ACTA ARITHMETICA
XXI (1972)

Ideals not prime to the conductor in quadratic orders

by

HUBERT S. BUTTS and GORDON PALL* (Baton Rouge, La.)

Dedicated to the memory of W. Sierpiński

1. If A $(= hA', A'$ primitive in $R_d)$ is an ideal in an order R_d of a quadratic field, and $N(A) = bc$, then (see [1]) if A is prime to the conductor the number of ideal divisors of A with norm b equals the number of ideals of norm (h, b, c). The present paper grew out of the desire to remove the hypothesis that A is prime to the conductor. This was found to be far from trivial, and required a substantial study of ideals not prime to the conductor.

2. Let d_0 denote the discriminant of a quadratic field. There is a unique order

$$R_d = [1, \omega] = Z + \omega Z,$$

said to be of discriminant d, corresponding to each element d of $D = \{d_0 s^2 \mid s > 0, s \text{ in } Z\}$. Here Z is the ring of integers, $\omega = (\varepsilon + \sqrt{d})/2$, ε $(= 0$ or $1)$ $\equiv d \pmod 2$. We write $d \to \omega$. Each nonzero ideal M in R_d is ([2], p. 32) a Z-module

$$k[m, r+\omega] = kmZ + k(r+\omega)Z, \quad \text{where} \quad m \mid N(r+\omega). \tag{1}$$

Here k, m, r are integers, k and m positive; and k, m, and the residue r modulo m are uniquely determined by R_d and M. If $k = 1$, M is called *primitive in* R_d.

We call M *invertible in* R_d if there is a nonzero ideal N in R_d such that $MN = hR_d$, h in Z. It is shown in [2], p. 34, that M is invertible in R_d if and only if

$$(m, d, N(r+\omega)/m) = 1. \tag{2}$$

A nonzero ideal M in R_d is invertible in a unique order, whose discriminant is necessarily a divisor of d. Further ([2], p. 34), the ideal M in (1) is invertible in R_d if and only if $M\overline{M} = k^2 mR_d$; and then k^2m is the norm of M.

* This work was supported in part by National Science Foundation grant GP-29105 X.

LEMMA 1. *Let $A_i = [m_i, r_i+\omega_i]$ be an ideal in R_{d_i} $(i = 1, 2)$. Then the product (as Z-modules) of A_1 and A_2 is an ideal in R_d, where $d = (d_1, d_2)$.*

Proof. Let $d_i \to \omega_i$ $(i = 1, 2)$. We can write $d_i = d_0 n_i^2$, $h = (n_1, n_2)$, $n_i = hq_i$ $(i = 1, 2)$, $d = d_0 h^2$. Thus $(q_1, q_2) = 1$ and integers s_i can be found such that

$$r_1+\omega_1 = s_1+q_1\omega, \quad r_2+\omega_2 = s_2+q_2\omega; \tag{3}$$

and integers v_i such that $v_1 q_1 + v_2 q_2 = 1$. Hence $d \to \omega$, $\omega = v_1\omega_1+v_2\omega_2+ +k$ (k in Z). Thus $\omega_1 A_1 \subset A_1$, $\omega_2 A_2 \subset A_2$, $v_i\omega_i A_1 A_2 \subset v_i A_1 A_2$ $(i = 1, 2)$; $\omega A_1 A_2 \subset A_1 A_2$, hence $A_1 A_2$ is an ideal in $[1, \omega]$.

COROLLARY 1. *If A_i is an ideal in $[1, \omega_i]$ $(i = 1, 2)$, then $A_1 A_2 = A_1 A_2[1, \omega]$. Also, $[1, \omega] = [1, \omega_1][1, \omega_2]$. Hence*

$$A_1 A_2 = A_1[1, \omega_2]\cdot A_2[1, \omega_1]. \tag{4}$$

Here $A_1[1, \omega_2]$ and $A_2[1, \omega_1]$ are ideals in $[1, \omega]$.

The following result appears as Lemma 5.1 in [2].

LEMMA 2. *If $A_1 = k[m_1, r_1+\omega_1]$ is an invertible ideal in $[1, \omega_1]$, then*

$$A_1[1, \omega_2] = ke_1[m_1/e_1^2, r+\omega], \tag{5}$$

where $e_1 = (m_1, s_1, q_1)$, m_1/e_1^2 is an integer, and r is defined by

$$q_1' r \equiv s_1' \pmod{m_1/e_1^2}, \quad \textit{where} \quad s_1 = e_1 s_1', \quad q_1 = e_1 q_1'. \tag{6}$$

COROLLARY 2. *If A_i is an invertible ideal in $[1, \omega_i]$ $(i = 1, 2)$,*

$$A_1 A_2 = e_1 e_2[m_1/e_1^2, r+\omega][m_2/e_2^2, s+\omega], \tag{7}$$

$$q_1' r \equiv s_1' \pmod{m_1/e_1^2}, \quad q_2' s \equiv s_2' \pmod{m_2/e_2^2},$$

with e_i, q_i', s_i' defined as shown in Lemma 2. If, in particular, $(m_1/e_1^2, m_2/e_2^2) = 1$, we can choose $r = s$ and have

$$A_1 A_2 = e_1 e_2[m_1 m_2/(e_1 e_2)^2, r+\omega]. \tag{8}$$

The problem of multiplying two ideals in any of the orders is thus reduced to that of multiplying two ideals in the same order. If $A = [m, r+\omega]$ is an ideal in $[1, \omega]$, and $m = \prod p^c$ is a product of powers of distinct primes p, then A is the product of the ideals $[p^c, r+\omega]$. In view of Corollary 2 the problem is reduced to that of finding the product of two ideals $[p^a, r+\omega]$ and $[p^b, s+\omega]$ with p a prime.

Primes p can be classified as follows relative to a discriminant d: (i) those such that $(d|p) = 1$; (ii) those satisfying $(d|p) = -1$; (iii) those for which $p|d$ but d/p^2 is not in D; (iv) primes p such that d/p^2 is in D. The first three types are familiar in the literature, usually with reference to the maximal order, in which case type (iv) does not occur. If $(d|p) = -1$, then in any order the only ideals whose norm is a power of p are expressed by $p^a R_d$. If $(d|p) = 1$, there are two ideals, $P = [p, r+\omega]$ and $\bar{P} = [p, r+\bar{\omega}]$, of norm p; $P\bar{P} = pR_d$ and any ideal of norm p^a which is primitive in R_d is P^a or $\bar{P}^a$. If p is of type (iii), there is a unique ideal $P = [p, r+\omega]$, and $P^2 = pR_d$. But ideals $[p^a, r+\omega]$ with p of type (iv) have been neglected. Their theory at first seemed chaotic, and we tried to bring some order into this chaos. We like to speak of such primes as *bad*.

3. Let n denote the largest integer for which $d_1 = d/p^{2n}$ is in D. Let p be a bad prime. Then $n \geqslant 1$. The module $[p^l, z+\omega]$ is an invertible ideal in R_d if and only if $p^l \| N(z+\omega)$, i.e.

$$4p^l | (2z+\varepsilon)^2 - p^{2n} d_1, \quad 4p^{l+1} \nmid (2z+\varepsilon)^2 - p^{2n} d_1. \tag{9}$$

Notice that (9) is impossible if l is odd and $< 2n$; if $p|d_1$ and $l > 2n+1$; if $(d_1|p) = -1$ and $l > 2n$; or if $l = 2n$ when $p = 2$ and $d_1 \equiv 1 \pmod 8$. Hence there are four types of invertible ideals $[p^l, z+\omega]$ when p is odd:

α_1: $l = 2k < 2n$, $2z+\varepsilon = p^k m$, $(m, p) = 1$;
α_2: $l = 2n$, $2z+\varepsilon = p^n m$, $m^2 - d_1$ prime to p;
α_3: $l = 2n+1$, $p|d_1$, $2z+\varepsilon = p^n m$, $p|m$;
α_4: $l > 2n$, $(d_1|p) = 1$, $2z+\varepsilon = p^n m$, $\pm m = m_1 + sp^{l-2n}$ with $(s, p) = 1$.

In the last type, m_1 denotes a fixed solution of $m_1^2 \equiv d_1 \pmod{p^{l-2n+1}}$, and we note that if $(d_1|p) = 1$ and $u \geqslant 1$, the two solutions $\pm m_1$ of $x^2 \equiv d_1 \pmod{p^{u+1}}$ satisfy $y^2 \equiv d_1 \pmod{p^u}$, and the only y's that do not serve as an x are those given by $\pm(m_1+sp^u)$ with $(s, p) = 1$; a similar remark applies to β_4 below. If $p = 2$, (9) reduces to $2^l \| z^2 - 2^{2n-2} d_1$ and we subdivide the cases in which this holds into five types:

β_1: $l = 2k < 2n-2$, $z = 2^k m$, m odd;
β_1': $l = 2n-2$, $z = 2^{n-1} m$, $m \not\equiv d_1 \pmod 2$;
β_2: $l = 2n$, $z = 2^{n-1} m$, m odd if $d_1 \equiv 5 \pmod 8$, $m \equiv 2$ or $0 \bmod 4$ acc. as $d_1 \equiv 8$ or $12 \bmod 16$;
β_3: $l = 2n+1$, $z = 2^{n-1} m$, $m \equiv 0$ or $2 \bmod 4$ acc. as $d_1 \equiv 8$ or $12 \bmod 16$;
β_4: $l > 2n$, $d_1 \equiv 1 \pmod 8$, $z = 2^{n-1} m$, $\pm m = m_1 + 2^{l+1-2n} s$, s odd.

Here m_1 is a fixed solution of $m_1^2 \equiv d_1 \pmod{2^{l+3-2n}}$.

We wish to count the invertible ideals $[p^a, r+\omega]$ with norm p^a. Here r is determined modulo p^a, and so for example if $a = 2h < 2n$, $2r+\varepsilon = p^h m'$, $(m', p) = 1$, p odd, we must count $2r+\varepsilon \bmod p^{2h}$, hence $m' \bmod p^h$, and have $\varphi(p^h)$ residues m'. In this manner we obtain

LEMMA 3. *The number $\psi(p^a)$ of primitive invertible ideals of norm p^a in R_d is zero if a is odd and $< 2n$, or $p|d_1$ and $a > 2n+1$, or $(d_1|p) = -1$ and $a > 2n$, or (if $p = 2$) $a = 2n$ and $d_1 \equiv 1 \pmod 8$; and is $\varphi(p^h)$ if*

$a = 2h < 2n$, or if $a = 2n$ and $p \mid d_1$; and is

$$(10)\qquad p^n \text{ if } a = 2n+1 \text{ and } p \mid d_1;\ p^n \text{ if } a = 2n \text{ and } (d_1 \mid p) = -1;\ p^{n-1}(p-2) \\ \text{if } a = 2n \text{ and } (d_1 \mid p) = 1;\ 2\varphi(p^n) \text{ if } a > 2n \text{ and } (d_1 \mid p) = 1.$$

Here φ is the Euler phi-function and $(d_1 \mid p)$ the Kronecker symbol.

Summing $\psi(p^a)+\psi(p^{a-2})+\ldots$ we have

LEMMA 4. *The number $\chi(p^t)$ of invertible ideals in R_d of norm p^t (so that $t = 2r+s$ in nonnegative integers r, s) is zero if t is odd and $(d_1 \mid p) = -1$, or if t $(< 2n)$ is odd; and is p^h if $t = 2h < 2n$; and is*

$$(11)\qquad p^n \text{ if } t \geqslant 2n \text{ and } p \mid d_1;\ p^n+p^{n-1} \text{ if } t\ (\geqslant 2n) \text{ is even and } (d_1 \mid p) = -1; \\ (t-2n+1)\varphi(p^n) \text{ if } t \geqslant 2n \text{ and } (d_1 \mid p) = 1.$$

The following remarkably simple formula for the product of two ideals holds even when p is of type (i) or (iii).

THEOREM 1. *Let p be a bad prime. Let $A = [p^a, r+\omega]$ and $B = [p^b, s+\omega]$ be invertible, and $b \geqslant a > 0$ (hence $a \geqslant 2$ if p is bad), and set $t = r+s+\varepsilon$. Then $B = \bar{A}$ if and only if $p^a \mid t$, and in this case*

$$(12)\qquad AB = (p^a) = p^a[1, \omega].$$

If $p^a \nmid t$, let $p^c \| t$. Then $0 < c < a$ and $p^c \mid u$ where $u = rs-(\varepsilon-d)/4$, and

$$(13)\qquad AB = p^c[p^{a+b-2c}, v+\omega], \qquad \textit{where} \qquad v \equiv u/t\ (\operatorname{mod} p^{a+b-2c}).$$

Proof. If $p^c \| t$ (take $c = \infty$ if $t = 0$) and $m = \min(a, c)$, then $p^m \mid u$ since

$$(14)\qquad rs \equiv -s^2-s\varepsilon \equiv (\varepsilon-d)/4\ (\operatorname{mod} p^m).$$

Suppose $p^a \mid t$. Then $m = a$ and

$$(15)\qquad AB = [p^{a+b}, p^a(s+\omega), p^b(r+\omega), u+t\omega] \\ = p^a[p^b, s+\omega, (r+\omega)p^{b-a}, (u+t\omega)p^{-a}] = p^a N, \text{ say}.$$

Hence N must have the Z-basis $[p^e, s+\omega]$, where p^e is the g.c.d. of p^b and the two integers

$$p^{b-a}(r+\omega)-p^{b-a}(s+\omega) = (r-s)p^{b-a}, \\ (u+t\omega)p^{-a}-t(s+\omega)p^{-a} = -N(s+\omega)p^{-a}.$$

Clearly p^{b-a} divides the latter precisely, and divides the former. Hence $AB = p^a[p^{b-a}, s+\omega]$. But a product of invertible ideals is invertible and, since p^{b-a+1} divides $N(s+\omega)$, AB cannot here be invertible unless $b = a$. Hence $b = a$, $AB = p^a[1, \omega] = A\bar{A}$, $B = \bar{A}$. Conversely, if $B = \bar{A}$ evidently $p^a \mid t$.

Suppose $p^a \nmid t$, i.e. $m = c$. Then $c > 0$ since $2p \mid (2r+\varepsilon)+(2s+\varepsilon)$, and

$$AB = p^c[p^{a+b-c}, (s+\omega)p^{a-c}, (r+\omega)p^{b-c}, (u+t\omega)p^{-c}].$$

Here tp^{-c} is an integer prime to p, and the module AB contains p^{a+b-2c} since this precisely divides each of

$$sp^{a-c}-(up^{a-c}p^{-c})/(tp^{-c}) = p^{a-c}N(s+\omega)/t, \\ rp^{b-c}-(up^{b-c}p^{-c})/(tp^{-c}) = p^{b-c}N(r+\omega)/t.$$

Hence (13) follows.

4. Let $A = [p^a, r+\omega]$, $L = [p^l, z+\omega]$ be primitive invertible ideals in R_d; $a > 0$, $l > 0$, c a nonnegative integer. We call A a *divisor* of p^cL, and write $A \mid p^cL$, if

$$(16)\qquad p^cL = AB, \quad \text{for an ideal } B \text{ in } R_d.$$

If B is primitive we call A a *precise divisor*, and write $A \| p^cL$.

LEMMA 5. *If $A \neq L$, $A \| p^cL$ if and only if $p^{a-c} \| r-z$; $A \mid p^cL$ if and only if $p^{a-c} \mid r-z$.*

Proof. If (16) holds with B primitive, $p^cL\bar{A} = p^aB$, $L\bar{A} = p^{a-c}B$, $a \geqslant c$, and, by Theorem 1, $p^{a-c} \| (-r-\varepsilon)+(z+\varepsilon) = z-r$. Conversely, if $a \geqslant c$ and $p^{a-c} \| r-z$, then $L\bar{A} = p^{a-c}B$ with B primitive by Theorem 1. The last part also follows.

THEOREM 2. *Consider an invertible primitive ideal $L = [p^l, z+\omega]$ in R_d, $l > 0$. The following table lists in the various possible cases the values c for which there exists a primitive ideal A of norm p^a which precisely divides p^cL, and gives in the third column the number of such precise divisors A for each c listed therewith.*

Case		*Values c*	*Number for each c*
$a < l$	$a\ (\leqslant 2n)$ *even*	$a/2$	$\psi(p^a)$
	$a > 2n$, $(d_1 \mid p) = 1$	n, $a-n$	$\varphi(p^n)$ *each*
$a > l$	$l \leqslant 2n$	$a-l/2$	$\psi(p^a)$
	$l > 2n$	$a+n-l$, $a-n$	$\varphi(p^n)$ *each*
$a = l$	$a < 2n$	$0, 1, \ldots, (a/2)-1$	$\varphi(p^c)$ *each*
		$a/2$	$(p-2)p^{c-1}$
	$a = 2n$	$0, 1, \ldots, (a/2)-1$	$\varphi(p^c)$ *each*
		$a/2$	$\{p-2-(d_1 \mid p)\}p^{c-1}$
	$a = 2n+1$, $p \mid d_1$	$0, 1, \ldots, n$	$\varphi(p^c)$ *each*
	$a > 2n$, $(d_1 \mid p) = 1$	$0, 1, \ldots, n-1$	$\varphi(p^c)$ *each*
		n	$(p-2)p^{n-1}$
		$a-n$	$\varphi(p^n)$

Proof. Let $p > 2$. We set $2r+\varepsilon = p^h m'$, where $h = a/2$ if $a \leqslant 2n$, $h = n$ if $a > 2n$; similarly for $2z+\varepsilon = p^k m$. We must study

$$p^{a-c} \| p^h m' - p^k m,$$

when L and A satisfy variously $\alpha_1, \ldots, \alpha_4$.

Cases with $a < l$. If $a < 2n$, then $p \nmid m'$ and $k > h$, $a-c = h = a/2$; if $a = 2n$, $l = 2n+1$, and $p \mid d_1$, then $p \nmid m'$, $p \mid m$, $a-c = n$; if $a = 2n$ and $(d_1|p) = 1$, $m'^2 \not\equiv d_1$, $m^2 \equiv d_1 \pmod p$, $a-c = n$; if $a > 2n$ and $(d_1|p) = 1$, $\pm m = m_1 + tp^{a-2n}$, $(t, p) = 1$, $m = m_1 + sp^{l-2n}$ (m_1 fixed), hence $p^{a-2n} \| m'-m$ and $a-c = a-n$, or $p \nmid m'-m$ (since $2m_1$ is prime to p) and $a-c = n$; note that t is determined mod p^n and has $\varphi(p^n)$ values in each case.

Cases with $a > l$. If $l \leqslant 2n$ we consider $p^h m' - p^k m$ and have $a-c = k = l/2$ and the full number $\psi(p^a)$ of divisors. If $l > 2n$ we have $(m'-m)p^n$ with $\pm m' = m_1 + tp^{a-2n}$ and $m = m_1 + sp^{l-2n}$ with s prime to p, hence $p^{l-2n} \| m'-m$ and $a-c = l-n$, or $p \nmid m'-m$ and $a-c = n$, much as before.

Cases with $a = l$. We consider $p^{a-c} \| p^h(m'-m)$ and count m' mod p^{a-h}. Denote by v_f the number of residues m' such that $p^f \| m'-m$ if $0 \leqslant f < a-h$, and let $v_{a-h} = 1$; then $a-c = f+h$ for such values m'. Suppose that m satisfies α_1, α_2, or α_3. Then $m' \equiv m \pmod p$ implies that m' satisfies the like condition α_1, α_2, or α_3. Hence if $f > 0$ we can set $m' = m + sp^f$, $(s, p) = 1$; counting s mod p^{a-h-f} we have $v_f = \varphi(p^{a-h-f})$. Let $f = 0$; if $a < 2n$, m' and m are prime to p, m' has $p-2$ residues mod p for which $p \nmid m'-m$, $v_0 = (p-2)p^{h-1}$; if $a = 2n$ and $p \mid d_1$, the same; if $a = 2n$ and $(d_1|p) = -1$, m' is arbitrary, $v_0 = (p-1)p^{n-1}$; if $(d_1|p) = 1$, m' must not be $0, m$, or $-m$ mod p, $v_0 = (p-3)p^{n-1}$; if $a = 2n+1$ and $p \mid d_1, p \mid (m', m)$, and we set $m' = m + ps$, $(s, p) = 1$, hence $v_0 = \varphi(p^n)$. Finally consider α_4 with $a > 2n$, $(d_1|p) = 1$, $\pm m' = m_1 + tp^{a-2n}$, $(st, p) = 1$, with t counted mod p^n. Thus $m'-m \equiv 2m_1 \pmod p$ and $a-c = n$ with $\varphi(p^n)$ divisors, or $m'-m = (s-t)p^{a-2n}$ and $a-c = n+(a-2n+e)$ where $p^e \| s-t$, hence on setting $t = s+qp^e$ with q prime to p we get $v_e = \varphi(p^{n-e})$ $(e = 1, \ldots, n)$, $v_0 = (p-2)p^{n-1}$.

The same final formulas are found when $p = 2$, and the work is usually much the same. We study $2^{a-c} \| r-z = 2^h m' - 2^k m$, with L and A satisfying $\beta_1, \ldots, \beta_4$. A few places are different: $a = 2n$, $l = 2n+1$, $2 \mid d_1$, $(m'-m)2^{n-1}$, $m'-m \equiv 2 \pmod 4$, $a-c = n = a/2$; $a = 2n = l$, $2 \mid d_1$, $(m'-m)2^{n-1}$, $m' \equiv m \equiv 2$ or 0 mod 4 acc. as $d_1 \equiv 8$ or 12 mod 16, thus m' is unique mod 4, and if v_f $(0 \leqslant f \leqslant n)$ is the number of residues m' mod 2^{n+1} for which $2^{f+1} \| m'-m$, $a-c = n-1+f+1$, etc.; if $a > l > 2n$, $(d_1|2) = 1$, $(m'-m)2^{n-1}$, $\pm m' = m_1 + t \cdot 2^{a+1-2n}$, $\pm m = m_1 + s \cdot 2^{l+1-2n}$, st odd, either $m'-m \equiv 2m_1 \pmod 4$, $a-c = n$, m' mod 2^{a-n+1}, t mod 2^n,

$\varphi(2^n)$ divisors, or $m'-m = t \cdot 2^{a+1-2n} - s \cdot 2^{l+1-2n}$, $2^{l-n} \| 2^{n-1}(m'-m)$, $c = a-l+n, \varphi(2^n)$ divisors; and so on.

5. We are now in a position to establish a generalization of the theorem which occupies the opening sentence of this article – without the hypothesis that the ideal is prime to the conductor. We first proved Theorem 3 by a mapping argument in the case where $g(p^t) \neq 0$ (and might then have treated the exceptional case directly). But we feel that much more is proved by our present method, and that the light thrown on the invertible ideals not prime to the conductor will be valuable for other purposes.

Given an invertible ideal $p^k L$, $L = [p^l, z+\omega]$, and a nonnegative integer t such that $\psi(p^t) \neq 0$, we wish to find the number $g(p^t)$ of (necessarily) invertible divisors of $p^k L$ with norm p^t; or, what is the same thing, the number of ordered pairs T, U such that $p^k L = TU$ with T and U ideals in R_d of given norms p^t and p^u, where $t+u = 2k+l$. Since $g(p^t) = g(p^u)$ we can suppose that $2t \leqslant 2k+l$.

Any such divisor T must be of the form $p^e[p^a, r+\omega]$ with $2e+a = t$; and if $A = [p^a, r+\omega]$ and $A \| p^c L$, then $k \geqslant e+c$. Hence $g(p^t) = 0$ if $k < k_0$, where k_0 denotes the minimum of the numbers $e+c$ for all decompositions $t = 2e+a$ (a and e nonnegative).

THEOREM 3. *Let* $s = \min(t, 2k+l-t)$. *Then*

$$g(p^t) = \chi(p^a), \tag{17}$$

where

$$a = \min(s, k + \min(n, l/2)); \tag{18}$$

except that

$$g(p^t) = 0 \quad \textit{when} \quad k < n \textit{ and } 2k < s < l. \tag{19}$$

Proof. We assume without loss that $t \leqslant k + (l/2)$. Hence $s = t$, and

$$k \geqslant t/2 \quad \text{if} \quad l \leqslant t, \tag{20}$$

$$a = t \quad \text{if} \quad l \leqslant 2n, \tag{21}$$

$$a = \min(t, k+n) \quad \text{if} \quad l > 2n. \tag{22}$$

Except when $a = l$, Theorem 2 assures the full number $\psi(p^a)$ (or $\varphi(p^n) = \psi(p^a)/2$) of divisors for each value of c for which $c+e \leqslant k$. If $a = l$, the $\psi(p^a)$ (or $\varphi(p^n)$) divisors are spread over an interval of values of c: in each such case it will be found that the largest $c+e$ for the interval satisfies $c+e \leqslant k$ under the stated conditions – and so one can treat these divisors as though they constituted a single batch of $\psi(p^a)$ (or $\varphi(p^n)$) divisors of norm p^t.

If $t \geqslant l$, we will show that $c+e \leqslant k$ holds for all allowable values of $c+e$, and the first part of Theorem 3 will follow from Theorem 2. For $t < l$, we will see that if $k_0 \leqslant k$ (k_0 defined above) then the values of $c+e$ such that $c+e \leqslant k$ yield, by Theorem 2, $g(p^t) = \chi(p^a)$; if $k < k_0$ then $g(p^t) = 0$.

Case $t \leqslant 2n$, $t < l$. We have $e = (t-a)/2$ and $c = a/2$ (by Theorem 2) for each even $a = 0, 2, \ldots, t$. Thus $e+c = t/2 = k_0$. Hence

$$g(p^t) = 0 \quad \text{if} \quad k < s/2 \leqslant n \text{ and } s < l. \tag{23}$$

Also, $a = t$, since when $l > 2n$ and $k \geqslant t/2$, $\min(t, k+n) = t$. The number of divisors is $\sum \psi(p^{t-2e}) = \chi(p^t)$.

Case $l \leqslant t \leqslant 2n$. Thus $a = t$. If $a = l$, $c = (l/2)-f$ and $e = (t-l)/2$; $k \geqslant t/2 \geqslant c+e$ for all $f \geqslant 0$. If $a < l$, $c = a/2$, $c+e = t/2 \leqslant k$. If $a > l$, $c = a-(l/2)$, $c+e \leqslant t-(l/2) \leqslant k$. For each a, Theorem 2 states that there are $\psi(p^a)$ divisors, $\chi(p^t)$ in all.

Case $p \mid d_1$, $t = 2n+1$. Since $a < 2n$ requires that a is even, only $a = 2n+1$ is possible. Also $a = t$ if $l \leqslant 2n$, and then $a > l$, $c = a-(l/2)$ $= c+e \leqslant t-(l/2) \leqslant k$. If $l = 2n+1$, then $k \geqslant t-(l/2)$ implies that $k \geqslant n+1$ and $a = \min(t, k+n) = t$; also $c = n-f$, and $k \geqslant n+1 > n-f = c+e$ $(f = 0, \ldots, n)$.

There remain only $(d_1 \mid p) = 1$, $t > 2n$, and one of

(a) $l > t$, $t \leqslant k+n$ (hence $a = t$);

(b) $l > t$, $t > k+n$ (hence $l > 2n$, $a = k+n$);

(c) $l \leqslant t$, $t \leqslant k+n$ (hence $a = t$);

(d) $l \leqslant t$, $t > k+n$ (hence $a = k+n$ and $l > 2n$).

Case (a). If a is even and $\leqslant 2n$, $c = a/2$, $c+e = t/2 < t-n \leqslant k$. If $a > 2n$, $c = n$ or $a-n$; $n+(t-a)/2 = (t/2)+(2n-a)/2 < t/2 < t-n \leqslant k$; $a-n+(t-a)/2 = (a/2)+(t/2)-n \leqslant t-n \leqslant k$; hence $c+e \leqslant k$ for all values of a. Note that $k_0 = n$, and $n \leqslant k$ since $2n < t \leqslant k+n$, so that $k < k_0$ is impossible.

Case (b). Since $l > a$, any a greater than $2n$ will have $c = n$ or $a-n$. The minimum value of $n+(t-a)/2$ here will be n and that of $a-n+(t-a)/2$ will be $t/2$ or $(t+1)/2$, both $> n$; and if t is even and $a \geqslant 2n$, $c+e = t/2 > n$. Hence $k_0 = n$, and

$$g(p^t) = 0 \quad \text{if} \quad k < n,\ l > s > 2n. \tag{24}$$

Note that (23) and (24) together yield (19). We may suppose then that $k \geqslant n$, and set $k = n+v$, $v \geqslant 0$.

Let t be even. The values a which are even and $\leqslant 2n$ have $c+e = t/2$, and will produce a batch of $\varphi(p^n)$ divisors if and only if $k \geqslant t/2$. We will verify that if $a = 2n+2, \ldots, t$, and $c = n$ or $a-n$, then exactly v cases occur with $\varphi(p^n)$ divisors if $k \geqslant t/2$ and $v+1$ cases occur if $k < t/2$, thus yielding $\chi(p^t) = (k-n+1)\varphi(p^n)$ divisors in all. Indeed, if $t-2v \geqslant 2n+2$ (i.e. $k < t/2$), then we have $v+1$ cases with $c = n$ (since $n+(t-a)/2 \leqslant k$ $= n+v$ if and only if $t \geqslant a \geqslant t-2v$) and none with $c = a-n$ (since $a-n+(t-a)/2 \geqslant n+v+1$ for $a \geqslant 2n+2$). If $t-2v < 2n+2$ (i.e. $k \geqslant t/2$), only $(t-2n)/2$ cases occur with $c = n$; and putting $a = 2n+2q$, $(2n+2q)/2 +$ $+(t/2)-n = n+v$ gives $q = k-(t/2)$ cases with $c = a-n$, and $q+1+$ $+(t-2n)/2 = k-n+1$ as required.

Let t be odd. If $t-2v \geqslant 2n+1$, $v+1$ cases already occur with $c = n$; and none with $c = a-n$, since $a/2+t/2-n \geqslant n+v+1$ if $a = 2n+1$. But if $t-2v < 2n+1$, or $t < 2k+1$, then only $(t-2n+1)/2$ cases occur with $c = n$; and if we set $a = 2n+2q-1$ $(q = 1, \ldots, (t-2n+1)/2)$, then there are r cases with $a/2+t/2-n \leqslant n+v$, given by $(2n+2r-1)/2+$ $+(t/2)-n = n+v$, i.e. $r = k-(t-1)/2$; and $r+(t-2n+1)/2 = k-n+1$, as required.

Case (c). We will show that there are exactly $t-2n+1$ batches of $\varphi(p^n)$ divisors corresponding to values of a such that $k \geqslant c+e$.

Suppose $l \leqslant 2n$, hence l even. One batch comes from $a = 0, 2, \ldots, 2n$ when t is even. If $a < l$, $c+e = t/2 \leqslant k$ since $2k+l \geqslant 2t$. If $a = l$, $c = a/2-$ $-f$ $(f = 0, 1, \ldots, a/2)$, $c+e = t/2-f \leqslant t/2 \leqslant k$. If $l < a \leqslant 2n$, $c = a-l/2$, $c+e = (t+a-l)/2 \leqslant (t/2)+n-l/2$. In each case, $k \geqslant c+e$, since $t > 2n$ implies that $k \geqslant t-l/2 > (t/2)+n-l/2$. Also, $\chi(p^{2n}) = \varphi(p^n)$. We have also to consider $2n < a \leqslant t$, $a \equiv t \pmod 2$, $c = a-l/2$, $c+(t-a)/2$ $= (a+t-l)/2 \leqslant t-l/2 \leqslant k$ since $t \geqslant a$. Every such a gives $2\varphi(p^n)$ divisors, and the number of values a is $[(t+1-2n)/2]$, giving $(t-2n+1)\varphi(p^n)$ in all.

Suppose $l > 2n$. Now $a \leqslant 2n$ (t even) gives $c+e = t/2 \leqslant t-l/2 \leqslant k$; one batch. If $l > a > 2n$, $c = n$ or $a-n$. If $c = n$, $n+(t-a)/2 < t-n \leqslant k$ since $n < a/2$ and $n < t/2$. If $c = a-n$, $a-n+(t-a)/2 \leqslant t-n \leqslant k$ since $a \leqslant t$. If $a = l > 2n$ and $c = a+n-l$, then $c+e = a+n-l+(t-a)/2 \leqslant t-n$ $\leqslant k$ since $2n \leqslant l$ and $a \leqslant t$; $c = a-n$ goes as before. Thus, $(t-2n+1)\varphi(p^n)$ divisors.

Case (d). If $a \leqslant 2n$ (t even), $c+e = t/2 \leqslant t-l/2 \leqslant k$. If $2n < a$ $\leqslant l$, $c = n$ (or $n-f$) or $a-n$. Here $n+(t-a)/2 \leqslant t-l/2$ holds for $a = 2n$, hence for $a > 2n$. If $2n < l < a$, $c = a+n-l$ or $a-n$. Here $a+n-l+$ $+(t-a)/2 = (a/2)+n-l+t/2 \leqslant t-l+n \leqslant t-l/2 \leqslant k$ since $2n \leqslant l$. Hence there are $(t/2)-n+1$ batches when t is even, $(t-2n+1)/2$ batches when t is odd, not counting any with $c = a-n$. To attain the number $k-n+1$ of batches we must verify that there are $k-[t/2]$ batches with $c = a-n$, $2n < a \leqslant t$. If t is even it follows easily that there are $k-t/2$ values of a such that $2n < a \leqslant t$ and $a-n+(t-a)/2 \leqslant k$; and there are $k-(t-1)/2$ such values a when t is odd. This completes the proof.

6. Let $\delta[\lambda, r+\omega]$ be a fixed invertible ideal in R_d, δ and λ in Z, and let τ, σ be positive integers such that $\delta^2\lambda = \tau\sigma$. We wish to determine the number $g(\tau)$ of divisors in R_d (necessarily invertible) of $\delta[\lambda, r+\omega]$ of norm τ, i.e. the number of ordered pairs T, S of invertible ideals in R_d such that $\delta[\lambda, r+\omega] = TS$, $N(T) = \tau$. For each prime p define integers k_p, l_p, n_p, s_p by: $p^{k_p}\|\delta$, $p^{l_p}\|\lambda$, $p^{s_p}\|(\lambda, \sigma)$; let n_p be the largest integer such that d/p^{2n_p} is in D.

If $n = 0$ in Theorem 3, i.e. if p is not a bad prime, then Theorem 3 becomes a special case of Theorem 1 of [1]. If z is a positive integer let $\chi(z)$ denote the number of invertible ideals in R_d of norm z. By Theorem 3 and Corollary 2 we now have

THEOREM 4. *If there exists a prime p such that $k_p < n_p$ and $2k_p < s_p < l_p$, then $g(\sigma) = g(\tau) = 0$. Otherwise,*

$$g(\sigma) = g(\tau) = \chi\left(\prod p^{a_p}\right), \quad \textit{where} \quad a_p = \min\bigl(s_p, k_p + \min(n_p, l_p/2)\bigr).$$

7. It may be of interest to mention that the result in the opening sentence of this article arose from a neat proof, essentially by descent, that if $a+bi$ is a Gauss integer of norm mn (m and n positive integers), then the number of nonassociate divisors of $a+bi$ of norm m is equal to the number of Gauss integers of norm (a, b, m, n). There is a similar result for quaternions, and presumably a corresponding theorem for factoring ideals in generalized quaternion orders. The analogous problem in cubic fields seems to be complicated. In [1] we gave an algorithm which associates the factorizations of an element $r(x_1+x_2\omega)$ in R_d as a product of elements of norms m and n with representations of $e = (r, m, n)$ by an explicitly given binary quadratic form φ of discriminant d. How φ is naturally connected with the given elements was left unclear. Hence it may be worth mentioning that φ can be transformed by an integral transformation into the primitive form associated in [2], Section 3, with the module $[m, r(x_1+x_2\omega)]$.

References

[1] H. S. Butts and G. Pall, *Factorization in quadratic rings*, Duke Math. Journ. 34 (1967), pp. 139–146.

[2] — — *Modules and binary quadratic forms*, Acta Arith. 15 (1968), pp. 23–44.

Received on 1. 8. 1971 (196)

ACTA ARITHMETICA
XXI (1972)

Differential rings of meromorphic functions

by

E. G. STRAUS (Los Angeles, Calif.)

To the memory of Wacław Sierpiński

1. Introduction. Let $\mathscr{R}$ be a differential ring of analytic functions, that is a ring closed under differentiation. We may assume without loss of a generality that $\mathscr{R}$ contains the constants C and is therefore an algebra over C. If $\mathscr{R}_0$ is a differential subring of $\mathscr{R}$ we can define the ring $\mathscr{L} = \mathscr{R}_0[D]$ of linear differential operators with coefficients in $\mathscr{R}_0$ and consider $\mathscr{R}$ as an $\mathscr{L}$-module.

1.1. DEFINITION. The elements $f_1, f_2, \ldots, f_n$ of $\mathscr{R}$ are *linearly dependent over $\mathscr{L}$* if there exist $L_1, \ldots, L_n \in \mathscr{L}$ not all 0 so that $L_1f_1 + \ldots + L_nf_n = 0$ and *linearly independent over $\mathscr{L}$* otherwise. The *dimension of $\mathscr{R}$ over $\mathscr{L}$* is the maximum number of linearly independent elements of $\mathscr{R}$ over $\mathscr{L}$.

We are interested in the following general conjectures:

1.2. CONJECTURE. *If $\mathscr{R}$ is a ring of entire functions which is finite dimensional over $\mathscr{L}$ then $\mathscr{R}$ is 0-dimensional over $\mathscr{L}$. That is, for every $f \in \mathscr{R}$ there exists an $L \in \mathscr{L}^*$ $(= \mathscr{L}\setminus\{0\})$ so that $Lf = 0$.*

The hypothesis that $\mathscr{R}$ be a ring of entire functions is certainly not superfluous since the conjecture in this form does not hold for rings of meromorphic functions (see § 3). However David Cantor has suggested the following two purely algebraic versions of our conjecture.

1.3. CONJECTURE. *Let $\mathscr{R}$ be an abstract differential ring with $D\mathscr{R} = \mathscr{R}$ and define $\mathscr{R}_0$ and $\mathscr{L}$ as before. If $\mathscr{R}$ is finite dimensional over $\mathscr{L}$ then $\mathscr{R}$ is 0-dimensional over $\mathscr{L}$ (at least if $D\mathscr{R}_0 = \{0\}$).*

1.4. CONJECTURE. *Let $\mathscr{R}, \mathscr{R}_0$ and $\mathscr{L}$ be as in Conjecture 1.3 but make the stronger assumption that $L\mathscr{R} = \mathscr{R}$ for every $L \in \mathscr{R}_0[D]$ whose leading coefficient is a unit of $\mathscr{R}_0$. Then, if $\mathscr{R}$ is finite dimensional over $\mathscr{L}$ it is 0-dimensional over $\mathscr{L}$.*

So far we have no algebraic attack on those conjectures. However we were able to show that there is an upper bound on the growth rates of the functions of $\mathscr{R}$ which is consistent with Conjecture 1.2 ([1]).