Proposition 63 *Let* m *be a positive integer. A modular integer* k *in* $\mathbb{Z}_m$ *has a reciprocal if, and only if, there exist integers* i *and* j *such that* $k \cdot i + m \cdot j = 1$.

PROOF: Let m be a pos. int.

Let k be an int s.t. $0 \leq k < m$.

RTP: k has a reciprocal

iff $\exists$ int i, j. $k i + m \cdot j = 1$

($\Rightarrow$) Assume k has a reciprocal; That is, there is $\bar{k}$ an int. s.t. $0 \leq \bar{k} < m$ with $k \bar{k} \equiv 1 \pmod{m}$.

Then $k \cdot \bar{k} - 1 = l \cdot m$ for an int l, and 1 is the int. linear comb. $k \cdot \bar{k} + (-l) \cdot m$.

($\Leftarrow$) Assume: $\exists\, i, j$ int. $k \cdot i + m j = 1$

RTP: $\exists\, \bar{k}$ s.t. $0 \leq \bar{k} < m$ and $k \cdot \bar{k} \equiv 1 \pmod{m}$.

Let i_0 and j_0 be int. s.t. $k \cdot i_0 + m j_0 = 1$

Then $k \cdot i_0 - 1$ is a multiple of m; and so $k \cdot i_0 \equiv 1 \pmod{m}$. Also $i_0 \equiv [i_0]_m \pmod{m}$ with $0 \leq [i_0]_m < m$. Thus, $k \cdot [i_0]_m \equiv 1 \pmod{m}$

$\boxtimes$

Integer linear combinations

Definition 64 *An integer* r *is said to be a* linear combination *of a pair of integers* m *and* n *whenever there are integers* s *and* t *such that* $s \cdot m + t \cdot n = r$.

Proposition 65 *Let* m *be a positive integer. A modular integer* k *in* $\mathbb{Z}_m$ *has a reciprocal if, and only if,* 1 *is an integer linear combination of* m *and* k.

Proposition Let a and b be integers. For all integers d, the following are equivalent:

1. $d \mid a$ and $d \mid b$
2. for all integers i and j, $d \mid (ai+bj)$

PROOF: Let a and b be int. Let d be int.

($\Rightarrow$) Assume: ① $d \mid a$ and ② $d \mid b$.

Let i, j. int. From ①, $a = d \cdot k$ for an int k, from ② $b = d \cdot l$ for an int l. Consider $ai+bj = k \cdot i \cdot d + l \cdot j \cdot d = (k \cdot i + l \cdot j) \cdot d$. Then $d \mid ai+bj$.

($\Leftarrow$) Assume $\forall$ int. i, j. $d \mid (ai + bj)$

In particular, this is the case instantiating $i = 1$ and $j = 0$, that is, $d \mid a$; analogously, instantiating $i = 0$ and $j = 1$, we have $d \mid b$.

$\boxtimes$

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

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

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.

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

Notations:

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

Set equality

Two sets are equal precisely when they have the same elements

Examples:

- $\{ x \in \mathbb{N} \,:\, 2 \mid x \ \wedge \ x \text{ is prime} \} = \{ 2 \}$
- For a positive integer m,
$$\{ x \in \mathbb{Z} \,:\, m \mid x \} = \{ x \in \mathbb{Z} \,:\, x \equiv 0 \pmod{m} \}$$
- $\{ d \in \mathbb{N} \,:\, d \mid 0 \} = \mathbb{N}$

Equivalent predicates specify equal sets:

$$\{ x \in A \mid P(x) \} = \{ x \in A \mid Q(x) \}$$

iff

$$\forall x.\ P(x) \iff Q(x)$$

Example: For a positive integer m,

$$\{ x \in \mathbb{Z}_m \mid x \text{ has a reciprocal in } \mathbb{Z}_m \}$$

$$=$$

$$\{ x \in \mathbb{Z}_m \mid 1 \text{ is an integer linear combination of } m \text{ and } x \}$$

Greatest common divisor

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

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

Example 67

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 68

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

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 71 (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:

$m \equiv \underline{rem}(m, n) \pmod{n}$

$\mathrm{CD}(m, n)$

$= \mathrm{CD}(\underline{rem}(m, n), n)$

$m \equiv m + in \pmod{n}$

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

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

Assume: ① $m \equiv m' \pmod{n}$

$$CD(m,n) \stackrel{?}{=} CD(m',n)$$

equiv

$$\forall d.\ (d \mid m \wedge d \mid n) \iff (d \mid m' \wedge d \mid n)$$

($\Rightarrow$) Assume: ② $d \mid m$ and ③ $d \mid n$

So $d \mid n$ and RTP: $d \mid m'$

From ① $m - m' = i \cdot n$ for an int. i.

So $m' = m + (-i)\,n$ and from ② and ③, d divides any int. lin. comb. of m and n; in particular, m'

($\Leftarrow$) Analogously.

$\boxtimes$

Lemma 73 *For all positive integers* m *and* n*,*

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

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

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

NB If $\mathtt{gcd}$ terminates on input (m, n) with output $\mathtt{gcd}(m, n)$ then $\mathrm{CD}(m, n) = \mathrm{D}\big(\mathtt{gcd}(m, n)\big)$.

Proposition 75 *For all natural numbers* m, n *and* a, b*, if* $\mathrm{CD}(m, n) = \mathrm{D}(a)$ *and* $\mathrm{CD}(m, n) = \mathrm{D}(b)$ *then* $a = b$.

Proposition 76 *For all natural numbers* m, n *and* k*, the following statements are equivalent:*

1. $\mathrm{CD}(m, n) = \mathrm{D}(k)$.
2. ▸ $k \mid m \;\wedge\; k \mid n$, *and*
   ▸ *for all natural numbers* d, $d \mid m \;\wedge\; d \mid n \implies d \mid k$.

Exercise

Definition 77 *For natural numbers* m, n *the unique natural number* k *such that*

- $k \mid m \;\wedge\; k \mid n$, *and*
- *for all natural numbers* d, $d \mid m \;\wedge\; d \mid n \implies d \mid k$.

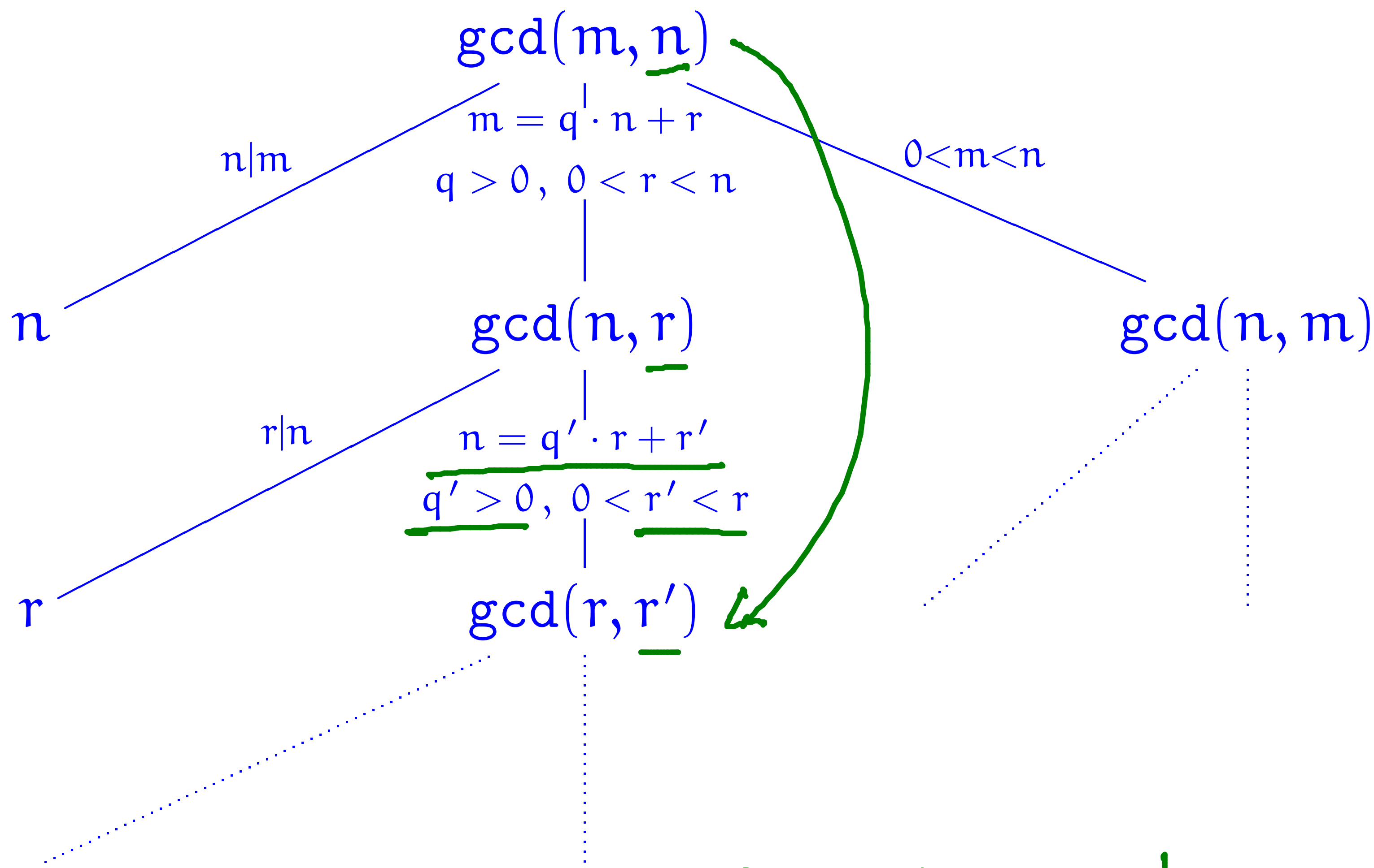
is called the greatest common divisor *of* m *and* n, *and denoted* $\gcd(m, n)$.

Theorem 78 *Euclid's Algorithm* $\mathtt{gcd}$ *terminates on all pairs of positive integers and, for such* m *and* n*, the positive integer* $\mathtt{gcd}(m, n)$ *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:



$$n = q' \cdot r + r' > q' \cdot r' + r' = (q'+1) \cdot r' \geq 2 \cdot r'$$

$$\Rightarrow r' < n/2$$