| | | | |
|---|---|---|---|
| $c = a + b$ | `mp_add(&a, &b, &c)` | $b = 2a$ | `mp_mul_2(&a, &b)` |
| $c = a - b$ | `mp_sub(&a, &b, &c)` | $b = a/2$ | `mp_div_2(&a, &b)` |
| $c = ab$ | `mp_mul(&a, &b, &c)` | $c = 2^b a$ | `mp_mul_2d(&a, b, &c)` |
| $b = a^2$ | `mp_sqr(&a, &b)` | $c = a/2^b, d = a \mod 2^b$ | `mp_div_2d(&a, b, &c, &d)` |
| $c = \lfloor a/b \rfloor, d = a \mod b$ | `mp_div(&a, &b, &c, &d)` | $c = a \mod 2^b$ | `mp_mod_2d(&a, b, &c)` |
| | | | |
| $a = b$ | `mp_set_int(&a, b)` | $c = a \vee b$ | `mp_or(&a, &b, &c)` |
| $b = a$ | `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)` |
| Compare $a$ and $b$ | `mp_cmp(&a, &b)` | $c = a^2 \mod b$ | `mp_sqrmod(&a, &b, &c)` |
| Is Zero? | `mp_iszero(&a)` | $c = a^{-1} \mod b$ | `mp_invmod(&a, &b, &c)` |
| Is Even? | `mp_iseven(&a)` | $d = a^b \mod c$ | `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)` |
| $buf \leftarrow a$ | `mp_to_unsigned_bin(&a, buf)` | Next prime after $a$ to $t$ rounds. | `mp_prime_next_prime(&a, t, bbs_style)` |
| $a \leftarrow buf[0..len-1]$ | `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)` | $c = \mathrm{lcm}(a, b)$ | `mp_lcm(&a, &b, &c)` |
| | | | |
| Greater Than | MP_GT | Equal To | MP_EQ |
| Less Than | MP_LT | Bits per digit | DIGIT_BIT |