Greatest common divisor as a product of primes

Clive Newstead, 18th March 2014

The Fundamental Theorem of Arithmetic (FTA) is all about products of primes: it tells you that every natural number greater than 1 has a representation as a product of primes, and moreover that expression is unique up to reordering. We can use this to find an expression of the greatest common divisor of two natural numbers by looking at their prime factorisation.

Let $a, b \in \mathbb{N}$ and let $p_1, p_2, \ldots, p_n$ be a list of prime numbers exhausting all the primes that appear in the factorisations of a and b. (Note that if $a = 1$ or $b = 1$ then there are no primes in their prime factorisations, but that's okay because raising a natural number to the power 0 gives 1.) We can then write

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$$
$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$$

where $\alpha_i, \beta_i \geqslant 0$ for all $1 \leqslant i \leqslant n$. (We need to allow them to be zero in case one of the primes appears in the factorisation of a but not b, for example.)

For $1 \leqslant i \leqslant n$ write $\delta_i = \min\{\alpha_i, \beta_i\}$.

Theorem. Given natural numbers a, b as above,

$$\gcd(a, b) = p_1^{\delta_1} p_2^{\delta_2} \cdots p_n^{\delta_n}$$

That is, the gcd can be calculated by raising all the prime factors that appear in the factorisations of a and b to the smallest power that appears.

Proof. Let $G = \gcd(a, b)$ and $P = p_1^{\delta_1} p_2^{\delta_2} \cdots p_n^{\delta_n}$. We'll prove $P \leqslant G$ and $G \leqslant P$ separately; together these will imply that $P = G$, and then we'll be done.

First we prove $P \leqslant G$. Since $\delta_i \leqslant \alpha_i$ and $\delta_i \leqslant \beta_i$, we can write $\alpha_i = \delta_i + k_i$ and $\beta_i = \delta_i + \ell_i$ for some $k_i, \ell_i \geqslant 0$. Hence

$$\begin{aligned}
a &= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} && \text{(prime factorisation)} \\
&= p_1^{\delta_1 + k_1} p_2^{\delta_2 + k_2} \cdots p_n^{\delta_n + k_n} && \text{(since } \alpha_i = \delta_i + k_i\text{)} \\
&= (p_1^{\delta_1} p_1^{k_1}) \cdot (p_2^{\delta_2} p_2^{k_2}) \cdots (p_n^{\delta_n} p_n^{k_n}) && \text{(properties of indices)} \\
&= (p_1^{\delta_1} p_2^{\delta_2} \cdots p_n^{\delta_n}) \cdot (p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}) && \text{(re-ordering the factors)} \\
&= P \cdot (p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}) && \text{(definition of } P\text{)}
\end{aligned}$$

Since $p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n} \in \mathbb{Z}$, we can deduce that $P \mid a$. Similarly we have

$$b = P \cdot p_1^{\ell_1} p_2^{\ell_2} \cdots p_n^{\ell_n}$$

and so $P \mid b$. Thus P is a common divisor of a and b. By definition of the gcd, $P \leqslant G$.

It remains to show $G \leqslant P$. We'll do this by first showing that $G \mid P$. Since $G, P \in \mathbb{N}$, the fact that $G \leqslant P$ will follow from Proposition 1(iv) in the lecture notes.

We can write $G = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_n^{\lambda_n} k$, where $\lambda_i \geqslant 0$ for all $1 \leqslant i \leqslant n$ and $k \in \mathbb{N}$, such that none of the p_i divide k. (That is, we've just taken the prime factorisation of G, and clustered together all the primes not amongst the p_is and called this number k.) We'll prove:

(1) $k = 1$. Then we'll just have $G = p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_n^{\lambda_n}$.

(2) $\lambda_i \leqslant \delta_i$ for all $1 \leqslant i \leqslant n$. Then we'll have $G \mid P$ (for the same reason as $P \mid a$ above).

We prove (1) and (2) by contradiction.

For (1), suppose $k \neq 1$. Then $k > 1$, so it has a prime factor by FTA, say q. By definition of k, $q \neq p_i$ for any i, because we specified that none of the p_is divide k. But $q \mid G$, and we know that $G \mid a$ since $G = \gcd(a, b)$, so by Proposition 1(i), $q \mid a$. By FTA, q appears in the prime factorisation of a, so $q = p_i$ for some i. But this contradicts our assumption that $q \neq p_i$ for any i. We conclude that $k = 1$.

For (2), suppose $\lambda_i > \delta_i$ for some i. Without loss of generality, $i = 1$ (otherwise just re-label the prime factors). Since $\delta_1 = \min\{\alpha_1, \beta_1\}$, we must have $\delta_1 = \alpha_1$ or $\delta_1 = \beta_1$. Without loss of generality, suppose $\delta_1 = \alpha_1$. (The case $\delta_1 = \beta_1$ is identical.) Then $\lambda_1 > \alpha_1$. Now $G \mid a$, so there exists $s \in \mathbb{N}$ such that $sG = a$. Looking at the prime factorisations, we have:

$$s \cdot p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_n^{\lambda_n} = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$$

Dividing by $p_1^{\alpha_1}$ gives, using laws of indices, that

$$s \cdot p_1^{\lambda_1 - \alpha_1} p_2^{\lambda_2} \cdots p_n^{\lambda_n} = p_1^{\alpha_1 - \alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$$

which, noticing that $p_1^{\alpha_1 - \alpha_1} = p_1^0 = 1$, can be rewritten as

$$s \cdot p_1^{\lambda_1 - \alpha_1} p_2^{\lambda_2} \cdots p_n^{\lambda_n} = p_2^{\alpha_2} \cdots p_n^{\alpha_n}$$

Since $\lambda_1 > \alpha_1$, we have $\lambda_1 - \alpha_1 > 0$, so p_1 divides the left-hand side of this equation. Hence p_1 divides the right-hand side. But by FTA, if p_1 divides the right-hand side then it would appear in the factorisation... so we have a contradiction! We conclude that $\lambda_i \leqslant \delta_i$ for all $1 \leqslant i \leqslant n$.

As mentioned above, this implies that $G \mid P$, and hence $G \leqslant P$ by Proposition 1(iv).

Since $G \leqslant P$ and $P \leqslant G$, we have $P = G$ by antisymmtery of $\leqslant$, and we're done. $\square$