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

ERR_get_error(3), **BN_add**(3)

COPYRIGHT