Euclid's Remainder Theorem

Fundamental Property of Integers

Any non-empty set of non-negative integers has a least element.

A Natural number is a non-negative integer, i.e.
$\mathbb{N} = \{n | n \in \mathbb{Z} \wedge n \geq 0\}$

Euclid's Remainder Thm.

For Natural numbers a and b with $b > 0$ there exists unique Natural numbers q and r such that

$$a = b * q + r \ \wedge \ 0 \leq r < b$$

- Case $a < b$

Let $q = 0$ and $r = a$ then $a = b * 0 + a$ and $0 \leq a < b$

Proof of Remainder Th^m.

- Case $a \geq b$

Let $A = \{x \,|\, x = a - m * b \wedge x \geq 0 \wedge m \in \mathbb{N}\}$
$A \neq \{\}$ as $a - b \in A$, because
$a - b = a - 1 * b \wedge a - b \geq 0 \wedge 1 \in \mathbb{N}$.
A is a non-empty set of positive integers and so has a least member, say, r .
Since $r \in A$, $r = a - m * b \wedge r \geq 0$, for some, m.
Show that $r < b$.
If not, then $r \geq b$, i.e. $r - b \geq 0$, but $r - b = (a - m * b) - b$
i.e. $r - b = (a - (m + 1) * b)$
i.e. $r - b \in A$ and $r - b < r$ since $b > 0$.
therefore, $r - b$ is in A and smaller than r which was the least member and so a contradiction, therefore $r < b$.

Operators Div and Mod

Integer division, *div*, and the modulo (or remainder) operation, *mod*, are standard operators in computing. The operations can be extended to $a \in \mathbb{Z}$, i.e. a can be negative. While *div* and *mod* can also be defined when b is negative, it is assumed $b > 0$.
Let $a, b \in \mathbb{Z}$ and $b > 0$ then

$$a\, div\, b = q \;\wedge\; a\, mod\, b = r \;\equiv\; a = b * q + r \wedge 0 \leq r < b$$

i.e.

$$a = b * (a\, div\, b) + a\, mod\, b \wedge 0 \leq a\, mod\, b < b$$

What is not standard is how these operations are implemented in programming languages for negative integers i.e. when $a \in \mathbb{Z}$ and $a < 0$.

Knuth Implementation of *div* and *mod*

While many program language implementations of *div* and *mod* do not satisfy the mathematical definition (above), Donald Knuth (Stanford) proposes the following implementation which does satisfy the above definition for *div* and *mod* where $a, b \in \mathbb{Z}$ and $b > 0$. The (Functional) programming languages Haskell and Microsoft's Excel uses the Knuth implementation.

Knuth Definition

Knuth defines $a\, div\, b$ so that: $a\, div\, b = \lfloor \frac{a}{b} \rfloor$

where $\lfloor x \rfloor$ 'floor x' is defined so that $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$
i.e. for $n \in \mathbb{Z}$ and $x \in \mathbb{R}$

$n = \lfloor x \rfloor \equiv n \leq x < n + 1$ i.e. $\lfloor x \rfloor$ is the greatest integer $\leq x$

Knuth Implementation of *div* and *mod* (Cont'd)

$a\ mod\ b$ is defined as: $a\ mod\ b = a - b * (a\ div\ b)$
Knuth's definition satisfies the property:
For $b > 0$,

$$a = b * (a\ div\ b) + a\ mod\ b\ \wedge\ 0 \leq a\ mod\ b < b$$

i.e.

$$a = b * \lfloor \tfrac{a}{b} \rfloor + (a - b * \lfloor \tfrac{a}{b} \rfloor)\ \wedge\ 0 \leq (a - b * \lfloor \tfrac{a}{b} \rfloor) < b$$

$0 \leq (a - b * \lfloor \frac{a}{b} \rfloor) < b$

Proof.

$0 \leq (a - b * \lfloor \frac{a}{b} \rfloor) < b$
$= b * \lfloor \frac{a}{b} \rfloor \leq a \wedge a < (b + b * \lfloor \frac{a}{b} \rfloor)$
{Since $b > 0$, dividing by b does not change sign}
$= \lfloor \frac{a}{b} \rfloor \leq \frac{a}{b} \wedge \frac{a}{b} < (1 + \lfloor \frac{a}{b} \rfloor)$
$= \lfloor \frac{a}{b} \rfloor \leq \frac{a}{b} < (1 + \lfloor \frac{a}{b} \rfloor)$
{From definition of $\lfloor x \rfloor$}
$= \mathit{True}$ $\square$

Knuth Implementation example

Using Knuth's definition of $a\,div\,b = \lfloor \frac{a}{b} \rfloor$ and
$a\,mod\,b = a - b * (a\,div\,b)$
i.e. $a\,mod\,b = a - b * \lfloor \frac{a}{b} \rfloor$ we get:

- $14\,div\,5 = \lfloor \frac{14}{5} \rfloor = \lfloor 2.8 \rfloor = 2$
  $14\,mod\,5 = 14 - 5 * 2 = 4$

$(-14)\,div\,5 = \lfloor \frac{-14}{5} \rfloor = \lfloor -2.8 \rfloor = -3$
$(-14)\,mod\,5 = (-14) - 5 * (-3) = 1$

Note:
$-(14\,div\,5) \neq (-14)\,div\,5$
$-(14\,mod\,5) \neq (-14)\,mod\,5$

Mod Arithmetic operations

For $n > 0$, $a, b \in \mathbb{Z}$:
Definition:$+_n$, $-_n$*and* $*_n$

$$a +_n b = (a + b)\ mod\ n$$
$$a -_n b = (a - b)\ mod\ n$$
$$a *_n b = (a * b)\ mod\ n$$

Properties of $+_n$ and $*_n$

$+_n$ is associative and commutative
$a +_n b = (a\ mod\ n) +_n (b\ mod\ n)$
$a -_n b = (a\ mod\ n) -_n (b\ mod\ n)$
$*_n$ is associative and commutative
$a *_n b = (a\ mod\ n) *_n (b\ mod\ n)$
$a *_n (b +_n c) = a *_n b +_n a *_n c$

Examples

e.g.

$16 +_{23} 19$	$16 *_{23} 19$
$= (16 + 19)\ mod\ 23$	$= (16 * 19)\ mod\ 23$
$= 35\ mod\ 23$	$\{\ 304 = 23 * 13 + 5\ \}$
$= 12$	$= 5$

$39 *_{23} 42$
$= ((39\ mod\ 23) * (42\ mod\ 23))\ mod\ 23$
$= (16 * 19)\ mod\ 23$
$= 5$

Congruent Modulo n

Notation: $n|m$ iff for some integer k, $m = k * n$.
((don't confuse with n/m))
Knuth suggests using $n \setminus m$ with the assumption that $n > 0$.
He considers that the symbol, $|$, is overused while the symbol, $\setminus$, is underused.
e.g. $9|27$ as $27 = k * 9$ when $k = 3$.
We can read $n|m$ as "n divides m (exactly)"
or read it as "n is a factor of m,
or read it as "m is multiple of n" .
Note: (for $n \neq 0$)
$n|0$ is true as $0 = k * n$ when $k = 0$ i.e. $0 = 0 * n$
$0|n$ is false as $n \neq k * 0$ for any k (assuming $n \neq 0$).
$0|0$ is undefined.

Congruent Modulo n

Congruent Modulo n: "$\equiv_n$"
Let n be an integer such that $n > 0$. Integers a and b are congruent modulo n iff $a - b$ is a multiple of n .
i.e.

$$a \equiv_n b \textit{ iff } n|(a-b)$$

e.g.
$27 \equiv_5 17$ as $5|(27-17)$.
$27 \equiv_5 2$ as $5|(27-2)$.

Congruent Modulo n (Cont'd)

In general,

$$k \equiv_n (k \, mod \, n)$$

Pf:
$n | (k - (k \, mod \, n))$ as
$k - (k \, mod \, n) = k - (k - n * (k \, div \, n)) = n * (k \, div \, n)$

When $n > 0$, we can implement $(a \, div \, n)$ as $\lfloor \frac{a}{n} \rfloor$ and therefore $a \, mod \, n = a - n * \lfloor \frac{a}{n} \rfloor$.

Properties of $\equiv_n$

1. $a \equiv_n a$
2. $a \equiv_n b$ iff $b \equiv_n a$
3. If $a \equiv_n b$ and $b \equiv_n c$ then $a \equiv_n c$
4. $a \equiv_n b$ iff $a \, mod \, n = b \, mod \, n$

Proof of 3.: If $a \equiv_n b$ and $b \equiv_n c$ then $a \equiv_n c$

Proof of Property 3.

Assume $a \equiv_n b$ and $b \equiv_n c$
i.e. $n|(a-b)$ and so $(a-b) = j*n$, for some j
and $n|(b-c)$ and so $(b-c) = k*n$, for some k
$\therefore (a-c) = (a-b)+(b-c) = j*n+k*n = (j+k)*n$
i.e. $n|(a-c)$
i.e. $a \equiv_n c$

Proof of 4.: $a \equiv_n b$ iff $a \bmod n = b \bmod n$

Show $(a \bmod n = b \bmod n) \equiv (a \equiv_n b)$

$a \bmod n = b \bmod n$

$\equiv (a \bmod n) - (b \bmod n) = 0$

$\equiv (a - n * q_a) - (b - n * q_b) = 0$, some q_a and q_b

$\equiv (a - b) - n * q_a + n * q_b = 0$

$\equiv (a - b) = n * (q_a - q_b)$

$\equiv n | (a - b)$

$\equiv a \equiv_n b$

Equations in mod arithmetic

For each $n > 0$, let $\mathbb{Z}_n = \{0, 1, 2, \ldots n - 1\}$
It is straightforward to solve for x in the equation where $a, b \in \mathbb{Z}_n$:

$$x +_n a = b$$

as we can 'add' $-a$ to both sided to get

$$\begin{aligned} x +_n a &= b \\ x +_n a -_n a &= b -_n a \\ x &= b -_n a \end{aligned}$$

e.g.
Find x such that $x +_{23} 16 = 3$.
$(-16)\ mod\ 23 = 7$ as $16 +_{23} 7 = 0$
$\therefore x = 3 +_{23} 7 = 10$.

Equation $a *_n x = b$

When $a, b \in \mathbb{Z}_n$ solving for x in the equation

$$a *_n x = b$$

depends on a having an inverse in $\mathbb{Z}_n$. If a has an inverse a^{-1} then $x = a^{-1} *_n b$.
An element a has an inverse a^{-1} in $\mathbb{Z}_n$ iff $a *_n a^{-1} = 1$.
e.g. Consider $\mathbb{Z}_7$, all non-zero elements have an inverse,

a	0	1	2	3	4	5	6
a^{-1}	–	1	4	5	2	3	6

In $\mathbb{Z}_7$ we can solve an equation such as $3 *_7 x = 4$. Let $x = 5 *_7 4 = 6$ as in $\mathbb{Z}_7$, 5 is the inverse of 3.

In $\mathbb{Z}_9$, not all non-zero elements have an inverse

a	0	1	2	3	4	5	6	7	8
a^{-1}	–	1	5	–	7	2	–	4	8

There is no x in $\mathbb{Z}_9$ such that $3 *_9 x = 4$ as 3 has no inverse in $\mathbb{Z}_9$.
Exercise:
Check $3 *_9 k$ for all $k \in \{0..8\}$.

Existence of Inverse

Finding an inverse of an an element a in $\mathbb{Z}_n$ is solving for x in $a *_n x = 1$ which can be rewritten as $(a * x)\ mod\ n = 1$.

From Euclid's Remainder Thm:

$a * x = n * b + ((a * x)\ mod\ n)$ where $b = ((a * x)\ div\ n)$

i.e. $a * x - n * b = (a * x)\ mod\ n$, for some b.

Therefore,

$(a * x)\ mod\ n = 1$

$\equiv a * x - n * b = 1$, for some b.

Therefore, $a *_n x = 1$ iff there is a b such that $a * x - n * b = 1$.

If we can find x and b such that $a * x - n * b = 1$ then
$a *_n x = 1$
as $a * x - n * b = (a * x) \; mod \; n$, for some b.
If $a *_n x = 1$ then
x is the inverse of a .

In Summary
An element $a \in \mathbb{Z}_n$ has an inverse, x,
iff $a * x - n * b = 1$, for some b.