Elementary Number Theory

CIS002-2 Computational Alegrba and Number Theory

David Goodwin

david.goodwin@perisic.com

University of Bedfordshire

09:00, Tuesday 25th October 2011

Contents

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

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

We call q the quotient and r the remainder.
q is the integer part of a/b and is symbolised by $[a/b]$.

University of Bedfordshire

Example (1.1)

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

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

$$\begin{array}{ll} r = 0 & n = 4\left(4q^2 + 2qr\right) + 0 \\ r = 1 & n = 4\left(4q^2 + 2qr\right) + 1 \\ r = 2 & n = 4\left(4q^2 + 2qr + 1\right) + 0 \\ r = 3 & n = 4\left(4q^2 + 2qr + 2\right) + 1 \end{array}$$

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* $|d| \leqslant |a|$

(E) *If* c *divides* $a_1, \ldots, a_k$, *then* c *divides* $a_1 u_1 + \cdots + a_k u_k$ *for all integers* $u_1, \ldots, u_k$

(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 $max\left(|a|, |b|\right)$. This is the greatest common divisor (or highest common factor) and is denoted by $gcd\left(a, b\right)$.

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 and 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. $\square$

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 aslo coprime, but the converse if 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.