

# The Integer class.

The **Integer** class provides multiple precision integer arithmetic facilities. Some representation details are discussed in the Representation section.

**Integers** may be up to  $b * ((1 \ll b) - 1)$  bits long, where **b** is the number of bits per short (typically 1048560 bits when **b = 16**). The implementation assumes that a **long** is at least twice as long as a **short**. This assumption hides beneath almost all primitive operations, and would be very difficult to change. It also relies on correct behavior of **unsigned** arithmetic operations.

Some of the arithmetic algorithms are very loosely based on those provided in the MIT Scheme **bignum.c** release, which is Copyright © 1987 Massachusetts Institute of Technology. Their use here falls within the provisions described in the Scheme release.

Integers may be constructed in the following ways:

|                                     |                                     |
|-------------------------------------|-------------------------------------|
| <b>Integer x;</b>                   | Declares an uninitialized Integer.  |
| <b>Integer x = 2; Integer y(2);</b> | Set x and y to the Integer value 2; |
| <b>Integer u(x); Integer v = x;</b> | Set u and v to the same value as x. |

**Integers** may be coerced back into longs via the **long** coercion operator. If the Integer cannot fit into a long, this returns MINLONG or MAXLONG (depending on the sign) where MINLONG is the most negative, and MAXLONG is the most positive representable long. The member function **fits\_in\_long()** may be used to test this. **Integers** may also be coerced into **doubles**, with potential loss of precision. **+/-HUGE** is returned if the Integer cannot fit into a double. **fits\_in\_double()** may be used to test this.

All of the usual arithmetic operators are provided (+, -, \*, /, %, +=, ++, -=, --, \*=, /=, %=, ==, !=, <, <=, >, >=). All

operators support special versions for mixed arguments of Integers and regular C++ longs in order to avoid useless coercions, as well as to allow automatic promotion of shorts and ints to longs, so that they may be applied without additional Integer coercion operators. The only operators that behave differently than the corresponding int or long operators are **++** and **--**. Because C++ does not distinguish prefix from postfix application, these are declared as **void** operators, so that no confusion can result from applying them as postfix. Thus, for Integers *x* and *y*, **++x; y = x;** is correct, but **y = ++x;** and **y = x++;** are not.

Bitwise operators (**~, &, |, ^, <<, >>, &=, |=, ^=, <<=, >>=**) are also provided. However, these operate on sign-magnitude, rather than two's complement representations. The sign of the result is arbitrarily taken as the sign of the first argument. For example, **Integer(-3) & Integer(5)** returns **Integer(-1)**, not -3, as it would using two's complement. Also, **~**, the complement operator, complements only those bits needed for the representation. Bit operators are also provided in the BitSet and BitString classes. One of these classes should be used instead of Integers when the results of bit manipulations are not interpreted numerically.

The following utility functions are also provided. (All arguments are Integers unless otherwise noted).

|                                          |                                                                                                                                            |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <b>void divide(x, y, q, r);</b>          | Sets <i>q</i> to the quotient and <i>r</i> to the remainder of <i>x</i> and <i>y</i> . ( <i>q</i> and <i>r</i> are returned by reference). |
| <b>Integer pow(Integer x, Integer p)</b> | returns <i>x</i> raised to the power <i>p</i> .                                                                                            |
| <b>Integer lpow(long x, long p)</b>      | returns <i>x</i> raised to the power <i>p</i> .                                                                                            |
| <b>Integer gcd(x, y)</b>                 | returns the greatest common divisor of <i>x</i> and <i>y</i> .                                                                             |
| <b>Integer lcm(x, y)</b>                 | returns the least common multiple of <i>x</i> and <i>y</i> .                                                                               |
| <b>Integer abs(x);</b>                   | returns the absolute value of <i>x</i> .                                                                                                   |
| <b>void x.negate();</b>                  | negates <i>x</i> .                                                                                                                         |

|                                                                             |                                                                                                                                                                   |
|-----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Integer sqr(x)</b>                                                       | returns $x * x$ ;                                                                                                                                                 |
| <b>Integer sqrt(x)</b>                                                      | returns the floor of the square root of x.                                                                                                                        |
| <b>long lg(x);</b>                                                          | returns the floor of the base 2 logarithm of abs(x)                                                                                                               |
| <b>int sign(x)</b>                                                          | returns -1 if x is negative, 0 if zero, else +1. Using <b>if (sign(x) == 0)</b> is a generally faster method of testing for zero than using relational operators. |
| <b>int even(x)</b>                                                          | returns true if x is an even number                                                                                                                               |
| <b>int odd(x)</b>                                                           | returns true if x is an odd number.                                                                                                                               |
| <b>void setbit(Integer&amp; x, long b)</b>                                  | sets the b'th bit (counting right-to-left from zero) of x to 1.                                                                                                   |
| <b>void clearbit(Integer&amp; x, long b)</b>                                | sets the b'th bit of x to 0.                                                                                                                                      |
| <b>int testbit(Integer x, long b)</b>                                       | returns true if the b'th bit of x is 1.                                                                                                                           |
| <b>Integer atol(char* asciinumber, int base = 10);</b>                      | converts the base base char* string into its Integer form.                                                                                                        |
| <b>void Integer::printon(ostream&amp; s, int base = 10, int width = 0);</b> | prints the ascii string value of <b>(*this)</b> as a base <b>base</b> number, in field width at least <b>width</b> .                                              |
| <b>ostream &lt;&lt; x;</b>                                                  | prints x in base ten format.                                                                                                                                      |
| <b>istream &gt;&gt; x;</b>                                                  | reads x as a base ten number.                                                                                                                                     |

|                                           |                                                                                    |
|-------------------------------------------|------------------------------------------------------------------------------------|
| <b>int compare(Integer x, Integer y)</b>  | returns a negative number if $x < y$ , zero if $x == y$ , or positive if $x > y$ . |
| <b>int ucompare(Integer x, Integer y)</b> | like compare, but performs unsigned comparison.                                    |
| <b>add(x, y, z)</b>                       | A faster way to say $z = x + y$ .                                                  |
| <b>sub(x, y, z)</b>                       | A faster way to say $z = x - y$ .                                                  |
| <b>mul(x, y, z)</b>                       | A faster way to say $z = x * y$ .                                                  |
| <b>div(x, y, z)</b>                       | A faster way to say $z = x / y$ .                                                  |
| <b>mod(x, y, z)</b>                       | A faster way to say $z = x \% y$ .                                                 |
| <b>and(x, y, z)</b>                       | A faster way to say $z = x \& y$ .                                                 |
| <b>or(x, y, z)</b>                        | A faster way to say $z = x   y$ .                                                  |
| <b>xor(x, y, z)</b>                       | A faster way to say $z = x ^ y$ .                                                  |
| <b>lshift(x, y, z)</b>                    | A faster way to say $z = x << y$ .                                                 |
| <b>rshift(x, y, z)</b>                    | A faster way to say $z = x >> y$ .                                                 |
| <b>pow(x, y, z)</b>                       | A faster way to say $z = \text{pow}(x, y)$ .                                       |
| <b>complement(x, z)</b>                   | A faster way to say $z = \sim x$ .                                                 |
| <b>negate(x, z)</b>                       | A faster way to say $z = -x$ .                                                     |

