Chapter 3: Introduction to Divisibility

SYLLABUS INCLUDES

Students will learn to prove properties and results, and solve non-routine problems involving:

Primes, coprimes, divisibility, modulo arithmetic, greatest common divisor, division algorithm

Students may use the following theorems and results in Numbers.

(i) (The Fundamental Theorem of Arithmetic) Every integer $n \geq 1$ can be expressed as a product of primes in a unique way apart from the order of the prime factors.

(ii) There exist infinitely many primes.

(iii) (Division Algorithm) Let a be an integer and b a positive integer. Then there exists unique integers q and r, with $0 \leq r < b$, such that $a = bq + r$.

(iv) If a and b are positive integers, then their greatest common divisor (gcd) is a linear combination of a and b, that is, there exists integers s and t such that $\gcd(a, b) = sa + tb$.

CONTENT

1 Introduction

Johann Carl Friedrich Gauss, German mathematician, astronomer and physicist said "*Die Mathematik ist die Königin der Wissenschaften und die Zahlentheorie ist die Königin der Mathematik*," which translated, means "Mathematics is the queen of sciences and number theory is the queen of mathematics." So perhaps it is appropriate that we begin our course with number theory.

So what exactly is number theory? In short, it is the study of natural numbers and the integers. The theory of numbers is one of the oldest branches of mathematics, and can be traced back to the Greeks and ancient Egyptians. However, the first rudiments of an actual theory are generally credited to Pythagoras and his disciples.

2 Divisibility

2.1 Division Algorithm

One theorem, the Division Algorithm, acts as the foundation stone upon which most of our results are built on.

Theorem 2.1.1 (Division Algorithm) Given integers *a* and *b*, with $b > 0$, there exist unique integers *q* and *r* satisfying

$$a = qb + r, \qquad 0 \le r < b$$

The integers *q* and *r* are called, respectively, the *quotient* and *remainder* in the division of *a* by *b*.

The proof of this result is not required for the H3 syllabus, but this result should be intuitive. For example, when we divide 17 by 5, we have a quotient of 3 and a remainder of 2. The theorem assures us that the quotient and remainder we speak of are unique.

However, let us illustrate the division algorithm when we replace the restriction that *b* must be positive by the simple requirement that $b \neq 0$. For example, let us take $b = -7$. Then, for the choices of $a = 1, -2, 61$ and -59, we obtain the expressions

$$\begin{aligned} 1 &= 0(-7) + 1 \\ -2 &= 1(-7) + 5 \\ 61 &= (-8)(-7) + 5 \\ -59 &= 9(-7) + 4 \end{aligned}$$

We wish to focus our attention on the applications of the Division Algorithm, and not so much on the algorithm itself. As a first illustration, note that with $b = 2$, the possible remainders are $r = 0$ and $r = 1$. When $r = 0$, the integer *a* has the form $a = 2q$ and is called *even*; when $r = 1$, the integer *a* has the form $a = 2q + 1$ and is called *odd*. Now a^2 is either of the form $a^2 = (2q)^2 = 4q^2$ or $a^2 = (2q+1)^2 = 4(q^2 + q) + 1$. The point to be made here is that the square of an integer always leaves the remainder of 0 or 1 upon division by 4.

Example 2.1.1
Show that the square of any odd integer leaves a remainder of 1 when divided by 8.

Example 2.1.2
Show that $\frac{a(a^2+2)}{3}$ is an integer for all $a \geq 1$.

2.2 Greatest Common Divisor (GCD)

Of special significance is the case in which the remainder in the Division Algorithm turns out to be zero. Let us look at this case now.

Definition 2.2.1 An integer b is said to be *divisible* by an integer $a \neq 0$, which we denote by $a \mid b$, if there exists some integer c such that $b = ac$. We write $a \nmid b$ to indicate that b is not divisible by a.

Thus, for example, -12 is divisible by 4, because $-12 = 4(-3)$. However, 31 is not divisible by 3; since there is no integer c satisfying $31 = 3c$.

There are also other ways to say $a \mid b$ than b is divisible by a. We can equivalently say that a is a divisor of b, that a is a factor of b, a divides b or b is a multiple of a. Do also note that whenever the notation $a \mid b$ is employed, it is understood that a is different from zero.

We also note that if a is a divisor of b, then b is also divisible by $-a$ (why?), so that the divisors of an integer always occur in pairs. To find all the divisors of a given integer, it is sufficient to obtain the positive divisors and then adjoin them to the corresponding negative integers. For this reason, we shall usually limit ourselves to a consideration of the positive divisors.

The following theorem is a list of results that follow from Definition 2.2.1. You should be able to prove them by yourself.

Theorem 2.2.1 For integers *a*, *b*, *c*, the following hold:

(a) $a \mid 0$, $1 \mid a$, $a \mid a$.

(b) $a \mid 1$ if and only if $a = \pm 1$.

(c) If $a \mid b$ and $c \mid d$, then $ac \mid bd$.

(d) If $a \mid b$ and $b \mid c$, then $a \mid c$ (transitivity).

(e) $a \mid b$ and $b \mid a$ if and only if $a = \pm b$.

(f) If $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$.

(g) If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for arbitrary integers *x* and *y*.

It is also worth pointing out that property (g) extends by induction to sums of more than two terms. That is, if $a \mid b_k$ for $k = 1, 2, \ldots, n$, then

$$a \mid (b_1 x_1 + b_2 x_2 + \ldots + b_n x_n)$$

for all integers x_i.

Example 2.2.1

Find all integers *n* such that $n^2 + 1 \mid n + 1$.

If a and b are arbitrary integers, then an integer d is said to the a *common divisor* of a and b if both $d \mid a$ and $d \mid b$. Because 1 is a divisor of every integer, 1 is a common divisor of a and b. Hence the set of positive common divisors is nonempty. Now every integer divides zero, so that if $a = b = 0$, then every integer serves as a common divisor of a and b. In this instance, the set of positive common divisors of a and b is infinite. However, when at least one of a or b is nonzero, there are only a finite number of positive common divisors. Among these, there is a largest one, which will call the greatest common divisor of a and b.

Definition 2.2.2 (Greatest Common Divisor)
Let a and b be given integers, with at least one of them different from zero. The *greatest common divisor* of a and b, which we denote by gcd(a, b), is the positive integer d satisfying the following:

(a) $d \mid a$ and $d \mid b$

(b) If $c \mid a$ and $c \mid b$, then $c \leq d$.

Example 2.2.2
Find

(a) gcd(5, −5)

(b) gcd(8, 17)

(c) gcd(−8, −36)

It is easy to compute the gcd of 2 numbers when they are small. What happens when they are large? We will discuss 2 methods in Section 2.3 and 2.4.

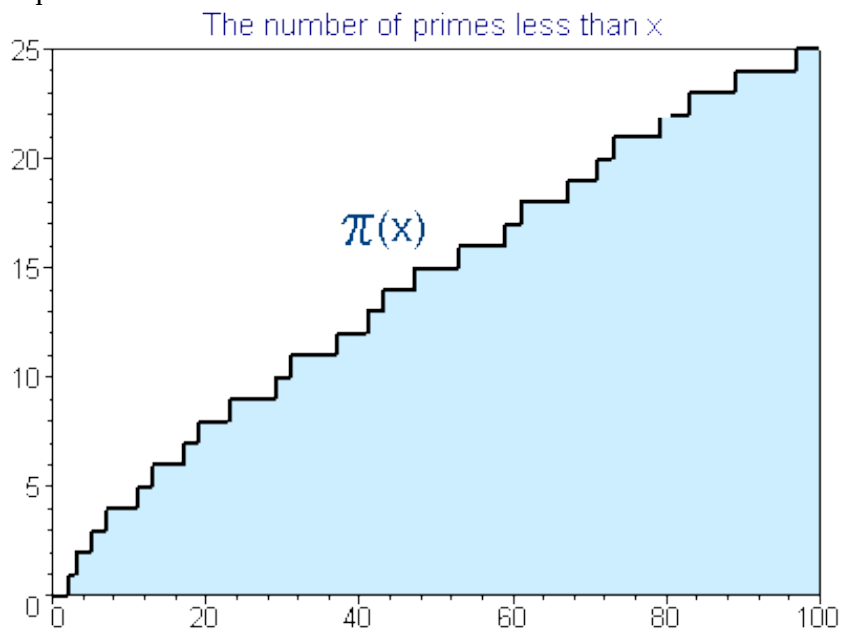
2.3 Prime and composite numbers

Since number theory is about the study of numbers, it is perhaps important for us to look at what we call the building blocks of these numbers, which are the prime numbers. So what are prime numbers?

Definition 2.3.1 An integer $p > 1$ is called a *prime number*, or simply a *prime*, if its only positive divisors are 1 and p. An integer greater than 1 that is not a prime is known as *composite*.

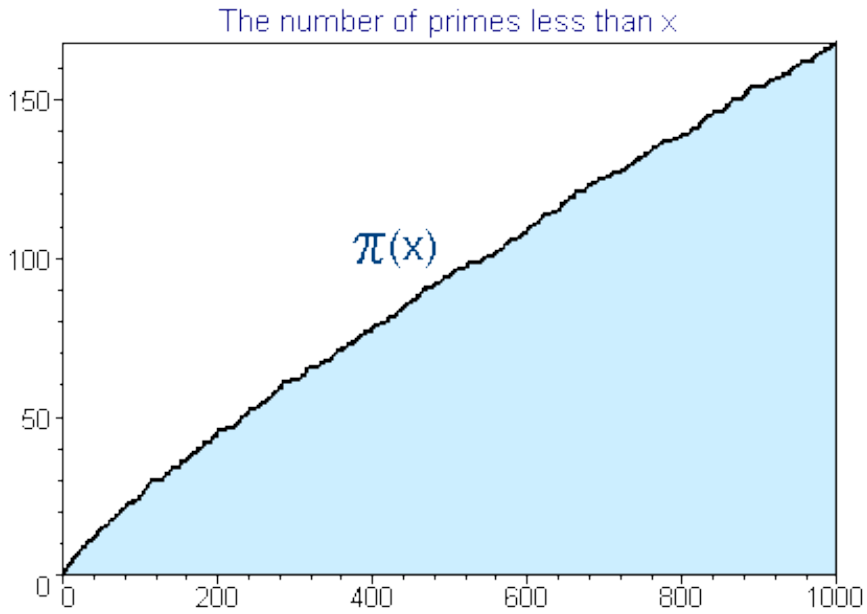
Among the first 10 positive integers, 2, 3, 5, 7 are primes and 4, 6, 8, 9, 10 are composite numbers. Note that 2 is the only even prime (why?), and according to our definition, the integer 1 is neither prime nor composite.
There are many questions concerning primes, in particular, with regard to its distribution. In fact, one of the millennium problems, the Riemann Zeta Function, is closely tied to the distribution of prime numbers.

Let x be a positive real number. The question "How many primes are there less than x?" has been so commonly asked that a function $\pi(x)$, which denotes the number of primes less than or equal to x has been defined.



For small x, it is easy to count. But it is interesting to note how irregular the graph is for small values of x.

Now let us zoom out.



So even though $\pi(x)$ doesn't seem regular at small values of x, there seems to be a definite trend to its values.

In particular, the Prime Number Theorem states that the number of primes not exceeding x is asymptotic to $\frac{x}{\ln x}$. What does this mean? This means for large x, we have

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1..$$

The table below further illustrates the trend:

x	$\pi(x)$	$\frac{x}{\ln x}$	$\frac{\pi(x)}{\frac{x}{\ln x}}$
1000	168	145	1.16
10000	1229	1086	1.13
100000	9592	8686	1.10
1000000	78498	72382	1.08
10000000	664579	620420	1.07
100000000	5761455	5428681	1.06

In this H3 course, we are not studying the distribution of the prime numbers. In fact any meaningful study of the distribution of prime numbers requires complex analysis and analytical number theory, usually advanced undergraduate/graduate course material.

However, there is one basic result established by Euler some 2000 years ago which you should know:

Theorem 2.3.1 (Euler) There are infinitely many primes.

Proof We proceed by contradiction. Suppose there is only a finite number of primes, say $p_1 < p_2 < ... < p_m$. Consider the number $P = p_1 p_2 \cdots p_m + 1$. If P is a prime, then $P > p_m$, contradicting the maximality of p_m. Hence P must be composite and thus has a prime divisor $p > 1$ which is one of $p_1, p_2, ..., p_m$, say p_k. Then it follows that $p_k \mid p_1 p_2 \cdots p_m + 1$ But this means that $p_k \mid 1$, which is a contradiction.

So let us come back to our discussion. Why are prime numbers the building blocks of the natural numbers? Let us consider the number 420. It is certainly composite. It can be represented, for instance, as 42 × 10. But each of the numbers 42 and 10 are composite, too. Indeed, 42 = 6 × 7, and 10 = 2 × 5. Since 6 = 2 × 3, we have 420 = 42 × 10 = 6 × 7 × 2 × 5 = 2 × 3 × 7 × 2 × 5 = 2 × 2 × 3 × 5 × 7. This is the complete "decomposition" of our number (its representation as a product of primes).

It is clear that we can factor any natural number greater than 1 in the same way. We just keep factoring the numbers we have into pairs of smaller numbers as long as we can (and if any one of the factors cannot be represented as such a product, then it is a prime factor).

But what if we try to factor the number 420 in some other way? For example, we can start with 420 = 15 × 28. It may surprise you that we will always end up with the same representation (products which differ only in the order of their factors are considered identical – we usually arrange the factors in increasing order).

This may seem obvious, but it is not immediate to prove. In fact, this is the **Fundamental Theorem of Arithmetic**:

Theorem 2.3.2 Fundamental Theorem of Arithmetic
Every positive integer $n>1$ is either a prime or a product of primes; this representation is unique, apart from the order in which the factors occur.

Proof The proof is not required in the H3 syllabus, but you should be able to get a rough understanding of it from the sketch we have provided below. There are some subtleties though, can you spot them?

We proceed by strong induction. Consider some integer $n > 1$. Either it is prime or it is composite. If it is prime, we are done. If it is composite, then there exists an integer $d \mid n$ and $1 < d < n$. Among all such integers d, choose the smallest, say p_1. Then p_1 must be prime. Hence we can write $n = p_1 n_1$ for some integer n_1 satisfying $1 < n_1 < n$. This completes the induction.

Example 2.3.1
Find
(a) gcd(2016, 1980)
(b) gcd(A, B), where $A = 2^3 \times 3^{10} \times 5 \times 7^2$ and $B = 2^5 \times 3 \times 11$.
(c) gcd(806, 12529)

It may happen that 1 is the only common (positive) divisor of a given pair of integers a and b, whence gcd(a, b) = 1. In fact, this situation occurs often enough to prompt a definition.

Definition 2.3.2 Two integers a and b, not both of which are zero, are said to be *relatively prime* (or *coprime*) whenever gcd(a, b) = 1.

Now let us discuss another definition of the gcd. The next theorem indicates that gcd(a, b) can be represented as a linear combination of a and b. By linear combination, we mean an expression of the form $ax + by$, where x and y are integers. This is illustrated by

$$\gcd(-12, 30) = 6 = (-12)2 + (30)1 \quad \text{or} \quad \gcd(-8, -36) = 4 = (-8)4 + (-36)(-1).$$

The proof of the theorem below is not required in the H3 syllabus.

Theorem 2.3.3 Given integers a and b, not both of which are zero, there exists integers x and y such that $\gcd(a, b) = ax + by$.

Do note the theorem only ensures the existence of integers x and y, but does not provide a practical method of finding the values of x and y. We will focus on the applications of this result and talk about how to find the x and y in Chapter 5 Section 1.

The following theorem characterizes relatively prime integers in terms of linear combinations.

Theorem 2.3.4 Let a and b be integers, not both zero. Then a and b are relatively prime if and only if there exist integers x and y such that $1 = ax + by$.

Proof

It is important for you to compare theorems 2.3.3 and theorems 2.3.4. Theorem 2.3.4 leads to an observation that is useful in certain situations; namely,

Corollary 1 If $\gcd(a, b) = d$, then $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Before starting with the proof proper, we should observe that a/d and b/d are integers (why?).

Proof

Corollary 2 If $a \mid c$ and $b \mid c$, with $\gcd(a, b) = 1$, then $ab \mid c$.

Proof

Question: Is the condition $\gcd(a, b) = 1$ necessary?

The following theorem is of fundamental importance, and is again a consequence of Theorem 2.3.4.

Theorem 2.3.5 If $a \mid bc$, with gcd(a, b) = 1, then $a \mid c$.

Proof

Question: Is the condition gcd(a, b) = 1 necessary?

The subsequent theorem often serves as a definition of gcd(a, b). The advantage of using it as a definition is that order relationship (compare to Definition 2.2.2) is not involved.

Theorem 2.3.6
Let a and b be given integers, with at least one of them different from zero. For a positive integer d, d = gcd(a, b) if and only if
(a) $d \mid a$ and $d \mid b$
(b) Whenever $c \mid a$ and $c \mid b$, then $c \mid d$.

Proof

2.4 Lowest Common Multiple (LCM)

There is a concept parallel to that of the greatest common divisor of two integers, known as their least common multiple. An integer c is said to be a *common multiple* of two nonzero integers a and b whenever $a \mid c$ and $b \mid c$. Evidently, zero is a common multiple of a and b. To see that there exist common multiples that are non trivial, just note that the product ab is a common multiple of a and b. Hence the set of positive common multiples of a and b must contain a smallest integer; which we call as the least common multiple of a and b.

Definition 2.4.1 The *lowest common multiple* of two nonzero integers a and b, denoted by lcm(a, b), is the positive integer m satisfying the following:
(a) $a \mid m$ and $b \mid m$
(b) If $a \mid c$ and $b \mid c$ with $c > 0$, then $m \leq c$.

For example, the positive common multiples of the integers 12 and 30 are 60, 120, 180, … . Hence lcm(12, 30) = 60. We lack a relationship between the ideas of greatest common divisor and lowest common multiple. The gap is filled by the following theorem.

Theorem 2.4.1 For positive integers a and b,

$$\gcd(a,b)\text{lcm}(a,b) = ab.$$

Proof

Perhaps the chief virtue of Theorem 2.4.1 is that it makes the calculation of the least common multiple of two integers dependent on the value of their greatest common divisor – which, in turn, can be calculated from the Euclidean Algorithm.

For instance, when considering the positive integers 682 and 264, we found that their gcd is 22. Hence $\text{lcm}(682, 264) = \dfrac{682(264)}{22} = 8184.$

Tutorial

1. Use the Division Algorithm to show that the square of any integer is either of the form $3k$ or $3k + 1$. Hence show that $3a^2 - 1$ is never a perfect square.

2. Show that the cube of any integer when divided by 7, gives remainder 0, 1 or 6.

3. Show that $\frac{n(n+1)(2n+1)}{6}$ is an integer for all positive integers n.

4. Find all terms in the following sequence that are perfect squares:

1, 11, 111, 1111, 11111, ….

5. Prove that, for a positive integer n and any integer a, gcd(a, $a + n$) divides n; hence, show any two consecutive integers are coprime.

For Questions 6 to 8, you should not use the Euclidean Algorithm.

6. For any integer a, show that
(a) $\gcd(2a+1, 9a+4) = 1$;
(b) $\gcd(5a+2, 7a+3) = 1$;
(c) if a is odd, then $\gcd(3a, 3a+2) = 1$.

7. If a and b are integers, not both of which are zero, prove that $\gcd(2a-3b, 4a-5b)$ divides b. Hence show that $2a + 3$ and $4a + 5$ are coprime for any integer a.

8. Show that if gcd(a, b) = 1, then $\gcd(a+b, a^2+b^2) \mid 2$.

Hence write down the possible values of $\gcd(a+b, a^2+b^2)$.

9. For nonzero integers a and b, verify that the following conditions are equivalent:
(a) $a \mid b$.
(b) gcd(a, b) = $|a|$.
(c) lcm(a, b) = $|b|$.

10. Lockers in a row are numbered 1, 2, 3, ..., 1000. At first, all the lockers are closed. A person walks by and opens every other locker, starting with locker #2. Thus lockers 2, 4, 6, . . . , 998, 1000 are open. Another person walks by, and changes the "state" (i.e., closes a locker if it is open, opens a locker if it is closed) of every third locker, starting with locker #3. Then another person changes the state of every fourth locker, starting with #4, etc. This process continues until no more lockers can be altered. Which lockers will be closed?

11. [852/2/1979/Dec/19]

For any positive integer n, let $\sigma(n)$ denote the sum of all positive integers (including 1 and n) which divide n.

(i) If $n = p^a$, where p is prime, show that $\sigma(n) = \dfrac{p^{a+1}-1}{p-1}$

Given that p is an odd prime, deduce that $\sigma(p^a)$ is odd if and only if p^a is a square.

(ii) If $n = 2^m p$, where p is an odd prime, and $\sigma(n) = 2n$, show that $p = 2^{m+1} - 1$.

12. [9225/2/Dec/1985/19]

(a) Explain what is meant by the following two statements concerning the integers a, b and c:

(i) a, b, c are relatively prime,

(ii) a, b, c are relatively prime in pairs.

Show that (i) is a necessary but not sufficient condition for (ii). [4]

(b) Show that $n^3 + 6n^2 + 11n + 6$ is divisible by 6 if n is even, and by 24 if n is odd. [8]

Assignment 3: Introduction to Divisibility

1. (i) Show that $x^k - 1 = (x-1)(x^{k-1} + x^{k-2} + ... + x + 1)$ for any positive integer k.

(ii) Prove that if $d \mid n$, then $2^d - 1 \mid 2^n - 1$.

(iii) Hence show that $2^{35} - 1$ is divisible by 31 and 127.

2. **[852/2/1983/Dec/19]**

State whether the following assertions are true or false. Prove those which you consider to be true and give counter-examples for those which you consider to be false.

For positive integers a and b,

(i) if $a^2 + 1$ is divisible by b, then $a^4 + 1$ is divisible by b.

(ii) if $a^2 - 1$ is divisible by b, then $a^4 - 1$ is divisible by b.

(iii) if b^2 is divisible by a prime p, then b is divisible by p.

(iv) if p is a prime and both a and $a^2 + b^2$ are divisible by p, then b is divisible by p.

(v) if p is a prime and both a and $a^2 + 6b^2$ are divisible by p, then b is divisible by p.

3. [852/1/1978/Dec/19 (modified)]

Show that if $(n, m) = 1$, then $(n, n - m) = 1$, where (n, m) denotes the greatest common divisor of n and m.

(i) Show that $(a + b, a^2 - ab + b^2) = (a + b, 3ab)$, and deduce that, if $(a, b) = 1$, then $(a + b, a^2 - ab + b^2) = 1$ or 3.

(ii) Show that $(n! + 1, (n + 1)! + 1) = 1$.

(iii) Show that, if $n > 1$, the sum of the positive integers less than n and coprime to n is $\frac{1}{2} n\varphi(n)$, where $\varphi(n)$ is the number of such integers.

(iv) Find also the sum of the positive integers less than $2n$ and coprime to n in a similar form.