Section 6.2 Divisibility among the integers

An integer $a \in \mathbb{Z}$ is *divisible* by $b \in \mathbb{Z}$ if there is an integer $c \in \mathbb{Z}$ such that $a = bc$. Note that 0 is divisible by any integer b, since $0 = b \cdot 0$. On the other hand, a is divisible by 0 only if $a = 0$: from $a = 0 \cdot c$ it follows that $a = 0$. The symbolic way of writing "a is divisible by b" is: $b \mid a$. Instead of "a is divisible by b" we also say that "b divides a", or that "b is a divisor of a", or "a is a multiple of b".

Note the obvious

Transitivity law for divisibility:

$$a \mid b \text{ and } b \mid c \implies a \mid c .$$

In case $b \neq 0$, a being divisible by b is the same as to say that $\frac{a}{b}$ is an integer; we cannot say this, however, if $b = 0$, since $\frac{a}{0}$ is meaningless. In particular, if $b \mid a$, then either $a=0$, or else $|b| \leq |a|$; in other words, for positive integers a and b such that $a<b$, $b \mid a$ is impossible (since then $0<\frac{a}{b}<1$, and $\frac{a}{b}$ cannot be an integer).

As far as divisibility is concerned, any integer a and its negative $-a$ behave in the same way: $b \mid a$ iff $b \mid -a$ iff $-b \mid a$. Therefore, e.g., when we want to account for all the divisors of an integer, we may restrict our search to the non-negative numbers. Always, $a \mid a$ and $a \mid -a$. Moreover, if both $a \mid a'$ and $a' \mid a$ hold, then either $a' = a$ or $a' = -a$.

In what follows, variables a, b, ... range over $\mathbb{Z}$, the set of all integers, unless otherwise stated.

Given any a and b such that $b > 0$, we may divide a by b with a remainder: we can find q and r such that

$$a = qb + r , \quad 0 \leq r < b . \tag{1}$$

E.g., with $a = 17$, $b = 5$, we have $q = 3$ and $r = 2$:

$17 = 3 \cdot 5 + 2, \quad 0 \le 2 < 5.$

In (1), q is the *quotient*, r is *remainder* when a is divided by b. The remainder being equal to 0 signifies, of course, that b divides a, $b \mid a$.

To prove the existence of the quotient/remainder representation, first let us assume that $a \ge 0$. The set X of all non-negative multiples of b that are less than or equal to a is nonempty ($0 \in X$), and bounded by a; thus, by the Greatest Number Principle (see the last section), it has a maximal element, say qb. Thus we have that $qb \in X$ but $(q+1)b \notin X$ (since $b \ne 0$, $qb < (q+1)b$). This means that $qb \le a < (q+1)b$. It follows that for $r = a - qb$, we have the relations in (1).

For the case when $a < 0$, we write $-a = qb + r$ by what we already know; from this, $a = (-q-1)b + (b-r)$ is the desired decomposition.

The *common divisors* of a and b are those integers that divide both a and b.

With any integers a and b, a(n *integer*) *linear combination* of a and b is any integer of the form $xa + yb$, with x and y also integers (although we usually say "linear combination" without the qualification "integer", we insist that the coefficients should also be integers!). Note that

any linear combination of linear combinations of a *and* b *is a linear combination of* a *and* b:

if $c = xa + yb$, $d = ua + vb$ and $e = sc + td$, then

$$e = s(xa + yb) + t(ua + vb) = (sx + tu)a + (sy + tv)b.$$

Also note that

any common divisor of a *and* b *is a divisor of any linear combination of* a *and* b :

if $c \mid a$, $c \mid b$, that is $a = uc$, $b = vc$, then

$$xa + yb = xuc + yvc = (xu + yv)c \ .$$

Now, if

$$a = qb + r \ , \qquad (2)$$

then a is a linear combination of b and r (since $a = qb + 1 \cdot r$) and also, since $r = a - qb = 1 \cdot a + (-q)b$, r is a linear combination of a and b . We may conclude that

under (2), *the common divisors of* a and b , *and the common divisors of* b and r *are the same*.

c is a *greatest common divisor* (gcd) of a and b if it is a common divisor of a and b , and a multiple of every common divisor of a and b at the same time; in other words,

$c \mid a$ and $c \mid b$

and

for all d such that $d \mid a$ and $d \mid b$, we have $d \mid c$.

Another way of putting the defining property of c is to say the common divisors of a and b are the same as the divisors of (the single) c : for any d ,

$d \mid a$ and $d \mid b \iff d \mid c$.

Note that it is not clear, at this point, that any pair of numbers a and b *has* a gcd; we will

prove this soon. However, one thing is pretty clear, namely that the gcd, if it exists, is essentially unique: if both c and c' are gcd's of a and b, then $c = c'$ or $c = -c'$; the reason is that, from the definition it follows that both $c \mid c'$ and $c' \mid c$ hold. To make the gcd completely unique, we agree that $\gcd(a, b)$ should denote the non-negative one of the two possible values.

A remark on the name "greatest common divisor". Assume that both a and b are positive (the only "interesting" case for $\gcd(a, b)$). Then $c=\gcd(a, b)$ is certainly the *greatest one* among the common divisors of a and b, since it is positive, and it divides all of them. One might then say that it is *obvious* that there is a *greatest one* among these common divisors, as there is always a *greatest one* among finitely many integers. However, if we denote this greatest of the common divisors by c, it is not clear that for every common divisor d of a and b we have $d \mid c$ as required in the definition of "gcd"; we only have that $d \leq c$, which, of course, is not enough for $d \mid c$. It is important to realize that the definition of "greatest common divisor" imposes a *stronger* condition than it appears from the wording of the concept.

These remarks explain why, to prove the existence of the gcd, we have to go through the considerably more sophisticated argument than just saying "take the largest of the common divisors". The argument that follows is not only one of the most important ones in all of mathematics, but it is also one of earliest ones: it appears in Euclid's "Elements", the classic ancient Greek treatise on mathematics.

Note that if $b \mid a$, then $\gcd(a, b) = |b|$; hence, $\gcd(0, b) = |b|$.

For the proof of the existence of the gcd, the first remark is that

$$\textit{if } a = qb + r \textit{, then } \gcd(a, b) = \gcd(b, r), \tag{3}$$

meaning that if one gcd exists, so does the other, and they are equal. The reason is that, in this case, the common divisors of the pair (a, b) and those of (b, r) are the same, as we noted above.

Let a and b be arbitrarily given integers; we want to compute $\gcd(a, b)$. We may

assume that $b > 0$; if $b = 0$, then $\gcd(a, 0) = |a|$ as said above, and if $b < 0$, we may pass to $-b$: $\gcd(a, b) = \gcd(a, -b)$. Now, assuming $b>0$, we can define, by recursion, the sequence

$$a_0, a_1, a_2, \quad , a_n, a_{n+1} \tag{3'}$$

by

$$a_0 \underset{\text{def}}{=} a$$

$$a_1 \underset{\text{def}}{=} b$$

and for any $i \geq 0$, if we have already defined a_i and a_{i+1},

and if a_{i+1} *is greater than* 0, (3")

a_{i+2} is defined as the remainder of a_i divided by a_{i+1}. In other words, the relations

$$a_i = q_i \cdot a_{i+1} + a_{i+2}, \quad 0 \leq a_{i+2} < a_{i+1} \tag{4}$$

hold with suitable q_i. When $a_{i+1} = 0$, we stop, that is, we do not define a_{i+2}, and we put $n = i$; thus, the sequence (3') will have been defined. Since the a_i's are strictly decreasing after $i = 1$ (see the second relation in (4)), by the "principle of the impossibility of infinite descent" (see the last section), we must reach a stage $i+1$ when a_{i+2} is no longer defined, that is, the condition (3") fails, that is, $a_{i+1} = 0$. Denote this i by n. Therefore, since $a_{n+1}=0$, we have by (4), for $i=n-1$, that

$$a_{n-1} = q_{n-1} \cdot a_n \ . \tag{5}$$

Now, since a_n is a divisor of a_{n-1}, $\gcd(a_{n-1}, a_n) = a_n$. The first relation in (4) tells us that

$$\gcd(a_i, a_{i+1}) = \gcd(a_{i+1}, a_{i+2}) \qquad (i+2 \leq n)$$

(see (3)). Thus, we have that

$$\gcd(a, b) = \gcd(a_0, a_1) = \gcd(a_1, a_2) = \ldots = \gcd(a_{n-1}, a_n) = a_n .$$

We have shown that $\gcd(a, b)$ exists, and in fact, have shown how to compute it. We can summarize the procedure this way: we construct the sequence the first two terms of which are the given numbers, and in which every term is the remainder when the previous term divides the term preceding it. The construction terminates when 0 is reached; the term previous to the zero term is the desired gcd.

E.g., let $a = 3293$, $b = 4107$. Then

$$3293 = 0 \times 4107 + 3293 ,$$

$$4107 = 1 \times 3293 + 814 ,$$

$$3293 = 4 \times 814 + 37 ,$$

$$814 = 22 \times 37 .$$

That is, in this case, $n = 3$, $a_2 = 814$ and $a_3 = 37$, and $\gcd(3293, 4107) = 37$.

The procedure described is called the *Euclidean algorithm*. It was known to the ancient Greeks; it appears in Euclid's "Elements". An important fact about it is that it is an *efficient* algorithm; for relatively large numbers, it terminates quite fast.

Besides a way of computing the gcd, the Euclidean algorithm also gives us an important theoretical conclusion:

the gcd *of any two numbers* a *and* b *is a linear combination of* a *and* b.

To see this, we prove by induction on $i \le n$ that a_i is a linear combination of a and b. For $i = 0$ and $i = 1$, this is certainly true: $a = 1 \cdot a + 0 \cdot b$ and $b = 0 \cdot a + 1 \cdot b$.

Assuming the result for all indices less than $i+2$, we have that

$$a_{i+2} = a_i - q_i a_{i+1} \qquad (6)$$

that is, a_{i+2} is a linear combination of a_i and a_{i+1}. Since, by the induction hypothesis, a_i and a_{i+1} are linear combinations of a and b, it follows that a_{i+2} is a linear combination of a and b as desired.

In the example,

$$37 = 3293 - 4\times 814,$$

$$814 = 4107 - 1\times 3293,$$

hence,

$$\gcd(4107, 3293) = 37 = 3293 - 4\times(4107 - 1\times 3293) = (-4)\times 4107 + 5\times 3293.$$

A *prime number* is any integer p which is not a unit, that is, not 1 or -1, but which is not divisible by any number other than 1, -1, p and $-p$. Clearly, p is prime iff $-p$ is prime; therefore, it is customary to restrict attention to positive primes; in what follows, by "prime number" we always mean a positive prime. Restated, p is prime if $p > 1$, and the only positive divisors of p are 1 and p.

A fundamental property of primes is this:

if p is a prime, and $p \mid ab$, then either $p \mid a$, or $p \mid b$ (or both).

Indeed, assume also that p does not divide a, to show that $p \mid b$. Then $\gcd(p, a) = 1$, since $\gcd(p, a)$ is a divisor of p, therefore it cannot be anything else but 1 or p, and it cannot be p, since then p would divide a. Since $\gcd(p, a)$ is a linear combination of p and a,

$$1 = xp + ya$$

for suitable integers x and y. Multiplying this equality with b, we get

$$b = xbp + yab\ .$$

Since, by assumption, ab is divisible by p, $ab = zp$ for a suitable z, we have

$$b = (xb + yz)p\ ,$$

that is, b is divisible by p, which is what we wanted to show.

An obvious generalization of the last fact is this:

if p *is a prime, and* $p \mid \prod_{i<k} a_i$, *then* $p \mid a_i$ *for at least one* $i < k$.

We **claim**:

Every non-zero, non-unit integer has at least one prime divisor.

Let a be any integer, $a \neq 1$, $a \neq -1$. We may assume that $a > 1$. The set X of all divisors of a that are greater than 1 is a non-empty set; a itself is an element of it. By the LNP, let p be the least element of X. p must be prime; otherwise, there would be a divisor x of p which is greater than 1 but less than p; x would be a non-unit divisor of a smaller than p, contrary to the choice of p. This proves the **claim**.

There are many prime numbers; in fact, there are *infinitely* many:

for any $n \in \mathbb{N}$, *there is a prime number greater than* n.

Indeed, consider the number $n! + 1$, and let p be a prime divisor of this number. p cannot be $\leq n$, since then p would be a divisor of $n!$, and hence also a divisor of $(n! + 1) - n! = 1$, which is absurd since p is not a unit. p is a prime number greater than n.

Next, we see that

Every non-zero number is the product of prime numbers.

Let n be any positive integer. If $n = 1$, n is the empty product of prime numbers. We treat the general case by induction, more precisely, by the WOP. Let $n > 1$. We know that n has at least one prime divisor; let p one such; let $m = \frac{n}{p}$. Since $m < n$, we may apply the induction hypothesis, and have that m is the product of prime numbers, $m = \prod_{i<k} p_i$. But then, $n = m \cdot p$, and $n = (\prod_{i<k} p_i) \cdot p$, and n is also a product of primes.

Let us use the notation p_i for the $i+1^{st}$ prime; see the end of the last section. With the fixed meaning of the p_i, we may write every positive n in the form

$$n = \prod_{i<k} p_i^{\alpha_i} \qquad (7)$$

with suitable natural exponents α_i. Indeed, we know that n is the product of a certain number of prime factors; by bringing together the equal factors into powers, and using the exponent 0 in case a specific p_i does not occur in the product, we get the form mentioned. E.g.,

$$2420 = 20 \times 121 = 2^2 \times 5 \times 11^2 = 2^2 \times 3^0 \times 5^1 \times 7^0 \times 11^2 ;$$

now, we can take $k = 5$.

Note that, in (7), k is not unique: it can be taken any number greater than the last i for which $\alpha_i \neq 0$; for all j , $i<j<k$, we can then take $\alpha_j = 0$. This is useful, since when we have two (or more) numbers as n , we can choose the k for the two to be the same.

We have:

Prime factorization is unique:

$$\text{if } n = \prod_{i<k} p_i^{\alpha_i} = \prod_{i<k} p_i^{\beta_i}, \tag{8}$$

then $\alpha_i = \beta_i$ *for all* $i < k$.

The proof is by induction on n (via the WOP). If $n = 1$, it is clear that $\alpha_i = \beta_i = 0$ for all $i < k$. Otherwise, for some $i < k$, say i_0 , we have that $\alpha_{i_0} \geq 1$; let $p = p_{i_0}$. p divides $n = \prod_{i<k} p_i^{\beta_i}$, and since p is prime, p divides at least one $p_i^{\beta_i}$. But if $i \neq i_0$, p does not divide $p_i^{\beta_0}$ (why?). Thus, p must divide $p_{i_0}^{\beta_{i_0}}$, which implies that $\beta_{i_0} \geq 1$. Now, dividing (8) by the factor p_{i_0} , we get

$$m \underset{\text{def}}{=} \prod_{i<k} p_i^{\alpha'_i} = \prod_{i<k} p_i^{\beta'_i}$$

where $\alpha'_i = \alpha_i$ for $i \neq i_0$, $\alpha'_{i_0} = \alpha_{i_0} - 1$, and similarly for the β'_i . Clearly, $m < n$. By the induction hypothesis, prime factorization for m is unique; hence, $\alpha'_i = \beta'_i$ for all $i < k$. This means that $\alpha_i = \beta_i$ for all $i \neq i_0$, and $\alpha_{i_0} = \alpha'_{i_0} + 1 = \beta'_{i_0} + 1 = \beta_{i_0}$, that is, $\alpha_i = \beta_i$ for all $i < k$, as desired.

In terms of prime factorization, divisibility may be characterized as follows:

$$\textit{if } n = \prod_{i<k} p_i^{\alpha_i},\ m = \prod_{i<k} p_i^{\beta_i}, \textit{ then } n \mid m \textit{ iff } \alpha_i \le \beta_i \textit{ for all } i < k .$$

The reason is simple: if $n \mid m$, then $m = n \cdot \ell$ for some ℓ; hence, if $\ell = \prod_{i<k} p_i^{\gamma_i}$ (with possibly a greater k; extend the range of the α's and β's by inserting 0's), we have that

$$m = \prod_{i<k} p_i^{\alpha_i} \cdot \prod_{i<k} p_i^{\gamma_i} = \prod_{i<k} p_i^{\alpha_i+\gamma_i} .$$

By the uniqueness of prime factorization, $\beta_i = \alpha_i+\gamma_i$; and since each $\gamma_i \ge 0$, we get that $\beta_i \ge \alpha_i$ as claimed.