

ELEMENTARY NUMBER THEORY

CIS002-2 COMPUTATIONAL ALGEBRA AND NUMBER THEORY

David Goodwin

david.goodwin@perisic.com



09:00, Tuesday 25th October 2011

① SOME DEFINITIONS

② DIVISIBILITY

Divisors

Euclid's Algorithm

Bezout's Identity

③ CLASS EXERCISES

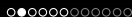
SOME TECHNICAL LANGUAGE

- theorem - a statement that has been proven on the basis of previously established statements
- lemma - a proven statement used as a stepping-stone toward the proof of another statement
- proof - a convincing demonstration that some mathematical statement is necessarily true
- corollary - a statement that follows readily from a previous statement



L. CARROLL

“Can you do Division? Divide a loaf by a knife - what’s the answer to that?”



THEOREM (1.1)

If a and b are integers with $b > 0$, then there is a unique pair of integers q and r such that

$$a = qb + r \quad \text{and} \quad 0 \leq r < b$$

We call q the quotient and r the remainder.

q is the integer part of a/b and is symbolised by $[a/b]$.

EXAMPLE (1.1)

If n is a square, then n leaves a remainder 0 or 1 when divided by 4

$$n = (4q + r)^2 = 16q^2 + 8qr + r^2$$

$$r = 0 \quad n = 4(4q^2 + 2qr) + 0$$

$$r = 1 \quad n = 4(4q^2 + 2qr) + 1$$

$$r = 2 \quad n = 4(4q^2 + 2qr + 1) + 0$$

$$r = 3 \quad n = 4(4q^2 + 2qr + 2) + 1$$

DEFINITION

If a and b are any integers, and $a = qb$ for some integer q , then we say that b divides a (or b is a factor of a , or a is a multiple of b). When b divides a we write $b \mid a$ and we use $b \nmid a$ when b does not divide a .

THEOREM (1.2)

- (A) *If $a \mid b$ and $b \mid c$ then $a \mid c$*
- (B) *If $a \mid b$ and $c \mid d$ then $ac \mid bd$*
- (C) *If $m \neq 0$, then $a \mid b$ if and only if $ma \mid mb$*
- (D) *If $d \mid a$ and $a \neq 0$ then $|d| \leq |a|$*
- (E) *If c divides a_1, \dots, a_k , then c divides $a_1u_1 + \dots + a_ku_k$ for all integers u_1, \dots, u_k*
- (F) *$a \mid b$ and $b \mid a$ if and only if $a = \pm b$*

GREATEST COMMON DIVISOR

DEFINITION

If $d \mid a$ and $d \mid b$ we say d is a common divisor (or common factor) of a and b . If a and b are both not 0, we find from Theorem (1.2.d) that no common divisor is greater than $\max(|a|, |b|)$. This is the greatest common divisor (or highest common factor) and is denoted by $\gcd(a, b)$.

EUCLID'S ALGORITHM

LEMMA (1.3)

If $a = qb + r$ then $\gcd(a, b) = \gcd(b, r)$

PROOF.

Any common divisor of b and r also divides $qb + r = a$ (from Theorem (1.2.e)), and since $r = a - qb$ it follows that any common divisor of a and b also divides r . Therefore the two pairs a, b and b, r have the same common divisors, and so the same greatest common divisor. □

BEZOUT'S IDENTITY

We use Euclid's algorithm to give a simple expression for

$$d = \gcd(a, b)$$

THEOREM (1.4)

If a and b are integers (not both 0), then there exists integers u and v such that

$$\gcd(a, b) = au + bv$$

THEOREM (1.5)

Let a and b be integers (both not 0) with greatest common divisor d . Then an integer c has the form $ax + by$ for some $x, y \in \mathbb{Z}$ if and only if c is a multiple of d . In particular, d is the least positive integer of the form $ax + by$ ($x, y \in \mathbb{Z}$).

DEFINITION

Two integers a and b are coprime (or relatively prime) if $\gcd(a, b) = 1$.

A set of integers are coprime if $\gcd(a_1, a_2, \dots) = 1$ and are mutually coprime if $\gcd(a_i, a_j) = 1$ whenever $i \neq j$.

If a set of integers are mutually coprime then they are also coprime, but the converse is false.

COROLLARY (1.6)

Two integers a and b are coprime if and only if there exists integers x and y such that

$$ax + by = 1$$

COROLLARY (1.7)

If $\gcd(a, b) = d$ then

$$\gcd(ma, mb) = md$$

for every integer $m > 0$, and

$$\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$$



COROLLARY (1.8)

Let a and b be coprime integers.

(A) *If $a \mid c$ and $b \mid c$ then $ab \mid c$*

(B) *If $a \mid bc$ then $a \mid c$*

QUESTIONS

- 1 What are the possible remainders when a perfect square is divided by 3, or by 5, or by 6?
- 2 If a divides b , and c divides d . must $a + c$ divide $b + d$?
- 3 Calculate $\gcd(1485, 1745)$ using Euclid's algorithm.
- 4 Calculate $\gcd(1485, 1745)$ using Bezout's Identity.