

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