

# Contents

<b>1</b>	<b>Functions</b>	<b>2</b>
1.1	factor.find – find a factor . . . . .	2
1.1.1	trialDivision – trial division . . . . .	2
1.1.2	pmom – $p - 1$ method . . . . .	2
1.1.3	rhomethod – $\rho$ method . . . . .	3

# Chapter 1

## Functions

### 1.1 `factor.find` – find a factor

All methods in this module return one of a factor of given integer. If it fails to find a non-trivial factor, it returns 1. Note that 1 is a factor anyway.

`verbose` boolean flag can be specified for verbose reports. To receive these messages, you have to prepare a logger (see [logging](#)).

#### 1.1.1 `trialDivision` – trial division

`trialDivision(n: integer, **options ) → integer`

Return a factor of `n` by trial divisions.

`options` can be either one of the following:

1. `start` and `stop` as range parameters. In addition to these, `step` is also available.
2. `iterator` as an iterator of primes.

If `options` is not given, the function divides `n` by primes from 2 to the floor of the square root of `n` until a non-trivial factor is found.

`verbose` boolean flag can be specified for verbose reports.

#### 1.1.2 `pmom` – $p - 1$ method

`pmom(n: integer, **options ) → integer`

Return a factor of `n` by the  $p - 1$  method.

The function tries to find a non-trivial factor of `n` using Algorithm 8.8.2 ( $p - 1$

first stage) of [?]. In the case of  $n = 2^i$ , the function will not terminate. Due to the nature of the method, the method may return the trivial factor only.

`verbose` Boolean flag can be specified for verbose reports, though it is not so verbose indeed.

### 1.1.3 rhomethod – $\rho$ method

**`rhomethod(n: integer, **options) → integer`**

Return a factor of `n` by Pollard's  $\rho$  method.

The implementation refers the explanation in [?]. Due to the nature of the method, a factorization may return the trivial factor only.

`verbose` Boolean flag can be specified for verbose reports.

#### Examples

```
>>> factor.find.trialDivision(1001)
7
>>> factor.find.trialDivision(1001, start=10, stop=32)
11
>>> factor.find.pmom(1001)
91
>>> import logging
>>> logging.basicConfig()
>>> factor.find.rhomethod(1001, verbose=True)
INFO:nzmath.factor.find:887 748
13
```