

University of Western Australia
DEPARTMENT OF MATHEMATICS

UWA ACADEMY
FOR YOUNG MATHEMATICIANS

Number Theory I

Greg Gamble

Introduction

Number Theory is principally concerned with properties of the *natural numbers*:

$$\mathbb{N} = \{1, 2, 3, \dots\}.$$

Nevertheless, we will still talk about the *integers*:

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$$

(an *integer* is a *whole number*); and sometimes we will talk about *rational numbers*: \mathbb{Q} , which includes all numbers that can be written as *fractions* (including the integers, e.g. $3 = \frac{3}{1}$), and even the *real numbers*: \mathbb{R} , which includes all the *rational numbers* and lots of other numbers like $\pi, \sqrt{2}, \dots$

In this first session of Number Theory we will be interested in divisibility and prime numbers. In the second half of the session we will discuss *congruences*.

Divisibility

We say a *natural number* a **divides** an *integer* b , if a *divides* “evenly” into b without a remainder. (We can also say this the other way round: “ a *divides* b ” means the same as “ b *is divisible by* a ”.) The above definition is a little vague – so more precisely:

A *natural number* a **divides** an *integer* b if $b = aq$ for some *integer* q .

(That is, we write

$$b = aq + r$$

where r (the *remainder*) is an integer satisfying $0 \leq r < a$) and say a **divides** b , if $r = 0$.) A convenient short-hand way of writing “ a *divides* b ” is:

$$a \mid b.$$

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).

Example 1.

(i) $3 \mid 6$, since $3 \cdot 2 = 6$ and 2 is an integer.

(ii) $3 \nmid 7$, (3 does not divide 7) since $3 \cdot 2 + 1 = 7$, and so 7 has non-zero remainder 1 when divided by 3.

Index laws

This section has been included as a reminder. By definition, if a is any number and n is a natural number then

$$a^n = \underbrace{a \times a \times \cdots \times a}_{n \text{ times}}.$$

Also, if $a \neq 0$ and n is a natural number then, we define

$$a^0 = 1; \text{ and}$$
$$a^{-n} = \frac{1}{a^n}.$$

(If $a = 0$ and n is a natural number then a^0 and a^{-n} are *undefined*.) So, if $a \neq 0$ and m, n are integers then

$$a^m \times a^n = \underbrace{a \times a \times \cdots \times a}_{m \text{ times}} \times \underbrace{a \times a \times \cdots \times a}_{n \text{ times}} = a^{m+n};$$

and

$$(a^m)^n = \underbrace{a^m \times a^m \times \cdots \times a^m}_{n \text{ times}} = a^{\overbrace{m+m+\cdots+m}^{n \text{ times}}} = a^{m \times n}.$$

Example 2.

(i) $(-3)^3 = -3 \times -3 \times -3 = -27;$

(ii) $(-3)^4 = -3 \times -3 \times -3 \times -3 = 81;$

(iii) $-3^4 = -(3 \times 3 \times 3 \times 3) = -81;$

(iv) $2^6 = (2^2)^3 = (2 \times 2) \times (2 \times 2) \times (2 \times 2) = 64.$

Exercise. What are the values of:

(i) $(-1)^7$

(iii) $(-1)^{2k}$

(ii) $(-1)^8$


(iv) $(-1)^{2k+1}$

where k is an integer.

Prime numbers

A *prime number* is usually described as a *natural number* that is only divisible by *itself* and 1. This, however, is not quite precise enough, as this definition would include 1. We regard 1 as quite special: it divides *every* natural number, *any number of times*. Essentially, it is because 1 has this property that we *exclude* 1 from being prime. Thus, by definition:

A natural number n is **prime** if $n > 1$ and its only divisors are n itself and 1.

 Technically, 1 is what we call a *unit*.

A natural number that is neither 1 nor prime is called *composite*. The reason that *primes* are 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*. In the example, we see that 2 divides 74844 *exactly* twice (and not three times, say) and 13 does not divide 74844 at all. If we included 1 as a prime then

$$74844 = 1^5 \cdot 2^2 \cdot 3^5 \cdot 7 \cdot 11,$$

say, would be “another prime decomposition”. To ensure the *prime decomposition* of a natural number could be done in a *unique* (in other words: just one) way mathematicians decided to exclude 1 as a prime. (Mathematicians often contrive definitions to make *theorems* simpler to write down.) The above fact is so important it is given a special name. Let’s give it its name and recap what it says:

Fundamental theorem of arithmetic. Any natural number n , other than 1, can be written uniquely as follows:

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

where k is a natural number, each p_i is a prime number and $1 < p_1 < p_2 < \cdots < p_k$, and each e_i is a natural number.

Another important result is the following:

Fundamental lemma. If a prime p divides a product of integers ab then p must divide at least one of a or b .

How can we decide whether a given, possibly quite large, natural number n is *prime*? Well ... if n is *composite* then $n = ab$ for some natural numbers a, b such that neither a nor b is 1 or n ; and either $a = b = \sqrt{n}$ or one of a or b is less than \sqrt{n} . Thus, to show n is prime we need only show it has no *prime* divisors less than or equal to \sqrt{n} .

Example 3.

(i) 97 is prime, since

- 2, 3, 5, 7 are the primes less than 10;
- $97 < 100$ and $100 = 10^2$ (we don’t need to find square-roots exactly!); and
- none of 2, 3, 5, 7 divides 97.

(ii) The primes less than 100 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.

This is easy to check, because at most we need only check divisibility by 2, 3, 5 and 7. Incidentally, there are 25 of them!

Important polynomial factorisations

Last week we saw that for any number q and any natural number n ,

$$1 - q^n = (1 - q)(1 + q + q^2 + \cdots + q^{n-1}).$$

This one factorisation turns up again and again in mathematics. Let's use it to get some related equations. Replacing q by $-q$ when n is *odd*, gives us a factorisation of $1 + q^n$ when n is *odd*:

$$\begin{aligned} 1 + q^n &= 1 - (-q)^n \\ &= (1 - (-q))(1 + (-q) + (-q)^2 + \cdots + (-q)^{n-1}) \\ &= (1 + q)(1 - q + q^2 - \cdots + q^{n-1}). \end{aligned}$$

Writing $q = b/a$, where $a \neq 0$, and then multiplying by a^n gives some more familiar factorisations:

$$\begin{aligned} a^n - b^n &= a^n(1 - (b/a)^n) \\ &= a(1 - (b/a)) \cdot a^{n-1}(1 + (b/a) + (b/a)^2 + \cdots + (b/a)^{n-1}) \\ &= (a - b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + b^{n-1}). \end{aligned}$$

Similarly, if n is *odd* then

$$a^n + b^n = (a + b)(a^{n-1} - a^{n-2}b + a^{n-3}b^2 - \cdots + b^{n-1}).$$

Notice, that the factorisations of $a^n - b^n$ and $a^n + b^n$ are still valid when $a = 0$ – so the restriction $a \neq 0$ can be lifted. Let's write down these factorisations explicitly for the cases $n = 2$ and $n = 3$:

$$\begin{aligned} a^2 - b^2 &= (a - b)(a + b) \\ a^3 - b^3 &= (a - b)(a^2 + ab + b^2) \\ a^3 + b^3 &= (a + b)(a^2 - ab + b^2) \end{aligned}$$

Congruence modulo m

Suppose $m \in \mathbb{N}$. Then for two integers a, b we say:

$$\begin{aligned} &a \text{ is congruent to } b \text{ modulo } m \\ &(\text{written: } a \equiv b \pmod{m}) \end{aligned}$$

if and only if

$$\begin{aligned} &a \text{ and } b \text{ give the same } \textit{remainder} \text{ on division by } m, \\ &(\text{in which case: } m \mid a - b). \end{aligned}$$

The reason that \equiv looks so much like $=$, is that it behaves very much like $=$ does between integers. In particular, *congruence* modulo m has the following properties.

- if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$.



This property is called *transitivity*.

- if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then

$$a + c \equiv b + d \pmod{m}$$

$$a \cdot c \equiv b \cdot d \pmod{m}$$

- if $a \equiv b \pmod{m}$ and n is a natural number then

$$a^n \equiv b^n \pmod{m}.$$

This follows from the previous (multiplication) property, since, if $a \equiv b \pmod{m}$ then

$$a^n \equiv a \cdot a \cdots a \pmod{m}$$

$$\equiv b \cdot b \cdots b \pmod{m}$$

$$\equiv b^n \pmod{m}$$



Also like = the problem: $ax \equiv b \pmod{m}$ where a, b are *known* integers and x is the *unknown*, need not have solutions for x .

Example 4.

- (i) $6 \equiv 1 \pmod{5}$ and $11 \equiv 1 \pmod{5}$. So $6 \equiv 11 \pmod{5}$. In fact, the integers n such that $n \equiv 1 \pmod{5}$ are precisely those integers that can be written in the form:

$$5k + 1$$

for some integer k . In fact, if k is an integer then

$$n = 5k \quad \text{if and only if} \quad n \equiv 0 \pmod{5}$$

$$n = 5k + 1 \quad \text{if and only if} \quad n \equiv 1 \pmod{5}$$

$$n = 5k + 2 \quad \text{if and only if} \quad n \equiv 2 \pmod{5}$$

$$n = 5k + 3 \quad \text{if and only if} \quad n \equiv 3 \pmod{5}$$

$$n = 5k + 4 \quad \text{if and only if} \quad n \equiv 4 \pmod{5}$$

- (ii) $7 \equiv 1 \pmod{6}$ and $231 \equiv 3 \pmod{6}$. So

$$7 + 231 \equiv 1 + 3 \pmod{6}$$

$$\equiv 4 \pmod{6}; \text{ and}$$

$$7 \cdot 231 \equiv 1 \cdot 3 \pmod{6}$$

$$\equiv 3 \pmod{6}.$$