Modular Arithmetic & Congruences

CIS002-2 Computational Alegrba and Number Theory

David Goodwin

david.goodwin@perisic.com

University of Bedfordshire

09:00, Tuesday 15th November 2011

Contents

Introduction

Many problems involving large integers can be simplified by a technique called **modular arithmetic**, where we use **congruences** in place of equations. The general idea is to choose a particular integer n (depending on the problem), called the **modulus**, and replace evergy integer with its remainder when divided by n. This remainder is usually smaller that the origional integer, and hence easier to deal with.

A simple example

Example (What is the day of the week?)

What day of the week will it be 100 days from now? We could solve this by getting out a diary and counting 100 days ahead, but a simpler method is to use the fact that the days of the week recur in cycles of length 7. Now $100 = (7 \times 14) + 2$, so the day of the week will be the same as it is 2 days ahead of now, Thursday (counting 2 days ahead of today instead of 100. Here we have choose $n = 7$ and replace 100 with its remainder on division by 7, namely 2.

Definition

Definition

Let n be a positive integer, and let a and b be any integers. We say that a is *congruent* to $b \mod (n)$, or a is a *residue* of $b \mod (n)$, written

$$a \equiv b \mod (n)$$

if a and b leave the same remainder when divided by n (other notations include $a \equiv (b \mod n)$, $a \equiv_n b$, or simply $a \equiv b$ if the value of n is understood).

University of Bedfordshire

Definition

To be more precise we use the division algorithm to put $a = qn + r$ with $0 \leq r < n$, and $b = q'n + r'$ with $0 \leq r' < n$, and hence we say that $a \equiv b \mod (n)$ if and only if $r = r'$.

For the previous example we can say $100 \equiv 2 \mod (7)$.

We use the notation $a \not\equiv b \mod (n)$ to denote that a and b are not congruent $\mod (n)$, that is, they leave different remainders when divided by n.

Some useful observations

If $a = qn + r$ and $b = q'n + r'$ as above

$$a - b = (q - q')n + (r - r') \quad \text{with} \quad -n < r - r' < n$$

If $a \equiv b \mod (n)$ then $r = r'$ so $a - b = (q - q')n$.

Lemma (5.1)

For any fixed $n \geq 1$ we have $a \equiv b \mod (n)$ if and only if $n \mid (a - b)$.

University of Bedfordshire

Some useful observations

Lemma (5.2)

for any fixed $n \geq 1$ we have:

(A) $a \equiv a \mod (n)$ *for all integers* a *[we have* $n \mid (a - a)$ *for all* a*]*

(B) *if* $a \equiv b \mod (n)$ *then* $b \equiv a \mod (n)$ *[if* $n \mid (a - b)$ *then* $n \mid (b - a)$*]*

(C) *if* $a \equiv b \mod (n)$ *and* $b \equiv c \mod (n)$ *then* $a \equiv c \mod (n)$ *[if* $n \mid (a - b)$ *and* $n \mid (b - c)$ *then* $n \mid (a - b) + (b - c) = a - c$*]*

These three properties are called the reflexivity, symmetry and transitivity axioms for an equivalence relation.

Congruence classes

It follows from the previous lemma, that for each fixed n, congruence $\mod (n)$ is an equivalence relation on $\mathbb{Z}$. It also follows that $\mathbb{Z}$ is partitioned into disjoint equivalence classes; these are **congruence classes**

$$\begin{aligned}[a] &= \{b \in \mathbb{Z} \mid a \equiv b \mod (n)\} \\ &= \{\dots, a-2n, a-n, a, a+n, a+2n, \dots\}\end{aligned}$$

for $a \in \mathbb{Z}$ (to emphasise the particular value of n being used, we can use the notation $[a]_n$). Each class belongs to one of the n possible remainders on division by n.

CONGRUENCE CLASSES

For a given $n \geq 1$, we denote the set of n equivalence classes mod (n) by $\mathbb{Z}_n$. Our next aim is to show how to do arithmetic with these congruence classes, so that $\mathbb{Z}_n$ becomes a number system with properties similar to those of $\mathbb{Z}$.

Operations on congruence classes

If $[a]$ and $[b]$ are elements of $\mathbb{Z}_n$ (that is, congruence classes mod (n)), we define their sum, difference and product to be the classes

$$\begin{aligned} [a] + [b] &= [a + b] \\ [a] - [b] &= [a - b] \\ [a][b] &= [ab] \end{aligned}$$

containing the integers $a + b$, $a - b$ and ab repectively.

Operations on congruence classes

If $a' \equiv a$ then $a' = a + kn$ for some integer k, and similarly we have $b' = b + ln$ for some integer l.

$$\begin{aligned} a' \pm b' &= (a \pm b) + (k \pm l)n \equiv a \pm b \\ a'b' &= (ab) + (al + bk + kln)n \equiv ab \end{aligned}$$

Lemma (5.3)

For any $n \geq 1$, if $a' \equiv a$ and $b' \equiv b$, then $a' \pm b' \equiv a \pm b$ and $a'b' \equiv ab$

Question

Prove by use of a counterexample, that $[a]^{[b]} \neq [a^b]$

Definition

A set of n integers, containing one representative from each of the n congruence classes $\mathbb{Z}_n$, is called a **complete set of residues** mod (n).

If we divide a by n to give $a = qn + r$ giving some unique r satisfying $0 \leq r < n$, each class $[a] \in \mathbb{Z}_n$ contains a unique $r = 0, 1, \ldots, n-1$ forming a complete set of residues called **least non-negative residues** mod (n). Similarly, the complete set of residues formed from $-n/2 < r \leq n/2$ is called the **least absolute residues** mod (n).

University of Bedfordshire

Polynomials

Lemma (5.4)

Let $f(x)$ be a polynomial with integer coefficients, and let $n \geq 1$. If $a \equiv b \mod (n)$ then $f(a) \equiv f(b) \mod (n)$.

Questions

Find the following without a calculator

1. Calculate the least non-negative residue of $28 \times 33 \mod (35)$.
2. Calculate the least non-negative residue of $34 \times 17 \mod (29)$.
3. Calculate the least absolute residue of $15 \times 59 \mod (75)$.
4. Calculate the least absolute residue of $19 \times 14 \mod (23)$.
5. Calculate the least non-negative residue of $3^8 \mod (13)$.
6. Find the remainder when 5^{10} is divided by 19.
7. Find the decimal digit of $1! + 2! +, \dots, +10!$
8. Prove that $a(a+1)(2a+1)$ is divisible by 6 for every integer a.

Questions

Prove the following polynomials have no integer roots

9. $x^5 - x^2 + x - 3$
10. $x^3 - x + 1$
11. $x^3 + x^2 - x + 1$
12. $x^3 + x^2 - x + 3$

University of Bedfordshire