Theory of Numbers

August 2022

1 Section 1

1.1 The Notion of Divisibility

As the name suggests, divisibility is certainly related to the idea of division. It may seem stupendously simple, but bear with me when I ask you to consider the problem of dividing 6 apples between 3 people, such that everyone gets the same number of apples. Of course, we know each person will get 2 apples. Why? Because we can write $6 = 2 + 2 + 2 = 3 \times 2$. But now, if I ask the same question - but with 5 apples instead of 6, the problem becomes slightly nontrivial. We would like to make some meaningful comments even in such a situation. Let us start with the simpler thing.

1.2 Divisibility and Tests

Given integers a, b, we say a is *divisible* by b (alternatively say b *divides* a) if there exists an integer c such that $a = b \cdot c$. If a is divisible by b, we denote this by the notation $b \mid a$.

A few important things to take away from the above definition, particularly stressing on the differences between division and divisibility:

1. Division by zero is almost meaningless as $0|a$ implies $a = 0$. Hence, we would usually assume $b \neq 0$ when we speak about $b|a$.

2. Even though nothing is ascertained about uniqueness of c, observe that if $b \neq 0$, then $a = bc = bc'$, then $b(c - c') = 0$. As $b \neq 0$, we get $c = c'$ by cancellation. However, one may define divisibility in a much more generic setup even when division or cancellation fails. See the later sections.

3. Every integer divides zero and is divisible by ± 1.

4. Further, if $n \neq 0$, then n and $-n$ divide n. In fact, $n|kn$ for each $k \in$ (kind of a converse).

5. If $a, b \neq 0$, observe that $a|b$ and $b|a$ implies $a = b$ or $a = -b$. So if they are assumed to be natural numbers, then $a|b$ and $b|a$ implies $a = b$.

6. In general, if $a, b \in$ and $a|b$, then $a \leq b$.

7. Let $a, b, c \neq 0$. The $a|b$ or $a|c$ implies $a|bc$. Further, $a|b$ and $b|c$ implies $a|c$. (Show that neither of their converses hold.)

8. Now suppose $a|b$ and $a|c$, then clearly $a|b + c$.

9. Similarly, $a|b$ and $c|d$ implies $ac|bd$.

In a lot of branches of mathematics, it is highly useful and relevant to consider and look at real world variants and applications of a certain concept or result. And in case of divisibility, we have some *divisibility rules* for some special integers. Of course, you're free to consider/create such rules for absurdly large numbers, but after a point divisibility tests lose it's practicality. Given an integer a written in it's decimal representation, we have the following tests for divisibility by n.

Number(s)	Test
$n = 2, 5$	Units digit is divisible by n
$n = 3, 9$	Sum of digits is divisible by n
$n = 4, 25$	If $a = \cdots xy$ in decimal, then $n\|10x + y$.
$n = 6$	Divisible by 2 and 3.
$n = 11$	Alternating sum of digits is divisible by n.
$n = 10$	Last digit is 0.

You will be able to prove these easily either by induction or by methods discussed in succeeding sections. (Also, try to find an easy divisibility test by 7.)

As a consequence of the notion of divisibility, we get a few new objects and definitions to work with.

An integer not equal to $0, 1, -1$ is said to be a *reducible* number, if it has a **positive** divisor other than 1 and its modulus. And if a number is not reducible, then we say it's an *irreducible* number.

Let us look at a few examples.

1. n is irreducible if and only if $-n$ is irreducible.

2. 2 is irreducible. Indeed $a|2$, $a > 0$ implies $a \leq 2$, so $a = 1$ or $a = 2$, as desired. In fact, 2 is the only irreducible positive even number.

3. 3 is also irreducible. To see this, observe that $a|3$, $a > 0$ implies $a = 1, 2, 3$. But $2 \nmid 3$. Hence, $a = 1$ or $a = 3$. Rest follows.

We will return to irreducible numbers in the following section.

1.3 Euclid's Division Lemma

Our previously mentioned example still deserves an explanation. It is true, that we cannot divide 5 by 2, but at the same time it is also true, that we can write $5 = 2 \times 2 + 1$, i.e. we can decompose (in a manner of speaking) the number 5 into a multiple of 2, plus another positive integer less than 2. That observation leads us to our first (relatively) nontrivial result, which we shall state and prove below.

Euclid's Division Lemma: Given natural numbers a, b, there are unique integers q, r with $0 \leq r < b$ such that $a = bq + r$. Further, $b|a$ if and only if $r = 0$.

Proof. The proof is a simple application of the well-ordering principle. Let $S = \{k \in : kb > a\}$. Then, by the Archimedean Property of , S is clearly non-empty. Hence, there is a least element, say k' in S.

Define $q = k' - 1$ and $r = a - qb$. Then $qb \leq a < k'b = qb + b$. So $0 \leq r = a - qb < b$. Hence, we get $a = bq + r$ with the desired properties.

As for uniqueness, say $a = bq' + r'$ for $r', q' \in$ with $0 \leq r < r'$, then $b(q - q') = (r' - r)$. Now $0 \leq r, r' < b$, so $-b < r' - r < b$. But $b|r' - r$. Hence, we get $r' - r = 0$, so $r = r'$. This implies $b(q - q') = 0$. But $b \neq 0$, Hence $q = q'$, as desired. The final claim is trivial by uniqueness. □

This is an extremely important result and some problems involving this would be discussed soon. As an exercise, try to generalise this lemma, under certain meaningful assumptions, to the whole of integers. This will be very useful and will be mentioned in the exercises.

Show that for every positive integer n, $n^3 + 5n + 3$ is odd and divisible by 3

Proof. One way to prove this is our simple inductive policy. But we give a much more direct proof. using Euclid's lemma. Firstly, n is either odd or even. That is, in terms of Euclid's lemma, either $n = 2k$ for some integer k or $n = 2k + 1$ for some k. In the first case $n^3 + 5n + 3 = 2(4k^3 + 5k + 2) + 1$ is odd. Likewise do the second case.

Now for divisibility by 3, by our division lemma there are $q, r \in, 0 \leq r < 3$ such that $n = 3q + r$. Then $f(n) = n^3 + 5n + 3 = 3(9q^3 + 9q^2r + 3qr^2 + 5q + 1) + (r^3 + 5r)$. So $3|f(n)$ if and only if $3|r^3 + 5r$. But for each $r = 0, 1, 2$, this division happens... voila!!! □

1.4 GCD and LCM

Let us now study what can be termed as the "maximal" divisor of a pair of numbers.

Given two integers a and b (not both zero), we say an integer c is a *common divisor* of both a, b if $c \mid a$ as well as $c \mid b$. We say a positive integer d is a *greatest common divisor* (a.k.a GCD) of a, b if given any common divisor c of a, b, then c also divides d. Two integers are said to be *coprime*, or *relatively prime*, if their GCD is 1. We denote the GCD of a, b by the symbol $\gcd(a, b)$ or simply (a, b).

Dually, one may define the notion of a minimal number divisible by our pair.

Given two nonzero integers a and b, we say an integer m is a *common multiple* of both a, b if $a \mid m$ as well as $b \mid m$. We say a positive integer l is a *least common multiple* (a.k.a LCM) of a, b if given any common multiple m of a, b, then l divides m. We denote the LCM of a, b by the symbol $\text{lcm}(a, b)$ or simply $[a, b]$.

All fine so far? Well I certainly hope so, because you *may* get bombarded with even more definitions and results soon enough. Nevertheless, here are some observations.

1. We didn't say the GCD is actually unique! That's because in general (yes, there exists a general notion of GCD - but that's beyond the scope this text), GCD of two elements need not be unique. Luckily, we don't have to go through all that confusion right now. As long as we're inside $\mathbb{Z}$, everything is good and fine. The GCD of two integers is unique, and is actually the *greatest* of all the common divisors, even in our usual ordering. Dually, the LCM is also unique and the smallest positive number divisible by both numbers in hand.

2. Let $a, b \neq 0$. Then suppose $g = (a, b)$. Clearly $g > 0$ and there exist $c, d \neq 0$ such that $a = gc, b = gd$. Now look at $l = |gcd|$. Though it spells our GCD, l is actually a common multiple. What might interest you is that l is indeed the LCM! Using this, one may show that $|ab| = (a, b)[a, b]$.

3. Observe that $(a, b) = (b, a)$ and $[a, b] = [b, a]$. Also, the GCD and LCM, when treated as a binary operation on , is associative (verify).

4. Given any two integers (not both zero) a, b, if $d = (a, b)$, and if $a' = \frac{a}{d}, b' = \frac{b}{d}$, then $(a', b') = 1$. More generally if $d > 0$, then $d|a$, $d|b$ implies $d|(a, b)$ and $(a/d, b/d) = (g/d)$.

5. Similarly, $(ca, cb) = c \cdot (a, b)$.

6. If $(a, b) = 1$, then $(a, cb) = (a, c)$. Further, $(c, ab) = (c, a) \cdot (c, b)$. Will these hold if $(a, b) \neq 1$?

7. If x is an irreducible integer, then $(x, y) = 1$ or $|x|$, for any integer y. The latter holds if and only if $x|y$. Can you establish a meaningful converse?

8. One may define GCD of an arbitrary subset S of consisting of non-zero integers as $d > 0$ such that $d|s$ for each $s \in S$ and $c|s$ for each $s \in S$ implies $c|d$. Try to prove similar properties and define an analogous LCM.

Using these, try to find similar properties for LCM. We now state an important method to find the GCD.

The Division Algorithm: By using the Division Lemma, it is possible to calculate the GCD of two integers. How, you might ask? Start with two integers a, b. Use the division lemma to divide $|a|$ by $|b|$. We get integers q_0, r_0, such that $|a| = |b|q_0 + r_0$. If $r_0 = 0$, we are done; because then b divides a, so the GCD will be $|b|$. Else, denote $a_0 = |a|, b_0 = |b|, a_1 = b_0, b_1 = r_0$. Now perform the division lemma to divide a_1 by b_1, to get integers q_1, r_1. Now let $a_2 = b_1, b_2 = r_1$ and repeat the procedure. This is better demonstrated in the following equation.

$$\text{Let } |a| = a_0, |b| = b_0, \text{ and } \forall\ n, a_n = b_n q_n + r_n, \text{ let } a_{n+1} = b_n \text{ and } b_{n+1} = r_n.$$

Note that this process makes each a_n, b_n smaller and smaller; and as each a_n, b_n is a non-negative integer, this process must terminate at some point (because there are only finitely many possible values for each a_n, b_n, and for each n the values keep decreasing). If the process terminates at, say the k^{th} step, then we'll have $r_k = 0$, meaning $b_k \mid a_k$. This b_k will be our desired GCD. As for why that happens, note that b_k actually divides all the a_p and all the b_p. And every common divisor of a, b also divides each a_p and each b_p as well; hence they also divide b_k. Thus by definition (and uniqueness) of GCD, we can say b_k is indeed the GCD of a, b.

Try to go through the above algorithm properly and get a hang of it. We now state an important corollary of the same.

[Bezout's Lemma.] Let $a, b \neq 0$ and $g = (a, b)$.

1. There exists integers x, y such that $ax + by = g$.

2. Further, $g = 1$ if and only if there are integers p, q such that $ap + bq = 1$.

We would like to generalise this further.

For any integer a, let $\langle a \rangle = \{a \times n \ :\ n \in \mathbb{Z}\}$. And for any finite set of integers $S = \{a_1, \ldots, a_n\}$, similarly define

$$\langle S \rangle = \{a_1 x_1 + \cdots + a_n x_n \ :\ x_1, \ldots, x_n \in \mathbb{Z}\}.$$

We're specifically interested in the two-element case, $S = \{a, b\}$.

Note that if $\gcd(a, b) = d$, then $d \mid ax + by$ for all $x, y \in \mathbb{Z}$. Thus, $\langle a, b \rangle \subseteq \langle d \rangle$. Now return to the division

algorithm. Observe that in each step, the r_i we obtained is actually in $\langle a, b\rangle$! For r_0 that is obvious. And in the second equation, we also get $r_1 = |b| - (|a| - |b|q_0)q_1 = |a|(-q_1) + |b|(1 + q_0q_1)$, and so on. Eventually, we obtain a k such that $r_k = 0$, and $r_{k-1} = d$. Thus, $d \in \langle a, b\rangle$. In other words, there exist integers x, y such that $d = ax + by$. Note that this also means, for any integer k, we have $dk = akx + bky$, meaning $\langle d\rangle \subseteq \langle a, b\rangle \subseteq \langle d\rangle$. This is known also known as Bézout's Lemma, and is stated below separately.

[Bézout's Lemma] For any two integers a, b (not both zero), $\gcd(a, b) = \min\{|ax + by| : x, y \in \mathbb{Z}\}$. In other words, for any two integers (not both zero) a, b, we can say that

$$\langle a, b\rangle = \langle \gcd(a, b)\rangle.$$

Generalized Bézout's Theorem: For a finite collection S of non-zero integers; if $\gcd(S)$ is the largest positive integer which divides every element of S, then $\langle \gcd(S)\rangle = \langle S\rangle$. More specifically,

$$\gcd(S) = \min\{|a_1x_1 + \cdots + a_nx_n| : a_i \in S, x_i \in \mathbb{Z}\}.$$

1.5 Exercises

1. For natural numbers a, m, n, prove that $\gcd(a^m - 1, a^n - 1) = a^{\gcd(m,n)} - 1$.
2. Prove that the expression $\frac{\gcd(m,n)}{m} \times \binom{m}{n}$ is an integer for all pairs of integers $m \geq n \geq 1$.
3. Show that the following classes of integers are reducible -
   (a) $4n^3 + 6n^2 + 4n + 1$, $n \geq 1$.
   (b) (RMO 1991) $n^4 + 4^n$, $n > 2$.
   (c) $5^n + 3^n + 1$ for $n \geq 1$.
4. Prove that $\gcd(n! + 1, (n + 1)! + 1) = 1$ for each $n \geq 1$. [Here $n! = n(n - 1) \ldots 1$ is the factorial of n.]
5. Let x, y, z be positive integers, such that $yz = zx + xy$. If $h = \gcd(x, y, z)$, then prove that $hxyz$ and $h(y - x)$ are perfect squares.
6. Find the minimum possible least common multiple (lcm) of twenty (not necessarily distinct) natural numbers whose sum is 801.
7. Let $m, n, l \in \mathbb{N}$ and $\text{lcm}[m + l, m] = \text{lcm}[n + l, n]$, then prove that $m = n$.
8. Let a, b be distinct positive integers such that $ab(a + b) \mid a^2 + ab + b^2$. Prove that $|a - b| > \sqrt[3]{ab}$.

9. Show that for any natural number n, one can find three distinct natural numbers a, b, c between n^2 and $(n+1)^2$, such that $c \mid a^2 + b^2$.

10. Find the positive integers n with exactly 12 divisors $1 = d_1 < \cdots < d_{12} = n$ such that *the divisor with index* d_4, i.e. d_{d_4} is equal to $1 + (d_1 + d_2 + d_4)d_8$.

11. Given a natural number n, show that any integer $k > \frac{n^4}{16}$ can be written in *at most one way* as the product of two of its divisors having difference *not exceeding* n.