

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