Queen Mary University of London

MTH4104 **Introduction to Algebra**

Greatest common divisors via prime factorisation **Spring 2022**

How does one find the greatest common divisor of two nonnegative integers? Consider, for example, 8633 and 9167. Finding the gcd looks like a difficult job. But, if you know that $8633 = 89 \cdot 97$ and $9167 = 89 \cdot 103$, and that all the factors are prime, you can easily see that $\gcd(8633, 9167) = 89$.

Here is how this procedure works in general. We first recall a theorem on prime factorisation. In the theorem I have grouped repeats of the same prime together with exponents: that is, instead of writing factorisations like $12 = 2 \cdot 2 \cdot 3$, I write $12 = 2^2 \cdot 3^1$. This makes the Proposition that follows the Theorem easier to write down.

Theorem (Fundamental Theorem of Arithmetic)**.** *Every positive integer n can be written as a product*

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

where $p_1, \ldots, p_k$ are different prime numbers and $e_1, \ldots, e_k$ are positive integers. This expression is unique up to reordering of the factors.

- "Up to X", in mathematical prose, means that we are counting two things (in this case factorisations) to be the same if their only difference is X (in this case reordering). This makes sure we don't count 89×97 and 97×89 as different factorisations.
- What is the factorisation of the number 1? It's the *empty* product, where $k = 0$ and there are no factors. The product of no numbers is 1.

We can insert extra primes into the factorisation provided by the Fundamental Theorem of Arithmetic, as long as we give them the exponent 0. This is helpful when we want to compare multiple factorisations:

$$\begin{aligned} 8633 &= 89^1 \cdot 97^1 \cdot 103^0 \text{ and} \\ 9167 &= 89^1 \cdot 97^0 \cdot 103^1 \text{ have gcd} \\ 89 &= 89^1 \cdot 97^0 \cdot 103^0. \end{aligned}$$

The following theorem supposes that we have done this, so that the same list of primes appears for two given integers.

Proposition. *Let a and b be positive integers, with factorisations $a = p_1^{e_1} \cdots p_k^{e_k}$ and $b = p_1^{f_1} \cdots p_k^{f_k}$.*

(a) $a \mid b$ if and only if $e_i \leq f_i$ for every $i = 1, \ldots, k$.

(b)

$$\gcd(a, b) = p_1^{\min(e_1, f_1)} \cdots p_k^{\min(e_k, f_k)}.$$

Proof. To (i). Suppose $a \mid b$, so that there is an integer c such that $b = ac$. Because a and b are positive, c must also be. Therefore c has a prime factorisation, say $c = p_1^{g_1} \cdots p_k^{g_k}$. (Again, we may throw these primes into the earlier lists with their exponents set to 0, so that we can use the same list of primes every time.) It follows by laws of exponents that

$$p_1^{f_1} \cdots p_k^{f_k} = b = ac = p_1^{e_1+g_1} \cdots p_k^{e_k+g_k}.$$

Because of the uniqueness part of the Fundamental Theorem of Arithmetic, the left and right hand sides of this equation must be the same factorisation, implying that $f_i = e_i + g_i$ for every $i = 1, \ldots, k$. Therefore $e_i \leq e_i + g_i = f_i$ for every such i.

Conversely, suppose that $e_i \leq f_i$ for every i. Since a is not zero, b/a is a rational number, and we can test whether a divides b by testing whether it is an integer. By the laws of exponents,

$$\frac{b}{a} = \frac{p_1^{f_1} \cdots p_k^{f_k}}{p_1^{e_1} \cdots p_k^{e_k}} = \frac{p_1^{f_1}}{p_1^{e_1}} \cdots \frac{p_k^{f_k}}{p_k^{e_k}} = p_1^{f_1-e_1} \cdots p_k^{f_k-e_k}.$$

If $e_i \leq f_i$ for each i, then all of the exponents on the right hand side are greater than or equal to 0, which means the right hand side is an integer, since it is a product of integers (primes, with possible repetitions).

To (ii). By part (i), an integer d is a divisor of a if and only if its factorisation is $d = p_1^{g_1} \cdots p_k^{g_k}$, where $g_i \leq e_i$ for each i (and primes that don't divide a don't appear in d either). Since the same is true with b and f_i in place of a and e_i, we see that d is a common divisor of a and b if and only if $g_i \leq e_i$ and $g_i \leq f_i$ for each i. This gives two different upper bounds on g_i. Whichever one is greater is redundant, so it is equivalent to keep only the lesser of the two, and require that $g_i \leq \min(e_i, f_i)$. Finally, to find the greatest of the common divisors d we can maximise all of these exponents independently. Therefore the gcd is $d = p_1^{g_1} \cdots p_k^{g_k}$, where each $g_i = \min(e_i, f_i)$ attains its upper bound. □