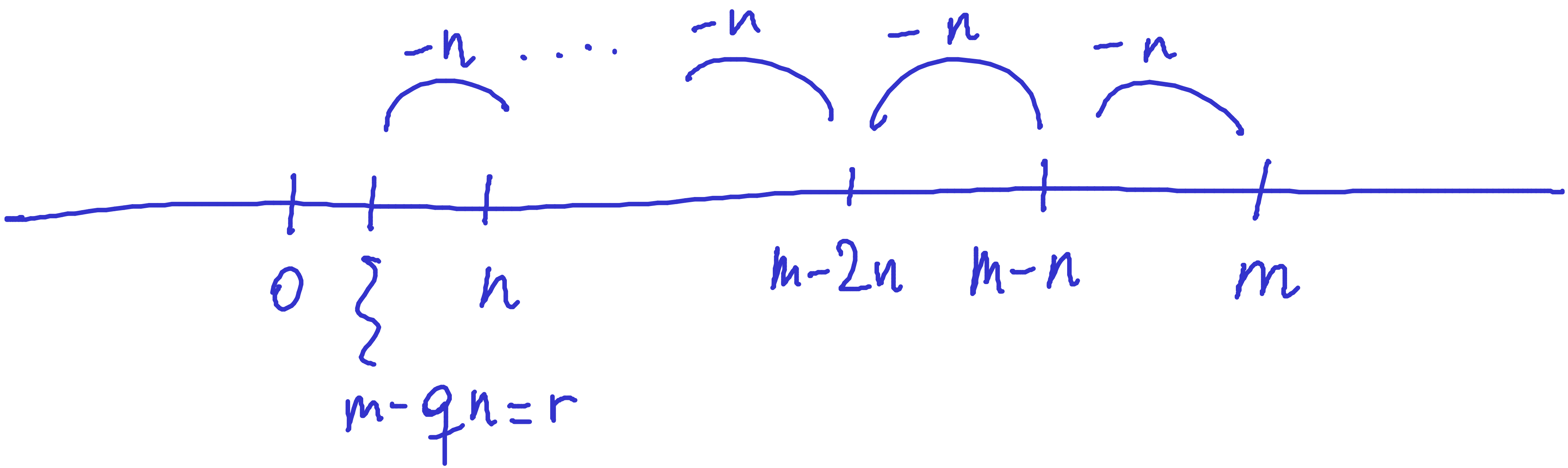
The division theorem and algorithm

Theorem 53 (Division Theorem) *For every natural number* m *and positive natural number* n*, there exists a unique pair of integers* q *and* r *such that* $q \geq 0$, $0 \leq r < n$, *and* $m = q \cdot n + r$.



The division theorem and algorithm

Theorem 53 (Division Theorem) *For every natural number* m *and positive natural number* n*, there exists a unique pair of integers* q *and* r *such that* $q \geq 0$*,* $0 \leq r < n$*, and* $m = q \cdot n + r$*.*

Definition 54 *The natural numbers* q *and* r *associated to a given pair of a natural number* m *and a positive integer* n *determined by the Division Theorem are respectively denoted* $\mathrm{quo}(m, n)$ *and* $\mathrm{rem}(m, n)$*.*

The Division Algorithm in ML:

Suppose $m = q \cdot n + r$

```
fun divalg( m , n )
  = let
      fun diviter( q , r )
        = if r < n then ( q , r )
          else diviter( q+1 , r-n )
    in
      diviter( 0 , m )
    end
```

✓

$m \overset{?}{=} (q+1) \cdot n + (r-n)$ ✓

$\boxed{m = \underbrace{\text{first arg}}_{0} \cdot n + \underbrace{\text{2nd arg}}_{m}.}$

$m = \text{quo}(m,n) \cdot n + \text{rem}(m,n).$

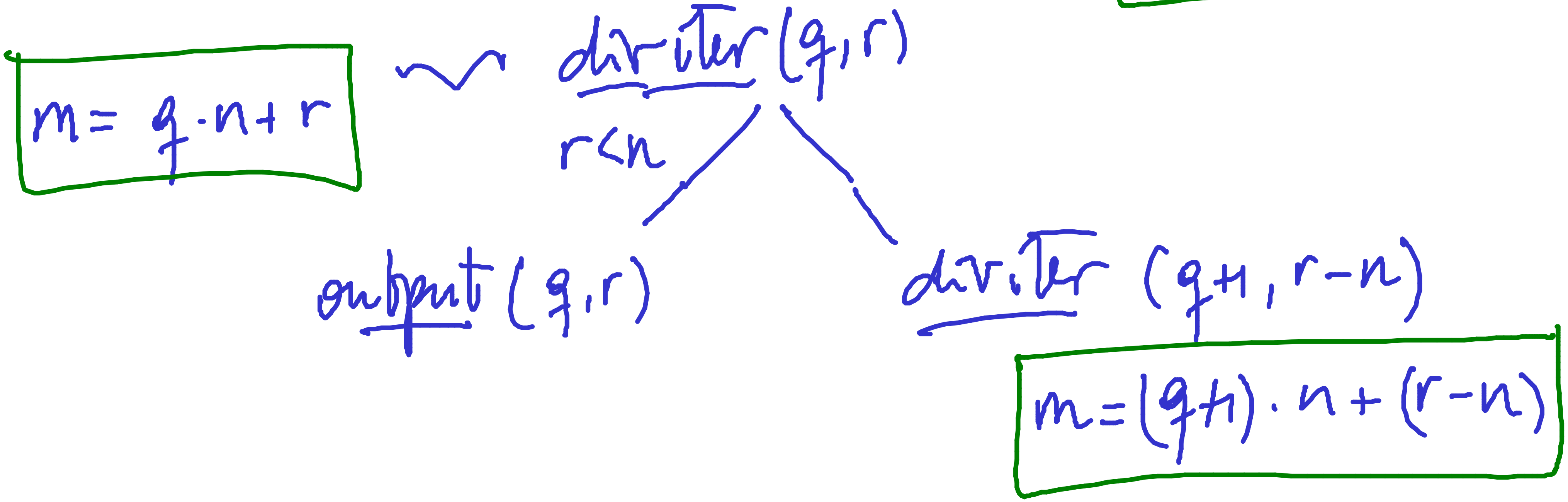
```
fun quo( m , n ) = #1( divalg( m , n ) )

fun rem( m , n ) = #2( divalg( m , n ) )
```

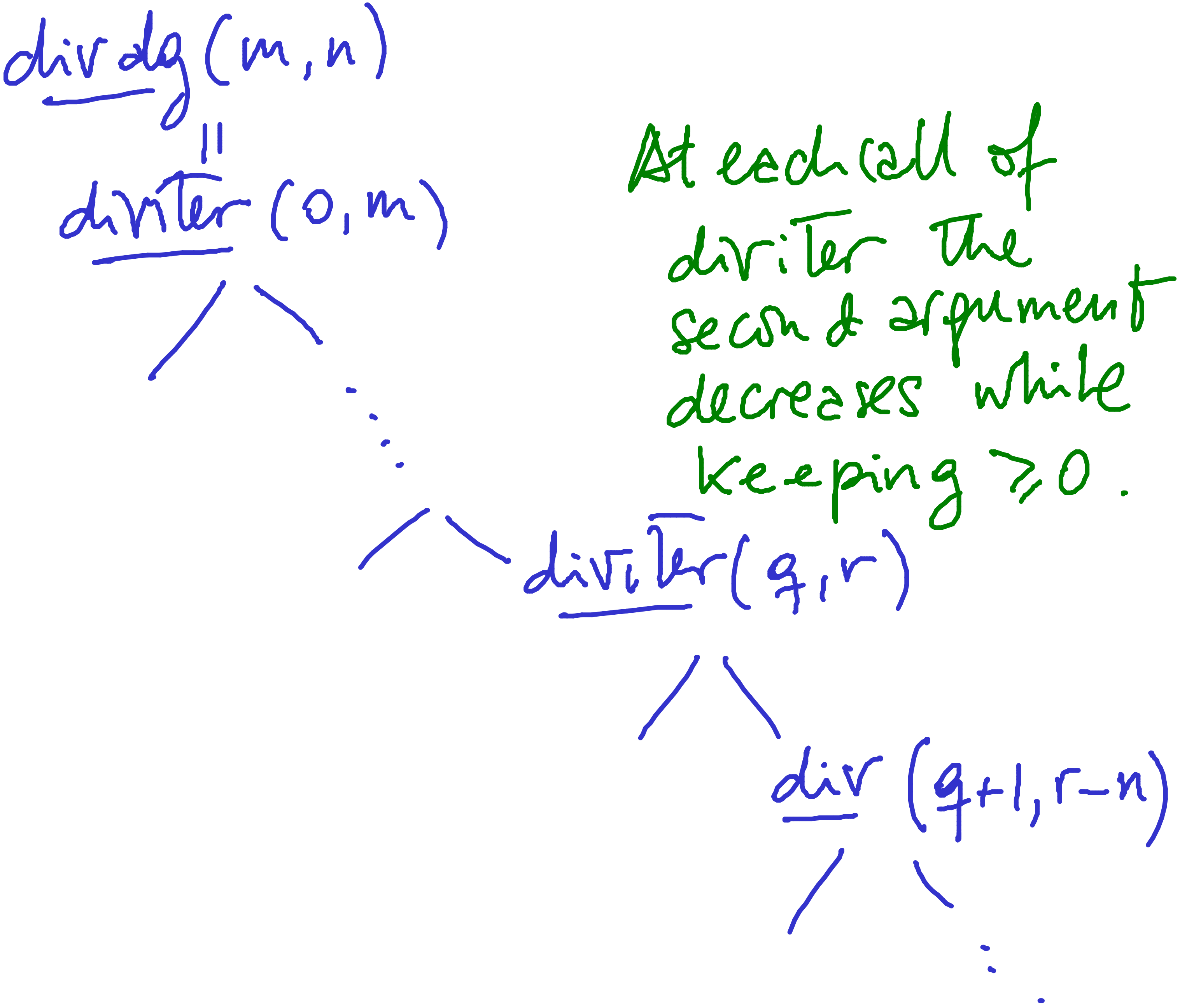
Theorem 56 *For every natural number* m *and positive natural number* n*, the evaluation of* $\mathtt{divalg}(m, n)$ *terminates, outputing a pair of natural numbers* (q_0, r_0) *such that* $r_0 < n$ *and* $m = q_0 \cdot n + r_0$.

PROOF:

$\underline{\mathrm{divalg}}(m,n) = \underline{\mathrm{diviter}}(0,m)$

$\rightsquigarrow \boxed{m = \mathrm{fst\ arg} \cdot n + \mathrm{snd\ arg}}$





At each call of diviter the second argument decreases while keeping $\geqslant 0$.

☒

- Every integer is either even or odd.
- Every natural is either even or odd.

For every natural number m there exist a pair q, r s.t. $m = 2q + r$ with $0 \leq r < 2$.

unique

Proposition 57 *Let m be a positive integer. For all natural numbers k and l,*

$$k \equiv l \pmod{m} \iff \mathrm{rem}(k, m) = \mathrm{rem}(l, m) \quad .$$

PROOF: Let m be a positive integer. Let k and l be natural numbers.

(⇒) Assume ① $k \equiv l \pmod{m}$

$k = q \cdot m + r$ with ④ $0 \le r < m$

and $l = q' \cdot m + r'$ with ⑤ $0 \le r' < m$

So ② $k \equiv r \pmod{m}$ and ③ $l \equiv r' \pmod{m}$

And therefore $r \equiv r' \pmod{m}$. From a previous result and using ④ & ⑤, we have $r = r'$.

(⇐) Exercise.

Corollary 58 *Let* m *be a positive integer.*

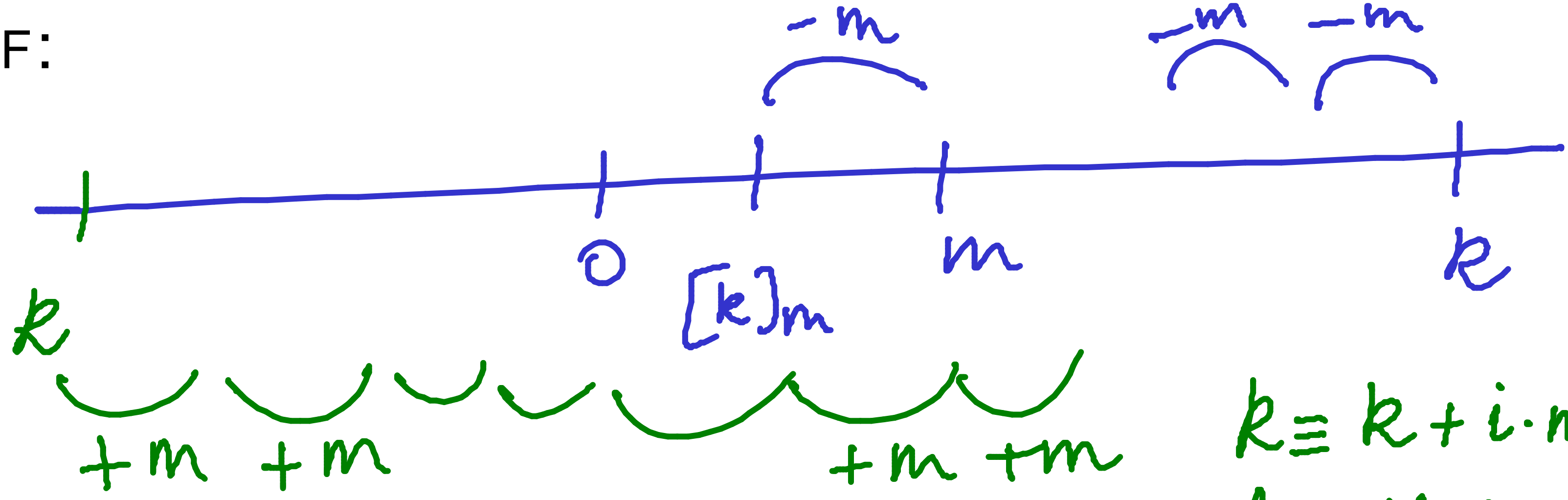
1. *For every natural number* n*,*

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

2. *For every integer* k *there exists a unique integer* $[k]_m$ *such that*

$$0 \le [k]_m < m \quad \text{and} \quad k \equiv [k]_m \pmod{m} \quad .$$

PROOF:



$k \equiv k + i \cdot m \pmod{m}$
for all i

For $i = -k$, $k + im$ is a nat. number

So we have $k \equiv [k+im]_m$

☒

Modular arithmetic

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

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

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 $0 \leq k, l < m$.

For k and l in $\mathbb{Z}_m$,

$$k +_m l \text{ and } k \cdot_m l$$

are the unique modular integers in $\mathbb{Z}_m$ such that

$$k +_m l \equiv k + l \pmod{m}$$

$$k \cdot_m l \equiv k \cdot l \pmod{m}$$

Example 60 *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 61 *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 62 *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

.

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

PROOF: Let m be a positive integer.

($\Rightarrow$) Let $0 \leq k < m$ with reciprocal $\bar{k}$, that is, $0 \leq \bar{k} < m$ and $k \cdot \bar{k} \equiv 1 \pmod{m}$. Then, $k \cdot \bar{k} - 1 = j \cdot m$ for some int. j. So $k \cdot \bar{k} + (-j) \cdot m = 1$. Hence, 1 is an int. linear combination of k and m.

($\Leftarrow$) Suppose: $k i + m \cdot j = 1$ Then $k \cdot i - 1$ is a multiple of m. Hence, $k \cdot i \equiv 1 \pmod{m}$ and k has a reciprocal. (namely $[i]_m$).

☒

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.