CHAPTER 6

Number Theory – introduction

Number Theory is mainly concerned with properties of $\mathbb{N}$ and more generally $\mathbb{Z}$. Throughout this chapter and the next two (also about Number Theory) we will use $a, b, c, d, m, n, q, r, N$ for integers, sometimes without explicitly stating that they are.

Division Algorithm. *For integers a, b with $a > 0$ there exist integers q (the **quotient**) and r (the **remainder**) such that*

$$b = aq + r \text{ and } 0 \leqslant r < a.$$

Essentially q, r are the numbers that make the following division work:

$$\begin{array}{r|l} & q \quad \textit{rem.} \quad r \\ \hline a & b \end{array}$$

(Often $b > 0$, but this is not necessary.)

Let's apply the Division Algorithm to a few examples:

$$\begin{array}{llll} \text{if } a = 7 & \text{and } b = 22 & \text{we write } 22 = 7 \cdot 3 + 1 & (\text{so } q = 3 \text{ and } r = 1); \\ \text{if } a = 113 & \text{and } b = 355 & \text{we write } 355 = 113 \cdot 3 + 16 & (\text{so } q = 3 \text{ and } r = 16); \\ \text{if } a = 8 & \text{and } b = 72 & \text{we write } 72 = 8 \cdot 9 + 0 & (\text{so } q = 9 \text{ and } r = 0). \end{array}$$

6.1 Divisibility

In the special case where the **division algorithm** applied to two integers a, b as described above yields a *remainder* of 0, we have the following.

Definition 6.1.1. The following are equivalent.

(i) $a, b \in \mathbb{Z}$ and $b = aq$ for some $q \in \mathbb{Z}$;

(ii) b is a **multiple** of a;

(iii) b is **divisible by** a (written: $b \vdots a$);

(iv) a is a **divisor** of b;

(v) a **divides** b (written: $a \,|\, b$).

If $a \,|\, b$ does not hold, then a does **not divide** b (written: $a \nmid b$). For example,

$$7 \,|\, 35, \quad -3 \,|\, 21, \quad 4 \,|\, 0 \quad \text{and } (a+1) \,|\, a^2 - 1 \text{ for any integer } a$$

but

$$7 \nmid 33, \quad -3 \nmid 22, \quad 0 \nmid 4.$$

Finally, the **divisors** of b are all d such that $d \,|\, b$, e.g. the *divisors* of 12 are those

$$d \in \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}.$$

Don't confuse the *divides* symbol: $\mid$ (which is a *vertical* stroke with a little space around it) with the *slash* symbol: / (which separates the numerator and denominator of a fraction). Also, note that despite the symmetry of the symbol: '$\mid$' cannot be used in reverse, i.e. $a \mid b$ and $b \mid a$ mean *different* things (see: Property 6.1.3(iv)). What may also be confusing is that $a \mid b$ means the same as $b/a \in \mathbb{Z}$; so *don't* slant '$\mid$'!

Note 6.1.2. While the dictionary meaning of **factor** is a synonym for *divisor*, we prefer to reserve *factor* (of an integer) for the *multiplicands* that make up a product, e.g. $6 = 2 \cdot 3$ writes 6 as the product of *factors* 2 and 3, whereas the *positive divisors* of 6 are 1, 2, 3, and 6.

Properties 6.1.3 (Properties of Divides).

(i) *If* $d \mid a$ *then* $d \mid ax$ *for all* $x \in \mathbb{Z}$.

(ii) *If* $d \mid a$ *and* $d \mid b$ *then* $d \mid a + b$.

(iii) *If* $d \mid a$ *and* $d \mid b$ *then* $d \mid ax + by$ *for all* $x, y \in \mathbb{Z}$.

(iv) *If* $a \mid b$ *and* $b \mid a$ *then* $a = \pm b$.

(v) *If* $a \mid b$ *and* $b \mid c$ *then* $a \mid c$. ***(transitivity)***

Proof of (i)–(iii). Suppose $d \mid a$, and choose arbitrary $x \in \mathbb{Z}$. Then

$$\begin{aligned} & a = dq, \text{ for some } q \in \mathbb{Z} \\ \implies\ & ax = dqx, \text{ where } qx \in \mathbb{Z} \\ \implies\ & d \mid ax. \end{aligned}$$

So (i) holds.
Now suppose also $d \mid b$. Then

$$\begin{aligned} & b = ds, \qquad \text{for some } s \in \mathbb{Z} \\ \implies\ & a + b = dq + ds \\ & \quad = d(q + s), \text{ where } q + s \in \mathbb{Z} \\ \implies\ & d \mid a + b. \end{aligned}$$

So (ii) holds.
Now suppose $d \mid a$ and $d \mid b$. Then,

$$\begin{aligned} & d \mid ax \text{ and } d \mid by \ \ \forall x, y \in \mathbb{Z}, && \text{by (i)} \\ \implies\ & d \mid ax + by, && \text{by (ii)} \end{aligned}$$

So (iii) holds. □

Definition 6.1.4. If p is a prime and α is a positive integer then we write $p^\alpha \parallel m$ if $p^\alpha \mid m$ but $p^{\alpha+1} \nmid m$. In this case we say p^α **exactly divides** m (or p^α **divides** m **exactly**).

6.2 Prime numbers

Definition 6.2.1.

1. $p \in \mathbb{N}$ is **prime** $\iff$ $p > 1$ and the only positive divisors of p are: 1 and p.
2. d is a **unit** $\iff$ $d \mid n$ for all $n \in \mathbb{N}$; 1 is a *unit*.
3. d is a **proper divisor** of N $\iff$ $d \mid N$ and $1 < d < N$.
4. $N \in \mathbb{N}$ is **composite** $\iff$ $N = ab$ for some $a, b \in \mathbb{N}$ such that $1 < a \leqslant b < N$
   $\iff$ N has a proper divisor.

Primality. The property of being prime is a number's **primality**. In the first 100 natural numbers, 25 are prime, namely,

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, and 97.

Lemma 6.2.2. *If $1 < n \in \mathbb{N}$ and n has no prime divisor $p \leqslant \sqrt{n}$ then n is prime.*

Proof. Let $1 < n \in \mathbb{N}$. Consider n is not prime, then n is composite, and so $n = ab$ for some $a, b \in \mathbb{N}$ such that $1 < a \leqslant b < n$ which implies $a \leqslant b = n/a$, i.e. $a^2 \leqslant n$ or $a \leqslant \sqrt{n}$. Thus having no prime divisors $p \leqslant \sqrt{n}$ implies n has no divisors $a \leqslant \sqrt{n}$ and hence n is not composite, and since $n > 1$, n is prime. □

What makes *primes* so interesting is that every *natural number* (other than 1) can be expressed in just one way (except that we may be able to arrange the factors in many ways) as the product of prime divisors, e.g.

$$74844 = 2^2 \cdot 3^5 \cdot 7 \cdot 11.$$

Such a factorisation is called a **prime decomposition** or **prime factorisation**.

If we were to include 1 as a prime then $74844 = 1^5 \cdot 2^2 \cdot 3^5 \cdot 7 \cdot 11$, say, would be "another prime decomposition". Excluding 1 as a prime ensures the *uniqueness* of *prime decompositions*.

The above fact is so important it is given a special name. Let's give it its name and recap what it says, and follow it up by an equally important result from the Greek, Euclid:

Theorem 6.2.3 (Fundamental theorem of arithmetic). *Any natural number n, can be written* uniquely *as follows:*

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},$$

where $k \in \mathbb{N}$, each p_i is a prime number and $1 < p_1 < p_2 < \cdots < p_k$, and each $e_i \in \mathbb{N}$.

Lemma 6.2.4 (Euclid's Lemma). *If p is prime and $p \mid ab$ then $p \mid a$ or $p \mid b$.*

Algorithm 6.2.5 (Sieve of Eratosthenes). * *For some $N \in \mathbb{N}$, to find all the* primes *p such that $p \leqslant N$, perform the following steps.*

1. *Start by writing down all the* natural numbers *from 1* upto *N.*
2. *Cross out 1 . . . 1 is* not *prime (by definition).*
3. *The first number* not *crossed out is 2 . . . it must be* prime; *put* a box *around it and cross out* all *multiples of 2 in the list . . . i.e. cross out 4, 6, 8, ...*
4. *Go back to the start of the list and* box *the first number that is* not *crossed out or boxed . . . it must be* prime; *and cross out* all *multiples of that number in the list. (*Note. *Some multiples may already have been crossed out.)*
5. *Repeat* Step 4. *until every number in the list is either* boxed *or crossed out.*

At the termination of the algorithm, the list of all *primes p such that $p \leqslant N$ are the numbers that are* boxed.

* *Eratosthenes* is pronounced: error-toss-the-knees.


Eratosthenes (c. 276 BC–194 BC) was a Greek mathematician, historian, astronomer, poet and geographer. Born at Cyrene in northern Africa he lived much of his life in Alexandria where he was the chief librarian. (At the time, Alexandria was famous for its library.) Eratosthenes was also famous for estimating the circumference of the earth using elementary *trigonometry* (i.e. *geometry*) and the lengths of shadows in two different places (measured at the same time of day.)

Example 6.2.6. *Let's use the* Sieve of Eratosthenes *to find all the primes less than or equal to 30. Below is the list of numbers from 1 to 30, after the method has been applied.*

~~1~~	[2]	[3]	~~4~~	[5]	~~6~~	[7]	~~8~~	~~9~~	~~10~~
[11]	~~12~~	[13]	~~14~~	~~15~~	~~16~~	[17]	~~18~~	[19]	~~20~~
~~21~~	~~22~~	[23]	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	[29]	~~30~~

The following are the steps required to obtain this.

1. *List* natural numbers *from 1* upto 30.
2. *Cross out 1.*
3. *The first number* not *crossed out is 2;* box *it and cross out 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30 (*all *multiples of 2 – other than 2 itself – in the list).*
4. *The first number* not *crossed out or boxed is now 3;* box *it and cross out 9, 15, 21, 27 (*all *multiples of 3 – other than 3 itself – in the list; 6, 12, 18, 24, 30 are also multiples of 3 but have already been crossed out).*
5. *The first number* not *crossed out or boxed is now 5;* box *it and cross out 25 (the only multiple of 5 left that hasn't already been crossed out or boxed; 10, 15, 20, 30 are also multiples of 5 but have already been crossed out).*
   On further repeats of Step 4. *we box 7, 11, 13, 17, 19, 23, 29 . . . it turns out that on each of these occasions there are no multiples left to cross out.*

So the list of primes less than or equal to 30 is: $2, 3, 5, 7, 11, 13, 17, 19, 23, 29$.

Observations.
1. *On each execution of Step 4. (or Step 3.), the first prime multiple crossed out is the square of the prime just boxed, since all smaller multiple of that prime were already crossed out earlier.*
2. *When performing the Sieve of Eratosthenes in Example 6.2.6 we observed in Step 5. that when we came to box 7, no further multiples of anything were left to cross out, and the reason for this is that* $7 > \sqrt{30}$.
3. *The Sieve of Eratosthenes is impractical for determining the primality of an integer* N, *especially as* N *gets larger. On the other hand it is relatively easy to determine divisibility by any given number.*

Example 6.2.7. *97 is prime, since*

- $97 < 100 = 10^2$;
- $2, 3, 5, 7$ *are the primes less than* $\sqrt{97} < 10$ *(we don't need to find square-roots* exactly!*);*
- *and none of* $2, 3, 5, 7$ *divides* 97. *Here, we use divisibility rules, or determine a remainder:*
  - $2 \nmid 7$ *(7 is last digit of* 97*)* $\implies 2 \nmid 97$.
  - $3 \nmid 16 = S(97) \implies 3 \nmid 97$ *(*$S(N)$ = *"the sum of digits of* N*", see Lemma 7.2.6).*
  - $5 \nmid 7$ *(7 is last digit of* 97*)* $\implies 5 \nmid 97$.
  - $97 = 7 \cdot 13 + 6 \implies 7 \nmid 97$.

Exercise Set 6.

1. Determine *simple* rules for divisibility by each of the following natural numbers:

   (i) 2 (iv) 5 (vii) 9 (x) 12
   (ii) 3 (v) 6 (viii) 10 (xi) 15
   (iii) 4 (vi) 8 (ix) 11

   Note: there is a rule for 7, but it's complicated and it is not much better than straight division.

2. The number $739ABC$ is divisible by 7, 8 and 9. What values can A, B and C take?

3. Show that $x^2 - y^2 = 2$ has no integer solutions.

4. Prove that for every integer n:

   (i) $3 \mid n^3 - n$; (iii) $30 \mid n^5 - n$; (v) $4 \nmid n^2 + 2$;
   (ii) $6 \mid n(n-1)(2n-1)$; (iv) $120 \mid n^5 - 5n^3 + 4n$; (vi) $121 \nmid n^2 + 3n + 5$.

5. Prove that for all integers a and b: 3 divides $(a+b)^3 - a^3 - b^3$.

6. Is 167 prime?

7. Show that if $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ is the prime decomposition of the positive integer n, then the number of positive divisors of n (including 1 and n) is $(e_1+1)(e_2+1)\cdots(e_k+1)$.

8. Which positive integers have exactly three positive divisors?

9. Which positive integers have exactly four positive divisors?

10. Show that a natural number n is an exact square if and only if it has an odd number of positive divisors.

∗11. There are 50 prisoners in a row of locked cells. With the return of the King from the Crusades, a partial amnesty is declared and it works like this. When the prisoners are still asleep, the jailer walks past the cells 50 times, each time walking from left to right. On the first pass, he turns the lock in every cell (so that every cell is now open). On the second pass he turns the lock on every second cell (meaning that these cells are now locked again). On the third pass, he turns the lock on every third cell, and so on. In general, on the kth pass, he turns the lock on every kth cell. The question is: which cells are unlocked at the end of the process so that the prisoner is free to go?

12. Is the following statement true or false? *The number $n^2 + n + 41$ is prime for all positive integers n.*

13. Is the list of prime numbers *finite?* i.e. is there a *largest* prime number?

14. Suppose p is prime.

    (i) Show that if $p \mid a^3$ then $p \mid a$.
    (ii) Show that if $p \mid b$ and $p \mid a^2 + b^2$ then $p \mid a$.

15. Obtain a complete list of primes less than 1000.
[*Hint.* There are 168 of them!]

Answer. Using the *Sieve of Eratosthenes,* the primes less than 1000 are:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, and 997.

If you avoided this problem because you thought it would take too long, note that $32^2 > 1000$; so ... once you have boxed 31 (the 11^{th} prime) all remaining numbers not crossed out must be prime. (So you only need to run through the algorithm 11 times.)