

**NAME**

BN\_add\_word, BN\_sub\_word, BN\_mul\_word, BN\_div\_word, BN\_mod\_word - arithmetic functions on BIGNUMs with integers

**SYNOPSIS**

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

int BN_add_word(BIGNUM *a, BN_ULONG w);

int BN_sub_word(BIGNUM *a, BN_ULONG w);

int BN_mul_word(BIGNUM *a, BN_ULONG w);

BN_ULONG BN_div_word(BIGNUM *a, BN_ULONG w);

BN_ULONG BN_mod_word(const BIGNUM *a, BN_ULONG w);
```

**DESCRIPTION**

These functions perform arithmetic operations on BIGNUMs with unsigned integers. They are much more efficient than the normal BIGNUM arithmetic operations.

*BN\_add\_word()* adds **w** to **a** (**a+=w**).

*BN\_sub\_word()* subtracts **w** from **a** (**a-=w**).

*BN\_mul\_word()* multiplies **a** and **w** (**a\*=w**).

*BN\_div\_word()* divides **a** by **w** (**a/=w**) and returns the remainder.

*BN\_mod\_word()* returns the remainder of **a** divided by **w** (**a%w**).

For *BN\_div\_word()* and *BN\_mod\_word()*, **w** must not be 0.

**RETURN VALUES**

*BN\_add\_word()*, *BN\_sub\_word()* and *BN\_mul\_word()* return 1 for success, 0 on error. The error codes can be obtained by [ERR\\_get\\_error\(3\)](#).

*BN\_mod\_word()* and *BN\_div\_word()* return **a%w** on success and **(BN\_ULONG)-1** if an error occurred.

**SEE ALSO**

[bn\(3\)](#), [ERR\\_get\\_error\(3\)](#), [BN\\_add\(3\)](#)

**HISTORY**

*BN\_add\_word()* and *BN\_mod\_word()* are available in all versions of SSLeay and OpenSSL. *BN\_div\_word()* was added in SSLeay 0.8, and *BN\_sub\_word()* and *BN\_mul\_word()* in SSLeay 0.9.0.

Before 0.9.8a the return value for *BN\_div\_word()* and *BN\_mod\_word()* in case of an error was 0.