

University of Western Australia  
DEPARTMENT OF MATHEMATICS  
**UWA ACADEMY  
FOR YOUNG MATHEMATICIANS**

Number **Theory I**

Greg Gamble

May 24, 1997

Number Theory is mainly concerned with properties of the *natural numbers* (or *positive integers*):

$$\mathbb{N} = \mathbb{Z}^+ = \{1, 2, 3, \dots\}$$

and more generally with the *integers*:

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

## Divisibility

If  $a, b \in \mathbb{Z}$  we say:  $a$  *divides*  $b$ , and write:  $a \mid b$ , if  $b = aq$  for some integer  $q$ . Otherwise,  $a$  *does not divide*  $b$  and we write:  $a \nmid b$ . For example,


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

but

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

If  $a \mid b$  then we also say:  $a$  is a *divisor* (or *factor*) of  $b$ , or that:  $b$  is a *multiple* of  $a$ . For example, if  $b = 12$  then the divisors (factors) of  $b$  are

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

 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:  $\mid$  the symbol cannot be used in reverse, i.e.  $a \mid b$  and  $b \mid a$  mean *different* things (in fact, if they are *both* true then  $a = \pm b$ ).

**Property 1.** If  $a \mid b$  and  $a \mid c$  then  $a \mid bx + cy$  for any integers  $x, y$ .

**Proof.** Suppose  $a \mid b$  and  $a \mid c$ . Then  $b = aq$  and  $c = ar$  for some integers  $q, r$ . So, for any integers  $x, y$ ,

$$bx + cy = a(qx + ry)$$

and  $qx + ry$  is an integer, and hence  $a \mid bx + cy$ . □


## Summary of divisibility terms

Summarising the above statements, all the following say the same thing about integers  $a, b$  where  $a \neq 0$ .

- $a$  divides  $b$ .
- $a \mid b$ .
- $a$  is a *divisor* of  $b$ .
- $a$  is a *factor* of  $b$ .
- $b = aq$  for some integer  $q$ .
- $b/a$  is an integer.
- $b$  is *divisible* by  $a$ .
- $b$  is a *multiple* of  $a$ .

## Prime numbers


A *prime number* is a *natural number* larger than 1 that is only divisible by *itself* and 1. A *natural number* that is neither 1 nor prime is called *composite*.

 Notice that 1 is neither *prime* nor *composite*. In fact, 1 is called a *unit* (the technical term for a number that divides all integers).

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*.

 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:

**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.

A fundamental property of *primes* is expressed in the following result:

**Euclid’s Lemma.** If a prime  $p$  divides  $ab$  then  $p \mid a$  or  $p \mid b$ .

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 1.** *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.

**Remark.** *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!*

## Greatest common divisor

The *greatest common divisor* (or *highest common factor*) of two integers  $a, b$ , denoted by  $\gcd(a, b)$  or  $\text{hcf}(a, b)$  or simply  $(a, b)$ , is the largest natural number that divides both  $a$  and  $b$ . (Here we must insist that  $a$  and  $b$  are not both zero.)

◊ If  $(a, b) = 1$  then  $a, b$  are said to be *relatively prime* or *coprime*.

You may be familiar with an algorithm for finding the gcd of two integers  $a, b$  which involves first finding the *prime decompositions* of  $a, b$ . While this procedure works well when  $a, b$  are small (particularly, if both  $a$  and  $b$  are smaller than 100, say), it is quite *inefficient* if  $a, b$  are large; since, in general, finding *prime decompositions* is difficult.

◊ The difficulty of finding *prime decompositions* is exploited in many *encryption* algorithms.

Below, we will see a method for finding *greatest common divisors* that doesn't require finding *prime decompositions*. The method requires application of the *Division Algorithm* (usually, several times) which we now describe.

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

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

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

$$\begin{array}{r} q \text{ rem. } r \\ a \overline{) b} \end{array}$$

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

- if  $a = 7$  and  $b = 22$  we write  $22 = 7 \cdot 3 + 1$  (so  $q = 3$  and  $r = 1$ );
- if  $a = 113$  and  $b = 355$  we write  $355 = 113 \cdot 3 + 16$  (so  $q = 3$  and  $r = 16$ );
- if  $a = 8$  and  $b = 72$  we write  $72 = 8 \cdot 9 + 0$  (so  $q = 9$  and  $r = 0$ ).

◊ Observe that  $r = 0$  precisely when  $a \mid b$ ; and that  $r > 0$  if  $a \nmid b$ .

The *greatest common divisor*  $d$  of two integers  $a, b$  has three interesting properties:

- $d$  also divides  $a - bm$  for any integer  $m$ ;
- $d = (a - bm, b)$  for any integer  $m$ ;
- there are integers  $x, y$  such that  $d = ax + by$ .

The first of these properties follows immediately from Property 1. The second property is the basis of the *Euclidean algorithm* method for finding the *greatest common divisor*  $d$  of two integers  $a, b$ , which is demonstrated below. The third property follows from retracing the steps of the *Euclidean algorithm*.

**Example 2.** To find the gcd of 234 and 180, perform the following steps.

1. Draw 3 parallel vertical lines.
2. Write 234 and 180 in the two internal columns.
3. Divide the smaller number 180 into the larger 234. Write the quotient in the column adjacent to 234, and the remainder below 234.
4. Repeatedly divide back and forth in a similar way to Step 3. until one number divides (evenly) into the other. At this point that number is the gcd.

$$1 \left| \begin{array}{c|c} 234 & 180 \\ \hline 180 & 162 \\ \hline 54 & 18 \end{array} \right| 3$$

Here 180 was divided into 234, it went once remainder 54; then 54 was divided into 180, it went 3 times remainder 18; and 18 divides 54 (so we stop) ... and so 18 is the gcd of 234 and 180.

Working backwards we can also find  $x, y$  such that  $234x + 180y = 18$ :

$$\begin{aligned} 18 &= 180 - 162 \\ &= 180 - 3 \cdot 54 \\ &= 180 - 3(234 - 1 \cdot 180) \\ &= 4 \cdot 180 - 3 \cdot 234. \end{aligned}$$

So  $x = 4$  and  $y = -3$  is one possibility. All pairs  $x, y$  satisfy

$$\begin{aligned} x &= 4 + 13t \\ y &= -3 - 10t \end{aligned}$$

for some integer  $t$ .



To see the existence of other pairs  $x, y$  satisfying  $234x + 180y = 18$ , observe that

$$\begin{aligned} 18 &= 4 \cdot 180 - 3 \cdot 234 \\ &= 4 \cdot 180 - 3 \cdot 234 + \left( \frac{234 \cdot 180}{18} \right) t - \left( \frac{234 \cdot 180}{18} \right) t \\ &= \left( 4 + \frac{234}{18} t \right) \cdot 180 + \left( -3 - \frac{180}{18} t \right) \cdot 234 \\ &= (4 + 13t) \cdot 180 + (-3 - 10t) \cdot 234. \end{aligned}$$

## Diophantine equations

We have just seen that if  $d = (a, b)$  then we can use the *Euclidean Algorithm* to find integers  $x, y$  that satisfy

$$ax + by = d.$$

What if the right-hand side of the above equation is not  $d$ ? i.e. can we still solve

$$ax + by = c$$

for  $x, y$  when  $c \neq d$ ? The question is answered by the theorem, below.

⚡ Equations of the form:  $ax + by = c$  are examples of *Diophantine Equations* (after Diophantus, an ancient Greek who was the first known to study them).

We will need the following lemma to prove the theorem.

**Lemma.** *If  $\alpha, \beta$  are non-zero relatively prime integers then all integer solutions of  $\alpha X + \beta Y = 0$  for  $X, Y$  are of form*

$$\begin{aligned} X &= \beta t, \\ Y &= -\alpha t, \end{aligned}$$

where  $t \in \mathbb{Z}$ .

**Proof.** Assume  $\alpha, \beta \in \mathbb{Z}$ ,  $\alpha, \beta \neq 0$  and  $(\alpha, \beta) = 1$ . Rearranging  $\alpha X + \beta Y = 0$ , we obtain

$$\beta Y = -\alpha X.$$

So  $\beta \mid -\alpha X$ , and since  $(\alpha, \beta) = 1$  we must have  $\beta \mid X$ , i.e.  $X = \beta t$  for some integer  $t$ , whence  $Y = -\alpha t$ .  $\square$

**Theorem.** *Let  $a, b, c \in \mathbb{Z}$  with  $a, b$  not both zero, and suppose  $d = (a, b)$ . Then  $ax + by = c$  has a solution for  $x, y$  if and only if  $d \mid c$ .*

*Moreover, if  $a, b$  are both non-zero,  $d \mid c$ , and  $x_0, y_0$  is one solution of  $ax + by = c$  then all possible solution pairs are of form*

$$\begin{aligned} x &= x_0 + \beta t \\ y &= y_0 - \alpha t \end{aligned}$$

where  $\alpha = a/d$ ,  $\beta = b/d$  and  $t \in \mathbb{Z}$ . (A 'starting solution'  $x_0, y_0$  is

$$\begin{aligned} x_0 &= x'q \\ y_0 &= y'q \end{aligned}$$

where  $q = c/d$  and  $x', y'$  is a solution of  $ax + by = d$  and may be obtained by applying the *Euclidean Algorithm* to  $a, b$ .)

**Proof.** If there is a solution then  $ax + by = c$  for some integers  $x, y$ . Now  $d \mid a$  and  $d \mid b$ , so  $d \mid ax + by = c$  by Property 1.

Now we prove the converse direction. Suppose  $d \mid c$  (so that  $c = dq$  for some integer  $q$ ). From the Euclidean Algorithm we can find integers  $x', y'$  such that

$$ax' + by' = d.$$

Hence

$$a \cdot x'q + b \cdot y'q = dq = c.$$

That is, a solution of  $ax + by = c$  exists (since  $x_0 = x'q, y_0 = y'q$  is a solution).

Now let us find the general solution when solutions exist. Suppose  $x, y$  is a solution. Then we have

$$\begin{aligned} ax + by &= c \\ ax_0 + by_0 &= c, \end{aligned}$$

whence on subtracting the equations we obtain

$$a(x - x_0) + b(y - y_0) = 0,$$


and on dividing by  $d$ , we get

$$\alpha(x - x_0) + \beta(y - y_0) = 0,$$

where  $\alpha = a/d, \beta = b/d$  and we have  $\alpha, \beta$  relatively prime and both non-zero. So by the lemma the general solution for  $x - x_0, y - y_0$  is given by

$$\begin{aligned} x - x_0 &= \beta t, \\ y - y_0 &= -\alpha t, \end{aligned}$$

where  $t \in \mathbb{Z}$ , which on rearranging gives the general solution stated in the theorem. □

 When giving the general solution in the case where  $d \mid c$ , the theorem required that both  $a, b$  be non-zero . . . but if one checks the given solutions still work if one or other of  $a, b$  is zero. So why include the restriction? . . . The trouble is there are *other* solutions, e.g. suppose  $b = 0$ , i.e. we wish to solve  $ax + 0 \cdot y = c$  where  $d = a \mid c$ . Then the solution for  $x$  is correct but notice it is just a complicated way of writing  $x = c/a$ , but  $y$  is allowed to be *any* integer (whereas the solution ‘suggests’ some integers don’t work . . . depending on what choice you take for  $y_0$ ).