NZM Number Theory 1

Michael Lee

1 Divisibility

Definition An integer b is divisble by an integer a, not zero, if there is an integer x such that $b = ax$, and we write $a \mid b$. In case b is not divisible by a, we write $a \nmid b$.

Theorem 1.1 *Some implications of divisibility.*
(1) $a \mid b$ implies $a \mid bc$ for any integer c.
(2) $a \mid b$ and $b \mid c$ imply $a \mid c$.
(3) $a \mid b$ and $a \mid c$ imply $a \mid (bx + cy)$ for any integers x, y.
(4) $a \mid b$ and $b \mid a$ imply $a = \pm b$;
(5) if $m \neq 0$, $a \mid b$ implies and is implied by $ma \mid mb$.

Theorem 1.2 *The division algorithm. Given any integers a and b, with $a<0$, there exist unique integers q and r such that $b = qa + r$, $0 \leq r<a$. If $a \nmid b$, then r satisfies the strnger inequalities $0<r<a$.*

Proof Consider the sequence of numbers $\cap_{i=0}^{n} b - ia$. In this sequence, select the smallest non-negative member and denote it by r. Thus by definition, r satisfies the inequalities of the theorem. But r belonging in the sequence, is of the form $b - qi$, and therefore q is defined in terms of r.
To prove the uniqueness of (q, r), suppose there is another pair (q_1, r_1) satisfying the same conditions. Proof by contradiction then follows, we presume that $r<r_1$ such that $0<r_1 - r<i$, then by substiution $r_1 - r = i(q - q_1)$ and therefore $i \mid (r_1 - r)$, which contradicts implication (5) of divisibility.

Definition The integer a is a common divisor of b and c in case $a \mid b$ and $a \mid c$. Since there is only a finite number of divisors of any nonzero integer, there is only a finite number of common divisors of b and c, except in the case $b = c = 0$. If at least one of b and c is not 0, the greatest among their common divisors is called the greatest common divisor of b and c and is denoted by (b, c). Similarly we denote the greatest common divisor g of the integers $b_1, b_2, \ldots, b_n$, not zero, by $(b_1, b_2, \ldots, b_n)$.

Theorem 1.3 *If g is the greatest common divisor of b and c, then there exist integers x_0 and y_0 such that $g = (b, c) = bx_0 + cy_0$.*

Theorem 1.4 *The greatest common divisor g of b and c can be characterized in the following two ways: (1) it is the least positive value of $bx + cy$ where x and y range over all integers; (@) it is the positive common divisor of b and c which is divisible by every common divisor.*

Theorem 1.5 *Given any integers $b_1, b_2, \ldots, b_n$ not all zero, with greatest common divisor g, thjere exist in integers $x_1, x_2, \ldots, x_n$ such that $g = (b_1, b_2, \ldots, b_n) = \sum_{j=1}^{n} b_j x_j$ Furthermore, g is the least positive value of the linear form $\sum j = 1^n b_j y_j$ where the y_j range over all integers; also g is the positive common divisor of $b_1, b_2, \ldots, b_n$ which is divisible by every common divisor.*

Theorem 1.6 *For any positive integer m, $(ma, mb) = m(a, b)$.*

Theorem 1.7 *If $d \mid a$ and $d \mid b$ and d>0, then $(\frac{a}{d}, \frac{b}{d}) = \frac{(a,b)}{d}$.*
If $(a, b) = g$, then $(\frac{a}{g}, \frac{b}{g}) = 1$.

Theorem 1.8 *If $(a, m) = (b, m) = 1$, then $(ab, m) = 1$.*

Definition We say that a and b are relatively prime in case $(a, b) = 1$, and that $a_1, a_2, \ldots, a_n$ are relatively prime in case $(a_1, a_2, \ldots, a_n) = 1$. We say that $a_1, a_2, \ldots, a_n$ are relatively prime in pairs in case $(a_i, a_j) = 1$ for all $i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, n$ with $i \neq j$.

Theorem 1.9 *For any x, $(a, b) = (b, a) = (a, -b) = (a, b + ax)$.*

Theorem 1.10 *If $c \mid ab$ and $(b, c) = 1$, then $c \mid a$.*

Theorem 1.11 *The Euclidean Algorithm. Given integers b and c>0, we make a repeated application of the division alogirthm to obtain a series of equations.*

$$
\begin{gathered}
b = cq_1 + r1,\ 0<r_1<c, \\
c = r_1 q_2 + r_2,\ 0<r_2<r_1, \\
r_1 = r_2 q_3 + r_3,\ 0<r_3<r_2, \\
\cdots \\
r_{j-2} = r_{j-1} q_j + r_j,\ 0<r_j<r_{j-1},
\end{gathered}
$$

$r_{j-1} = r_j q_{j+1}$
The greatest common divisor (b, c) of b and c is r_j, the last nonzero remainder in the division process. Values of x_0 and y_0 in $(b, c) = bx_0 + cy_0$ can be obtained by eliminating $r_{j-1}, \ldots, r_2, r_1$ from the set of equations.

Definition The integers $a_1, a_2, \ldots, a_n$, all different from zero, have a common multiple b if $a_i \mid b$ for $i = 1, 2, \ldots, n$. The ;least of the positive common multiplies is called the least common multiple, and it is denoted by $[a_1, a_2, \ldots, a_n]$.

Theorem 1.12 *If b is any common multiple of $a_1, a_2, \ldots, a_n$, then $[a_1, a_2, \ldots, a_n] \mid b$. This is the same as saying that if h dnotes the least common multiple, then $0, \pm h, \pm 2h, \pm 3h, \ldots compriseallth$*

Theorem 1.13 *If* $m>0$*,* $[ma, mb] = m[a, b]$*. Also* $[a, b]\dot{(}a, b) = | ab |$*.*

Proof Let $H = [ma, mb]$, and $h = [a, b]$. Then mh is a multiple of ma and mb, such that $mh \geq H$. Also H is a multiple of both ma and mb, and so $\frac{H}{m}$ is a multiple of a and b. Therefore $\frac{H}{m} \geq h$, from which it follows that $mh = H$, and this establishes the first part of the theorem.
The second part of the theorem states that the product between the least common multiple and the greater common divisor between two numbers a and b, is the product of the two numbers themselves. Let g be (a, b), therefore $(\frac{a}{g}, \frac{b}{g}) = 1$ Now by substitution, $[\frac{a}{g}, \frac{b}{g}](\frac{a}{g}, \frac{b}{g}) = \frac{a}{g}, \frac{b}{g}$, multiplying by g^2, $[a, b](a, b) = | a\dot{b} |$.

Assignment NZM 1.2: 1, 2, 3, 4, 8, 9, 13, 14, 15, 21, 22, 23, 28, 29

2 Prime Numbers

Definition An integer $p>1$ is called a prime number, or a prime, in case there is no divisor d of p satisfying $1<d<p$. If an intger $a>1$ is not a prime, it is called a composite number.

Theorem 2.1 *Every integer* n *greater than* 1 *can be expressed as a product of primes (with perhaps only one factor).*

Proof If the integer n is prime, then let the theorem stand. Otherwise n can be factored into n_1n_2 where they are between 1 and n. If n_1 is prime, let the theorem stand, otherwise it will factor into n_3n_4. This series of reductions must terminate because the factors are smaller than the composite number itself , and yet each factor is an integer greater than 1. Thus we can write n as a product of primes, and since the prime factors are not necessarily distinct, n can be written thus

$$n = p_1^a p_2^b p_3^c \dots$$

Theorem 2.2 *If* $p \mid ab$*,* p *being a prime, then* $p \mid a$ *or* $p \mid b$*. More generally, if* $p \mid a_1a_2a_3 \dots a_n$*, then* p *divides at least one factor* a_i *of the product.*

Proof If $p \nmid a$, then $(a, p) = 1$, then $p \nmid b$ by theorem 1.10. Proof by induction then follows for any number n factors of the product. An alternative method of contradiction can be used: assume $p \mid ab$ and $p \nmid a$ and $p \nmid b$.

$$ab = pt$$
$$a = ps + u \text{ and } b = pv + w$$
$$ab = (ps + u)(pv + w) = pt)$$
$$p^2sv + psw + pvu + uw = pt$$
$$p(psv + sw + vu) + uw = pt$$
$$uw = p(t - (psv + sw + vu))$$

$uw/p = (t - (psv + sw + vu))$ uw/p must be an integer but p can divide neither u nor w therefore the statement is false and the theorem is proved true by contradiction.

Theorem 2.3 *The fundamental theorem of arithmetic, or the unique factorization theorem. The factoring of any integer $n>1$ into primes is unique apart from the order of the prime factors.*

Theorem 2.4 *The number of primes is infinite.*

Proof Suppose there are a finite number of primes. Then the number n is 1 greater than the product of the set of finite primes. n can not be divisible by any of the preexisting primes, and thereore, any prime divisor p of n can not be in the pre-existing set of primes, therefore by induction, there are an infinite amount of distinct primes.

Theorem 2.5 *There are arbitarily large gaps in the series of primes.*

Theorem 2.6 *The product of any k consecutive integers is divisible by $k!$.*

Assignment NZM 1.3: 4, 7, 10, 22, 42