Modular arithmetic

For every positive integer m, the *integers modulo* m are:

$$\mathbb{Z}_{\mathrm{m}} \ : \quad 0 \ , \quad 1 \ , \quad \ldots \ , \quad \mathrm{m}-1 \ .$$

with arithmetic operations of addition $+_{\mathrm{m}}$ and multiplication $\cdot_{\mathrm{m}}$ defined as follows

$$\begin{aligned} \mathrm{k} +_{\mathrm{m}} \mathrm{l} \ &= \ [\mathrm{k}+\mathrm{l}]_{\mathrm{m}} \ = \ \mathrm{rem}(\mathrm{k}+\mathrm{l},\mathrm{m}) \ , \\ \mathrm{k} \cdot_{\mathrm{m}} \mathrm{l} \ &= \ [\mathrm{k}\cdot\mathrm{l}]_{\mathrm{m}} \ = \ \mathrm{rem}(\mathrm{k}\cdot\mathrm{l},\mathrm{m}) \end{aligned}$$

for all $0 \leq \mathrm{k}, \mathrm{l} < \mathrm{m}$.

Example 49 *The addition and multiplication tables for* $\mathbb{Z}_4$ *are:*

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Note that the addition table has a cyclic pattern, while there is no obvious pattern in the multiplication table.

From the addition and multiplication tables, we can readily read tables for additive and multiplicative inverses:

	additive inverse
0	0
1	3
2	2
3	1

	multiplicative inverse
0	—
1	1
2	—
3	3

Interestingly, we have a non-trivial multiplicative inverse; namely, 3.

Example 50 *The addition and multiplication tables for* $\mathbb{Z}_5$ *are:*

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Again, the addition table has a cyclic pattern, while this time the multiplication table restricted to non-zero elements has a permutation pattern.

From the addition and multiplication tables, we can readily read tables for additive and multiplicative inverses:

	additive inverse
0	0
1	4
2	3
3	2
4	1

	multiplicative inverse
0	$-$
1	1
2	3
3	2
4	4

Surprisingly, every non-zero element has a multiplicative inverse.

Proposition 51 *For all natural numbers* $m > 1$*, the modular-arithmetic structure*

$$(\mathbb{Z}_m, 0, +_m, 1, \cdot_m)$$

is a commutative ring.

NB Quite surprisingly, modular-arithmetic number systems have further mathematical structure in the form of multiplicative inverses .

Important mathematical jargon : Sets

Very roughly, sets are the mathematicians' data structures. Informally, we will consider a *set* as a (well-defined, unordered) collection of mathematical objects, called the *elements* (or *members*) of the set.

Set membership

The symbol '$\in$' known as the *set membership* predicate is central to the theory of sets, and its purpose is to build statements of the form

$$x \in A$$

that are true whenever it is the case that the object x is an element of the set A, and false otherwise.

Defining sets

	of even primes		$\{2\}$	
The set	of booleans	is	$\{\mathbf{true}, \mathbf{false}\}$	
	$[-2..3]$		$\{-2, -1, 0, 1, 2, 3\}$	

Set comprehension

The basic idea behind set comprehension is to define a set by means of a property that precisely characterises all the elements of the set.

Notations:

$$\{x \in A \mid P(x)\} \quad , \qquad \{x \in A : P(x)\}$$

$$a \in \{x \in A \mid P(x)\} \iff (a \in A \wedge P(a))$$

Greatest common divisor

Given a natural number n, the set of its *divisors* is defined by set comprehension as follows

$$D(n) = \{ d \in \mathbb{N} : d \mid n \} \ .$$

the set of divisors of n

Example 53

1. $D(0) = \mathbb{N}$
2. $D(1224) = \left\{ \begin{array}{c} 1, 2, 3, 4, 6, 8, 9, 12, 17, 18, 24, 34, 36, 51, 68, \\ 72, 102, 136, 153, 204, 306, 408, 612, 1224 \end{array} \right\}$

Remark Sets of divisors are hard to compute. However, the computation of the greatest divisor is straightforward. :)

Going a step further, what about the *common divisors* of pairs of natural numbers? That is, the set

$$\mathrm{CD}(m, n) = \{\, d \in \mathbb{N} : d \mid m \wedge d \mid n \,\}$$

for $m, n \in \mathbb{N}$.

Example 54

$$\mathrm{CD}(1224, 660) = \{\, 1, 2, 3, 4, 6, 12 \,\}$$

Since $\mathrm{CD}(n, n) = \mathrm{D}(n)$, the computation of common divisors is as hard as that of divisors. But, what about the computation of the *greatest common divisor*?

Lemma 56 (Key Lemma) *Let* m *and* m' *be natural numbers and let* n *be a positive integer such that* $m \equiv m' \pmod{n}$*. Then,*

$$\mathrm{CD}(m, n) = \mathrm{CD}(m', n) .$$

PROOF: m, m', n nat numbers n is positive.

Assume (1) $m \equiv m' \pmod{n}$

RTP: $d \in CD(m,n) \iff d \in CD(m',n)$ $\forall d$

($\Longrightarrow$) Assume $d \in CD(m,n) \iff d \mid m \wedge d \mid n$ (2) (3)

RTP: $d \in CD(m',n) \iff d \mid m' \wedge d \mid n$

$m - m' = kn$
for some k
$\Rightarrow m' = m - kn$

RTP: $d \mid m'$

+ (2) +
Lemma

We are done ☒

RTP: $d \mid n$

holds by (3).

☒

Lemma

$d \mid a \wedge d \mid b \Rightarrow d \mid p \cdot a + q \cdot b \quad \forall p, q.$

integer linear combination.

$CD(m,n) = CD(\mathrm{rem}(m,n), n)$ $\quad \mathrm{rem}(m,n) \equiv m \pmod n$

$= CD(m-n, n)$ $\quad m-n \equiv m \ (m>n)$

$CD(kn, n) = D(n)$

Lemma 58 *For all positive integers* m *and* n*,*

$$\text{greatest}\,\mathrm{CD}(m,n) = \begin{cases} \text{greatest}\,\mathrm{D}(n) = n & \text{, } \textit{if } n \mid m \\ \text{greatest}\,\mathrm{CD}\big(n, \mathrm{rem}(m,n)\big) & \text{, } \textit{otherwise} \end{cases}$$

Lemma 58 *For all positive integers* m *and* n,

$$\mathrm{CD}(m,n) = \begin{cases} \mathrm{D}(n) & \text{, } \textit{if } n \mid m \\ \mathrm{CD}\big(n, \mathrm{rem}(m,n)\big) & \text{, } \textit{otherwise} \end{cases}$$

Since a positive integer n is the greatest divisor in $\mathrm{D}(n)$, the lemma suggests a recursive procedure:

$$\gcd(m,n) = \begin{cases} n & \text{, if } n \mid m \\ \gcd\big(n, \mathrm{rem}(m,n)\big) & \text{, otherwise} \end{cases}$$

for computing the *greatest common divisor*, of two positive integers m and n. This is

Euclid's Algorithm

gcd

```
fun gcd( m , n )
  =  let
       val ( q , r ) = divalg( m , n )
     in
       if r = 0 then n
       else gcd( n , r )
     end
```

Example 59 ($\mathrm{gcd}(13, 34) = 1$)

$$
\begin{aligned}
\mathrm{gcd}(13, 34) &= \mathrm{gcd}(34, 13) \\
&= \mathrm{gcd}(13, 8) \\
&= \mathrm{gcd}(8, 5) \\
&= \mathrm{gcd}(5, 3) \\
&= \mathrm{gcd}(3, 2) \\
&= \mathrm{gcd}(2, 1) \\
&= 1
\end{aligned}
$$

Theorem 60 *Euclid's Algorithm* $\mathtt{gcd}$ *terminates on all pairs of positive integers and, for such* m *and* n, $\mathtt{gcd}(m,n)$ *is the greatest common divisor of* m *and* n *in the sense that the following two properties hold:*

(i) *both* $\mathtt{gcd}(m,n) \mid m$ *and* $\mathtt{gcd}(m,n) \mid n$, *and*

(ii) *for all positive integers* d *such that* $d \mid m$ *and* $d \mid n$ *it necessarily follows that* $d \mid \mathtt{gcd}(m,n)$.

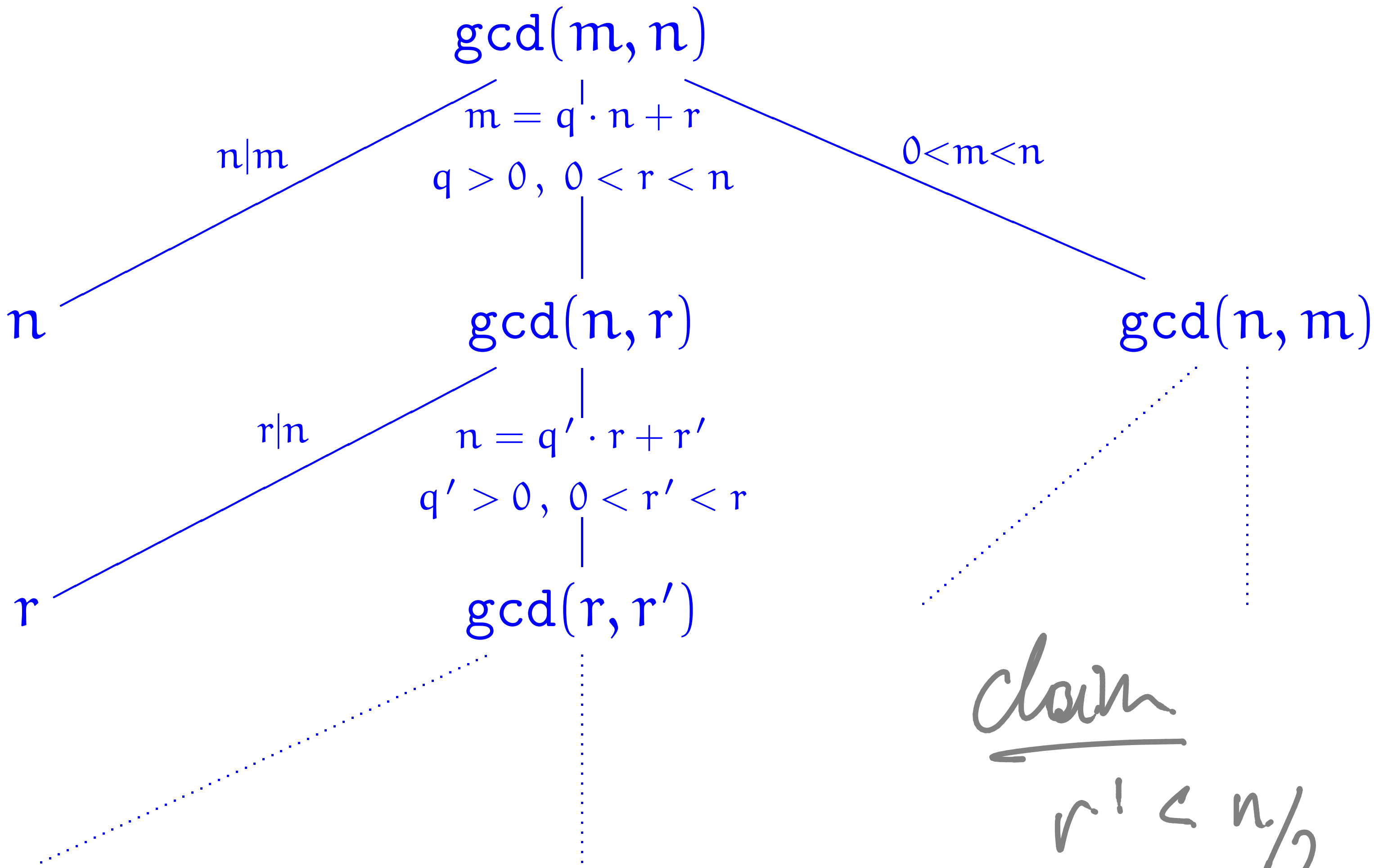
PROOF:

Partial correctness: Because

Exercise

$$\underline{CD}(m,n) = D(\underline{gcd}(m,n))$$

by design of the algorithm.



<u>claim</u>

$r' < n/2$

$2r' < r + r' \leq q' \cdot r + r' = n$

~~Idea:~~

Running Time and Fibonacci:

Calculate $gcd(F_{n+1}, F_n)$

and look at its running time.

Fractions in lowest terms

```
fun lowterms( m , n )
  = let
      val gcdval = gcd( m , n )
    in
      ( m div gcdval , n div gcdval )
    end
```