Modular arithmetic

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

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

with arithmetic operations of addition $+_m$ and multiplication $\cdot_m$ defined as follows

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

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

3 has multiplicative inverse, namely itself.

2 has no multiplicative inverse.

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

$3 \cdot_4 3 = 1$

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.

Every number in $\mathbb{Z}_5$ has multiplicative inverse!

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.

$(\mathbb{Z}_m, 0, +_m)$ abelian group

$=_{def}$ commutative monoid with inverses

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

$+$ distributive law.

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

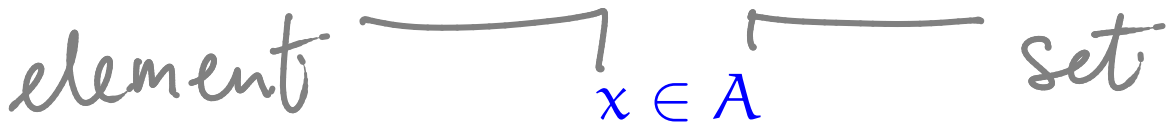
.

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



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		$\{\mathbf{true}, \mathbf{false}\}$
	$[-2..3]$		$\{-2, -1, 0, 1, 2, 3\}$

$2 \in \{2\}$ true while $3 \in \{2\}$ false

$\{\text{true}, \text{false}\} = \{\text{false}, \text{true}\}$

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

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:

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

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 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*?

Assume: (1) $m - m' = kn$ for k int.

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,*

$a|b \wedge a|c \Rightarrow a|ib+jc$

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

PROOF: $\{d \in \mathbb{N} : d|m \wedge d|n\}$ $\{e \in \mathbb{N} : e|m' \wedge e|n\}$

RTP:

$$\forall d \in \mathbb{N}.\,(d|m \wedge d|n) \Rightarrow (d|m' \wedge d|n) \quad (1)$$

$$\wedge\ \forall e \in \mathbb{N}.\,(e|m' \wedge e|n) \Rightarrow (e|m \wedge e|n) \quad (2)$$

(1) Let $d \in \mathbb{N}$. Assume (2) $d|m$ and (3) $d|n$.

RTP: (i) $d|m'$ RTP: (ii) $d|n$ holds by assumption

From (1) $m' = m - kn$

From (2) $d|m$, from (3) $d|n$. So $d \mid m - kn = m'$.

To compute

$$CD(m,n) = CD(m_1, n) \qquad m_1 \equiv m$$

$$= CD(m_2, n) \qquad m_2 \equiv m_1$$

$$\vdots$$

How do we chose m_i ?

$$CD(m,n) = CD(m-n, n) \qquad m \overset{?}{\equiv} m-n \pmod{n}$$

$$\| \; CD(\underline{\max}(m,n) - \min(m,n), \underline{\min}(m,n))$$

$$CD(m,n) = CD(m+n, n)$$

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

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

greatest = n

greatest

greatest

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

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

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

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

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

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
```

$\gcd(m,n) = \gcd(n,m)$ if $m<n$

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

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

13 and 34 are coprime

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

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

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

PROOF: By construction

$$CD(m,n) = D(g.c.d(m,n))$$

which is equivalent to (i) and (ii).

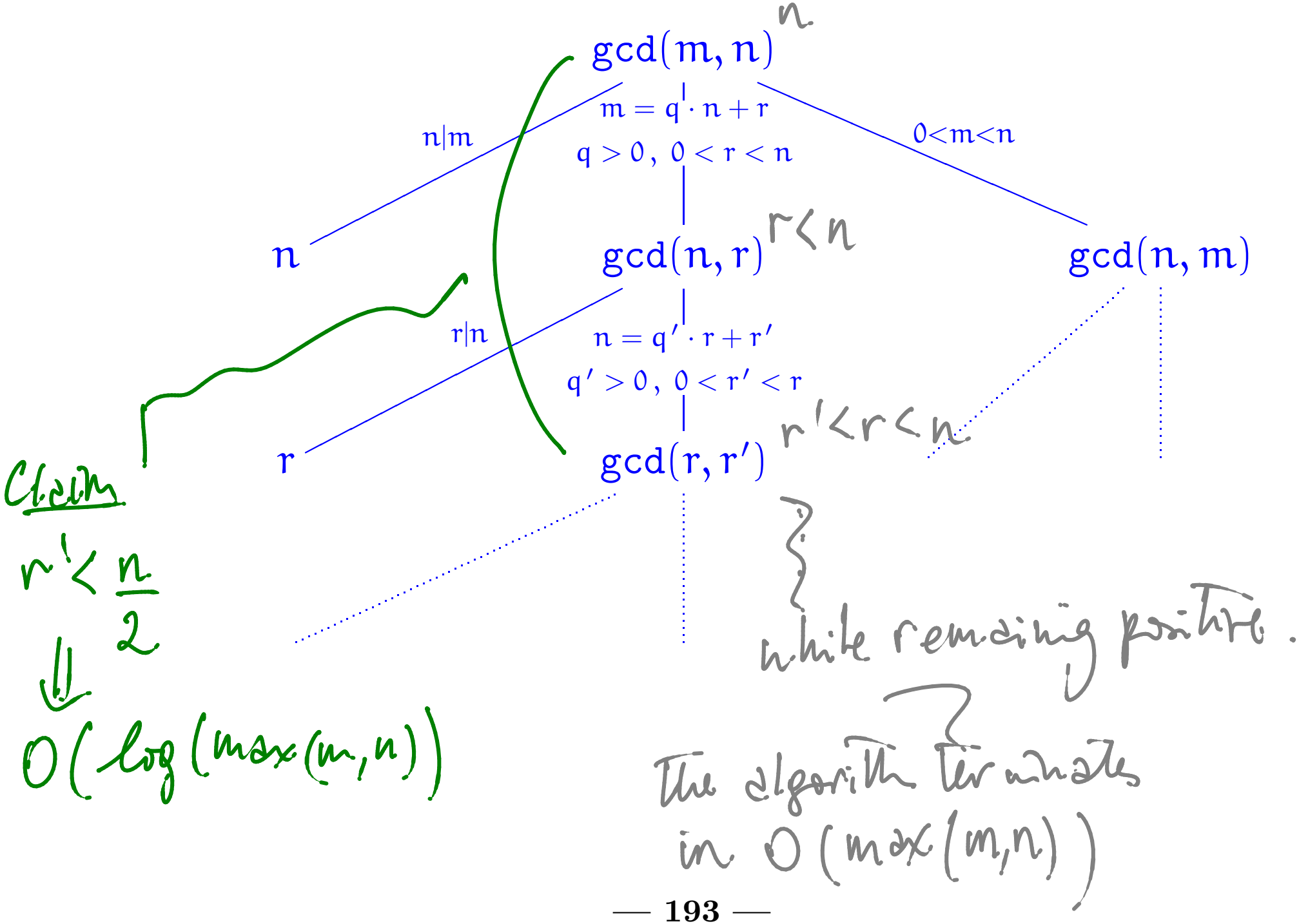
PROOF PRINCIPLE for showing that a number x is the greatest common divisor of m and n.

(1) Prove that it is a common divisor:

$$x \mid m \quad \wedge \quad x \mid n$$

(2) Prove that

if $d \mid m \wedge d \mid n$ then $d \mid x$


gcd(m, n)
n
m = q · n + r
q > 0, 0 < r < n
n|m
0<m<n
gcd(n, r)
r<n
gcd(n, m)
r|n
n = q′ · r + r′
q′ > 0, 0 < r′ < r
r
gcd(r, r′)
r′<r<n
Claim
r′ < n/2
⇓
O(log(max(m,n)))
while remains positive.
The algorithm terminates
in O(max(m,n))