} - r g^{(b+1-j)} \right). \tag{7}$$

Suppose $f^{(a)} \neq \delta$; say $N(\delta - f^{(a)}) = t$. By (1), $Nf^{(j+a)} \geq t/p^j$ if $j \geq 1$. By (1) and (3) the norm of $g^{(b-j)} - rg^{(b+1-j)}$ is greater than p^j if $j \geq 1$, since $p \mid Ng^{(b-j)}$. Therefore each term in the sum in (7) has norm greater than $(t/p^j) \cdot p^j = t$, which contradicts our assumption that the norm of this sum is t. Thus $f^{(a)} = \delta$, so f is in standard form.

By repeated application of Lemma 3 it follows that, if h is in standard form and is a product of several functions, then h is also the product of the corresponding standard forms of these functions. In this context, the theorem of Cashwell and Everett can be stated in the following unit-free form:

If Nh is a power of p, and h is in standard form, then h is a product of prime factors each in standard form, uniquely except for the order of arranging the factors.

LEMMA 4. *Suppose* $Nf = p$, $Ng = p^b$, *and* f *is in standard form. Then*

$$\sum_{k=0}^{b+1} \left((fg)^{(k)} - r(fg)^{(k+1)}\right)(r-f)^k = 0.$$

Proof. With the aid of (4), and using the fact that $f' = \delta$, the sum can be rewritten as

$$\sum_{k=0}^{b+1} \left\{\left(g^{(k-1)} - rg^{(k)}\right)(r-f)^k - \left(g^{(k)} - rg^{(k+1)}\right)(r-f)^{k+1}\right\},$$

which telescopes to zero. (In the first term, we understand $g^{(-1)} = rg$.)

THEOREM 1. *Let* h *be in standard form,* $Nh = p^c$. *Consider the following polynomial over* D:

$$P(f) = \sum_{k=0}^{c} \left(h^{(k)} - rh^{(k+1)}\right)(r-f)^k.$$

The roots of P *lying in* D *are exactly the divisors of* h *of norm* p, *in standard form.*

Proof. If $h = fg$, with f in standard form and of norm p, then Lemma 4 shows that $P(f) = 0$. Conversely, suppose $P(f) = 0$. Each coefficient $h^{(k)} - rh^{(k+1)}$ has zero derivative by (3), so $r - f$ has zero derivative by Lemma 2, so $f' = r' = \delta$. The constant term, when P is written in powers of f, is $P(0) = \sum_{k=0}^{c}(h^{(k)} - rh^{(k+1)})r^k$, which telescopes to $h^{(0)} = h$, so $f \mid h$. Thus $Nf = p^a$ for some a. But $f(p) = f'(1) = \delta(1) = 1$, which shows that $a = 1$ and f is in standard form.

Note that $P(f)$ is of degree c in f and is monic, since the coefficient of $f^{(c)}$ is $(-1)^k\delta$, a unit. For later use we write out the polynomials $P(f)$, in powers of f rather than $r - f$, for the cases $c = 2$, $c = 3$ and $c = 4$, respectively:

$$f^2 - (h' + r)f + h, \tag{8}$$

$$-f^3 + (h'' + 2r)f^2 - (h' + rh'' + r^2)f + h, \tag{9}$$

$$f^4 - (h''' + 3r)f^3 + (h'' + 2rh''' + 3r^2)f^2 - (h' + rh'' + r^2h''' + r^3)f + h. \tag{10}$$

From (8) we notice

THEOREM 2. *A function h, of norm p^2 and in standard form, is a square if and only if h satisfies the differential equation*

$$(h' + r)^2 - 4h = 0;$$

and h is a prime if and only if $(h' + r)^2 - 4h$ is not a square.

To facilitate the further discussion of polynomials with coefficients in D, it will be convenient to regard them as polynomials over K, the field of quotients of D. This simplifies the proofs of some of the following theorems, and justifies the use of long division of polynomials in §§5 through 7.

THEOREM 3. *Let h be in standard form, $Nh = p^c$. Consider the following polynomial over D:*

$$Q(f) = \sum_{k=0}^{c} (h^{(k)} - rh^{(k+1)})f^{c-k}(rf - h)^k/h.$$

The roots of Q lying in D are exactly the divisors of h of norm p^{c-1}, in standard form.

Proof. By construction $Q(f) = P(h/f)f^c/h$, where P is the polynomial of Theorem 1. If $h = fg$, with f in standard form and of norm p^{c-1}, then $g = h/f$ is in standard form and of norm p, and $P(g) = 0$ by Theorem 1, so $Q(f) = 0$.

Conversely, suppose $Q(f) = 0$. Then $P(h/f) = 0$, where $h/f \in K$. Since P is monic, $h/f \in D$, so $f|h$. By Theorem 1, $N(h/f) = p$, so $Nf = p^{c-1}$. Also by Theorem 1, h/f is in standard form, so f is in standard form.

When $c = 3$ or $c = 4$, $Q(f)$ is respectively,

$$-f^3 + (h' + h'' + r^2)f^2 - h(h'' + 2r)f + h^2, \tag{11}$$

$$f^4 - (h' + rh'' + r^2h''' + r^3)f^3 + h(h'' + 2rh''' + 3r^2)f - h^2(h''' + 3r)f + h^3. \tag{12}$$

Let h_0 and h_1 be two arithmetic functions, each assumed to be in standard form and having norm a power of p. By a *differential polynomial* (DP) in h_0 and h_1 we mean a polynomial in r, h_0, h_1 and their derivatives, with constant coefficients. By a *differential rational form* (DRF) in h_0 and h_1 we mean an arithmetic function expressed as a quotient of two DP's in h_0 and h_1. The main purpose of this paper is to show that, at least if neither Nh_0 nor Nh_1 exceeds p^4, the GCD $L = (h_0, h_1)$ is always expressible as a DRF in h_0 and h_1 (but in general is not expressible as a DP). The first nontrivial case to consider is

4. The case $Nh_0 = Nh_1 = p^2$. Let h_0 and h_1 be in standard form and not equal. Then L is either δ or has norm p. Assuming the latter case, $f = L$ is a common root of the two polynomials in (8) formed taking $h = h_0$ and $h = h_1$ respectively. Forming the difference of these two polynomials yields the equation

$$\Delta h' L - \Delta h = 0,$$

where $\Delta h = h_1 - h_0$. Since $\Delta h \neq 0$, we must have also $\Delta h' \neq 0$, and in fact $\Delta h' | \Delta h$. Therefore $L = \Delta h / \Delta h'$, expressed as a DRF in h_0 and h_1. Also, $\Delta h / \Delta h'$ must be a root of each of the two polynomials P, and the equation $(\Delta h')^2 P(\Delta h / \Delta h') = 0$ can be written in the form (13) no matter which one of h_0 and h_1 is used in forming P.

Conversely, suppose h_0 and h_1 satisfy (13). Then $\Delta h' \neq 0$, and the element $\Delta h / \Delta h'$ of K is a root of both polynomials P in (8). Since (8) is monic, $\Delta h / \Delta h' \in D$, and by Theorem 1 $\Delta h / \Delta h'$ is a common divisor of h_0 and h_1, in standard form and of norm p, so $\Delta h / \Delta h' = L$.

These results may be summarized as follows.

THEOREM 4. *Let h_0, h_1 be in standard form, not equal, each of norm p^2. Then h_0 and h_1 have a nonunit common divisor if and only if they satisfy the differential equation*

$$(\Delta h)^2 - (h_0' h_1 - h_0 h_1' + r \Delta h) \Delta h' = 0, \tag{13}$$

and if (13) *holds, this common divisor, in standard form, is $L = \Delta h / \Delta h'$.*

We ask whether the formula $\Delta h / \Delta h'$ for L as a quotient of two DP's could be written as a single DP. The answer is negative.

THEOREM 5. *There is no DP in h_0 and h_1 which is equal to L whenever h_0 and h_1 are of norm p^2, in standard form, and having $NL = p$.*

Proof. Here (and later, when $Nh_0 = Nh_1$) it is convenient to introduce a numerical parameter x by defining, for all n,

$$h_x(n) = (1 - x)h_0(n) + xh_1(n).$$

Then, for every x, the function h_x is in standard form and has the same norm as h_0 and h_1; also, $(h_0, h_x) = (h_0, h_1) = L$ whenever $x \neq 0$.

Suppose there exists a DP as described in the theorem. In this expression replace h_1 by $h_x = h_0 + x\Delta h$, and h_1' by $h_0' + x\Delta h'$. For fixed n, the value of this expression is a polynomial in x which is equal to $L(n)$ for each $x \neq 0$. Therefore L is equal to the sum of those terms of the DP not containing x, i.e. not containing Δh or $\Delta h'$. Thus $L = (h_0, h_1)$ is represented by a formula independent of h_1, which is absurd.

5. The case $Nh_0 = p^2$, $Nh_1 = p^3$. We assume $h_0 \nmid h_1$, so L must be either δ or of norm p. In the latter case, $f = L$ is a common root of the quadratic polynomial (8) formed taking $h = h_0$, and the cubic polynomial (9) formed taking $h = h_1$. Dividing the former into the latter yields a linear remainder

$$\left((h_0')^2 - h_0h_1'' - h_0 + h_1'\right)f - (h_0h_0' - h_0h_1'' - rh_0 + h_1)$$

of which L is also a root. Thus there is just one possible value for L, and it is a DRF in h_0 and h_1.

THEOREM 6. *Let h_0, h_1 be in standard form, with $Nh_0 = p^2$, $Nh_1 = p^3$, $h_0 \nmid h_1$. Then L is either δ, of norm 1, or*

$$\frac{h_0h_0' - h_0h_1'' - rh_0 + h_1}{(h_0')^2 - h_0'h_1'' - h_0 + h_1'},$$

of norm p.

6. The case $Nh_0 = Nh_1 = p^3$. Let h_0, h_1 be in standard form and not equal. If L is not δ, its norm must be p^2 or p. We assume first the former case and use the "h_x method" introduced in §4. L is a root of (11) with h replaced by h_x, for every x. We may equate to zero, in particular, the x^2-component of (11), which gives $\Delta h\Delta h''L - (\Delta h)^2 = 0$, or $L = \Delta h/\Delta h''$.

We turn to the more difficult case $NL = p$. L is a common root of the two polynomials (9) formed using h_0 and h_1 respectively. The difference of these two polynomials is

$$\Delta h''f^2 - (\Delta h' + r\Delta h'')f + \Delta h, \tag{14}$$

and L is a root of this. If $\Delta h'' = 0$, we obtain immediately $L = \Delta h/\Delta h'$. If we assume $\Delta h'' \neq 0$, and divide the quadratic polynomial (14) into the cubic polynomial (9) corresponding to h_0, the constant term of the linear remainder is, apart from a nonzero factor $\delta/(\Delta h'')^2$,

$$h_0(\Delta h'')^2 - h_0''\Delta h\Delta h'' + \Delta h\Delta h' - r\Delta h\Delta h''. \tag{15}$$

We shall show that (15) is not zero. This will guarantee that the linear remainder is not identically zero, and, since its coefficients are DP's and L is a root of it, we shall obtain a DRF for L.

Suppose then that (15) is zero and $\Delta h'' \neq 0$. Divide (15) by L and rewrite in the form

$$(\Delta h'')^2 h_0/L = (h_0''\Delta h'' - \Delta h' + r\Delta h'')\Delta h/L.$$

Since h_0/L and $\Delta h/L$ are relatively prime, the former divides $h_0''\Delta h'' - \Delta h' + r\Delta h''$. This last quantity is not zero but has zero second derivative, which contradicts the fact that it is divisible by h_0/L, of norm p^2.

After specifically carrying out the long division outlined above, and rewriting the resulting DRF in a form symmetric in h_0 and h_1, we may summarize these results as follows.

THEOREM 7. *Let h_0, h_1 be in standard form, not equal, each of norm p^3. Then L is either δ, of norm 1, or $\Delta h/\Delta h''$, of norm p^2, or*

$$\frac{\Delta h\Delta h' + \Delta h''(h_0h_1'' - h_0''h_1 - r\Delta h)}{(\Delta h')^2 + \Delta h''(h_0'h_1'' - h_0''h_1' - \Delta h)}, \quad \textit{of norm } p. \tag{16}$$

In case $\Delta h'' = 0$, (16) reduces to $\Delta h/\Delta h'$, a DRF in the single variable Δh. Even if $\Delta h'' \neq 0$, we see from (14) that L is "almost" a function of Δh, since knowledge of Δh restricts L to be one of at most two possible functions. However, (16) cannot in general be expressed in terms of Δh alone. To see this, suppose for example that q_1 and q_2 are distinct arithmetic functions, each of norm p and in standard form. Let s be an arithmetic function of norm $p + 1$ which takes the value zero on all multiples of p. Define

$$h_0 = q_1^3,$$
$$h_1 = q_1^3 + sq_1q_2.$$

Then h_0 and h_1 are in standard form, of norm p^3, with $\Delta h = sq_1q_2$ and $L = q_1$. Reversing the roles of q_1 and q_2 gives another pair h_0, h_1 with the same Δh but different L, namely $L = q_2$.

7. The case $Nh = p^4$. We have seen that if neither Nh_0 nor Nh_1 exceeds p^3, the value of L is always expressible as a DRF in h_0 and h_1. The author conjectures that this is true for Nh_0 and Nh_1 any powers of p. A proof of this result for one or both norms as large as p^4 will illustrate the difficulties to be expected in the general case.

THEOREM 8. *Let h_0, h_1 be in standard form, each having norm a power of p not exceeding p^4. Then L is always expressible as a DRF in h_0 and h_1.*

In proving the theorem as stated, we may assume $Nh_0 = Nh_1 = p^4$. For if each norm is less than p^4 there is nothing to prove; and if say $Nh_0 = p^4$, $Nh_1 = p^c$ $(c \leq 3)$, and the theorem has been proved for $L^* = (h_0, r^{4-c}h_1)$, then the result is true also for $L = (h_0, h_1)$, because L is equal either to L^* or to L^* divided by a power of r, since r is a prime in D.

We may further assume $h_0 \neq h_1$ and $L \neq \delta$, so NL is either p^3, p^2 or p. In the first case, by applying the "h_x method" to (12), and setting the x^3-component equal to zero, we obtain $L = \Delta h/\Delta h'''$.

For the case $NL = p$, we form the difference of the two polynomials (10) corresponding to h_0 and h_1, obtaining

$$(17) \qquad -\Delta h'''f^3 + (\Delta h'' + 2r\Delta h''')f^2 - (\Delta h' + r\Delta h'' + r^2\Delta h''')f + \Delta h,$$

of which L is a root. If $\Delta h'' = 0$, we get immediately $L = \Delta h/\Delta h'$. If $\Delta h''' = 0$ and $\Delta h'' \neq 0$, (17) reduces to (14). Dividing the quadratic (14) into the quartic polynomial (10) corresponding to h_0, we obtain a linear remainder whose constant term, apart from a nonzero factor $\delta/(\Delta h'')^3$, is of form $h_0(\Delta h'')^3 - J\Delta h$, where J is a DP having zero third derivative. As for (15), we are able to argue that this constant term is not zero. For if it were zero, we would have that h_0/L divides $J\Delta h/L$, and therefore h_0/L divides J. But since $N(h_0/L) = p^3$, this contradicts the fact that $J''' = 0$. Therefore the above linear remainder is not zero, and, since L is its root, we obtain a DRF for L.

If $\Delta h''' \neq 0$, divide the cubic (17) into the quartic polynomial (10) corresponding to h_0. The quadratic remainder R has constant term, apart from a nonzero factor,

$$(18) \qquad h_0(\Delta h''')^2 - h_0''\Delta h\Delta h''' + \Delta h\Delta h'' - r\Delta h\Delta h'''.$$

Arguing as for (15) we see that (18) is not zero, so R is not identically zero. If R is in fact a linear polynomial we are through, since its coefficients are DP's and its root is L.

Suppose R is of degree 2, with second root say f_0; f_0 lies in K, the field of quotients of D. We may assume f_0 is also a common root of the two polynomials (10) corresponding to h_0 and h_1, for otherwise division of R into one of these polynomials will produce a linear polynomial with DP coefficients having L as its root, and we are through. Since (10) is monic, f_0 lies in D, and by Theorem 1 f_0 is a common divisor of h_0 and h_1, of norm p and in standard form. Thus $f_0 = L$, so L is a double root of R. Therefore the discriminant of R if zero, and we obtain a DRF for L.

We turn finally to the case $NL = p^2$. Theorems 1 and 3 are no longer applicable and we have to replace them by the somewhat less satisfactory

THEOREM 9. *Let h be in standard form, of norm p^4. There is a sixth-degree polynomial*

$$T(f) = f^6 + Af^5 + Bf^4 + Cf^3 + Bhf^2 + Ah^2f + h^3, \tag{19}$$

where A, B, C are DP's in h, of norms p^2, p^4, p^6 respectively, such that every divisor f of h, of norm p^2 and in standard form, is a root of T. Furthermore, every root of T lying in D is a divisor of h, of norm p^2.

(T, when written out fully, has 38 distinct terms, and its coefficients B and C exhibit irregular patterns of formation, as contrasted with the coefficients of the polynomials P and Q of Theorems 1 and 3. Also, in contrast with P and Q, it is not known that every root of T lying in D is in standard form.)

Proof. First suppose $h = fg$, with f, g in standard form and $Nf = Ng = p^2$. By repeated differentiation of h we obtain

$$h = fg,$$

$$h' = f'g + fg' - rf'g', \tag{20}$$

$$h'' = f + f'g' + g - rf' - rg', \tag{21}$$

$$h''' = f' + g' - r. \tag{22}$$

Between these four equations in f, f', g, g' we wish to eliminate f', g' and g. We first solve (22) for f' and substitute in (20) and (21); then by adding multiples of (20) and (21) to one another we obtain one polynomial equation free of g'. This equation is of degree 3 in each of f and g. If we multiply it through by f^3 and replace fg by h, to eliminate g, we obtain the expression (19) set equal to zero. Thus f is a root of T.

Conversely, suppose f is a root of T lying in D. If $Nf < p^2$, the term f^6 in (19) would be the unique term of smallest norm, so $T(f) \neq 0$. Similarly, we cannot have $Nf > p^2$; thus $Nf = p^2$. Next we show that f divides

h. By unique factorization, if $f \nmid h$ there is a prime $q \in D$ which divides f to a power higher than that to which it divides h; say $q^m \mid f$, $q^m \nmid h$, $q^{m-1} \mid h$. Every term of $T(f)$ is then divisible by q^{3m-2} except for the last, so $T(f) \neq 0$; thus $f \nmid h$ is impossible.

Now $f = L$ is a root of T, with h replaced by h_x, for every x. The coefficient of x^3 in $T(f)$ is (after cancelling a nonzero factor Δh)

$$V(f) = (\Delta h''')^2 f^3 - \Delta h'''(\Delta h' + r\Delta h'' + r^2 \Delta h''')f^2 + \Delta h(\Delta h'' + 2r\Delta h''')f - (\Delta h)^2, \tag{23}$$

and L is a root of V. If $\Delta h''' = 0$ we get $L = \Delta h/\Delta h''$, so we assume henceforth that $\Delta h''' \neq 0$.

LEMMA 5. *Let f be any root of V lying in D. Then $f \mid \Delta h$ and $f'' = \delta$.*

Proof. The first assertion follows as in the proof of Theorem 9. To prove that $f'' = \delta$, we notice that, by analogy with the polynomial (11) of Theorem 3, we can rewrite the equation $V(f) = 0$ in the form

$$\sum_{k=0}^{3} (\Delta h''')^{3-k}(\Delta h^{(k)} - r\Delta h^{(k+1)})(r\Delta h''' - \Delta h/f)^k = 0.$$

By Lemma 2 the derivative of $r\Delta h''' - \Delta h/f$ is zero; that is, $\Delta h''' = (\Delta h/f)'$. If we now divide each term of (23) by f^2, differentiate each term and replace $(\Delta h/f)'$ by $\Delta h'''$, and then factor $\Delta h'''$ from each term, we obtain the equation

$$\Delta h'''f' - \Delta h'' - r\Delta h''' + \Delta h/f = 0.$$

Again differentiating both sides, replacing $(\Delta h/f)'$ by $\Delta h'''$ and factoring out $\Delta h'''$, we obtain simply $f'' - \delta = 0$.

The proof of Theorem 8 is now completed as follows. Referring to the paragraph preceding Lemma 5, the coefficient of x^2 in $T(f)$ is a quartic polynomial in f, and the remainder when it is divided by the cubic polynomial V has constant term (apart from a nonzero factor) exactly equal to (18). The proof used earlier when $NL = p$ serves also to show that (18) is not zero in the present case. Let W denote this remainder, having nonzero constant term. W is a linear or quadratic polynomial having L as a root. If W is linear, we are through.

Suppose W is of degree 2, with second root say f_1; f_1 lies in the field K. We may assume f_1 is also a common root of the two polynomials (19) corresponding to h_0 and h_1, and also a root of V, for otherwise division of W into one of these three polynomials will produce a linear polynomial with DP coefficients having L as a root, and we are through. Since (19) is

monic, f_1 lies in D, and by Theorem 9 f_1 is a common divisor of h_0 and h_1, of norm p^2. Also, since f_1 is a root of V we have $f_1'' = \delta$ by Lemma 5, so f_1 is in standard form. Thus $f_1 = L$, so L is a double root of W. Therefore the discriminant of W is zero, and we obtain again a DRF for L.

8. The GCD of three functions. Suppose each of h_0, h_1 and h_2 has norm p^3. We may assume $N(h_0, h_1) = N(h_0, h_2) = N(h_1, h_2) = p^2$ and $N(h_0, h_1, h_2) = p$, for in any other case the three-fold GCD (h_0, h_1, h_2) reduces to one of the above two-fold GCD's. We write $(h_0, h_1, h_2) = ((h_0, h_1), (h_1, h_2))$ and apply first Theorem 7, then Theorem 4. The result is

THEOREM 10. *Let h_0, h_1, h_2 be in standard form, each of norm p^3, with $N(h_0, h_1) = N(h_0, h_2) = N(h_1, h_2) = p^2$, $N(h_0, h_1, h_2) = p$. Then*

$$(h_0, h_1, h_2) = \frac{(h_1'' - h_0'')(h_2 - h_0) - (h_2'' - h_0'')(h_1 - h_0)}{(h_1'' - h_0'')(h_2' - h_0') - (h_2'' - h_0'')(h_1' - h_0')}.$$

If instead we write $(h_0, h_1, h_2) = ((h_0, h_1), h_2)$ and use first Theorem 7, then Theorem 6, we obtain a DRF which represents (h_0, h_1, h_2) whenever the two conditions $N(h_0, h_1) = p^2$ and $N(h_0, h_1, h_2) = p$ are satisfied.

REFERENCES

[1] E. D. Cashwell and C. J. Everett, *The ring of arithmetic functions*, Pacific J. Math., **9** (1959), 975–985.

[2] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 4th edition, Oxford, 1960.

Received November 20, 1981.

UNIVERSITY OF COLORADO
BOULDER, CO 80309