```
c = a + b
                                                                 b=2a
                         mp_add(&a, &b, &c)
                                                                                                 mp_mul_2(&a, &b)
                        mp_sub(&a, &b, &c)
                                                                 b = a/2
c = a - b
                                                                                                 mp_div_2(&a, &b)
                        mp_mul(&a, &b, &c)
                                                                 c=2^ba
c = ab
                                                                                                 mp_mul_2d(&a, b, &c)
b = a^2
                                                                 c = a/2^b, d = a \mod 2^b
                        mp_sqr(&a, &b)
                                                                                                 mp_div_2d(&a, b, &c, &d)
c = |a/b|, d = a \mod b \mod b mp_div(&a, &b, &c, &d)
                                                                 c = a \mod 2^b
                                                                                                 mp_mod_2d(&a, b, &c)
                        mp_set_int(&a, b)
                                                                                                 mp_or(&a, &b, &c)
a = b
                                                                 c = a \vee b
b = a
                        mp_copy(&a, &b)
                                                                 c = a \wedge b
                                                                                                 mp_and(&a, &b, &c)
                                                                 c = a \oplus b
                                                                                                 mp_xor(&a, &b, &c)
b = -a
                        mp_neg(&a, &b)
                                                                 d = a + b \mod c
                                                                                                 mp_addmod(&a, &b, &c, &d)
b = |a|
                        mp_abs(&a, &b)
                                                                 d = a - b \mod c
                                                                                                 mp_submod(&a, &b, &c, &d)
                                                                 d = ab \mod c
                                                                                                 mp_mulmod(&a, &b, &c, &d)
                                                                 c = a^2 \mod b
Compare a and b
                                                                                                 mp_sqrmod(&a, &b, &c)
                        mp_cmp(&a, &b)
                                                                 c = a^{-1} \mod b
                        mp_iszero(&a)
Is Zero?
                                                                                                 mp_invmod(&a, &b, &c)
                                                                 d = a^b \mod c
Is Even?
                         mp_iseven(&a)
                                                                                                 mp_exptmod(&a, &b, &c, &d)
Is Odd?
                        mp_isodd(&a)
||a||
                        mp_unsigned_bin_size(&a)
                                                                 res = 1 if a prime to t rounds?
                                                                                                 mp_prime_is_prime(&a, t, &res)
                        mp_to_unsigned_bin(&a, buf)
                                                                 Next prime after a to t rounds.
                                                                                                mp_prime_next_prime(&a, t)
buf \leftarrow a
a \leftarrow buf[0..len - 1]
                        mp_read_unsigned_bin(&a, buf, len)
b = \sqrt{a}
                        mp_sqrt(&a, &b)
                                                                 c = \gcd(a, b)
                                                                                                 mp_gcd(&a, &b, &c)
c = a^{1/b}
                        mp_n_root(&a, b, &c)
                                                                 c = lcm(a, b)
                                                                                                 mp_lcm(&a, &b, &c)
Greater Than
                         MP_{-}GT
                                                                 Equal To
                                                                                                 MP_EQ
Less Than
                         MP_LT
                                                                 Bits per digit
                                                                                                 DIGIT_BIT
```