

MATHEMATICAL OLYMPIADS LECTURE NOTES

Divisibility

Greg Gamble

Divisibility is primarily a concept from *Number Theory*. Number Theory is principally concerned with properties of the *natural numbers*:

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

and sometimes the *integers*:

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

(Recall that an *integer* is a *whole number*.) Suppose we attempt to *divide* a natural number a into an integer b :

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

so that:

$$a \text{ goes into } b, q \text{ times and leaves a remainder of } r.$$

In other words,

$$b = a \times q + r.$$

The number q is called the *quotient* of the division and r is called the *remainder*, (the bit that is left over). If you think about this you will see that the *remainder* r ought to be smaller than a , i.e.

$$0 \leq r < a.$$

⚡ Since we are not allowing fractions here this sort of division is sometimes called *integer division*.

⊥ If after dividing b by a the *remainder* is 0, i.e. if a *divides* “evenly” into b without a remainder then we say:

$$a \text{ divides } b.$$

You might find it convenient to abbreviate this to:

$$a \mid b.$$

(Actually, the **standard** abbreviation is: $a \mid b$. However, students are sometimes confused by it – see the double dangerous bend below.)

⚡ The *divides* symbol \mid is supposed to remind you of the $)$ of a short or long division.

⊥ We often say this the other way round, i.e. instead of “ a divides b ” we say:

$$b \text{ is divisible by } a.$$


or

$$b \text{ is a multiple of } a.$$

In symbols we will write this:

$$b \mid a.$$

⚡ The *is divisible by* symbol \mid is a mirror reflection of the *divides* symbol \mid , ... just like $>$ is a mirror reflection of $<$. [Note that: $a > b$ means the same as $b < a$.]


 Actually, in the literature there is **no** symbol for *is divisible by* and the symbol for *divides* is \mid (which is a *vertical* stroke with a little space around it) but this symbol is too easily confused with the *slash* symbol: $/$ (that separates the numerator and denominator of a fraction) and it doesn't have a mirror reflection different from itself.

If the *remainder* is not 0 when we perform an *integer division* of b by a then we write:


$$a \nmid b$$

[**a does not divide b**]

or

$$b \not\mid a$$

[**b is not divisible by a**]


 When a *natural number* a **divides** b , the number a is called a **divisor** of b , and b is called a **multiple** of a . So all of the following mean the same thing, where a is a *natural number* and b is an *integer*:

- a divides b .
- $a \mid b$.
- a is a *divisor* of b .
- b is divisible by a .
- $b \mid a$.
- b is a *multiple* of a .

Some theorems

We would like to prove the following theorem.

Theorem 1. *Let $a + b = n$. Then a, b are coprime if and only if a, n are coprime.*

Recall that two integers a, b are *coprime* if their *greatest common divisor* is 1, (i.e. they do *not* share any common *prime* divisors). Now this follows immediately from a few very simple little theorems, we will call lemmas. Always d is a natural number and a, b, n etc. are integers.

Lemma 2. *If $d \mid a$ and $d \mid b$ then $d \mid a + b$.*

Proof. Suppose $d \mid a$ and $d \mid b$. Then

$$\begin{aligned}
 d \mid a & \text{ means } a = dk \text{ for some integer } k; \text{ and} \\
 d \mid b & \text{ means } b = d\ell \text{ for some integer } \ell.
 \end{aligned}$$

$$\begin{aligned}
 \text{So } \dots a + b &= d(k + \ell) \\
 &= dm \text{ for some integer } m = k + \ell.
 \end{aligned}$$

i.e. $d \mid a + b$. □

Lemma 3. If $d \mid b$ then $d \mid -b$.

Proof. Suppose $d \mid b$. Then $b = d\ell$ for some integer ℓ .
Hence $-b = d(-\ell)$ for some integer $-\ell$.
i.e. $d \mid -b$. □

Now, Lemma 2 is true for any integer b . So it is true in the case where b is replaced by $-b$, i.e.

If $d \mid -b$ then $d \mid b$.

So, in fact, we have:

Lemma 4. $d \mid b$ if and only if $d \mid -b$.

This means whenever we see the condition: “ $d \mid -b$ ” in a theorem we will be able to substitute “ $d \mid b$ ”. Going back to Lemma 1, we see that its meaning is unchanged if it is written as follows.

Lemma 5. Let $d \mid a$. If $d \mid b$ then $d \mid a + b$.

Also, this statement is still true if we replace b by $-(a + b)$, i.e.

Let $d \mid a$. If $d \mid -(a + b)$ then $d \mid -b$.

Now, using Lemma 3 twice, we can replace the condition: “ $d \mid -(a + b)$ ” by “ $d \mid a + b$ ”, and the condition: “ $d \mid -b$ ” by “ $d \mid b$ ”, i.e.

Let $d \mid a$. If $d \mid a + b$ then $d \mid b$.

Thus we have

Lemma 6. Let $d \mid a$. Then $d \mid b$ if and only if $d \mid a + b$.

So choosing d to be as big as it can be, i.e. choosing d to be the *greatest common divisor* of a and b , we get ...

Lemma 7. $\gcd(a, b) = \gcd(a, a + b)$.

... from which it follows that ...

Corollary 8. $\gcd(a, b) = 1$ if and only if $\gcd(a, a + b) = 1$.

This last corollary if you look closely is in fact Theorem 1.

Now all of the above could have been done in a lot less space. The purpose of doing it the way we did was to show how one can extend a few very simple ideas using almost *mindless* steps to go quite a long way.