

NAME

BN_cmp, BN_ucmp, BN_is_zero, BN_is_one, BN_is_word, BN_abs_is_word, BN_is_odd, BN_are_coprime – BIGNUM comparison and test functions

SYNOPSIS

```
#include <openssl/bn.h>

int BN_cmp(const BIGNUM *a, const BIGNUM *b);
int BN_ucmp(const BIGNUM *a, const BIGNUM *b);

int BN_is_zero(const BIGNUM *a);
int BN_is_one(const BIGNUM *a);
int BN_is_word(const BIGNUM *a, const BN_ULONG w);
int BN_abs_is_word(const BIGNUM *a, const BN_ULONG w);
int BN_is_odd(const BIGNUM *a);

int BN_are_coprime(BIGNUM *a, const BIGNUM *b, BN_CTX *ctx);
```

DESCRIPTION

BN_cmp() compares the numbers *a* and *b*. **BN_ucmp()** compares their absolute values.

BN_is_zero(), **BN_is_one()**, **BN_is_word()** and **BN_abs_is_word()** test if *a* equals 0, 1, *w*, or $|w|$ respectively. **BN_is_odd()** tests if *a* is odd.

BN_are_coprime() determines if **a** and **b** are coprime. **ctx** is used internally for storing temporary variables. The values of **a** and **b** and **ctx** must not be NULL.

RETURN VALUES

BN_cmp() returns -1 if $a < b$, 0 if $a == b$ and 1 if $a > b$. **BN_ucmp()** is the same using the absolute values of *a* and *b*.

BN_is_zero(), **BN_is_one()**, **BN_is_word()**, **BN_abs_is_word()** and **BN_is_odd()** return 1 if the condition is true, 0 otherwise.

BN_are_coprime() returns 1 if the **BIGNUM**'s are coprime, otherwise it returns 0.

HISTORY

Prior to OpenSSL 1.1.0, **BN_is_zero()**, **BN_is_one()**, **BN_is_word()**, **BN_abs_is_word()** and **BN_is_odd()** were macros.

The function **BN_are_coprime()** was added in OpenSSL 3.1.

COPYRIGHT

Copyright 2000–2021 The OpenSSL Project Authors. All Rights Reserved.

Licensed under the Apache License 2.0 (the "License"). You may not use this file except in compliance with the License. You can obtain a copy in the file LICENSE in the source distribution or at [<https://www.openssl.org/source/license.html>](https://www.openssl.org/source/license.html).