A NEW DEFINITION OF DIVISION IN RINGS OF QUOTIENTS OF EUCLIDEAN RINGS

M. W. BUNDER
The University of Wollongong, Wollongong, N.S.W. 2500, Australia

INTRODUCTION

It is known that notions such as that of divisibility and greatest common divisor can be defined in any Euclidean ring. Such notions can be defined similarly in the corresponding ring of quotients, and there these notions, in general, become trivial. In this paper, we show that minor alterations to some of these definitions lead to many interesting results concerning divisibility and greatest common divisors as well as primes and congruences. In each case these results generalize ones that hold in the original ring.

The set of integers Z, the set of finite polynomials $P[x]$ over a field, and the set of complex numbers $Z[i]$, with integer real and imaginary parts, form Euclidean rings. The results we obtain on rings of quotients then apply to rational numbers, quotients of polynomials, and complex numbers with real and imaginary parts which are rationals (or square roots of rationals, depending on the definition).

QUOTIENTS OF EUCLIDEAN RINGS

Throughout this paper, R will denote a Euclidean ring with unity, as defined in [1]. The norm function associated with R will be denoted by g, and the set of divisors of zero in R by Θ. If g, in addition to its two commonly accepted properties, also satisfies

$$g(ab) = g(a)g(b) \text{ for all } a,\ b,\ ab \in R - \{0\},$$

then R will be called a Euclidean$^+$ ring.

In R, we use the standard definitions, as found in [1], for divides, greatest common divisor, mutually prime, unit, prime, congruence modulo c, and $\leq$.

The ring of quotients of R, as defined in [1], will be denoted here by R' and the elements of R' by (a, b) where $b \notin \Theta$. The zero of R' will be denoted by $(0, 1)$ and the unity by $(1, 1)$.

If R is a Euclidean domain, so that $\Theta = \{0\}$, then it is obvious that for $(c, d) \neq (0, 1)$ we have

$$(a, b) = (ad, bc) \cdot (c, d) + (0, 1)$$

so that with norm function g' given by

$$g'(a, b) = g'(1, 1) = g(1),$$

R' is a Euclidean ring.

If Θ is larger than $\{0\}$ it may not be possible to define a g' on R' which extends g.

Since the division algorithm given above is a trivial one, we now give definitions that will lead to a nontrivial division algorithm which applies to any ring of quotients of a Euclidean$^+$ ring.

Definition 1: (a) $(a, b) < (c, d)$ if $g(a)g(d) < g(c)g(b)$,
(b) $(a, b) \leq (c, d)$ if $(a, b) < (c, d)$ or $(a, b) = (c, d)$.

The symbol $<$ can easily be shown to be irreflexive, asymmetric, and transitive, while the symbol $\leq$ is a partial ordering of R'.

Definition 2: If $(a, b) \neq (0, 1)$, we say that (a, b) divides (c, d), that is,

$$(a, b) \mid (c, d),$$

if there is a $q \in R$ such that $(c, d) = (q, 1)(a, b)$; in other words, if $ad \mid bc$.

Note that the q in Definition 2 is unique if $a \notin \Theta$ and that this definition is a generalization of division as defined in R. We can now prove

Theorem 1: If a, b, c, d are elements of a Euclidean$^+$ ring R, and $(a, b) \mid (c, d)$, then $(a, b) < (c, d)$ or $g(a)g(d) = g(b)g(c)$.

Proof: If $(a, b) \mid (c, d)$, then for some $q \in R$,

$$qad = bc.$$

When $g(q) = 1$, we have $g(a)g(d) = g(b)g(c)$; otherwise $g(b)g(c) > g(a)g(d)$, so the theorem holds. We can define units and primes in R' just as we did in R.

Definition 3: (a, b) is a unit if for some $(c, d) \in R'$,

$$(a, b) \cdot (c, d) = (1, 1).$$

Definition 4: (a, b) is a prime if it is not a unit and if

$$(a, b) = (c, d) \cdot (e, f)$$

implies that (c, d) or (e, f) is a unit.

If $a \notin \Theta$, we have $(a, b) \cdot (b, a) = (1, 1)$, so (a, b) is a unit and hence not a prime.

If $a \in \Theta$ and $(a, b) \cdot (c, d) = (1, 1)$, then $bda' = 0$, where $aa' = 0$. Now, as $b \notin \Theta$, $da' = 0$, and so $d \in \Theta$, which is impossible. Hence we have:

Theorem 2: $a \in \Theta$ if and only if (a, b) is not a unit.

Suppose $a \in \Theta$ and $a = a_1a_2a_3$, with a_1, $a_2 \in \Theta$, then

$$(a, b) = (a_1, b) \cdot (a_2a_3, 1),$$

where (a_1, b) and $(a_2a_3, 1)$ are not units, so (a, b) is not prime.

If $a \in \Theta$ and $a = a_1a_2$, where $a_1 \in \Theta$ is prime, $a_2 \notin \Theta$, and

$$(a, b) = (c, d) \cdot (e, f), \text{ with } a, b, c, d, e, \text{ and } f \text{ mutually prime,}$$

then $a_1a_2df = ceb$. When $a_1 \mid c$, $e \mid a_2df$, so that $e \notin \Theta$ and (e, f) is a unit.

Similarly, if $a_1 \mid e$, (c, d) is a unit. Hence in this case (a, b) is prime.

We have therefore proved

Theorem 3: If $a \in \Theta$, then (a, b), where a and b are mutually prime, is prime if and only if $a = a_1a_2$, where $a_1 \in \Theta$ is prime in R and $a_2 \notin \Theta$.

In addition to the above, we can prove the following version of the fundamental theorem of arithmetic, which connects primes in R with elements of R'.

Theorem 4: If a and b are unequal elements of R, then (a, b) can be expressed as

$$(u, 1) \cdot (p_1, 1) \cdot (p_2, 1) \ldots (p_k, 1) \cdot (1, q_1) \cdot (1, q_2) \ldots (1, q_m),$$

where $p_1, p_2, \ldots, p_k, q_1, q_2, \ldots, q_m$ are primes of R and u is a unit of R. This representation is unique except for the order of the factors. (In the case where a and b are units, $k = m = 0$.)

Proof: Let $(a, b) = (a_1, b_1)$ where a_1 and b_1 are mutually prime.

Any non-unit can be represented uniquely as a unit times a product of primes of R (see [2]). For a unit this holds as well, but the number of primes is zero. Thus

$$a_1 = u_1 p_1 p_2 \cdots p_k$$
$$b_1 = u_2 q_1 q_2 \cdots q_m,$$

where $p_1, p_2, \ldots, p_k, q_1, q_2, \ldots, q_m$ are primes and u_1 and u_2 are units.

Then

$$(a_1, b_1) = (u_1, u_2) \cdot (p_1, 1) \cdot (p_2, 1) \cdots (p_k, 1) \cdot (1, q_1) \cdot (1, q_2) \cdots (1, q_m).$$

If $u_2 v = 1$ and $u = u_1 v$, this becomes

$$(a, b) = (u, 1) \cdot (p_1, 1) \cdot (p_2, 1) \cdots (p_k, 1) \cdot (1, q_1) \cdot (1, q_2) \cdots (1, q_m).$$

We now state the new division algorithm.

Theorem 5: If R is a Euclidean$^+$ ring and $(a, b), (c, d) \neq (0, 1)$, then there is a $q \in R$ and $(r, s) \in R'$ such that

$$(a, b) = (q, 1) \cdot (c, d) + (r, s),$$

where $(r, s) < (c, d)$ or $(r, s) = (0, 1)$.

Proof: Since $bc \neq 0$ and $ad \neq 0$, there exist $q, r \in R$ such that

$$ad = qcb + r$$

with $r = 0$ or $g(r) < g(cb)$.

Thus

$$(a, b) = (qcb + r, bd) = (q, 1) \cdot (c, d) + (r, bd).$$

If $r = 0$, then $(r, bd) = (0, 1)$. If $r \neq 0$, then $g(r)g(d) < g(c)g(bd)$.

Letting $s = bd$, we have

$$(a, b) = (q, 1) \cdot (c, d) + (r, s)$$

where $(r, s) = (0, 1)$ or $(r, s) < (c, d)$.

We will show later that this algorithm allows us to find a greatest common divisor of (a, b) and (c, d) as defined below.

Definition 5: (e, f) is a g.c.d. of (a, b) and (c, d) if

$$(e, f) \mid (a, b), \quad (e, f) \mid (c, d), \text{ and } (i, j) \mid (a, b)$$

and

$$(i, j) \mid (c, d) \text{ implies } (i, j) \mid (e, f).$$

In R, if d_1 and d_2 are both g.c.d.s of a and b, then $g(d_1) = g(d_2)$. Similarly here, if (e_1, f_1) and (e_2, f_2) are g.c.d.s of (a, b) and (c, d), we have

$$g(e_1 f_2) = g(e_2 f_1).$$

The following theorem relates g.c.d.s in R with g.c.d.s in R'.

Theorem 6: If i is a g.c.d. of a and c and j is a g.c.d. of b and d, then (ij, bd) is a g.c.d. of (a, b) and (c, d).

Proof: We can assume without loss of generality that a and b and c and d are mutually prime.

Let i be a g.c.d. of a and c and j be a g.c.d. of b and d and $a = ia_1$ and $d = jd_1$, then

$$(ij, bd) \cdot (a_1 d_1, 1) = (ad, bd) = (a, b),$$

so

$$(ij, bd) \mid (a, b).$$

Similarly,

$$(ij, bd) \mid (c, d).$$

If $(r, s)|(a, b)$ and $(r, s)|(c, d)$, where again we assume that r and s are mutually prime, we have, for some $t, u \in R$,

$$trb = sa \quad \text{and} \quad urd = sc.$$

Thus $r|a$ and $r|c$ so $r|i$, and $b|s$ and $d|s$ so $bd|js$. Therefore,

$$rbd|ijs \quad \text{and} \quad (r, s)|(ij, bd).$$

Thus (ij, bd) is a g.c.d. of (a, b) and (c, d).

Corollary: If the only units of R are 1 and -1, then any two g.c.d.s of two elements of R' are equal or are additive inverses of each other.

Several other standard theorems on g.c.d.s and divisibility hold in R':

Theorem 7: If (e, f) and (e', f') are g.c.d.s of (a, b) and (c, d), where $e \notin \Theta$, then there is a unit u of R such that $(e, f) = (u, 1) \cdot (e', f')$.

Proof: Assuming that e and f and e' and f' are mutually prime, we have

$$(e, f)|(e', f') \quad \text{and} \quad (e', f')|(e, f).$$

Thus, for some $m, n \in R$, $ef' = me'f$ and $e'f = nef'$. Therefore,

$$ee'ff'(1 - mn) = 0.$$

Since $e \notin \Theta$, $e' \notin \Theta$, and m and n are units of R, the theorem holds.

Theorem 8: If (e, f) is a g.c.d. of (a, b) and (c, d), there exist $m, n \in R$ such that

$$(e, f) = (m, 1)(a, b) + (n, 1)(c, d).$$

Proof: In the notation of the proof of Theorem 6, (ij, bd) is a g.c.d. of (a, b) and (c, d), where i is a g.c.d. of a and c and j is a g.c.d. of b and d.

Then ij will be a g.c.d. of ad and bc. Hence, by a property for R, there are elements k and h of R such that

$$ij = kad + hbc.$$

Thus

$$(ij, bd) = (kad + hbc, bd) = (k, 1)(a, b) + (h, 1)(c, d).$$

If (e, f) is any g.c.d. of (a, b) and (c, d), then

$$\begin{aligned}(e, f) &= (t, 1)(ij, bd), \text{ for some } t \in R,\\ &= (m, 1)(a, b) + (n, 1)(c, d),\end{aligned}$$

where $m = tk$ and $n = th$.

Theorem 9: Any g.c.d. of $(a, b) \cdot (c, d)$ and $(a, b) \cdot (e, f)$ can be written as (a, b) times a g.c.d. of (c, d) and (e, f).

Proof: Any g.c.d. of $(a, b) \cdot (c, d)$ and $(a, b) \cdot (e, f)$ will, by Theorems 6 and 7, take the form $(ukh, bdbf)$, where k is a g.c.d. of ac and ae, h is a g.c.d. of bd and bf, and u is a unit.

Then $k = ai$ and $h = bj$, where i is a g.c.d. of c and e, and j is a g.c.d. of f and d. Thus

$$(ukh, bdbf) = (uabij, bdbf) = (a, b) \cdot (uij, df),$$

which is the form required by the theorem.

Theorem 10: If $(a, b) = (q, 1)(c, d) + (r, s)$, then any g.c.d. of (a, b) and (c, d) is a g.c.d. of (c, d) and (r, s).

Proof: Similar to that for R.

Theorem 10 and part of the proof of Theorem 5 give us a technique for finding the g.c.d.s of two elements of R' where R is Euclidean$^+$.

Given (a, b) and (c, d) in R', we have, by the proof of Theorem 5, $q, r \in R$ such that

$$(a, b) = (q, 1) \cdot (c, d) + (r, bd),$$

where $g(r) < g(bc)$ or $r = 0$.

Now if $r \neq 0$, as $cb \neq 0$, there are q_1 and r_1 in R such that

$$cb = q_1 r + r_1,$$

where $g(r_1) < g(r)$ or $r_1 = 0$.

Therefore,

$$cbd = q_1 rd + r_1 d$$

and so

$$(c, d) = (q_1, 1) \cdot (r, bd) + (r_1, bd),$$

where $g(r_1) < g(r)$ or $r_1 = 0$.

Again, if $r_1 \neq 0$, we can obtain $q_2, r_2 \in R$ such that

$$(r, bd) = (q_2, 1)(r_1, bd) + (r_2, bd),$$

where $g(r_2) < g(r_1)$ or $r_2 = 0$, etc.

As each $g(r_i)$ is a positive integer, this process terminates, and for some r_k we have

$$(r_{k-2}, bd) = (q_k, 1)(r_{k-1}, bd) + (r_k, bd)$$

and

$$(r_{k-1}, bd) = (q_{k+1}, 1)(r_k, bd).$$

Then (r_k, bd) and (r_{k-1}, bd) have (r_k, bd) as a g.c.d. and this, by repeated use of Theorem 9, can be seen to be a g.c.d. of (a, b) and (c, d).

If $a, b \notin \Theta$, the g.c.d. is, by Theorem 7, unique except for a factor $(u, 1)$, where u is a unit of R.

Using our unique representation of elements of R' given by Theorem 4 and writing all factors of the form $(p, 1)$ and $(1, q)$ for both (a, b) and (c, d), using zero exponents where necessary, it is clear that any g.c.d. of

$$(u, 1)(p_1, 1)^{i_1}(p_2, 1)^{i_2} \dots (p_e, 1)^{i_e}(p_{e+1}, 1)^{i_{e+1}} \dots (p_f, 1)^{i_f}(1, q_1)^{j_1}(1, q_2)^{j_2} \dots (1, q_m)^{j_m}(1, q_{m+1})^{j_{m+1}} \dots (1, q_g)^{j_g}$$

and

$$(v, 1)(p_1, 1)^{r_1}(p_2, 1)^{r_2} \dots (p_e, 1)^{r_e}(p_{e+1}, 1)^{r_{e+1}} \dots (p_f, 1)^{r_f}(1, q_1)^{s_1}(1, q_2)^{s_2} \dots (1, q_m)^{s_m}(1, q_{m+1})^{s_{m+1}} \dots (1, q_g)^{s_g},$$

where all powers are integers ≥ 0, is

$$(w, 1)(p_1, 1)^{t_1}(p_2, 1)^{t_2} \dots (p_f, 1)^{t_f}(1, q_1)^{n_1}(1, q_2)^{n_2} \dots (1, q_g)^{n_g},$$

where $t_k = \min(i_k, r_k)$ and $n_k = \max(j_k, s_k)$ and w is an arbitrary unit of R.

If a g.c.d. of (a, b) and (c, d) is $(1, 1)$, it follows that $(a, b) = (e, 1)$ and $(c, d) = (f, 1)$ for some $e, f \in R$ which are mutually prime.

The following definition extends the notion of mutually prime elements of R to R'.

Definition 6: If a and b as well as c and d are mutually prime and a and b are not both zero, then (a, b) and (c, d) are mutually prime if $(1, bd)$ is a g.c.d. of (a, b) and (c, d).

The special case where $b = d = 1$ conforms to the definition for R

The property:

> If $x \mid yz$ and x and y are mutually prime, then $x \mid z$, which holds in R for $y, z \notin \Theta$, fails in R'.

For example, if $R = Z$, $3 \mid 4 \cdot \frac{3}{4}$ in R' $(= Q)$ and 3 and 4 are mutually prime, but $3 \nmid \frac{3}{4}$.

The following seems to be the most general replacement for the above that we can prove.

Theorem 11: If $(a, b) \mid (c, d) \cdot (e, f)$, where (a, b) and (c, d) as well as f and c are mutually prime, then $(a, b) \mid (e, f)$.

Proof: Assume that a and b, c and d, f and c and e and f are mutually prime and that $(a, b) \mid (c, d) \cdot (e, f)$. Then $adf \mid bce$.

Now, if (a, b) and (c, d) are mutually prime, so are a and c. Therefore, $a \mid e$ and $f \mid b$, and hence $af \mid be$.

We define congruence in R' as follows.

Definition 7: $(a, b) \equiv (c, d) \mod (e, f)$, if $(e, f) \mid \{(a, b) - (c, d)\}$.

Alternatively, $(a, b) \equiv (c, d) \mod (e, f)$, if $bde \mid (adf - bcf)$. Congruence mod (e, f) is clearly an equivalence relation over R'.

The equivalence class of (c, d), mod (e, f), will consist of all elements of the form $(cf + dke, df)$, it will include elements of the form $(h, 1)$ only if $d \mid f$.

From our division algorithm,

$$(a, b) = (q, 1)(e, f) + (r, s),$$

it follows that (a, b) and the remainder (r, s) upon division by (e, f) are in the same equivalence class, mod (e, f). Also, all the elements in the equivalence class of $(a, b) \mod (e, f)$, will have common g.c.d.s with (a, b) and (e, f).

Each equivalence class, mod (e, f), can therefore be uniquely determined by a particular divisor (w, t) of (e, f); the elements of the class will all be of the form (kw, t).

If all remainders (r, s) obtained upon division by (e, f) in a particular R' are unique, the set of all such remainders can be said to form a set of least residues mod (e, f). If when such remainders are not unique they always form a "positive" and "negative" pair, the positive remainders can be said to be least positive residues mod (e, f).

The usual elementary theorems about residues can be summed up as follows.

Theorem 12: If $(a, b) \equiv (c, d) \mod (e, f)$, $(a', b') \equiv (c', d') \mod (e, f)$, ... and ϕ is any polynomial in several variables with integer coefficients, then

$$\phi((a, b), (a', b'), \ldots) \equiv \phi((c, d), (c', d'), \ldots) \mod (e, f).$$

The following cancellation theorem:

If d is a g.c.d. of e and c, $e \notin \Theta$, and $ae \equiv be \mod c$, then $a \equiv b \mod \frac{c}{d}$, which holds in R, fails in R'. For example, in Z', the set of rationals

$$2\tfrac{1}{3} \cdot 4 \equiv 2\tfrac{1}{3} \cdot \tfrac{6}{7} \mod 3\tfrac{2}{3},$$

but

$$4 \not\equiv \tfrac{6}{7} \mod 11.$$

We can prove the following more restricted generalization of the above theorem for R.

Theorem 13: If a and b, c and d, e and f and k and h are mutually prime pairs of elements of R, $k \notin \Theta$, m is a g.c.d of k and e, n a g.c.d. of f and h, $e = e_1 m$, $k = k_1 m$, and $f = f_1 n$, where k_1 is mutually prime to b and d, and if

$$(k, h) \cdot (a, b) \equiv (k, h) \cdot (c, d) \mod (e, f),$$

then

$$(a, b) \equiv (c, d) \mod (e_1, f_1).$$

Proof: If the conditions of the theorem hold, then

$$bhde \mid (ad - bc)kf.$$

Letting $h = h_1 n$, we have $m, n \notin \Theta$ and $bh_1 de_1 \mid (ad - bc)k_1 f_1$. Then, as $e_1 bd$ and k_1 are mutually prime and $k_1 \notin \Theta$,

$$bde_1 \mid (ad - bc)f_1$$

and so

$$(a, b) \equiv (c, d) \mod (e_1, f_1).$$

Under the conditions of the theorem, we can also obtain, from the proof:

$$(a, b) \equiv (c, d) \mod (eh, kf)$$

and

$$(a, b) \equiv (c, d) \mod (e_1 h_1, k_1 f_1).$$

We now consider the solution of the linear congruence

$$(a, b) \cdot (x, y) \equiv (c, d) \mod (e, f).$$

Clearly if $a \notin \Theta$, $(x, y) = (bc, ad) + (teb, fa)$ is a solution for every $t \in R$. It is therefore of more interest to find solutions with $y = 1$.

Conditions for the existence of such solutions are given in the next theorem.

Theorem 14: (i) If i is a g.c.d. of a and e and j is a g.c.d. of b and f and

(1) $$(a, b) \cdot (x, 1) \equiv (c, d) \mod (e, f),$$

has a solution, then $(ij, bf) \mid (c, d)$.

(ii) If $b = b_1 j$ and $e = e_1 i$, the solution is unique mod $b_1 e_1$.

Proof: (i) If (1) has a solution, (a, b), (c, d) and (e, f), by our earlier work on the division algorithm, clearly have a common g.c.d. Thus, if i and j are defined as in the theorem, $(ij, bf) \mid (c, d)$.

(ii) If we have a solution to (1), we also have a solution to

(2) $$dfax \equiv bcf \mod bed.$$

Let $a = a_1 i$, $e = e_1 i$, $b = b_1 j$, and $f = f_1 j$. Assume that a and b, e and f and c and d are mutually prime. Since (2) has a solution, $di \mid b_1 cf$ so that $i \mid c$ and $d \mid b_1 f$.

Let $c = c_1 i$ and $kd = b_1 f$, then (2) becomes

$$f_1 a_1 x \equiv kc_1 \mod b_1 e_1.$$

If also $f_1 a_1 x' \equiv kc_1 \mod b_1 e_1$, we have

$$f_1 a_1 (x - x') \equiv 0 \mod b_1 e_1.$$

Since $f_1 a_1$ and $b_1 e_1$ are mutually prime,

$$x \equiv x' \mod b_1 e_1.$$

Thus the solution x is unique mod $b_1 e_1$.

Corollary: If (k, h) is a g.c.d. of (a, b) and (e, f), then

$$(a, b) \cdot (x, 1) \equiv (c, d) \mod (e, f),$$

if and only if $(k, h) \mid (c, d)$.

Proof: By the fact that $(k, h) \mid (ij, bf)$ and $(ij, bf) \mid (k, h)$ in the notation of the above proof.

In the case where the ring R is Z, the set of integers, we can determine the total number of different solutions mod (e, f), or $\frac{e}{f}$.

This number of solutions will be the smallest positive integer n such that

$$(nb_1e_1, 1) \equiv 0 \mod (e, f),$$

i.e., such that $e \mid nb_1e_1f$.

Now, as we can assume that e and f and a and b are mutually prime, this reduces to $i \mid n$, so the smallest n is i.

Thus in the ring of integers, the number of noncongruent solutions mod (e, f) of (1) is i.

Take, as an example,

$$15\tfrac{5}{39}x \equiv \tfrac{5}{6} \mod 20\tfrac{5}{52}.$$

Clearly, g.c.d. $\left(15\frac{5}{39}, 20\frac{5}{52}\right) = \frac{5}{156} \left| \frac{5}{6}\right.$, and we can obtain $x = -89$ as a solution to

$$4(15.39 + 5)x \equiv 26.5 \mod (60.52 + 15).$$

Now b_1 comes to 3 and e_1 to 209, so the simplest noncongruent positive integer solutions, mod $20\frac{5}{52}$, are 194, 821, 1448, 2075, and 2702.

REFERENCES

1. N. H. McCoy. *Rings and Ideals.* The Mathematical Association of America, 1948.
2. E. H. Patterson & O. E. Rutherford. *Abstract Algebra.* Edinburgh: Oliver and Boyd, 1965.

*****

A RECURSION-TYPE FORMULA FOR SOME PARTITIONS

AMIN A. MUWAFI
The American University of Beirut, Beirut, Lebanon

If $p(n)$ denotes the number of unrestricted partitions of n, the following recurrence formula, known as Euler's identity, permits the computation of $p(n)$ if $p(k)$ is already known for $k < n$.

$$(1) \quad p(n) = p(n-1) + p(n-2) - p(n-5) - p(n-7) + p(n-12) + p(n-15) - - + + \cdots$$

$$= \sum_{j \neq 0} (-1)^{j+1} p\left(n - \frac{1}{2}(3j^2 + j)\right),$$

where the sum extends over all integers j, except $j = 0$, for which the arguments of the partition function are nonnegative.

Hickerson [1] gave a recursion-type formula for $q(n)$, the number of partitions of n into distinct parts, in terms of $p(k)$ for $k \leq n$, as follows,

$$(2) \quad q(n) = \sum_{j=-\infty}^{\infty} (-1)^j p(n - (3j^2 + j)),$$

where the sum extends over all integers j for which the arguments of the partition function are nonnegative.

Alder and Muwafi [2] gave a recursion-type formula for $p'(0, k - r, 2k + a; n)$, the number of partitions of n into parts $\not\equiv 0, \pm(k - r) \mod 2k + a$, where $0 \leq r \leq k - 1$.