New Zealand Mathematical Olympiad Committee

The Euclidean Algorithm

Arkadii Slinko

1 Introduction

These notes, the second in a series of tutorials on number theory, describe the Euclidean algorithm for finding the greatest common divisor of two integers.

2 The number of divisors of n

Let n be a positive integer with the prime factorisation

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}, \tag{1}$$

where p_i are distinct primes and α_i are positive integers. How can we find all divisors of n? Let d be a divisor of n. Then $n = dm$, for some m, thus

$$n = dm = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}.$$

Since the prime factorisation of n is unique, all the prime factors of d are among the primes $p_1, p_2, \dots, p_r$. Also, a prime p_i in the prime factorisation of d cannot have an exponent greater than α_i. Therefore

$$d = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}, \qquad 0 \le \beta_i \le \alpha_i, \qquad i = 1, 2, \dots, r. \tag{2}$$

Theorem 1. *The number of positive divisors of n is*

$$d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_r + 1). \tag{3}$$

Proof. Indeed, we have exactly $\alpha_i + 1$ possibilities to choose β_i in (2), namely $0, 1, 2, \dots, \alpha_i$. Thus the total number of divisors will be exactly the product $(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_r + 1)$. □

The numbers kn, where $k = 0, \pm 1, \pm 2, \dots$, are called *multiples of n*. It is clear that any multiple of n given by (1) has the form

$$m = k p_1^{\gamma_1} p_2^{\gamma_2} \dots p_r^{\gamma_r}, \qquad \gamma_i \ge \alpha_i, \qquad i = 1, 2, \dots, r,$$

where k has none of the primes $p_1, p_2, \dots, p_r$ in its prime factorisation. The number of multiples of n is infinite.

3 Greatest common divisor and least common multiple

Let a and b be two positive integers. If d is a divisor of a and also a divisor of b, then we say that d is a common divisor of a and b. As there are only a finite number of common divisors, there is a *greatest common divisor*, denoted by $\gcd(a, b)$. The number m is said to be a common multiple of a and b if m is a multiple of a and also a multiple of b. Among all common multiples there is a minimal one (by the Least-Integer Principle!). It is called the *least common multiple* and it is denoted by $\operatorname{lcm}(a, b)$.

In the decomposition (1) we had all exponents positive. However, sometimes it is convenient to allow some exponents to be 0. This is especially convenient when we are considering prime factorisations of two numbers a and b, looking for $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$, since we may assume that both a and b have the same set of primes in their prime factorisations.

Theorem 2. *Let*

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}, \qquad b = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r},$$

where $\alpha_i \geq 0$ and $\beta_i \geq 0$, be two arbitrary positive integers. Then

$$\gcd(a,b) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \dots p_r^{\min(\alpha_r,\beta_r)}, \tag{4}$$

and

$$\operatorname{lcm}(a,b) = p_1^{\max(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)} \dots p_r^{\max(\alpha_r,\beta_r)}. \tag{5}$$

Moreover,

$$\gcd(a,b) \cdot \operatorname{lcm}(a,b) = a \cdot b. \tag{6}$$

Proof. Formulas (4) and (5) follow from our description of common divisors and common multiples. To prove (6) we have to notice that $\min(\alpha_i,\beta_i) + \max(\alpha_i,\beta_i) = \alpha_i + \beta_i$. □

It is suspected (in fact it is an open question) that prime factorisation is computationally difficult. No easy algorithms for it are known. Fortunately, the greatest common divisor $\gcd(a,b)$ of numbers a and b can be found without knowing the prime factorisations for a and b. This algorithm was known to Euclid – it is even possible that he discovered it.

Theorem 3 (Euclidean Algorithm). *Let a and b be positive integers. Suppose we use the division algorithm several times to find:*

$$\begin{array}{lcll} a & = & q_1 b + r_1, & 0 < r_1 < b, \\ b & = & q_2 r_1 + r_2, & 0 < r_2 < r_1, \\ r_1 & = & q_3 r_2 + r_3, & 0 < r_3 < r_2, \\ \vdots & & & \\ r_{s-2} & = & q_s r_{s-1} + r_s, & 0 < r_s < r_{s-1}, \\ r_{s-1} & = & q_{s+1} r_s, & \end{array}$$

that is, halting when r_{s+1} reaches 0. (Which must eventually happen. For if not, then we can continue the algorithm forever, obtaining $b > r_1 > r_2 > \cdots > 0$, which contradicts the Least-Integer Principle.)

Then $r_s = \gcd(a,b)$.

Proof. The key observation is that if $a = qb + r$, then $\gcd(a,b) = \gcd(b,r)$. Indeed, if d is a common divisor of a and b, then $a = a'd$ and $b = b'd$ and then $r = a - qb = a'd - qb'd = (a' - qb')d$ and d is also a common divisor of b and r. Conversely, if d is a common divisor of b and r, then $b = b'd$, $r = r'd$ and $a = qb + r = qb'd + r'd = (qb' + r')d$, whence d is a common divisor of a and b.

Proceeding inductively down the table, it is clear that

$$\gcd(a,b) = \gcd(b,r_1) = \gcd(r_1,r_2) = \ldots = \gcd(r_{s-1},r_s) = r_s.$$

□

Theorem 4 (Extended Euclidean Algorithm). *Draw up the following table, with two rows R_1, R_2:*

$$\begin{pmatrix} a & 1 & 0 \\ b & 0 & 1 \end{pmatrix}.$$

Perform the Euclidean algorithm on a and b, and simultaneously construct rows of this table, as follows: First we create the third row R_3 by subtracting from the first row the second row times q_1; that is,

$$R_3 := R_1 - q_1 R_2.$$

In general, create R_k, for any $k \leq s$, by taking R_{k-2} and subtracting R_{k-1} times q_{k-2}; that is,

$$R_k := R_{k-2} - q_{k-2} R_{k-1}.$$

Suppose the table we eventually obtain is

$$\begin{pmatrix} a & 1 & 0 \\ b & 0 & 1 \\ r_1 & 1 & -q_1 \\ r_2 & -q_2 & 1+q_1q_2 \\ & \vdots & \\ r_s & m & n \end{pmatrix};$$

Then $\gcd(a,b) = r_s = am + bn$.

Proof. We will prove this by induction. Let the integers in the k-th row of the table be

$$R_k = (u_k, v_k, w_k).$$

Certainly $u_1 = av_1 + bw_1$ and $u_2 = av_2 + bw_2$.

Suppose that for some $k < s$, for all $i \leq k-1$, $u_i = av_i + bw_i$. Then

$$\begin{aligned} u_k &= u_{k-2} - q_k u_{k-1} \\ &= av_{k-2} + bw_{k-2} - q_k(av_{k-1} + bw_{k-1}) \\ &= a(v_{k-2} - q_k v_{k-1}) + b(w_{k-2} - q_k w_{k-1}) \\ &= av_k + bw_k. \end{aligned}$$

Thus for all $i \leq k$, $u_i = av_i + bw_i$.

It follows by induction that for all $i \leq s$, $u_i = av_i + bw_i$. In particular, this is true for the last row, which gives us $r_s = am + bn$. □

Example 1. Let $a = 321$, $b = 843$. Find the greatest common divisor $\gcd(a,b)$, the least common multiple $\operatorname{lcm}(a,b)$, and a linear presentation of the greatest common divisor in the form $\gcd(a,b) = ka + mb$.

Solution: The Euclidean algorithm gives:

$$\begin{aligned} 321 &= 0 \cdot 843 + 321 \\ 843 &= 2 \cdot 321 + 201 \\ 321 &= 1 \cdot 201 + 120 \\ 201 &= 1 \cdot 120 + 81 \\ 120 &= 1 \cdot 81 + 39 \\ 81 &= 2 \cdot 39 + 3 \\ 39 &= 13 \cdot 3 + 0, \end{aligned}$$

and therefore $\gcd(321, 843) = 3$ and $\operatorname{lcm}(321, 843) = \dfrac{321 \cdot 843}{3} = 107 \cdot 843 = 90201$.

The extended Euclidean algorithm gives:

$$\begin{pmatrix} 321 & 1 & 0 \\ 843 & 0 & 1 \\ 321 & 1 & 0 \\ 201 & -2 & 1 \\ 120 & 3 & -1 \\ 81 & -5 & 2 \\ 39 & 8 & -3 \\ 3 & 21 & 8 \end{pmatrix},$$

obtaining the linear presentation $\gcd(321, 843) = 3 = (-21) \cdot 321 + 8 \cdot 843$. □

4 Relatively prime numbers

If $\gcd(a, b) = 1$, the numbers a and b are said to be *relatively prime* (or *coprime*). The following properties of relatively prime numbers are often used.

Lemma 5. *Let a and b be relatively prime integers; that is, integers for which* $\gcd(a, b) = 1$. *Then*

(a) *a and b do not have common primes in their prime factorisations.*

(b) *If c is a multiple of a and also a multiple of b, then c is a multiple of ab.*

(c) *If ac is a multiple of b, then c is a multiple of b.*

(d) *There exist integers m, n such that $ma + nb = 1$.*

Proof. (a) follows from equation (4), (b) and (c) follow from (a), and (d) follows from Theorem 4. □

Theorem 6 (Chinese Remainder Theorem)**.** *Let a and b be two relatively prime integers, and let r and s be integers with $0 \le r < a$ and $0 \le s < b$. Then there exists a unique number N with $0 \le N < ab$, such that*

$$r \equiv N \pmod{a} \quad \textit{and} \quad s \equiv N \pmod{b}, \tag{7}$$

i.e., such that N has remainder r on dividing by a and remainder s on dividing by b.

Proof. Let us prove first, that there exists at most one integer N with the conditions required. Assume, on the contrary, that for two integers N_1 and N_2 we have $0 \le N_1 < ab$, $0 \le N_2 < ab$ and

$$r \equiv N_1 \equiv N_2 \pmod{a} \quad \text{and} \quad s \equiv N_1 \equiv N_2 \pmod{b}.$$

Without loss of generality $N_1 \ge N_2$. Then the number $M = N_1 - N_2$ satisfies $0 \le M < ab$, and

$$0 \equiv M \pmod{a} \quad \text{and} \quad 0 \equiv M \pmod{b}. \tag{8}$$

By Lemma 5 part 3, condition (8) implies that M is divisible by ab, whence $M = 0$, so N_1 and N_2 are actually equal.

Next we will find an integer N', not necessarily between 0 and ab, such that $r = N' \pmod{a}$ and $s = N' \pmod{b}$. Indeed, by Theorem 4 there are integers m, n such that $\gcd(a, b) = 1 = ma + nb$. Multiplying this equation by $r - s$ we get

$$r - s = (r - s)ma + (r - s)nb = m'a + n'b.$$

Now it is clear that the number

$$N' = r - m'a = s + n'b$$

satisfies the condition (7).

Finally, choose N to be N''s remainder on division by ab; that is, $0 \le N < ab$ and

$$N' = q \cdot ab + N.$$

This N also satisfies (7). So the theorem is proved. □

This proof of the Chinese Remainder Theorem is constructive; that is, it also gives an algorithm for calculating such an N with property (7). A shorter but nonconsructive proof which uses the Pigeonhole Principle can be found in the notes “Primes that are Sums of Two Squares” (Tutorial 4), where the theorem is used to prove a result of Fermat.

January 24, 2009
http://www.mathsolympiad.org.nz