Elementary Number Theory II

CIS002-2 Computational Alegrba and Number Theory

David Goodwin

david.goodwin@perisic.com

University of Bedfordshire

09:00, Tuesday 1st November 2011

Contents

Example of Euclid's Algorithm

Example (Euclid's Algorithm)

Calculate $gcd(1485, 1745)$ using Euclid's algorithm.
If $a = qb + r$ then $gcd\,(a, b) = gcd\,(b, r)$. We use the equation $a = qb + r$ to find r, then to repeat using $gcd\,(b, r)$. Remember the constraints $\{q \mid q \in \mathbb{Z}\}$ and $\{r \mid r \in \mathbb{Z} \text{ and } r < b\}$.

$$
\begin{array}{rlr}
1745 = 1485q + r & q = 1 & r = 260 \\
1485 = 260q + r & q = 5 & r = 185 \\
260 = 185q + r & q = 1 & r = 75 \\
185 = 75q + r & q = 2 & r = 35 \\
75 = 35q + r & q = 2 & r = 5 \\
35 = 5q + r & q = 7 & r = 0
\end{array}
$$

Therefore $gcd\,(1485, 1745) = 5$

Example of Bezout's Identity

Example (Bezout's Identity)

Express $gcd(1485, 1745)$ in the form $1485u + 1745v$.
From the previous example we found $gcd(1485, 1745) = 5$

$$
\begin{aligned}
5 &= 75 - (2 \times 35) \\
&= 75 - 2 \times (185 - (2 \times 75)) \\
&= (5 \times 75) - (2 \times 185) \\
&= 5 \times (260 - (1 \times 185)) - (2 \times 185) \\
&= (5 \times 260) - (7 \times 185) \\
&= (5 \times 260) - 7 \times (1485 - (5 \times 260)) \\
&= (40 \times 260) - (7 \times 1485) \\
&= 40 \times (1745 - (1 \times 1485)) - (7 \times 1485) \\
&= (40 \times 1745) - (47 \times 1485) = 69800 - 69795 = 5
\end{aligned}
$$

Least Common Multiples

Definition

If a and b are integers, then a **common multiple** of a and b is an integer c such that $a \mid c$ and $b \mid c$. If a and b are both non-zero, then they have **positive common multiples** (such as $|ab|$), so by the well-ordered principle they have a **least common multiple** (to be more precise **least positive common multiple**). The least common multiple of two integers a and b is denoted by $lcm(a, b)$.

Least Common Multiples

Theorem (2.1)

Let a and b be positive integers, with $d = gcd(a, b)$ and the **least common multiple** $l = lcm(a, b)$. *Then*

$$dl = ab \qquad \text{since } a, b > 0$$

Example

Let $a = 12$ and $b = 8$, then $d = gcd(12, 8) = 4$ and $l = lcm(12, 8) = 24$.

$$\begin{aligned} dl &= ab \\ 4 \times 24 &= 12 \times 8 = 96 \end{aligned}$$

University of Bedfordshire

Diophantus of Alexandria

Diophantus of Alexandria (*c. A.D. 250*) carried out extensive studies of problems relating to indeterminate equations[1]. Although Diophantus accepted any solution in rational numbers, the name **Diophantus equations** today refers exclusively to equations with **integer solutions**.

[1] equations with an infinite set of solutions

Linear Diophantine Equations

Theorem (2.2)

Let a, b and c be integers with a and b not both zero, and let $d = gcd(a, b)$. Then the equation

$$ax + by = c$$

has an integer solution x, y if and only if $d \mid c$, in which case there are infinitely many solutions. The following are the pairs of solutions

$$x = x_0 + \frac{bn}{d}, \qquad y = y_0 - \frac{an}{d} \qquad (n \in \mathbb{Z})$$

note that if $c = 1$ then a and b are coprime (corollary (1.7))

Method of solution to Linear Diophantine Equations

We can find the solutions of any linear Diophantine equation $ax + by = c$ by the following method:

1. Calculate $d = gcd(a, b)$ by Euclid's algorithm.
2. Check if $d \mid c$ (if not then there are no solutions)
3. Use Bezout's Identity to find integers u and v such that $au + bv = d$. Then if $c = de$, we find $x_0 = ue$ and $y_0 = ve$.
4. Now use theorem (2.2) to find the general solution x, y of the equation $ax + by = c$.

Example of a Linear Diophantine Equation

Find the positive integer values of x and y that satisfy the equation

$$2x + 5y = 32$$

Example (Linear Diophantine Equation)

$$\begin{aligned} 5 &= 2q + r & q &= 2 & r &= 1 \\ 2 &= 1q + r & q &= 2 & r &= 0 \end{aligned}$$

$gcd(2, 5) = 1$
$1 \mid 32$ therefore solutions exist.

$$1 = 5 - (2 \times 2)$$

Example (Linear Diophantine Equation (cont.))

$$
\begin{aligned}
d &= 2u + 5v \\
u &= -2 \\
v &= 1
\end{aligned}
$$

If $c = 32$ and $d = 1$, then if $c = de$, $e = 32$.

$$
\begin{aligned}
x_0 &= ue = -64 \\
y_0 &= ve = 32
\end{aligned}
$$

Example (Linear Diophantine Equation (cont.))

Now we can find all solutions from the equation

$$x = x_0 + \frac{bn}{d}, \qquad y = y_0 - \frac{an}{d} \qquad (n \in \mathbb{Z})$$
$$x = -64 + \frac{5n}{1}, \qquad y = 32 - \frac{2n}{1}$$

For this example, the paired solutions are (here for the integers $n = \ldots, 0, 1, 2, 3, 4, \ldots$)

$$\{\ldots, (-64, 32), (-59, 30), (-54, 28), (-49, 26), (-44, 24), \ldots\}$$

Prime numbers

Definition

An integer $p > 1$ is said to be **prime** if the only positive divisors of p are 1 and p itself.

Prime numbers

Lemma (2.3)

Let p be prime, and let a and b be any integers

A *either $p \mid a$, or a and p are coprime.*

B *if $p \mid ab$, then $p \mid a$ or $p \mid b$.*

Corollary (2.4)

If p is prime and p divides $a_1 \ldots a_k$ then p divides a_i for some integer i.

Prime-Power Factorisation

The next result, known as the **fundamental theorem of arithmetic**, explains why prime numbers are so important: they are the basic building blocks out of which all integers can be constructed.

Theorem (2.5)

Each integer $n > 1$ has a prime-power factorisation

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

where $p_1, \dots, p_k$ are distinct primes and $e_1, \dots, e_k$ are positive integers; this factorisation is unique, apart from permutations of the factors.

Prime-Power Factorisation

Example

200 has the prime-power factorisation $2^3 \times 5^2$, or alternatively $5^2 \times 2^3$ if we permute the factors, but it has no other prime-power factorisations.

Example

1200 has the prime-power factorisation $2^4 \times 3^1 \times 5^2$.

University of Bedfordshire

Prime numbers < 100

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.

Prime numbers < 1000

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,
101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199,
211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293,
307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397,
401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499,
503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599,
601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691
701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797,
809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887,
907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997.

Euclid's Theorem

Theorem (2.6)

There are infinitely many primes

A Proof of Euclid's Theorem

Proof.

The proof is by contradiction: we assume that there are only finitely many primes, and then we obtain a contradiction from this, so it follows that there must be infinitely many primes.
Suppose then that the only primes are $p_1, p_2, \ldots, p_k$. Let

$$m = p_1 p_2 \ldots p_k + 1$$

Since n is an integer greater than 1, theorem (2.5) implies that it is divisible by some prime p (this includes the possibility that $m = p$). By our assumption, this prime p must be one of $p_1, p_2, \ldots, p_k$, so p divides their product $p_1 p_2 \ldots p_k$. Since p divides both m and the product $p_1 p_2 \ldots p_k$ it divides $m - p_1 p_2 \ldots p_k = 1$, which is impossible. $\square$

Prove the fundamental theorem of arithmatic to be true.