

## List of Mathematica Commands Useful for Number Theory

**NOTE:** On a MacIntosh commands are entered by hitting the enter key. On machines with Unix a command is entered by hitting the return key.

### Basic Mathematica Commands

**BaseForm[n,b]:** Gives the base b expansion of n.

**Divisors[n]:** Gives a list of integers that divide n.

**EulerPhi[n]:** Gives the value of the Euler Phi Function  $\phi(n)$ .

**ExtendedGCD[m,n]:** Gives  $\{d, \{r, s\}\}$  where  $d$  is the greatest common divisor of  $m$  and  $n$  and  $r, s$  satisfy  $d = mr + ns$ .

**GCD[m,n]:** Gives the greatest common divisor of  $m$  and  $n$ . Can also be used with more than two integers.

**FactorInteger[n]:** Gives the factorization of  $n$  into a product of prime numbers.  $\{p, b\}$  indicates a factor of  $p^b$ .

**FactorInteger[n, FactorComplete-> False]:** Does a fast but not necessarily complete factorization that can be useful if trying to factor a very large integer  $n$ .

**IntegerExponent[n,p]:** Gives the exponent of prime  $p$  in the factorization of  $n$ .

**JacobiSymbol[n,m]:** Gives the Jacobi symbol  $(\frac{n}{m})$  which is the same as the Legendre symbol when  $m$  is an odd prime.

**LCM[m,n]:** Gives the least common multiple of  $m$  and  $n$ . Can also be used with more than two integers.

**Mod[a,m]:** Gives  $a \pmod{m}$ .

**PowerMod[a,b,m]:** Gives  $a^b \pmod{m}$ .

**PrimeQ[n]:** Gives True if  $n$  is prime, False if  $n$  is not prime.

**Quotient[a,b]:** Gives the integer part of  $a$  divided by  $b$ .

**Quit:** terminates a Mathematica session.

**Random[Integer,{min,max}]:** Gives a random integer between  $min$  and  $max$ .

### More Advanced Mathematica Commands

More advanced commands are available by loading what are called Packages into any Mathematica session you are running. There are several Number Theory packages. Ones of possible interest to us are FactorIntegerECM, NumberTheoryFunctions, and PrimeQ.

**\$Packages:** Lists packages currently loaded.

**<< NumberTheory'FactorIntegerECM':** Loads the FactorIntegerECM package. The following command is in this package. This command also has options which can be learned about by looking in Mathematica Help.

**FactorIntegerECM[n]:** Finds a single factor of a composite number  $n$  by using elliptic curves. This can be used to find a single factor of a large number when the usual FactorInteger command fails.

<< **NumberTheory‘NumberTheoryFunctions’**: Loads the NumberTheoryFunctions package. The following commands are available in this package. There are other commands which can be learned about by looking at the package file or Mathematica Help.

**ChineseRemainder**[{*a*, *b*}, {*m*, *n*}]: Gives the unique solution to the congruences  $x \equiv a \pmod{m}$ ,  $x \equiv b \pmod{n}$  when  $\gcd(m, n) = 1$ .

**NextPrime**[*n*]: Gives the smallest prime number greater than *n*.

**PrimitiveRoot**[*n*]: Gives a primitive root modulo *n* when  $n = p$  or  $n = 2p$ , where *p* is a prime.

**SqrtMod**[*d*, *n*]: Gives the square root of *d* modulo *n* when it exists.

<< **NumberTheory‘PrimeQ’**: Loads the PrimeQ package. This package is useful for testing the primality of integers larger than  $10^{16}$ , where the built-in PrimeQ command can be inaccurate. It also is of interest because it can be used to give a reason *n* is prime or composite.

The following commands are in this package. There are other commands which can be learned about by consulting the package or Mathematica Help.

**ProvablePrimeQ**[*n*]: Gives True if *n* can be proved to be prime and False if *n* can be proved to be composite.

If the PrimeQ command returns False *n* is composite, but for  $n > 10^{16}$  it can incorrectly return True, i.e. can incorrectly claim a composite number is prime. Thus if PrimeQ returns True for a large integer, one should use ProvablePrimeQ[*n*] before assuming the integer is prime.

**PrimeQCertificate**[*n*]: Prints a certificate that proves *n* is prime or composite. A certificate is a set of data that indicates why *n* is prime or composite.

Example: PrimeQCertificate[3837523] returns {2, 3837522, 3837523} If a list of three numbers is given the number is composite. The above means  $\not\equiv 1 \pmod{3837523}$ .

A certificate indicating why an integer is prime is much more complicated. References are given under Mathematica Help.