# FUNCTIONS OF COPRIME DIVISORS OF INTEGERS

BY E. T. BELL

1. *Unique Decompositions.* If a set $U$ of distinct positive integers $1, u_1, u_2, \cdots$ is such that*

$$(1) \qquad (u_i, u_j) = 1, \qquad i \neq j, \qquad i, j = 1, 2, \cdots,$$

we call $U$ a *coprime set.* If to $U$ we adjoin all positive integral powers $u_1^{\alpha_1}, u_2^{\alpha_2}, \cdots, \alpha_1>0, \alpha_2>0, \cdots$ of integers in $U$, we get the *extended set* $E(U)$. If $m$ is in $E(U)$, we call $m$ a *U-integer.*

THEOREM 1. *If $n>1$ is representable as a product of powers of integers $>1$ in $U$, the representation is unique (up to permutations of the factors), say*

$$(2) \qquad n = u_1^{c_1} \cdots u_r^{c_r}, \qquad u_i > 1, \qquad c_i > 0, \qquad i = 1, \cdots, r.$$

For, by the definition of $U$, the $u_i$ in (2) are distinct, and by (1) a prime $p$ such that $p|n$ is such that $p|u_j$ for precisely one $j$, $0<j\leqq r$. We call (2) the *U-decomposition* of $n$.

Obviously there exist $U$'s such that some $n>1$ are not $U$-decomposable. From the fundamental theorem of arithmetic we have the following theorem:

THEOREM 2. *If $P\equiv p_1, p_2, \cdots$ is the set of all positive primes, the only $U$ such that every integer $n>1$ is $U$-decomposable is $U\equiv P$.*

We shall consider also another type of unique decomposition, valid for all $n>1$, which has the distinguishing property of $U$-decomposition as in (2), namely, *every $n>1$ is uniquely a product of powers of coprime integers $>1$.*

If the integer $s>0$ is divisible by the square of no prime, we call $s$ simple. Let $S\equiv 1, s_1, s_2, \cdots$ be the set of all distinct simple integers; $S$ includes $P$ and is not a coprime set. Without confusion we may denote by $E(S)$ the set obtained by adjoining to $S$ all positive integral powers $s_1^{\alpha_1}, s_2^{\alpha_2}, \cdots, \alpha_1>0, \alpha_2>0, \cdots$, of simple integers.

Let $n=p_1^{a_1} \cdots p_r^{a_r}$ be the $P$-decomposition of $n$. If $a_1, \cdots, a_r$ are all different, this is by definition also the *S-decomposition.* If

* In the customary notations, $(m, n)$ is the G.C.D. of $m, n$, and $m|n$ signifies that $m$ divides $n$ arithmetically.

$a_1, \cdots, a_r$ are not all different, let $\alpha_1, \cdots, \alpha_j$ be all the unequal integers among $a_1, \cdots, a_r$, and let $a_{i1}, \cdots, a_{iq_i}$ be all those of the $a_1, \cdots, a_r$ equal to $\alpha_i$. Writing $s_i \equiv p_{i1} \cdots p_{iq_i}$, we have $n = s_1^{\alpha_1} \cdots s_j^{\alpha_j}$, and this, the *S-decomposition of n*, is unique.

THEOREM 3. *Every integer $n > 1$ is uniquely a product of positive integer powers of coprime simple integers $> 1$; the unicity is attained when the exponents of the powers are required to be all different.*

Note that since $E(S)$ contains $E(P)$, every $n > 1$ has two decompositions, which coincide only if the exponents are all different, into a product of powers of coprime simple numbers, the $P$-decomposition and the $S$-decomposition as above defined, both of which are unique. Thus if $n = 2^2 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11^3$, this is the $P$-decomposition, while $n = (2 \cdot 3)^2 \cdot 7 \cdot (5 \cdot 11)^3$ is the $S$ decomposition, from the coprime simple integers $2 \cdot 3$, 7, $5 \cdot 11$, with the respective exponents 2, 1, 3, all different.

2. *U-divisors, S-divisors.* Referring to (2) we define the $(c_1+1) \cdots (c_r+1)$ integers

$$u_1^{k_1} \cdots u_r^{k_r}, \qquad 0 \leqq k_i \leqq c_i, \qquad i = 1, \cdots, r, \tag{3}$$

to be the *U-divisors* of the $n$ in (2). If $m$ is a $U$-divisor of $n$ we write $(m|n)_U$. Similarly, if

$$s = s_1^{a_1} \cdots s_t^{a_t}, \tag{4}$$

is the $S$-decomposition of $s$, the *S-divisors* of $s$ are the $(a_1+1) \cdots (a_t+1)$ integers

$$s_1^{j_1} \cdots s_t^{j_t}, \qquad 0 \leqq j_i \leqq a_i, \qquad i = 1, \cdots, t. \tag{5}$$

By an obvious change of notation everything defined next for $U$ is defined also for $S$, and we need state only the definitions for $U$.

If $(m|n)_U$, there is a unique $U$-divisor $t$ of $n$ such that $mt = n$; $m, t$ are *conjugate U-divisors* of $n$.

If $(d|m)_U$, $(d|n)_U$, $d$ is a *common U-divisor* of $m, n$. If $g$ is a common $U$-divisor of $m, n$ which is such that $(d|g)_U$ for every common $U$-divisor $d$ of $m, n$, then $g$ is unique, and we call $g \equiv (m, n)_U$ the *greatest common U-divisor* of $m, n$.

If $m$, $n$, $t$ are $U$-integers such that $m=nt$, and hence $(n|m)_U$, $(t|m)_U$, we call $m$ a *$U$-multiple* of $n$ (or of $t$). The $U$-integers $m$, $n$ determine a unique $U$-integer $l\equiv\{m, n\}_U$, the *least common $U$-multiple* of $m$, $n$, such that if $(m|e)_U$ and $(n|e)_U$, then $(l|e)_U$.

THEOREM 4. *If $m$, $n$ are $U$-integers,*

$$(m, n)_U\{m, n\}_U = mn.$$

This is proved as in $E(P)$. Let $u_a, \cdots, u_d$ be all the integers $u_\alpha, \cdots, u_\beta, u_\gamma, \cdots, u_\delta$ in $U$ occurring in the $U$-decompositions as in (2) of the $U$-integers $m$, $n$, $mn\neq 1$. Then we may write

$$m = u_\alpha^{\gamma_\alpha} \cdots u_\beta^{\gamma_\beta} = u_a^{h_a} \cdots u_d^{h_d},$$

$$n = u_\gamma^{t_\gamma} \cdots u_\delta^{t_\delta} = u_a^{k_a} \cdots u_d^{k_d},$$

in which some of the $h$, $k$ may be zero. Writing $\max(h_i, k_i)=g_i$, $\min(h_i, k_i)=l_i$, we have

$$(m, n)_U = u_a^{l_a} \cdots u_d^{l_d}, \qquad \{m, n\}_U = u_a^{g_a} \cdots u_d^{g_d},$$

and hence the theorem.

If $(m, n)_U=1$, then $m$, $n$ are called *$U$-coprime.*

In what follows, the particular $U$-divisors $u_1, \cdots, u_r$ of $n$ as in (2) play the part of the distinct primes dividing $n$ in the $P$-decomposition; $u_1, \cdots, u_r$ will be called the *primitive $U$-divisors* of $n$. By a previous remark, primitive $S$-divisors are therefore also defined.

3. *Functions of $U$-divisors.* By a change of notation, everything stated for $U$ holds for $P$, $S$, as in §2. The numerous functions depending on the $P$-decomposition of integers that occur in the theory of numbers,* together with all of their properties depending only on the fact that the $P$-decomposition is unique (into a product of powers of coprime integers), go over unchanged to the like for $U$-decompositions by a few obvious changes in notation and terminology. We take first the example that started the entire theory of such functions for $P$.

Let $n=p_1^{a_1}\cdots p_r^{a_r}$ be the $P$-decomposition of $n$. Then the number $\phi(n)$ of integers $<n$ and prime to $n$ is

$$\phi(n) = n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_r}\right), \qquad \phi(1)\equiv 1. \tag{6}$$

* See Dickson's *History of the Theory of Numbers*, vol. 1, 1919, chapters 5, 10, 19; also the writer's *Algebraic Arithmetic*, 1927.

The corresponding theorem for $U$ is as follows. Let $m = u_1^{c_1} \cdots u_t^{c_t}$ be the $U$-decomposition of $m$. Then the number $\phi_U(m)$ of integers $<m$ and not divisible by any one of the primitive $U$-divisors $u_1, \cdots, u_t$ of $m$ is

$$(7) \qquad \phi_U(m) = m\left(1 - \frac{1}{u_1}\right) \cdots \left(1 - \frac{1}{u_t}\right), \qquad \phi_U(1) \equiv 1.$$

The proof of (7) is precisely similar to that of (6) by means of the principle of cross-classification,* with the remark that $(a, b) = 1$, $a \mid k$, $b \mid k$ together imply $ab \mid k$. From the explicit form of $\phi(n)$ in (6), a common algebraic proof gives Gauss' result

$$(8) \qquad \sum \phi(d) = n, \qquad d \mid n.$$

Hence (7) implies

$$(9) \qquad \sum \phi_U(t) = m, \qquad (t \mid m)_U.$$

Generally, to pass from $P$ to $U$, $P \to U$, we have

$$(10) \qquad \begin{array}{ll} P & \to \quad U, \\ \text{“prime”} & \to \text{“primitive”}, \\ \text{“divisor”} & \to \text{“}U\text{-divisor”}, \\ (m, n) & \to (m, n)_U. \end{array}$$

If $f(x)$ is single-valued and finite for integer values $>0$ of $x$, $f(x)$ is (as usual) called a *numerical function of* $x$. The *unit numerical* function $\eta(x)$ is defined by $\eta(1) = 1$, $\eta(x) = 0$, $x \neq 1$. A generalization of Dedekind's inversion formula, proved in a previous paper,† is of great use in the algebra of numerical functions. If, and only if, $f(1) \neq 0$ there exists a unique numerical function $f'(x)$, such that

$$(11) \qquad \sum f(d) f'(\delta) = \eta(n), \qquad n = 1, 2, \cdots,$$

the sum referring to all pairs $d$, $\delta$ of conjugate $P$-divisors of $n$. Passing from $P$ to $U$ by means of (10), we get the theorem corresponding to (11) on making the single change $U$ for $P$ in the

* First stated as a general principle in arithmetic, apparently, by da Silva in 1854, Memorias da Academia Real das Sciencias de Lisboa, N.S.I., pp. 8–9; see Dickson, loc. cit., p. 119. A special form of the principle was noted in 1857 by H. J. S. Smith; see his *Collected Mathematical Papers*, vol. 1, p. 36.

† Tôhoku Mathematical Journal, vol. 17 (1920), pp. 221–231. Simplified proof, ibid., vol. 43 (1937), pp. 77–78.

foregoing statement. The proof may be given precisely as in the references cited. The generalization mentioned is as follows. If $f(x)$, $g(x)$, $h(x)$ are numerical functions such that

$$\sum f(d)g(\delta) = h(n), \qquad n = 1, 2, \cdots, \qquad g(1) \neq 0,$$
$$\sum g(d)g'(\delta) = \eta(n), \qquad n = 1, 2, \cdots,$$

then

$$f(n) = \sum g'(d)h(\delta), \qquad n = 1, 2, \cdots, \tag{12}$$

all sums referring to all pairs $d$, $\delta$ of conjugate $P$-divisors of $n$. If $g(n) \equiv u(n)$, $=1$ for $n=1, 2, \cdots$, $g'$ is Möbius' $\mu$, and (12) becomes Dedekind's inversion. To pass from (12) to its $U$-correspondent it suffices to replace $P$ by $U$ as for (11). The $U$-correspondent of Dedekind's inversion is obtained by replacing "conjugate $P$-divisors" by "conjugate $U$-divisors," and $\mu$ by $\mu_U$, where $\mu_U(n)$ is zero if $n$ is divisible by the square of any primitive $U$-integer, and otherwise is $+1$ or $-1$ according as $n$ is the product of an even or an odd number of primitive $U$-divisors of $n$; by convention $\mu_U(1)=1$. A similar convention holds for any $f_U(n)$ which is not otherwise defined when $n=1$, namely, $f_U(1)=1$.

In previous papers* the algebra of numerical functions based on $P$-decomposition was constructed from (11), (12). It follows that there is a simply isomorphic algebra for any $U$-decomposition. In the $P$-algebra it was noted that the theorems hold for any set in which there is a unique decomposition. Hence the like is true for $U$-decompositions in such a set, for example the ideals of an algebraic number field.

CALIFORNIA INSTITUTE OF TECHNOLOGY

---

* Some are listed in my paper, Journal of the Indian Mathematical Society, vol. 17 (1927–28), pp. 249–260.