

Package ‘gmp’

January 21, 2012

Version 0.5-1

Date 2012-01-20

Title Multiple Precision Arithmetic

Author Antoine Lucas, Immanuel Scholz, Rainer Boehme
<rb-gmp@reflex-studio.de>, Sylvain Jasson
<jasson@toulouse.inra.fr>, Martin Maechler <maechler@stat.math.ethz.ch>

Maintainer Antoine Lucas <antoinelucas@gmail.com>

Description Multiple Precision Arithmetic (big integers and rationals, prime number tests, matrix computation), ‘‘arithmetic without limitations’’ using the C library gmp.

Depends methods

Suggests Rmpfr

SystemRequirements gmp (>= 4.1.4)

License GPL

URL <http://mulcyber.toulouse.inra.fr/projects/gmp>

Repository CRAN

Date/Publication 2012-01-21 07:56:32

R topics documented:

apply	2
Bigq	3
bigq	4
Bigq operators	5
bigz	6
bigz operators	9
cumsum	11

Extract	12
Extremes	13
factorialZ	14
factorization	15
frexpZ	16
gcd.bigz	17
gcdex	18
gmp.utils	19
isprime	19
lucnum	20
matrix	21
modulus	23
nextprime	24
Oakley	25
powm	26
Random	27
Relational Operator	28
sizeinbase	28
solve.bigz	29
Stirling	30

Index 33

apply *Apply Functions Over Matrix Margins (Rows or Columns)*

Description

These are S3 [methods](#) for `apply()` which we re-export as S3 generic function. They “overload” the `apply()` function for big rationals (“bigq”) and big integers (“bigz”).

Usage

```
## S3 method for class 'bigz'
apply(X, MARGIN, FUN, ...)
## S3 method for class 'bigq'
apply(X, MARGIN, FUN, ...)
```

Arguments

X	a matrix of class bigz or bigq, see e.g., matrix.bigz .
MARGIN	1: apply function to rows; 2: apply function to columns
FUN	function to be applied
...	(optional) extra arguments for FUN(), as e.g., in lapply .

Value

The bigz and bigq methods return a vector of class “bigz” or “bigq”, respectively.

Author(s)

Antoine Lucas

See Also[apply](#); [lapply](#) is used by our `apply()` method.**Examples**

```
x <- as.bigz(matrix(1:12,3))
apply(x,1,min)
apply(x,2,max)

x <- as.bigq(x ^ 3, d = (x + 3)^2)
apply(x,1, min)
apply(x,2, sum)
## now use the "..." to pass na.rm=TRUE :
x[2,3] <- NA
apply(x,1, sum)
apply(x,1, sum, na.rm = TRUE)
```

Bigq*Relational Operators*

Description

Binary operators which allow the comparison of values in atomic vectors.

Usage

```
## S3 method for class 'bigq'
sign(x)

## S3 method for class 'bigq'
e1 < e2
## S3 method for class 'bigq'
e1 <= e2
## S3 method for class 'bigq'
e1 == e2
## S3 method for class 'bigq'
e1 >= e2
## S3 method for class 'bigq'
e1 > e2
## S3 method for class 'bigq'
e1 != e2
```

Argumentsx, e1, e2 Object or vector of class `bigq`

Examples

```
x <- as.bigq(8000,21)
x < 2 * x
```

bigq

Large sized rationals

Description

Type class supporting arithmetic operations on very large rationals.

Usage

```
as.bigq(n, d = 1)
## S3 method for class 'bigq'
as.character(x, b=10,...)
## S3 method for class 'bigq'
as.double(x,...)
as.bigz.bigq(a, mod=NA)
## S3 method for class 'bigq'
is.na(x)
## S3 method for class 'bigq'
print(x, quote=FALSE, ...)
denominator(x)
numerator(x)
```

Arguments

n,d	either integer, numeric or string value (String value: either starting with 0x for hexadecimal, 0b for binary or without prefix for decimal values. Any format error results in 0). n stands for numerator, d for denominator
a	an element of class "bigq"
mod	optional modulus to convert into biginteger
x	numeric value
b	base: from 2 to 36
...	additional arguments passed to methods
quote	(for printing:) logical indicating if the numbers should be quoted (as characters are); the default used to be TRUE (implicitly) till 2011.

Details

as.bigz.bigq() returns the smallest integers not less than the corresponding rationals bigq.

Value

An R object of (S3) class "bigq" representing the parameter value.

Author(s)

Antoine Lucas

References

<http://mulcyber.toulouse.inra.fr/projects/gmp/>

Examples

```
x <- as.bigq(21,6)
x
# 7 / 2
# Wow ! result is simplified.

y <- as.bigq(5,3)

# addition works !
x + y

# You can even try multiplication, division...
x * y / 13

# convert to string, double
as.character(x)
as.double(x)
```

Bigq operators

Basic arithmetic operators for large rationals

Description

Addition, subtraction, multiplication, division, and absolute value for large rationals, i.e. "bigq" class R objects.

Usage

```
add.bigq(e1, e2)
## S3 method for class 'bigq'
e1 + e2

sub.bigq(e1, e2=NULL)
## S3 method for class 'bigq'
e1 - e2
```

```
mul.bigq(e1, e2)
## S3 method for class 'bigq'
e1 * e2

div.bigq(e1, e2)
## S3 method for class 'bigq'
e1 / e2

## S3 method for class 'bigq'
abs(x)
```

Arguments

`e1, e2, x` of class "bigq", or (e1 and e2) integer or string from an integer

Details

Operators can be use directly when the objects are of class "bigq": $a + b$, $a * b$, etc.

Value

A bigq class representing the result of the arithmetic operation.

Author(s)

Immanuel Scholz and Antoine Lucas

References

<http://mulcyber.toulouse.inra.fr/projects/gmp/>

Examples

```
## 1/3 + 1 = 4/3 :
as.bigq(1,3) + 1
```

bigz

Large Sized Integer Values

Description

Class "bigz" encodes arbitrarily large integers (via GMP)

Usage

```

as.bigz(a, mod = NA)
## S3 method for class 'bigz'
as.character(x, b = 10, ...)

## S3 method for class 'bigz'
is.na(x)
## S3 method for class 'bigz'
print(x, quote=FALSE, ...)

```

Arguments

a	either integer , numeric (i.e., double) or character vector. If character: the strings either start with 0x for hexadecimal, 0b for binary, 0 for octal, or without a 0* prefix for decimal values. Formatting errors are signalled as with stop .
b	base: from 2 to 36
x	numeric value
...	additional arguments passed to methods
mod	an integer, numeric, string or bigz of the internal modulus, see below.
quote	(for printing:) logical indicating if the numbers should be quoted (as characters are); the default used to be TRUE (implicitly) till 2011.

Details

Bigz's are integers of arbitrary, but given length (means: only restricted by the host memory). Basic arithmetic operations can be performed on bigzs as addition, subtraction, multiplication, division, modulation (remainder of division), power, multiplicative inverse, calculating of the greatest common divisor, test whether the integer is prime and other operations needed when performing standard cryptographic operations.

For a review of basic arithmetics, see [add.bigz](#).

Comparison are supported, i.e., "=", "!=", "<", "<=", ">", and ">=".

Objects of class "bigz" may have an attribute mod which specifies a modulus that is applied after each arithmetic operation. When the object has such a modulus m , all arithmetic is performed "*modulo m*", i.e.,

```
result <- mod.bigz(result, m) ## == result %% m
```

is called after performing the arithmetic operation and the result will have the attribute mod set accordingly.

Powers of bigzs can only be performed, if either a modulus is going to be applied to the result bigz or if the exponent fits into an integer value. So, if you want to calculate a power in a finite group ("modulo c "), for large c do not use $a \wedge b \% c$, but rather `as.bigz(a,c) ^ b`.

The following rules for the result's modulus apply when performing arithmetic operations on bigzs:

- If none of the operand has a modulus set, the result will not have a modulus.

- If both operands have a different modulus, the result will not have a modulus, except in case of `mod.bigz`, where the second operand's value is used.
- If only one of the operands has a modulus or both have a common (the same), it is set and applied to the result, except in case of `mod.bigz`, where the second operand's value is used.

Value

An R object of (S3) class "bigz", representing the argument `x`.

Note

```
x <- as.bigz(12345678901234567890123456789012345678901234567890)
```

will not work as R converts the number to a double, losing precision and only then convert to a "bigz" object.

Instead, use the syntax

```
x <- as.bigz("1234567890123456789012345678901234567890")
```

Author(s)

Immanuel Scholz

References

The GNU MP Library, see <http://gmplib.org>

Examples

```
## 1+1=2
a <- as.bigz(1)
a + a

## Two non-small Mersenne primes:
two <- as.bigz(2)
p1 <- two^107 - 1 ; isprime(p1); p1
p2 <- two^127 - 1 ; isprime(p2); p2

## Calculate c = x^e mod n
## -----
x <- as.bigz("0x123456789abcdef") # my secret message
e <- as.bigz(3) # something smelling like a dangerous public RSA exponent
(n <- p1 * p2) # a product of two primes
as.character(n, b=16) # as both primes were Mersenne's..

## recreate the three numbers above [for demo below]:
n. <- n; x. <- x; e. <- e # save
Rev <- function() { n <<- n.; x <<- x.; e <<- e.}
```

```

# first way to do it right
modulus(x) <- n
c <- x ^ e ; c ; Rev()

# similar second way (makes more sense if you reuse e) to do it right
modulus(e) <- n
c2 <- x ^ e
stopifnot(identical(c2, c)) ; Rev()

# third way to do it right
c3 <- x ^ as.bigz(e, n) ; stopifnot(identical(c3, c))

# fourth way to do it right
c4 <- as.bigz(x, n) ^ e ; stopifnot(identical(c4, c))

# WRONG! (although very beautiful. Ok only for very small 'e' as here)
cc <- x ^ e %% n
cc == c

# Return result in hexa
as.character(c, b=16)

```

bigz operators

Basic Arithmetic Operators for Large Integers ("bigz")

Description

Addition, subtraction, multiplication, (integer) division, remainder of division, multiplicative inverse, power and logarithm functions.

Usage

```

add.bigz(e1, e2)
sub.bigz(e1, e2 = NULL)
mul.bigz(e1, e2)
div.bigz(e1, e2)
divq.bigz(e1,e2) ## == e1 %% e2
mod.bigz(e1, e2) ## == e1 %% e2
## S3 method for class 'bigz'
abs(x)

inv.bigz(a, b,...)## == (1 / a) (modulo b)

pow.bigz(e1, e2,...)## == e1 ^ e2

## S3 method for class 'bigz'
log(x, base=exp(1))

```

```
## S3 method for class 'bigz'
log2(x)
## S3 method for class 'bigz'
log10(x)
```

Arguments

x	bigz, integer or string from an integer
e1, e2, a, b	bigz, integer or string from an integer
base	base of the logarithm; base e as default
...	Additional parameters

Details

For details about the internal modulus state, see the manpage of [bigz](#).

div or "/" return a rational number; divq or "%/%" return the quotient of integer division.

Operators can be used directly when objects are of class bigz: a + b, log(a), etc.

Value

A bigz class representing the result of the arithmetic operation.

Author(s)

Immanuel Scholz and Antoine Lucas

References

The GNU MP Library, see <http://gmplib.org>

Examples

```
# 1+1=2
as.bigz(1) + 1
as.bigz(2)^10
as.bigz(2)^200

# if my.large.num.string is set to a number, this returns the least byte
(my.large.num.string <- paste(sample(0:9, 200, replace=TRUE), collapse=""))
mod.bigz(as.bigz(my.large.num.string), "0xff")

# power exponents can be up to MAX_INT in size, or unlimited if a
# bigz's modulus is set.
pow.bigz(10, 10000)

## Modulo 11, 7 and 8 are inverses :
as.bigz(7, mod = 11) * 8 ## ==> 1 (mod 11)
inv.bigz(7, 11)## hence, 8
a <- 1:10
(i.a <- inv.bigz(a, 11))
```

```

d <- as.bigz(7)
a %% d # = divq(a, d)
a %% d # = mod.bigz (a, d)

stopifnot(inv.bigz(7, 11) == 8,
          all(as.bigz(i.a, 11) * a == 1),
          identical(a %% d, divq.bigz(1:10, 7)),
          identical(a %% d, mod.bigz (a, d))
)

```

cumsum

(Cumulative) Sums, Products of Large Integers and Rationals

Description

These are methods to ‘overload’ the `sum()`, `cumsum()` and `prod()` functions for big rationals and big integers.

Usage

```

## S3 method for class 'bigz'
cumsum(x)
## S3 method for class 'bigq'
cumsum(x)
## S3 method for class 'bigz'
sum(..., na.rm = FALSE)
## S3 method for class 'bigq'
sum(..., na.rm = FALSE)
## S3 method for class 'bigz'
prod(..., na.rm = FALSE)
## S3 method for class 'bigq'
prod(..., na.rm = FALSE)

```

Arguments

<code>x, ...</code>	R objects of class <code>bigz</code> or <code>bigq</code> or ‘simple’ numbers.
<code>na.rm</code>	logical indicating if missing values (<code>NA</code>) should be removed before the computation.

Value

return an element of class `bigz` or `bigq`.

Author(s)

Antoine Lucas

See Also[apply](#)**Examples**

```
x <- as.bigz(1:12)
cumsum(x)
prod(x)
sum(x)
```

```
x <- as.bigq(1:12)
cumsum(x)
prod(x)
sum(x)
```

Extract*Extract or Replace Parts of an Object*

Description

Operators acting on vectors, arrays and lists to extract or replace subsets.

Usage

```
## S3 method for class 'bigz'
c(..., recursive = FALSE)
## S3 method for class 'bigq'
c(..., recursive = FALSE)
## S3 method for class 'bigz'
rep(x,times, ...)
## S3 method for class 'bigq'
rep(x,times, ...)
```

Arguments

<code>x</code>	R object of class "bigz" or "bigq", respectively.
<code>...</code>	further arguments, notably for <code>c()</code> .
<code>times</code>	integer
<code>recursive</code>	unused here

Note

Unlike standard matrices, `x[i]` and `x[i,]` do the same.

Examples

```

a <- as.bigz(123)
## indexing "outside" --> extends the vectors (filling with NA)
a[2] <- a[1]
a[4] <- -4

## create a vector of 3 a
c(a,a,a)

## repeate a 5 times
rep(a,5)

## with matrix
m <- matrix.bigz(1:6,3)

## these do the same:
m[1,]
m[1]
m[-c(2,3),]
m[-c(2,3)]
m[c(TRUE,FALSE,FALSE)]

##_modification on matrix
m[2,-1] <- 11

```

Extremes

Extrema (Maxima and Minima)

Description

We provide S3 [methods](#) for `min` and `max` for big rationals (`bigq`) and big integers (`bigz`); consequently, `range()` works as well.

Usage

```

## S3 method for class 'bigz'
max(..., na.rm=FALSE)
## S3 method for class 'bigq'
max(..., na.rm=FALSE)
## S3 method for class 'bigz'
min(..., na.rm=FALSE)
## S3 method for class 'bigq'
min(..., na.rm=FALSE)

```

Arguments

```

...           numeric arguments
na.rm        a logical indicating whether missing values should be removed.

```

Value

return an element of class `bigz` or `bigq`.

Author(s)

Antoine Lucas

See Also

[max](#)

Examples

```
x <- as.bigz(1:10)
max(x)
min(x)
range(x) # works correctly via default method

Q <- as.bigq(1:10, 3)
max(Q)
min(Q)

stopifnot(range(x) == c(1,10), 3*range(Q) == c(1,10))
```

factorialZ

Factorial and Binomial Coefficient as Big Integer

Description

Efficiently compute the factorial $n!$ or a binomial coefficient $\binom{n}{k}$ as big integer (class `bigz`).

Usage

```
factorialZ(n)
chooseZ(n, k)
```

Arguments

`n` non-negative integer (scalar for now), for `factorialZ`. For `chooseZ`, may be a `bigz` big integer, also negative.

`k` non-negative integer.

Value

a number of (S3) class `bigz`.

See Also

[factorial](#) and [gamma](#) in base R;

Examples

```
factorialZ(200)

n <- 1000
f1000 <- factorialZ(n)
stopifnot(1e-15 > abs(as.numeric(1 - lfactorial(n)/log(f1000))))

system.time(replicate(8, f1e4 <- factorialZ(10000)))
nchar(as.character(f1e4))# 35660 ... (too many to even look at ..)

chooseZ(1000, 100)
chooseZ(as.bigz(2)^120, 10)
```

factorization

Factorize a number

Description

Give all primes numbers to factor the number

Usage

```
factorize(n)
```

Arguments

n Either integer, numeric or string value (String value: either starting with 0x for hexadecimal, 0b for binary or without prefix for decimal values.) Or an element of class bigz.

Details

The factorization function uses the Pollard Rho algorithm.

Value

Vector of class bigz.

Author(s)

Antoine Lucas

References

The GNU MP Library, see <http://gmplib.org>

Examples

```
factorize(34455342)
```

fexpZ

*Split Number into Fractional and Exponent of 2 Parts***Description**

Breaks the number x into its binary significand (“fraction”) $d \in [0.5, 1)$ and ex , the integral exponent for 2, such that $x = d \cdot 2^{ex}$.

If x is zero, both parts (significand and exponent) are zero.

Usage

```
fexpZ(x)
```

Arguments

x integer or big integer ([bigz](#)).

Value

a [list](#) with the two components

d a numeric vector whose absolute values are either zero, or in $[\frac{1}{2}, 1)$.

exp an integer vector of the same length.

Author(s)

Martin Maechler

See Also

[log2](#), etc; for [bigz](#) objects built on (the C++ equivalent of) `fexp()`, actually GMP’s ‘`mpz_get_d_2exp()`’.

Examples

```
fexpZ(1:10)
## and confirm :
with(fexpZ(1:10), d * 2^exp)
x <- rpois(1000, lambda=100)
stopifnot(all.equal(x, with(fexpZ(x), d* 2^exp)))
```

`gcd.bigz`*Greatest Common Divisor, Least Common Multiple*

Description

Compute the greatest common divisor (GCD) and least common multiple (LCD) of two (big) integers.

Usage

```
## S3 method for class 'bigz'  
gcd(a, b)  
lcm.bigz(a, b)
```

Arguments

`a, b` Either integer, numeric, `bigz` or a string value; if a string, either starting with `0x` for hexadecimal, `0b` for binary or without prefix for decimal values.

Value

An element of class `bigz`

Author(s)

Antoine Lucas

References

The GNU MP Library, see <http://gmplib.org>

See Also

[gcdex](#)

Examples

```
gcd.bigz(210,342) # or also  
lcm.bigz(210,342)  
a <- 210 ; b <- 342  
stopifnot(gcd.bigz(a,b) * lcm.bigz(a,b) == a * b)
```

`gcdex`*Compute Bezoult coefficient*

Description

Compute g,s,t as $as + bt = g = \text{gcd}(a,b)$. s and t are also known as Bezoult coefficients.

Usage

```
gcdex(a, b)
```

Arguments

a, b Either integer, numeric or string value (String value: either starting with `0x` for hexadecimal, `0b` for binary or without prefix for decimal values.) Or an element of class `bigz`.

Value

3 values:

g, s, t Elements of class `bigz`

Author(s)

Antoine Lucas

References

The GNU MP Library, see <http://gmplib.org>

See Also

[gcd.bigz](#)

Examples

```
gcdex(342, 654)
```

`gmp.utils`*GMP Number Utilities*

Description

`gmpVersion()` returns the version of the GMP library which **gmp** is currently linked to.

Usage

```
gmpVersion()
```

References

The GNU MP Library, see <http://gmplib.org>

Examples

```
gmpVersion()
```

`isprime`*Determine if number is (very probably) prime*

Description

Determine whether the number is prime or not. 2: number is prime, 1, number is probably prime (without being certain), 0 number is composite.

Usage

```
isprime(n, reps = 40)
```

Arguments

<code>n</code>	integer number, to be tested
<code>reps</code>	integer number of repeats

Details

This function does some trial divisions, then some Miller-Rabin probabilistic primary tests. `reps` controls how many such tests are done, 5 to 10 is a reasonable number. More will reduce the chances of a composite being returned as “probably prime”.

Value

0	<i>n</i> is not prime
1	<i>n</i> is probably prime
2	<i>n</i> is prime

Author(s)

Antoine Lucas

References

The GNU MP Library, see <http://gmplib.org>

See Also

[nextprime](#)

Examples

```
isprime(210)
isprime(71)

# All primes numbers from 1 to 100
t <- isprime(1:99)
(1:99)[t > 0]

table(isprime(1:10000))# 0 and 2 : surely prime or not prime

primes <- function(n) {
  ## all primes <= n
  stopifnot(length(n) == 1, n <= 1e7) # be reasonable
  p <- c(2L, as.integer(seq(3, n, by=2)))
  p[isprime(p) > 0]
}

## quite quickly, but for these small numbers
## still slower than e.g., sfsmisc::primes()
system.time(p100k <- primes(100000))

## The first couple of Mersenne primes:
p.exp <- primes(1000)
Mers <- as.bigz(2) ^ p.exp - 1
isp.M <- sapply(seq_along(Mers), function(i) isprime(Mers[i], reps=256))
cbind(p.exp, isp.M)[isp.M > 0,]
Mers[isp.M > 0]
```

lucnum

Compute Fibonacci and Lucas numbers

Description

fibnum compute n-th Fibonacci number. fibnum2 compute (n-1)-th and n-th Fibonacci number.
 lucnum compute n-th lucas number. lucnum2 compute (n-1)-th and n-th lucas number.

Fibonacci numbers are define by: $F_n = F_{n-1} + F_{n-2}$ Lucas numbers are define by: $L_n = F_n + 2F_{n-1}$

Usage

```
fibnum(n)
fibnum2(n)
lucnum(n)
lucnum2(n)
```

Arguments

n Integer

Value

Fibonacci numbers and Lucas number.

Author(s)

Antoine Lucas

References

The GNU MP Library, see <http://gmplib.org>

Examples

```
fibnum(10)
fibnum2(10)
lucnum(10)
lucnum2(10)
```

matrix

Matrix manipulation with gmp

Description

Overload of “all” standard tools useful for matrix manipulation adapted to large numbers.

Usage

```
## S3 method for class 'bigz'
matrix(data = NA, nrow = 1, ncol = 1, byrow = FALSE, dimnames = NULL, mod = NA, ...)

## S3 method for class 'bigz'
x %*% y
## S3 method for class 'bigq'
x %*% y
## S3 method for class 'bigq'
crossprod(x, y=NULL)
```

```
## S3 method for class 'bigz'
tcrossprod(x, y=NULL)
## ..... etc
```

Arguments

data	an optional data vector
nrow	the desired number of rows
ncol	the desired number of columns
byrow	logical. If FALSE (the default), the matrix is filled by columns, otherwise the matrix is filled by rows.
dimnames	not implemented for "bigz" or "bigq" matrices.
mod	optional modulus (when data is "bigz").
...	Not used
x,y	numeric, bigz, or bigq matrices or vectors.

Details

Extract function is the same use for vector or matrix. Then, `x[i]` return same value as `x[i,]`.

Special features concerning the "bigz" class: the modulus can be

Unset: Just play with large numbers

Set with a vector of size 1: Example: `matrix.bigz(1:6,nrow=2,ncol=3,mod=7)` This means you work in Z/nZ , for the whole matrix. It is the only case where the `%%` and `solve` functions will work in Z/nZ .

Set with a vector smaller than data: Example: `matrix.bigz(1:6,nrow=2,ncol=3,mod=1:5)`. Then, the modulus is repeated to the end of data. This can be used to define a matrix with a different modulus at each row.

Set with same size as data: Modulus is defined for each cell

Value

A matrix of class bigz or bigq

Author(s)

Antoine Lucas

See Also

Solving linear algebra system `solve.bigz`; `matrix`

Examples

```

V <- as.bigz(v <- 3:7)
crossprod(V)# scalar product
(C <- t(V))
stopifnot(dim(C) == dim(t(v)), C == v,
          dim(t(C)) == c(length(v), 1),
          crossprod(V) == sum(V * V),
          tcrossprod(V) == outer(v,v),
          identical(C, t(t(C))) )

## a matrix
x <- diag(1:4)
## invert this matrix
(xI <- solve(x))

## matrix in Z/7Z
y <- as.bigz(x,7)
## invert this matrix (result is *different* from solve(x)):
(yI <- solve(y))
stopifnot(yI %%% y == diag(4),
          y %%% yI == diag(4))

## matrix in Q
z <- as.bigq(x)
## invert this matrix (result is the same as solve(x))
(zI <- solve(z))

stopifnot(abs(zI - xI) <= 1e-13,
          z %%% zI == diag(4),
          identical(crossprod(zI), zI %%% t(zI))
          )

A <- matrix(2^as.bigz(1:12), 3,4)
for(a in list(A, as.bigq(A, 16), factorialZ(20), as.bigq(2:9, 3:4))) {
  a.a <- crossprod(a)
  aa. <- tcrossprod(a)
  stopifnot(identical(a.a, crossprod(a,a)),
            identical(a.a, t(a) %%% a)
            ,
            identical(aa., tcrossprod(a,a)),
            identical(aa., a %%% t(a))
            )
}# {for}

```

modulus

*Modulus of a Big Integer***Description**

The modulus of a **bigz** number a is “unset” when a is a regular integer, $a \in \mathbb{Z}$. Or the modulus can be set to m which means $a \in \mathbb{Z}/m \cdot \mathbb{Z}$, i.e., all arithmetic with a is performed ‘modulo m ’.

Usage

```
modulus(a)
modulus(a) <- value
```

Arguments

a R object of class "bigz"
value integer number or object of class "bigz".

Examples

```
x <- as.bigz(24)
modulus(x) # NULL, i.e. none

# x element of Z/31Z :
modulus(x) <- 31
x+x # 48 |-> (17 %% 31)
10*x # 240 |-> (23 %% 31)
x31 <- x

# reset modulus to "none":
modulus(x) <- NA; x; x. <- x
x <- x31
modulus(x) <- NULL; x

stopifnot(identical(x, as.bigz(24)), identical(x, x.),
          identical(modulus(x31), as.bigz(31)))
```

nextprime

Next prime number

Description

Return next prime number greater than n

Usage

```
nextprime(n)
```

Arguments

n Integer

Details

This function uses probabilistic algorithm to identify primes. For practical purposes, it's adequate, the chance of a composite passing will be extremely small.

Value

A (probably) prime number

Author(s)

Antoine Lucas

References

The GNU MP Library, see <http://gmplib.org>

See Also

[isprime](#)

Examples

```
nextprime(14)
```

Oakley	<i>RFC 2409 Oakley Groups - Standardized Parameters for Diffie-Hellman Key Exchange</i>
--------	---

Description

RFC 2409 standardizes global unique prime numbers and generators for the purpose of secure asymmetric key exchange on the Internet.

Usage

```
Oakley1  
Oakley2
```

Value

Oakley1 returns an object of class [bigz](#) for a 768 bit Diffie-Hellman group. The generator is stored as value with the respective prime number as modulus attribute.

Oakley2 returns an object of class [bigz](#) for a 1024 bit Diffie-Hellman group. The generator is stored as value with the respective prime number as modulus attribute.

References

The Internet Key Exchange (RFC 2409), Nov. 1998

Examples

```
data(Oakley1)  
isprime(modulus(Oakley1))
```

powm

Exponentiation function

Description

This function return $x^y \bmod n$

Usage

```
powm(x, y, n)
```

Arguments

x	Integer or big integer - possibly a vector
y	Integer or big integer - possibly a vector
n	Integer or big integer - possibly a vector

Details

This function return $x^y \bmod n$

pow.bigz do the same when modulus is set.

Value

A bigz class representing the parameter value.

Author(s)

A. L.

See Also

[pow.bigz](#)

Examples

```
powm(4, 7, 9)
```

```
x = as.bigz(4,9)
x ^ 7
```

Random	<i>Generate a random number</i>
--------	---------------------------------

Description

Generate a uniformly distributed random number in the range 0 to $2^{size} - 1$, inclusive.

Usage

```
urand.bigz(nb=1,size=200, seed = 0)
```

Arguments

nb	Integer: number of random numbers to be generated (size of vector returned)
size	Integer: number will be generated in the range 0 to $2^{size} - 1$
seed	Bigz: random seed initialisation

Value

A biginteger of class bigz.

Author(s)

Antoine Lucas

References

'mpz_urandomb' from the GMP Library, see <http://gmplib.org>

Examples

```
# Integers are different
urand.bigz()
urand.bigz()
urand.bigz()

# Integers are the same
urand.bigz(seed="234234234324323")
urand.bigz(seed="234234234324323")

# Vector
urand.bigz(nb=50,size=30)
```

 Relational Operator *Relational Operators*

Description

Binary operators which allow the comparison of values in atomic vectors.

Usage

```
## S3 method for class 'bigz'
sign(x)
## S3 method for class 'bigz'
e1 == e2
## S3 method for class 'bigz'
e1 < e2
## S3 method for class 'bigz'
e1 >= e2
```

Arguments

x, e1, e2 R object (vector or matrix-like) of class "[bigz](#)".

See Also

[mod.bigz](#) for arithmetic operators.

Examples

```
x <- as.bigz(8000)
x ^ 300 < 2 ^ x

sign(as.bigz(-3:3))
sign(as.bigq(-2:2, 7))
```

 sizeinbase *Compute size of a bigz in a base*

Description

Return size (number of digits) written in base b.

Usage

```
sizeinbase(a, b=10)
```

Arguments

a big integer, i.e. "bigz"
b base

Value

integer of the same length as a: the size, i.e. number of digits, of each a[i].

Author(s)

Antoine Lucas

References

The GNU MP Library, see <http://gmplib.org>

Examples

```
sizeinbase(342434, 10)# 6 obviously

Iv <- as.bigz(2:7)^500
sizeinbase(Iv)
stopifnot(sizeinbase(Iv) == nchar(as.character(Iv)),
           sizeinbase(Iv, b=16) == nchar(as.character(Iv, b=16)))
```

solve.bigz

Solve a system of equation

Description

This generic function solves the equation $a\% * \%x = b$ for x , where b can be either a vector or a matrix.

If a and b are rational, return is a rational matrix.

If a and b are big integers (of class bigz) solution is in $\mathbb{Z}/n\mathbb{Z}$ if there is a common modulus, or a rational matrix if not.

Usage

```
## S3 method for class 'bigz'
solve(a, b, ...)
## S3 method for class 'bigq'
solve(a, b, ...)
```

Arguments

a,b A element of class bigz or bigq
... Unused

Details

It uses the Gauss and truncmuch algo ... (to be detailed).

Value

If a and b are rational, return is a rational matrix.

If a and b are big integers (of class bigz) solution is in $\mathbb{Z}/n\mathbb{Z}$ if there is a common modulus, of a rational matrix if not.

Author(s)

Antoine Lucas

See Also

[solve](#)

Examples

```
x <- matrix(1:4,2,2)
## standard solve
solve(x)

q <- as.bigq(x)
## solve with rational
solve(q)

z <- as.bigz(x)
modulus(z) <- 7
## solve in  $\mathbb{Z}/7\mathbb{Z}$ 
solve(z)

b <- c(1,3)

solve(q,b)

solve(z,b)
```

Description

Compute Eulerian numbers and Stirling numbers of the first and second kind, possibly vectorized for all k “at once”.

Usage

```

Stirling1(n, k)
Stirling2(n, k, method = c("lookup.or.store", "direct"))
Eulerian (n, k, method = c("lookup.or.store", "direct"))

Stirling1.all(n)
Stirling2.all(n)
Eulerian.all (n)

```

Arguments

n	positive integer (0 is allowed for Eulerian()).
k	integer in 0:n.
method	for Eulerian() and Stirling2(), string specifying the method to be used. "direct" uses the explicit formula (which may suffer from some cancelation for "large" n).

Details

Eulerian numbers:

$A(n, k)$ = the number of permutations of $1, 2, \dots, n$ with exactly k ascents (or exactly k descents).

Stirling numbers of the first kind:

$s(n, k) = (-1)^{n-k}$ times the number of permutations of $1, 2, \dots, n$ with exactly k cycles.

Stirling numbers of the second kind:

$S_n^{(k)}$ is the number of ways of partitioning a set of n elements into k non-empty subsets.

Value

$A(n, k)$, $s(n, k)$ or $S(n, k) = S_n^{(k)}$, respectively.

Eulerian.all(n) is the same as `sapply(0:(n-1), Eulerian, n=n)` (for $n > 0$),

Stirling1.all(n) is the same as `sapply(1:n, Stirling1, n=n)`, and

Stirling2.all(n) is the same as `sapply(1:n, Stirling2, n=n)`, but more efficient.

Note

For typical double precision arithmetic,

Eulerian*(n, *) overflow (to Inf) for $n \geq 172$,

Stirling1*(n, *) overflow (to \pm Inf) for $n \geq 171$, and

Stirling2*(n, *) overflow (to Inf) for $n \geq 220$.

Author(s)

Martin Maechler ("direct": May 1992)

References**Eulerians:**

NIST Digital Library of Mathematical Functions, 26.14: <http://dlmf.nist.gov/26.14>

Stirling numbers:

Abramowitz and Stegun 24,1,4 (p. 824-5 ; Table 24.4, p.835); Closed Form : p.824 "C."

NIST Digital Library of Mathematical Functions, 26.8: <http://dlmf.nist.gov/26.8>

See Also

[chooseZ](#) for the binomial coefficients.

Examples

```
Stirling1(7,2)
```

```
Stirling2(7,3)
```

```
stopifnot(
```

```
  Stirling1.all(9) == c(40320, -109584, 118124, -67284, 22449, -4536, 546, -36, 1)
```

```
,
```

```
  Stirling2.all(9) == c(1, 255, 3025, 7770, 6951, 2646, 462, 36, 1)
```

```
,
```

```
  Eulerian.all(7) == c(1, 120, 1191, 2416, 1191, 120, 1)
```

```
)
```

Index

- `!=.bigq` (Bigq), 3
- `!=.bigz` (Relational Operator), 28
- *Topic **arithmetic**
 - Stirling, 30
- *Topic **arith**
 - `apply`, 2
 - `Bigq`, 3
 - `bigq`, 4
 - `Bigq operators`, 5
 - `bigz`, 6
 - `bigz operators`, 9
 - `cumsum`, 11
 - `Extract`, 12
 - `Extremes`, 13
 - `factorialZ`, 14
 - `factorization`, 15
 - `frexpZ`, 16
 - `gcd.bigz`, 17
 - `gcdex`, 18
 - `gmp.utils`, 19
 - `isprime`, 19
 - `lucnum`, 20
 - `matrix`, 21
 - `modulus`, 23
 - `nextprime`, 24
 - `powm`, 26
 - `Random`, 27
 - `Relational Operator`, 28
 - `sizeinbase`, 28
 - `solve.bigz`, 29
- *Topic **data**
 - Oakley, 25
- `*.bigq` (Bigq operators), 5
- `*.bigz` (bigz operators), 9
- `+.bigq` (Bigq operators), 5
- `+.bigz` (bigz operators), 9
- `-.bigq` (Bigq operators), 5
- `-.bigz` (bigz operators), 9
- `/.bigq` (Bigq operators), 5
- `/.bigz` (bigz operators), 9
- `<.bigq` (Bigq), 3
- `<.bigz` (Relational Operator), 28
- `<=.bigq` (Bigq), 3
- `<=.bigz` (Relational Operator), 28
- `==.bigq` (Bigq), 3
- `==.bigz` (Relational Operator), 28
- `>.bigq` (Bigq), 3
- `>.bigz` (Relational Operator), 28
- `>=.bigq` (Bigq), 3
- `>=.bigz` (Relational Operator), 28
- `[.bigq` (Extract), 12
- `[.bigz` (Extract), 12
- `[<-.bigq` (Extract), 12
- `[<-.bigz` (Extract), 12
- `[[.bigq` (Extract), 12
- `[[.bigz` (Extract), 12
- `[[<-.bigq` (Extract), 12
- `[[<-.bigz` (Extract), 12
- `%*%` (matrix), 21
- `%/%.bigz` (bigz operators), 9
- `%%.bigz` (bigz operators), 9
- `^.bigz` (bigz operators), 9
- `abs.bigq` (Bigq operators), 5
- `abs.bigz` (bigz operators), 9
- `add.bigq` (Bigq operators), 5
- `add.bigz`, 7
- `add.bigz` (bigz operators), 9
- `apply`, 2, 2, 3, 12
- `as.bigq` (bigq), 4
- `as.bigz` (bigz), 6
- `as.bigz.bigq` (bigq), 4
- `as.character.bigq` (bigq), 4
- `as.character.bigz` (bigz), 6
- `as.double.bigq` (bigq), 4
- `as.double.bigz` (bigz), 6
- `as.matrix.bigq` (matrix), 21
- `as.matrix.bigz` (matrix), 21
- `as.vector.bigq` (matrix), 21

- as.vector.bigz (matrix), 21
- Bigq, 3
- bigq, 3, 4, 5, 6
- Bigq operators, 5
- bigz, 6, 10, 14, 16, 17, 22–25, 28, 29
- bigz operators, 9
- c.bigq (Extract), 12
- c.bigz (Extract), 12
- cbind.bigq (matrix), 21
- cbind.bigz (matrix), 21
- character, 7
- chooseZ, 32
- chooseZ (factorialZ), 14
- crossprod (matrix), 21
- cumsum, 11, 11
- denominator (bigq), 4
- denominator<- (bigq), 4
- dim.bigq (matrix), 21
- dim.bigz (matrix), 21
- dim<-.bigq (matrix), 21
- dim<-.bigz (matrix), 21
- div.bigq (Bigq operators), 5
- div.bigz (bigz operators), 9
- divq.bigz (bigz operators), 9
- double, 7
- Eulerian (Stirling), 30
- Extract, 12
- Extremes, 13
- factorial, 14
- factorialZ, 14
- factorization, 15
- factorize (factorization), 15
- fibnum (lucnum), 20
- fibnum2 (lucnum), 20
- frexp (frexpZ), 16
- frexpZ, 16
- function, 2
- gamma, 14
- gcd (gcd.bigz), 17
- gcd.bigz, 17, 18
- gcdex, 17, 18
- gmp.utils, 19
- gmpVersion (gmp.utils), 19
- integer, 7
- inv (bigz operators), 9
- is.na.bigq (bigq), 4
- is.na.bigz (bigz), 6
- isprime, 19, 25
- lapply, 2, 3
- lcm (gcd.bigz), 17
- length.bigq (Extract), 12
- length.bigz (Extract), 12
- length<-.bigq (Extract), 12
- length<-.bigz (Extract), 12
- list, 16
- log.bigz (bigz operators), 9
- log10.bigz (bigz operators), 9
- log2, 16
- log2.bigz (bigz operators), 9
- lucnum, 20
- lucnum2 (lucnum), 20
- matrix, 21, 22
- matrix.bigz, 2
- max, 13, 14
- max.bigq (Extremes), 13
- max.bigz (Extremes), 13
- methods, 2, 13
- min, 13
- min.bigq (Extremes), 13
- min.bigz (Extremes), 13
- mod.bigz, 8, 28
- mod.bigz (bigz operators), 9
- modulus, 23
- modulus<- (modulus), 23
- mul.bigq (Bigq operators), 5
- mul.bigz (bigz operators), 9
- NA, 11
- ncol.bigq (matrix), 21
- ncol.bigz (matrix), 21
- nextprime, 20, 24
- nrow.bigq (matrix), 21
- nrow.bigz (matrix), 21
- numerator (bigq), 4
- numerator<- (bigq), 4
- numeric, 7
- Oakley, 25
- Oakley1 (Oakley), 25
- Oakley2 (Oakley), 25

pow (bigz operators), 9
pow.bigz, 26
powm, 26
print.bigq (bigq), 4
print.bigz (bigz), 6
prod, 11
prod.bigq (cumsum), 11
prod.bigz (cumsum), 11

Random, 27
range, 13
rbind.bigq (matrix), 21
rbind.bigz (matrix), 21
Relational Operator, 28
rep.bigq (Extract), 12
rep.bigz (Extract), 12

sign.bigq (Bigq), 3
sign.bigz (Relational Operator), 28
sizeinbase, 28
solve, 22, 30
solve.bigq (solve.bigz), 29
solve.bigz, 22, 29
Stirling, 30
Stirling1 (Stirling), 30
Stirling2 (Stirling), 30
stop, 7
sub.bigq (Bigq operators), 5
sub.bigz (bigz operators), 9
sum, 11
sum.bigq (cumsum), 11
sum.bigz (cumsum), 11

t.bigq (matrix), 21
t.bigz (matrix), 21
tcrossprod (matrix), 21

urand.bigz (Random), 27