Number Theory

P. Danziger

1 Quotient Remainder Theorem: Mod and Div

Theorem 1 (Quotient Remainder Theorem) *Given $n \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$, there exists unique numbers q and r such that*

$$n = dq + r, \text{ with } 0 \leq r < d.$$

Definition 2

1. *q is called the quotient of n with respect to d.*
2. *r is called the remainder of n with respect to d.*
3. *We define the function mod: $n \bmod d = r$.*
4. *We define the function div: n div $d = q$.*

Notes:

- $n \bmod d$ always yields a number less than d
- $a \bmod n = b$, if and only if $n \,|\, (a - b)$
- The following are equivalent:
  1. $d \,|\, n$,
  2. $n \bmod d = 0$,
  3. $\exists\, m \in \mathbb{Z}$ such that $n = m \cdot d$.
- C and Java use % to denote mod, i.e. $a \,\%\, b$ means $a \bmod b$

Example 3

1. $7 \bmod 6 = 1$, $12 \bmod 6 = 0$, $1 \bmod 6 = 1$.
   $7 \text{ div } 6 = 1$, $12 \text{ div } 6 = 2$, $1 \text{ div } 6 = 0$.
2. $12 \bmod 7 = 5$, $34 \bmod 7 = 6$, $28 \bmod 7 = 0$.
   $12 \text{ div } 7 = 1$, $34 \text{ div } 7 = 4$, $28 \text{ div } 7 = 4$.
3. An array a_{ij} ($i = 0$ to $m - 1$, $j = 0$ to $n - 1$) is stored in computer memory as a contiguous block of memory, that is a_{10} is in the next memory location after a_{0n}.
   Given that a_{ij} is stored in memory location d places after a_{00}, find i and j. i.e. given d find i and j:

   $i = d \text{ div } n$,
   $j = d \bmod n$.

4. Two variables, a and b are defined in a computer program, both are 1 byte.
   If $a = 217$ and $b = 126$ what is $a + b$?

   $a + b = (217 + 126) \bmod 256 = 343 \bmod 256 = 89$

5. Suppose that the days of the week are represented by
   0 - Sunday, 1 - Monday, 2 - Tuesday, 3 - Wednesday, 4 - Thursday, 5 - Friday.

   Given that today is a Thursday what day of the week will it be in 342 days time?

   $342 \bmod 7 = 6$.
   Today is 4, $4 + 6 \bmod 7 = 3$. So in 342 days it will be a Wednesday.

   In general $DayN = (DayT + N) \bmod 7$.
   Where $DayN$ is the day we wish to know about, and $DayT$ is today.

   Of course this algorithm does not take into account leap years.

6. Leap years occur according to the following algorithm, x is the year:

   if $x \bmod 400 = 0$ then it is a leap year
   else if ($x \bmod 4 = 0$ and $x \bmod 100 \neq 0$) then it is a leap year
   else it is not a leap year

   When is the next leap year? When was the last leap year? Is 2000 a leap year? Was 1900 a leap year?

1.1 The Congruence Relation

Definition 4 *Given a positive integer n, we define the relation, Congruence Modulo n from $\mathbb{Z}$ to $\mathbb{Z}$ by a is congruent to b modulo n if and only if $(a \bmod n) = (b \bmod n)$.*

We write $a \equiv b \pmod{n}$ to indicate that a is congruent to b modulo n.
Symbolically: Given $n \in \mathbb{Z}$,

$$\forall a, b \in \mathbb{Z},\ a \equiv b \pmod{n} \Leftrightarrow a \bmod n = b \bmod n.$$

Notes

1. $a \bmod n$ is always an integer less than n, but the a and b in $a \equiv b \pmod{n}$ can be any integers.

2. $a \equiv b \pmod{n}$ if and only if $n \,|\, (a - b)$.

Example 5

1. Congruence modulo 6, let $n = 6$, $1 \equiv 7 \pmod{6} \equiv 13 \pmod{6} \equiv 19 \pmod{6} \equiv 25 \pmod{6} \equiv \ldots$

2. Congruence modulo 2, take $n = 2$.
   $a = 0 \bmod 2$ if and only if $a = 2m$ for some $m \in \mathbb{Z}$, i.e. a is even.
   So all even numbers are congruent to each other modulo 2.
   $a = 1 \bmod 2$ if and only if $a = 2m + 1$ for some $m \in \mathbb{Z}$, i.e. a is odd.
   So all odd numbers are congruent to each other modulo 2.

3. Congruence modulo 4, take $n = 4$.
   The members of the following sets are all congruent to each other modulo 4:

   $0 \pmod 4$:
   $\{x \in \mathbb{Z} \,|\, \exists\, m \in \mathbb{Z} \text{ such that } x = 4m\} = \{\ldots, -12, -8, -4, 0, 4, 8, 12, \ldots\}$,
   $1 \pmod 4$:
   $\{x \in \mathbb{Z} \,|\, \exists\, m \in \mathbb{Z} \text{ such that } x = 4m + 1\} = \{\ldots, -11, -7, -3, 1, 5, 9, 13, \ldots\}$,
   $2 \pmod 4$:
   $\{x \in \mathbb{Z} \,|\, \exists\, m \in \mathbb{Z} \text{ such that } x = 4m + 2\} = \{\ldots, -10, -6, -2, 2, 6, 10, 14, \ldots\}$,
   $3 \pmod 4$:
   $\{x \in \mathbb{Z} \,|\, \exists\, m \in \mathbb{Z} \text{ such that } x = 4m + 3\} = \{\ldots, -9, -5, -1, 3, 7, 11, 15, \ldots\}$.

Definition 6 *Given n the set of numbers which are congruent to each other modulo n is called a congruence class modulo n.*

The set of congruence classes for a given n are a partition of the integers.

1.2 Modular Arithmetic

Theorem 7 *For any integers $a, b, c, d \in \mathbb{Z}$, if $a \equiv c \pmod n$ and $b \equiv d \pmod n$ then $a+b \equiv (c+d) \pmod n$.*

Proof:
Let $n \in \mathbb{N}$ and $a, b, c, d \in \mathbb{Z}$
Suppose that $a \equiv c \pmod n$ and $b \equiv d \pmod n$. [We must show that $a + b \equiv c + d \bmod n$.]
Define $x, y \in \mathbb{Z}$ by $x = a \bmod n = c \bmod n$ and $y = b \bmod n = d \bmod n$.
Note $0 \leq x, y < n$ (QRT)
Then $(a + b) \bmod n = (x + y) \bmod n$ and $(c + d) \bmod n = (x + y) \bmod n$. $\square$
This theorem effectively says that $(a + b) \bmod n = (a \bmod n) + (b \bmod n)$
This allows us to define arithmetic "modulo n"

Example 8
Let $n = 5$. $3 + 1 = 4 \bmod 5$ $3 + 2 = 0 \bmod 5$ $3 + 3 = 1 \bmod 5$ etc.
This theorem means that all the usual algebraic rules for addition and subtraction are inherited by modular arithmetic.

2 Division Into Cases

We wish to prove a statement of the form $\forall x \in S, P(x)$.
Suppose that $\{A_1, A_2, \ldots, A_n\}$ is a partition of S. i.e. $A_1 \cup A_2 \cup \ldots \cup A_n = S$ and the A_i are mutually disjoint ($A_i \cap A_j = \phi$ whenever $i \neq j$).
If we can prove $\forall x \in A_1, P(x) \wedge \forall x \in A_2, P(x) \wedge \ldots \wedge \forall x \in A_n, P(x)$ we have shown $\forall x \in S, P(x)$.
This is called division into cases.

Lemma 9 *If n is odd then $n \bmod 6 = 1, 3$ or 5.*

To Prove: $\forall n \in \mathbb{Z}, n \bmod 6$ is 1, 3 or 5.
Proof:
Let $n \in \mathbb{Z}$ with n odd.
$\Rightarrow \exists\, k \in \mathbb{Z}$ such that $n = 2k + 1$ (Definition of odd)
We consider the three cases of k modulo 3:

$k \bmod 3 = 0$
- $\Rightarrow \exists\, j \in \mathbb{Z}$ such that $k = 3j$. (Definition of mod)
- $\Rightarrow n = 2(3j) + 1 = 6j + 1$ (Substitution)
- So $n \bmod 6 = 1$. (Definition of mod)

$k \bmod 3 = 1$
- $\Rightarrow \exists\, j \in \mathbb{Z}$ such that $k = 3j + 1$. (Definition of mod)
- $\Rightarrow n = 2(3j + 1) + 1 = 6j + 3$ (Substitution)
- So $n \bmod 6 = 3$. (Definition of mod)

$k \bmod 3 = 2$
- $\Rightarrow \exists\, j \in \mathbb{Z}$ such that $k = 3j + 2$. (Definition of mod)
- $\Rightarrow n = 2(3j + 2) + 1 = 6j + 5$ (Substitution)
- So $n \bmod 6 = 5$. (Definition of mod)

Thus $n \bmod 6 = 1, 3$ or 5 □

Theorem 10 *If p is a prime greater than 3, then $p \bmod 6 = 1$ or 3.*

To Prove $\forall p \in \mathbb{P}, p \neq 2 \wedge p \neq 3 \Rightarrow p \bmod 6 = 1$ or 3
Proof:

Let $p \in \mathbb{P}$ (p is prime), with $p \neq 2$ and $p \neq 3$.	
Since p is a prime not equal to 2, $p \neq 2$	(The only even prime is 2).
Thus $p \bmod 6 = 1, 3$ or 5.	(Previous Lemma)
We must show that $p \bmod 6 \neq 3$.	
Suppose not, that is suppose that $p \bmod 6 = 3$.	
$\Rightarrow \exists k \in \mathbb{Z}$ such that $p = 6k + 3 = 3(2k + 1)$.	(Definition of mod, Distribution)
But $2k + 1 \in \mathbb{Z}$	(Closure)
So either p is not prime, or $2k + 1 = 1$.	(definition of prime)
But if $2k + 1 = 1$, then $k = 0$ and hence $p = 3$	(Algebra).
This contradicts the assumption that p is prime and $p \neq 3$.	(Negation)
Thus $p \bmod 6 \neq 3$.	(Contradiction) □

Theorem 11 *The square of any integer is 0 or 1 modulo 4.*

To Prove $\forall n \in \mathbb{Z}, n^2 \bmod 4 = 0$ or 1.
Proof:
Let $n \in \mathbb{Z}$
We consider the cases of n modulo 2:

$n \bmod 2 = 0$ (n is even)

$\Rightarrow \exists\, k \in \mathbb{Z}$ such that $n = 2k$	(Definition of mod)
$\Rightarrow n^2 = 4k^2$.	(Substitution)
$k^2 \in \mathbb{Z}$	(Closure)
So $n^2 \bmod 4 = 0$.	(Definition of mod)

$n \bmod 2 = 1$ (n is odd)

$\Rightarrow \exists\, k \in \mathbb{Z}$ such that $n = 2k + 1$	(Definition of mod)
$\Rightarrow n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$	(Substitution, Distribution)
$(k^2 + k) \in \mathbb{Z}$	(Closure)
So $n^2 \bmod 4 = 1$.	(Definition of mod)

Thus $n^2 \bmod 4 = 0$ or 1. $\square$
Division into cases is similar to the **case** statement in C or Java.