LibTomMath User Manual
v1.3.1

LibTom Projects
www.libtom.net

March 8, 2025

This text, the library and the accompanying textbook are all hereby placed in the public domain. This book has been formatted for B5 [176x250] paper using the LaTeX *book* macro package.

Open Source. Open Academia. Open Minds.
LibTom Projects
& originally
Tom St Denis,
Ontario, Canada

Contents

1 Introduction **1**
- 1.1 What is LibTomMath? . . . 1
- 1.2 License . . . 1
- 1.3 Building LibTomMath . . . 1
  - 1.3.1 Static Libraries . . . 2
  - 1.3.2 Shared Libraries . . . 2
  - 1.3.3 Testing . . . 4
- 1.4 Build Configuration . . . 5
  - 1.4.1 Build Depends . . . 5
  - 1.4.2 Build Tweaks . . . 6
  - 1.4.3 Build Trims . . . 6
- 1.5 Purpose of LibTomMath . . . 7

2 Getting Started with LibTomMath **9**
- 2.1 Building Programs . . . 9
- 2.2 Return Codes . . . 9
- 2.3 Data Types . . . 10
- 2.4 Function Organization . . . 10
- 2.5 Initialization . . . 10
  - 2.5.1 Single Initialization . . . 10
  - 2.5.2 Single Free . . . 11
  - 2.5.3 Multiple Initializations . . . 12
  - 2.5.4 Other Initializers . . . 12
- 2.6 Maintenance Functions . . . 14
  - 2.6.1 Clear Leading Zeros . . . 14
  - 2.6.2 Zero Out . . . 14
  - 2.6.3 Reducing Memory Usage . . . 14
  - 2.6.4 Adding additional digits . . . 15

3 Basic Operations **17**
- 3.1 Copying . . . 17
- 3.2 Bit Counting . . . 17
- 3.3 Small Constants . . . 17
  - 3.3.1 Single Digit . . . 18

3.3.2 Int32 and Int64 Constants . . . 18
3.3.3 Long Constants - platform dependant . . . 19
3.3.4 Long Long Constants - platform dependant . . . 20
3.3.5 Initialize and Setting Constants . . . 20
3.4 Comparisons . . . 21
3.4.1 Unsigned comparison . . . 21
3.4.2 Signed comparison . . . 22
3.4.3 Single Digit . . . 23
3.5 Logical Operations . . . 24
3.5.1 Multiplication by two . . . 24
3.5.2 Polynomial Basis Operations . . . 26
3.5.3 AND, OR, XOR and COMPLEMENT Operations . . . 27
3.5.4 Bit Picking . . . 27
3.6 Addition and Subtraction . . . 27
3.7 Sign Manipulation . . . 27
3.7.1 Negation . . . 27
3.7.2 Absolute . . . 28
3.8 Integer Division and Remainder . . . 28

4 Multiplication and Squaring 29
4.1 Multiplication . . . 29
4.2 Squaring . . . 30
4.3 Tuning Polynomial Basis Routines . . . 30

5 Modular Reduction 33
5.1 Straight Division . . . 33
5.2 Barrett Reduction . . . 33
5.3 Montgomery Reduction . . . 35
5.4 Restricted Diminished Radix . . . 37
5.5 Unrestricted Diminished Radix . . . 38
5.6 Combined Modular Reduction . . . 38

6 Exponentiation 39
6.1 Single Digit Exponentiation . . . 39
6.2 Modular Exponentiation . . . 39
6.3 Modulus a Power of Two . . . 39
6.4 Root Finding . . . 39

7 Logarithm 41
7.1 Integer Logarithm . . . 41
7.1.1 Example . . . 41

8 Prime Numbers 43
8.1 Trial Division . . . 43
8.2 Fermat Test . . . 43
8.3 Miller-Rabin Test . . . 43

8.3.1 Required Number of Tests 44
8.4 Strong Lucas-Selfridge Test 46
8.5 Frobenius (Underwood) Test 47
8.6 Primality Testing 47
8.7 Next Prime 48
8.8 Random Primes 48

9 Random Number Generation **49**
9.1 PRNG 49

10 Input and Output **51**
10.1 ASCII Conversions 51
10.1.1 To ASCII 51
10.1.2 From ASCII 51
10.2 Binary Conversions 52

11 Algebraic Functions **55**
11.1 Extended Euclidean Algorithm 55
11.2 Greatest Common Divisor 55
11.3 Least Common Multiple 55
11.4 Jacobi Symbol 55
11.5 Kronecker Symbol 56
11.6 Modular square root 56
11.7 Modular Inverse 56
11.8 Single Digit Functions 56

12 Little Helpers **59**
12.1 Function Macros 59
12.1.1 Renamings 59
12.1.2 Shortcuts 60

Appendices **63**

A Computing Number of Miller-Rabin Trials **63**

List of Figures

1.1 LibTomMath Valuation 8

2.1 Return Codes 9

3.1 Comparison Codes for a, b 21

8.1 Primality Generation Options 48

Chapter 1

Introduction

1.1 What is LibTomMath?

LibTomMath is a library of source code which provides a series of efficient and carefully written functions for manipulating large integer numbers. It was written in portable ISO C source code so that it will build on any platform with a conforming C compiler.

In a nutshell the library was written from scratch with verbose comments to help instruct computer science students how to implement "bignum" math. However, the resulting code has proven to be very useful. It has been used by numerous universities, commercial and open source software developers. It has been used on a variety of platforms ranging from Linux and Windows based x86 to ARM based Gameboys and PPC based MacOS machines.

1.2 License

As of the v0.25 the library source code has been placed in the public domain with every new release. As of the v0.28 release the textbook "Implementing Multiple Precision Arithmetic" has been placed in the public domain with every new release as well. This textbook is meant to compliment the project by providing a more solid walkthrough of the development algorithms used in the library.

Since both[1] are in the public domain everyone is entitled to do with them as they see fit.

1.3 Building LibTomMath

LibTomMath is meant to be very "GCC friendly" as it comes with a makefile well suited for GCC. However, the library will also build in MSVC, Borland C out of

[1] Note that the MPI files under mtest/ are copyrighted by Michael Fromberger. They are not required to use LibTomMath.

the box. For any other ISO C compiler a makefile will have to be made by the end developer. Please consider to commit such a makefile to the LibTomMath developers, currently residing at `http://github.com/libtom/libtommath`, if successfully done so.

Intel's C-compiler (ICC) is sufficiently compatible with GCC, at least the newer versions, to replace GCC for building the static and the shared library. Editing the makefiles is not needed, just set the shell variable `CC` as shown below.

```
CC=/home/czurnieden/intel/bin/icc make
```

ICC does not know all options available for GCC and LibTomMath uses two diagnostics `-Wbad-function-cast` and `-Wcast-align` that are not supported by ICC resulting in the warnings:

```
icc: command line warning #10148: option '-Wbad-function-cast' not supported
icc: command line warning #10148: option '-Wcast-align' not supported
```

It is possible to mute this ICC warning with the compiler flag `-diag-disable=10148`[2].

1.3.1 Static Libraries

To build as a static library for GCC issue the following

```
make
```

command. This will build the library and archive the object files in "libtommath.a". Now you link against that and include "tommath.h" within your programs. Alternatively to build with MSVC issue the following

```
nmake -f makefile.msvc
```

This will build the library and archive the object files in "tommath.lib". This has been tested with MSVC version 6.00 with service pack 5.

To run a program to adapt the Toom-Cook cut-off values to your architecture type

```
make tune
```

This will take some time.

1.3.2 Shared Libraries

GNU based Operating Systems

To build as a shared library for GCC issue the following

```
make -f makefile.shared
```

[2]It is not recommended to suppress warnings without a very good reason but there is no harm in doing so in this very special case.

This requires the "libtool" package (common on most Linux/BSD systems). It will build LibTomMath as both shared and static then install (by default) into /usr/lib as well as install the header files in /usr/include. The shared library (resource) will be called "libtommath.la" while the static library called "libtommath.a". Generally you use libtool to link your application against the shared object.

To run a program to adapt the Toom-Cook cut-off values to your architecture type

```
make -f makefile.shared tune
```

This will take some time.

Microsoft Windows based Operating Systems

There is limited support for making a "DLL" in windows via the "makefile.cygwin_dll" makefile. It requires Cygwin to work with since it requires the auto-export/import functionality. The resulting DLL and import library "libtommath.dll.a" can be used to link LibTomMath dynamically to any Windows program using Cygwin.

OpenBSD

OpenBSD replaced some of their GNU-tools, especially `libtool` with their own, slightly different versions. To ease the workload of LibTomMath's developer team, only a static library can be build with the included `makefile.unix`.

The wrong `make` will result in errors like:

```
*** Parse error in /home/user/GITHUB/libtommath: Need an operator in 'LIBNAME' )
*** Parse error: Need an operator in 'endif' (makefile.shared:8)
*** Parse error: Need an operator in 'CROSS_COMPILE' (makefile_include.mk:16)
*** Parse error: Need an operator in 'endif' (makefile_include.mk:18)
*** Parse error: Missing dependency operator (makefile_include.mk:22)
*** Parse error: Missing dependency operator (makefile_include.mk:23)
...
```

The wrong `libtool` will build it all fine but when it comes to the final linking fails with

```
...
cc -I./ -Wall -Wsign-compare -Wextra -Wshadow -Wsystem-headers -Wdeclaration-afo...
cc -I./ -Wall -Wsign-compare -Wextra -Wshadow -Wsystem-headers -Wdeclaration-afo...
cc -I./ -Wall -Wsign-compare -Wextra -Wshadow -Wsystem-headers -Wdeclaration-afo...
libtool --mode=link --tag=CC cc  bn_error.lo bn_s_mp_invmod_fast.lo bn_fast_mp_mo
libtool: link: cc bn_error.lo bn_s_mp_invmod_fast.lo bn_s_mp_montgomery_reduce_fast0
bn_error.lo: file not recognized: File format not recognized
cc: error: linker command failed with exit code 1 (use -v to see invocation)
Error while executing cc bn_error.lo bn_s_mp_invmod_fast.lo bn_fast_mp_montgomery0
gmake: *** [makefile.shared:64: libtommath.la] Error 1
```

To build a shared library with OpenBSD[3] the GNU versions of `make` and `libtool` are needed.

```
$ sudo pkg_add gmake libtool
```

At this time two versions of `libtool` are installed and both are named `libtool`, unfortunately but GNU `libtool` has been placed in `/usr/local/bin/` and the native version in `/usr/bin/`. The path might be different in other versions of OpenBSD but both programms differ in the output of `libtool --version`

```
$ /usr/local/bin/libtool --version
libtool (GNU libtool) 2.4.2
Written by Gordon Matzigkeit <gord@gnu.ai.mit.edu>, 1996

Copyright (C) 2011 Free Software Foundation, Inc.
This is free software; see the source for copying conditions.  There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
$ libtool --version
libtool (not (GNU libtool)) 1.5.26
```

The shared library should build now with

```
LIBTOOL="/usr/local/bin/libtool" gmake -f makefile.shared
```

You might need to run a `gmake -f makefile.shared clean` first.

NetBSD

NetBSD is not as strict as OpenBSD but still needs `gmake` to build the shared library. `libtool` may also not exist in a fresh install.

```
pkg_add gmake libtool
```

Please check with `libtool --version` that installed libtool is indeed a GNU libtool. Build the shared library by typing:

```
gmake -f makefile.shared
```

1.3.3 Testing

To build the library and the test harness type

```
make test
```

This will build the library, “test” and “mtest/mtest”. The “test” program will accept test vectors and verify the results. “mtest/mtest” will generate test vectors using the MPI library by Michael Fromberger[4]. Simply pipe mtest into test using

[3] Tested with OpenBSD version 6.4

[4] A copy of MPI is included in the package

```
mtest/mtest | test
```

If you do not have a "/dev/urandom" style RNG source you will have to write your own PRNG and simply pipe that into mtest. For example, if your PRNG program is called "myprng" simply invoke

```
myprng | mtest/mtest | test
```

This will output a row of numbers that are increasing. Each column is a different test (such as addition, multiplication, etc) that is being performed. The numbers represent how many times the test was invoked. If an error is detected the program will exit with a dump of the relevant numbers it was working with.

1.4 Build Configuration

LibTomMath can configured at build time in three phases we shall call "depends", "tweaks" and "trims". Each phase changes how the library is built and they are applied one after another respectively.

To make the system more powerful you can tweak the build process. Classes are defined in the file "tommath_superclass.h". By default, the symbol "LTM_ALL" shall be defined which simply instructs the system to build all of the functions. This is how LibTomMath used to be packaged. This will give you access to every function LibTomMath offers.

However, there are cases where such a build is not optional. For instance, you want to perform RSA operations. You don't need the vast majority of the library to perform these operations. Aside from LTM_ALL there is another pre–defined class "SC_RSA_1" which works in conjunction with the RSA from LibTomCrypt. Additional classes can be defined base on the need of the user.

1.4.1 Build Depends

In the file tommath_class.h you will see a large list of C "defines" followed by a series of "ifdefs" which further define symbols. All of the symbols (technically they're macros ...) represent a given C source file. For instance, BN_MP_ADD_C represents the file "bn_mp_add.c". When a define has been enabled the function in the respective file will be compiled and linked into the library. Accordingly when the define is absent the file will not be compiled and not contribute any size to the library.

You will also note that the header tommath_class.h is actually recursively included (it includes itself twice). This is to help resolve as many dependencies as possible. In the last pass the symbol LTM_LAST will be defined. This is useful for "trims".

1.4.2 Build Tweaks

A tweak is an algorithm "alternative". For example, to provide tradeoffs (usually between size and space). They can be enabled at any pass of the configuration phase.

Define	Purpose
BN_MP_DIV_SMALL	Enables a slower, smaller and equally functional mp_div() function

1.4.3 Build Trims

A trim is a manner of removing functionality from a function that is not required. For instance, to perform RSA cryptography you only require exponentiation with odd moduli so even moduli support can be safely removed. Build trims are meant to be defined on the last pass of the configuration which means they are to be defined only if LTM_LAST has been defined.

Moduli Related

Restriction	Undefine
Exponentiation with odd moduli only	BN_S_MP_EXPTMOD_C BN_MP_REDUCE_C BN_MP_REDUCE_SETUP_C BN_S_MP_MUL_HIGH_DIGS_C BN_FAST_S_MP_MUL_HIGH_DIGS_C
Exponentiation with random odd moduli	(The above plus the following) BN_MP_REDUCE_2K_C BN_MP_REDUCE_2K_SETUP_C BN_MP_REDUCE_IS_2K_C BN_MP_DR_IS_MODULUS_C BN_MP_DR_REDUCE_C BN_MP_DR_SETUP_C
Modular inverse odd moduli only	BN_MP_INVMOD_SLOW_C
Modular inverse (both, smaller/slower)	BN_FAST_MP_INVMOD_C

Operand Size Related

Restriction	Undefine
Moduli $\leq$ 2560 bits	BN_MP_MONTGOMERY_REDUCE_C BN_S_MP_MUL_DIGS_C BN_S_MP_MUL_HIGH_DIGS_C BN_S_MP_SQR_C
Polynomial Schmolynomial	BN_MP_KARATSUBA_MUL_C BN_MP_KARATSUBA_SQR_C BN_MP_TOOM_MUL_C BN_MP_TOOM_SQR_C

1.5 Purpose of LibTomMath

Unlike GNU MP (GMP) Library, LIP, OpenSSL or various other commercial kits (Miracl), LibTomMath was not written with bleeding edge performance in mind. First and foremost LibTomMath was written to be entirely open. Not only is the source code public domain (unlike various other GPL/etc licensed code), not only is the code freely downloadable but the source code is also accessible for computer science students attempting to learn "BigNum" or multiple precision arithmetic techniques.

LibTomMath was written to be an instructive collection of source code. This is why there are many comments, only one function per source file and often I use a "middle-road" approach where I don't cut corners for an extra 2% speed increase.

Source code alone cannot really teach how the algorithms work which is why I also wrote a textbook that accompanies the library (beat that!).

So you may be thinking "should I use LibTomMath?" and the answer is a definite maybe. Let me tabulate what I think are the pros and cons of LibTomMath by comparing it to the math routines from GnuPG[5].

[5]GnuPG v1.2.3 versus LibTomMath v0.28

Criteria	**Pro**	**Con**	**Notes**
Few lines of code per file	X		GnuPG = 300.9, LibTomMath = 71.97
Commented function prototypes	X		GnuPG function names are cryptic.
Speed		X	LibTomMath is slower.
Totally free	X		GPL has unfavourable restrictions.
Large function base	X		GnuPG is barebones.
Five modular reduction algorithms	X		Faster modular exponentiation for a variety of moduli.
Portable	X		GnuPG requires configuration to build.

Figure 1.1: LibTomMath Valuation

It may seem odd to compare LibTomMath to GnuPG since the math in GnuPG is only a small portion of the entire application. However, LibTomMath was written with cryptography in mind. It provides essentially all of the functions a cryptosystem would require when working with large integers.

So it may feel tempting to just rip the math code out of GnuPG (or GnuMP where it was taken from originally) in your own application but I think there are reasons not to. While LibTomMath is slower than libraries such as GnuMP it is not normally significantly slower. On x86 machines the difference is normally a factor of two when performing modular exponentiations. It depends largely on the processor, compiler and the moduli being used.

Essentially the only time you wouldn't use LibTomMath is when blazing speed is the primary concern. However, on the other side of the coin LibTomMath offers you a totally free (public domain) well structured math library that is very flexible, complete and performs well in resource constrained environments. Fast RSA for example can be performed with as little as 8KB of ram for data (again depending on build options).

Chapter 2

Getting Started with LibTomMath

2.1 Building Programs

In order to use LibTomMath you must include "tommath.h" and link against the appropriate library file (typically libtommath.a). There is no library initialization required and the entire library is thread safe.

2.2 Return Codes

There are three possible return codes a function may return.

Code	**Meaning**
MP_OKAY	The function succeeded.
MP_VAL	The function input was invalid.
MP_MEM	Heap memory exhausted.
MP_YES	Response is yes.
MP_NO	Response is no.

Figure 2.1: Return Codes

The last two codes listed are not actually "return'ed" by a function. They are placed in an integer (the caller must provide the address of an integer it can store to) which the caller can access. To convert one of the three return codes to a string use the following function.

```
char *mp_error_to_string(int code);
```

This will return a pointer to a string which describes the given error code. It will not work for the return codes MP_YES and MP_NO.

2.3 Data Types

The basic "multiple precision integer" type is known as the "mp_int" within LibTomMath. This data type is used to organize all of the data required to manipulate the integer it represents. Within LibTomMath it has been prototyped as the following.

```
typedef struct  {
    int used, alloc, sign;
    mp_digit *dp;
} mp_int;
```

Where "mp_digit" is a data type that represents individual digits of the integer. By default, an mp_digit is the ISO C "unsigned long" data type and each digit is $28-$bits long. The mp_digit type can be configured to suit other platforms by defining the appropriate macros.

All LTM functions that use the mp_int type will expect a pointer to mp_int structure. You must allocate memory to hold the structure itself by yourself (whether off stack or heap it doesn't matter). The very first thing that must be done to use an mp_int is that it must be initialized.

2.4 Function Organization

The arithmetic functions of the library are all organized to have the same style prototype. That is source operands are passed on the left and the destination is on the right. For instance,

```
mp_add(&a, &b, &c);       /* c = a + b */
mp_mul(&a, &a, &c);       /* c = a * a */
mp_div(&a, &b, &c, &d);   /* c = [a/b], d = a mod b */
```

Another feature of the way the functions have been implemented is that source operands can be destination operands as well. For instance,

```
mp_add(&a, &b, &b);       /* b = a + b */
mp_div(&a, &b, &a, &c);   /* a = [a/b], c = a mod b */
```

This allows operands to be re-used which can make programming simpler.

2.5 Initialization

2.5.1 Single Initialization

A single mp_int can be initialized with the "mp_init" function.

```
int mp_init (mp_int * a);
```

This function expects a pointer to an mp_int structure and will initialize the members of the structure so the mp_int represents the default integer which is zero. If the functions returns MP_OKAY then the mp_int is ready to be used by the other LibTomMath functions.

```
int main(void)
{
   mp_int number;
   int result;

   if ((result = mp_init(&number)) != MP_OKAY) {
      printf("Error initializing the number.  %s",
             mp_error_to_string(result));
      return EXIT_FAILURE;
   }

   /* use the number */

   return EXIT_SUCCESS;
}
```

2.5.2 Single Free

When you are finished with an mp_int it is ideal to return the heap it used back to the system. The following function provides this functionality.

```
void mp_clear (mp_int * a);
```

The function expects a pointer to a previously initialized mp_int structure and frees the heap it uses. It sets the pointer[1] within the mp_int to **NULL** which is used to prevent double free situations. Is is legal to call mp_clear() twice on the same mp_int in a row.

```
int main(void)
{
   mp_int number;
   int result;

   if ((result = mp_init(&number)) != MP_OKAY) {
      printf("Error initializing the number.  %s",
             mp_error_to_string(result));
      return EXIT_FAILURE;
   }

   /* use the number */

   /* We're done with it. */
   mp_clear(&number);
```

[1] The "dp" member.

```
   return EXIT_SUCCESS;
}
```

2.5.3 Multiple Initializations

Certain algorithms require more than one large integer. In these instances it is ideal to initialize all of the mp_int variables in an "all or nothing" fashion. That is, they are either all initialized successfully or they are all not initialized.

The mp_init_multi() function provides this functionality.

```
int mp_init_multi(mp_int *mp, ...);
```

It accepts a **NULL** terminated list of pointers to mp_int structures. It will attempt to initialize them all at once. If the function returns MP_OKAY then all of the mp_int variables are ready to use, otherwise none of them are available for use. A complementary mp_clear_multi() function allows multiple mp_int variables to be free'd from the heap at the same time.

```
int main(void)
{
   mp_int num1, num2, num3;
   int result;

   if ((result = mp_init_multi(&num1,
                               &num2,
                               &num3, NULL)) != MP_OKAY) {
      printf("Error initializing the numbers.  %s",
             mp_error_to_string(result));
      return EXIT_FAILURE;
   }

   /* use the numbers */

   /* We're done with them. */
   mp_clear_multi(&num1, &num2, &num3, NULL);

   return EXIT_SUCCESS;
}
```

2.5.4 Other Initializers

To initialized and make a copy of an mp_int the mp_init_copy() function has been provided.

```
int mp_init_copy (mp_int * a, mp_int * b);
```

This function will initialize a and make it a copy of b if all goes well.

```
int main(void)
{
   mp_int num1, num2;
   int result;

   /* initialize and do work on num1 ... */

   /* We want a copy of num1 in num2 now */
   if ((result = mp_init_copy(&num2, &num1)) != MP_OKAY) {
     printf("Error initializing the copy.  %s",
             mp_error_to_string(result));
      return EXIT_FAILURE;
   }

   /* now num2 is ready and contains a copy of num1 */

   /* We're done with them. */
   mp_clear_multi(&num1, &num2, NULL);

   return EXIT_SUCCESS;
}
```

Another less common initializer is mp_init_size() which allows the user to initialize an mp_int with a given default number of digits. By default, all initializers allocate **MP_PREC** digits. This function lets you override this behaviour.

```
int mp_init_size (mp_int * a, int size);
```

The *size* parameter must be greater than zero. If the function succeeds the mp_int *a* will be initialized to have *size* digits (which are all initially zero).

```
int main(void)
{
   mp_int number;
   int result;

   /* we need a 60-digit number */
   if ((result = mp_init_size(&number, 60)) != MP_OKAY) {
      printf("Error initializing the number.  %s",
             mp_error_to_string(result));
      return EXIT_FAILURE;
   }

   /* use the number */

   return EXIT_SUCCESS;
}
```

2.6 Maintenance Functions

2.6.1 Clear Leading Zeros

This is used to ensure that leading zero digits are trimed and the leading "used" digit will be non-zero. It also fixes the sign if there are no more leading digits.

```
void mp_clamp(mp_int *a);
```

2.6.2 Zero Out

This function will set the "bigint" to zeros without changing the amount of allocated memory.

```
void mp_zero(mp_int *a);
```

2.6.3 Reducing Memory Usage

When an mp_int is in a state where it won't be changed again[2] excess digits can be removed to return memory to the heap with the mp_shrink() function.

```
int mp_shrink (mp_int * a);
```

This will remove excess digits of the mp_int a. If the operation fails the mp_int should be intact without the excess digits being removed. Note that you can use a shrunk mp_int in further computations, however, such operations will require heap operations which can be slow. It is not ideal to shrink mp_int variables that you will further modify in the system (unless you are seriously low on memory).

```
int main(void)
{
   mp_int number;
   int result;

   if ((result = mp_init(&number)) != MP_OKAY) {
      printf("Error initializing the number.  %s",
             mp_error_to_string(result));
      return EXIT_FAILURE;
   }

   /* use the number [e.g. pre-computation]  */

   /* We're done with it for now. */
   if ((result = mp_shrink(&number)) != MP_OKAY) {
      printf("Error shrinking the number.  %s",
             mp_error_to_string(result));
```

[2] A Diffie-Hellman modulus for instance.

```
      return EXIT_FAILURE;
   }

   /* use it .... */


   /* we're done with it. */
   mp_clear(&number);

   return EXIT_SUCCESS;
}
```

2.6.4 Adding additional digits

Within the mp_int structure are two parameters which control the limitations of the array of digits that represent the integer the mp_int is meant to equal. The *used* parameter dictates how many digits are significant, that is, contribute to the value of the mp_int. The *alloc* parameter dictates how many digits are currently available in the array. If you need to perform an operation that requires more digits you will have to mp_grow() the mp_int to your desired size.

```
int mp_grow (mp_int * a, int size);
```

This will grow the array of digits of a to $size$. If the *alloc* parameter is already bigger than $size$ the function will not do anything.

```
int main(void)
{
   mp_int number;
   int result;

   if ((result = mp_init(&number)) != MP_OKAY) {
      printf("Error initializing the number.  %s",
             mp_error_to_string(result));
      return EXIT_FAILURE;
   }

   /* use the number */

   /* We need to add 20 digits to the number  */
   if ((result = mp_grow(&number, number.alloc + 20)) != MP_OKAY) {
      printf("Error growing the number.  %s",
             mp_error_to_string(result));
      return EXIT_FAILURE;
   }


   /* use the number */
```

```
   /* we're done with it. */
   mp_clear(&number);

   return EXIT_SUCCESS;
}
```

Chapter 3

Basic Operations

3.1 Copying

A so called "deep copy", where new memory is allocated and all contents of a are copied verbatim into b such that $b = a$ at the end.

```
int mp_copy (mp_int * a, mp_int *b);
```

You can also just swap a and b. It does the normal pointer changing with a temporary pointer variable, just that you do not have to.

```
void mp_exch (mp_int * a, mp_int *b);
```

3.2 Bit Counting

To get the position of the lowest bit set (LSB, the Lowest Significant Bit; the number of bits which are zero before the first zero bit)

```
int mp_cnt_lsb(const mp_int *a);
```

To get the position of the highest bit set (MSB, the Most Significant Bit; the number of bits in teh "bignum")

```
int mp_count_bits(const mp_int *a);
```

3.3 Small Constants

Setting mp_ints to small constants is a relatively common operation. To accommodate these instances there is a small constant assignment function. This function is used to set a single digit constant. The reason for this function is efficiency. Setting a single digit is quick but the domain of a digit can change (it's always at least $0 \ldots 127$).

3.3.1 Single Digit

Setting a single digit can be accomplished with the following function.

```
void mp_set (mp_int * a, mp_digit b);
```

This will zero the contents of a and make it represent an integer equal to the value of b. Note that this function has a return type of **void**. It cannot cause an error so it is safe to assume the function succeeded.

```
int main(void)
{
   mp_int number;
   int result;

   if ((result = mp_init(&number)) != MP_OKAY) {
      printf("Error initializing the number.  %s",
             mp_error_to_string(result));
      return EXIT_FAILURE;
   }

   /* set the number to 5 */
   mp_set(&number, 5);

   /* we're done with it. */
   mp_clear(&number);

   return EXIT_SUCCESS;
}
```

3.3.2 Int32 and Int64 Constants

These functions can be used to set a constant with 32 or 64 bits.

```
void mp_set_i32 (mp_int * a, int32_t b);
void mp_set_u32 (mp_int * a, uint32_t b);
void mp_set_i64 (mp_int * a, int64_t b);
void mp_set_u64 (mp_int * a, uint64_t b);
```

These functions assign the sign and value of the input `b` to `mp_int a`. The value can be obtained again by calling the following functions.

```
int32_t mp_get_i32 (mp_int * a);
uint32_t mp_get_u32 (mp_int * a);
uint32_t mp_get_mag_u32 (mp_int * a);
int64_t mp_get_i64 (mp_int * a);
uint64_t mp_get_u64 (mp_int * a);
uint64_t mp_get_mag_u64 (mp_int * a);
```

These functions return the 32 or 64 least significant bits of a respectively. The unsigned functions return negative values in a twos complement representation. The absolute value or magnitude can be obtained using the mp_get_mag functions.

```
int main(void)
{
   mp_int number;
   int result;

   if ((result = mp_init(&number)) != MP_OKAY) {
      printf("Error initializing the number.  %s",
             mp_error_to_string(result));
      return EXIT_FAILURE;
   }

   /* set the number to 654321 (note this is bigger than 127) */
   mp_set_u32(&number, 654321);

   printf("number == %" PRIi32, mp_get_i32(&number));

   /* we're done with it. */
   mp_clear(&number);

   return EXIT_SUCCESS;
}
```

This should output the following if the program succeeds.

```
number == 654321
```

3.3.3 Long Constants - platform dependant

```
void mp_set_l (mp_int * a, long b);
void mp_set_ul (mp_int * a, unsigned long b);
```

This will assign the value of the platform-dependent sized variable b to the mp_int a.

To retrieve the value, the following functions can be used.

```
long mp_get_l (mp_int * a);
unsigned long mp_get_ul (mp_int * a);
unsigned long mp_get_mag_ul (mp_int * a);
```

This will return the least significant bits of the mp_int a that fit into a "long".

3.3.4 Long Long Constants - platform dependant

```
void mp_set_ll (mp_int * a, long long b);
void mp_set_ull (mp_int * a, unsigned long long b);
```

This will assign the value of the platform-dependent sized variable b to the mp_int a.

To retrieve the value, the following functions can be used.

```
long long mp_get_ll (mp_int * a);
unsigned long long mp_get_ull (mp_int * a);
unsigned long long mp_get_mag_ull (mp_int * a);
```

This will return the least significant bits of the mp_int a that fit into a "long long".

3.3.5 Initialize and Setting Constants

To both initialize and set small constants the following two functions are available.

```
int mp_init_set (mp_int * a, mp_digit b);
int mp_init_i32 (mp_int * a, int32_t b);
int mp_init_u32 (mp_int * a, uint32_t b);
int mp_init_i64 (mp_int * a, int64_t b);
int mp_init_u64 (mp_int * a, uint64_t b);
int mp_init_l   (mp_int * a, long b);
int mp_init_ul  (mp_int * a, unsigned long b);
int mp_init_ll  (mp_int * a, long long b);
int mp_init_ull (mp_int * a, unsigned long long b);
```

Both functions work like the previous counterparts except they first mp_init a before setting the values.

```
int main(void)
{
   mp_int number1, number2;
   int    result;

   /* initialize and set a single digit */
   if ((result = mp_init_set(&number1, 100)) != MP_OKAY) {
      printf("Error setting number1: %s",
             mp_error_to_string(result));
      return EXIT_FAILURE;
   }

   /* initialize and set a long */
   if ((result = mp_init_l(&number2, 1023)) != MP_OKAY) {
```

```
      printf("Error setting number2: %s",
             mp_error_to_string(result));
      return EXIT_FAILURE;
   }

   /* display */
   printf("Number1, Number2 == %" PRIi32 ", %" PRIi32,
          mp_get_i32(&number1), mp_get_i32(&number2));

   /* clear */
   mp_clear_multi(&number1, &number2, NULL);

   return EXIT_SUCCESS;
}
```

If this program succeeds it shall output.

```
Number1, Number2 == 100, 1023
```

3.4 Comparisons

Comparisons in LibTomMath are always performed in a "left to right" fashion. There are three possible return codes for any comparison.

Result Code	Meaning
MP_GT	$a > b$
MP_EQ	$a = b$
MP_LT	$a < b$

Figure 3.1: Comparison Codes for a, b

In figure 3.1 two integers a and b are being compared. In this case a is said to be "to the left" of b.

3.4.1 Unsigned comparison

An unsigned comparison considers only the digits themselves and not the associated *sign* flag of the mp_int structures. This is analogous to an absolute comparison. The function mp_cmp_mag() will compare two mp_int variables based on their digits only.

```
int mp_cmp_mag(mp_int * a, mp_int * b);
```

This will compare a to b placing a to the left of b. This function cannot fail and will return one of the three compare codes listed in figure 3.1.

```
int main(void)
{
   mp_int number1, number2;
   int result;

   if ((result = mp_init_multi(&number1, &number2, NULL)) != MP_OKAY) {
      printf("Error initializing the numbers.  %s",
             mp_error_to_string(result));
      return EXIT_FAILURE;
   }

   /* set the number1 to 5 */
   mp_set(&number1, 5);

   /* set the number2 to -6 */
   mp_set(&number2, 6);
   if ((result = mp_neg(&number2, &number2)) != MP_OKAY) {
      printf("Error negating number2.  %s",
             mp_error_to_string(result));
      return EXIT_FAILURE;
   }

   switch(mp_cmp_mag(&number1, &number2)) {
       case MP_GT:  printf("|number1| > |number2|"); break;
       case MP_EQ:  printf("|number1| = |number2|"); break;
       case MP_LT:  printf("|number1| < |number2|"); break;
   }

   /* we're done with it. */
   mp_clear_multi(&number1, &number2, NULL);

   return EXIT_SUCCESS;
}
```

If this program[1] completes successfully it should print the following.

```
|number1| < |number2|
```

This is because $|-6| = 6$ and obviously $5 < 6$.

3.4.2 Signed comparison

To compare two mp_int variables based on their signed value the mp_cmp() function is provided.

```
int mp_cmp(mp_int * a, mp_int * b);
```

[1]This function uses the mp_neg() function which is discussed in section 3.7.1.

This will compare a to the left of b. It will first compare the signs of the two mp_int variables. If they differ it will return immediately based on their signs. If the signs are equal then it will compare the digits individually. This function will return one of the compare conditions codes listed in figure 3.1.

```
int main(void)
{
   mp_int number1, number2;
   int result;

   if ((result = mp_init_multi(&number1, &number2, NULL)) != MP_OKAY) {
      printf("Error initializing the numbers.  %s",
             mp_error_to_string(result));
      return EXIT_FAILURE;
   }

   /* set the number1 to 5 */
   mp_set(&number1, 5);

   /* set the number2 to -6 */
   mp_set(&number2, 6);
   if ((result = mp_neg(&number2, &number2)) != MP_OKAY) {
      printf("Error negating number2.  %s",
             mp_error_to_string(result));
      return EXIT_FAILURE;
   }

   switch(mp_cmp(&number1, &number2)) {
       case MP_GT:  printf("number1 > number2"); break;
       case MP_EQ:  printf("number1 = number2"); break;
       case MP_LT:  printf("number1 < number2"); break;
   }

   /* we're done with it. */
   mp_clear_multi(&number1, &number2, NULL);

   return EXIT_SUCCESS;
}
```

If this program[2] completes successfully it should print the following.

```
number1 > number2
```

3.4.3 Single Digit

To compare a single digit against an mp_int the following function has been provided.

[2]This function uses the mp_neg() function which is discussed in section 3.7.1.

```
int mp_cmp_d(mp_int * a, mp_digit b);
```

This will compare a to the left of b using a signed comparison. Note that it will always treat b as positive. This function is rather handy when you have to compare against small values such as 1 (which often comes up in cryptography). The function cannot fail and will return one of the tree compare condition codes listed in figure 3.1.

```
int main(void)
{
   mp_int number;
   int result;

   if ((result = mp_init(&number)) != MP_OKAY) {
      printf("Error initializing the number.  %s",
             mp_error_to_string(result));
      return EXIT_FAILURE;
   }

   /* set the number to 5 */
   mp_set(&number, 5);

   switch(mp_cmp_d(&number, 7)) {
       case MP_GT:  printf("number > 7"); break;
       case MP_EQ:  printf("number = 7"); break;
       case MP_LT:  printf("number < 7"); break;
   }

   /* we're done with it. */
   mp_clear(&number);

   return EXIT_SUCCESS;
}
```

If this program functions properly it will print out the following.

```
number < 7
```

3.5 Logical Operations

Logical operations are operations that can be performed either with simple shifts or boolean operators such as AND, XOR and OR directly. These operations are very quick.

3.5.1 Multiplication by two

Multiplications and divisions by any power of two can be performed with quick logical shifts either left or right depending on the operation.

When multiplying or dividing by two a special case routine can be used which are as follows.

```
int mp_mul_2(mp_int * a, mp_int * b);
int mp_div_2(mp_int * a, mp_int * b);
```

The former will assign twice a to b while the latter will assign half a to b. These functions are fast since the shift counts and maskes are hardcoded into the routines.

```
int main(void)
{
   mp_int number;
   int result;

   if ((result = mp_init(&number)) != MP_OKAY) {
      printf("Error initializing the number.  %s",
             mp_error_to_string(result));
      return EXIT_FAILURE;
   }

   /* set the number to 5 */
   mp_set(&number, 5);

   /* multiply by two */
   if ((result = mp_mul_2(&number, &number)) != MP_OKAY) {
      printf("Error multiplying the number.  %s",
             mp_error_to_string(result));
      return EXIT_FAILURE;
   }
   switch(mp_cmp_d(&number, 7)) {
       case MP_GT:  printf("2*number > 7"); break;
       case MP_EQ:  printf("2*number = 7"); break;
       case MP_LT:  printf("2*number < 7"); break;
   }

   /* now divide by two */
   if ((result = mp_div_2(&number, &number)) != MP_OKAY) {
      printf("Error dividing the number.  %s",
             mp_error_to_string(result));
      return EXIT_FAILURE;
   }
   switch(mp_cmp_d(&number, 7)) {
       case MP_GT:  printf("2*number/2 > 7"); break;
       case MP_EQ:  printf("2*number/2 = 7"); break;
       case MP_LT:  printf("2*number/2 < 7"); break;
   }

   /* we're done with it. */
   mp_clear(&number);
```

```
   return EXIT_SUCCESS;
}
```

If this program is successful it will print out the following text.

```
2*number > 7
2*number/2 < 7
```

Since $10 > 7$ and $5 < 7$.

To multiply by a power of two the following function can be used.

```
int mp_mul_2d(mp_int * a, int b, mp_int * c);
```

This will multiply a by 2^b and store the result in "c". If the value of b is less than or equal to zero the function will copy a to "c" without performing any further actions. The multiplication itself is implemented as a right-shift operation of a by b bits.

To divide by a power of two use the following.

```
int mp_div_2d (mp_int * a, int b, mp_int * c, mp_int * d);
```

Which will divide a by 2^b, store the quotient in "c" and the remainder in "d'. If $b \leq 0$ then the function simply copies a over to "c" and zeroes d. The variable d may be passed as a **NULL** value to signal that the remainder is not desired. The division itself is implemented as a left-shift operation of a by b bits.

It is also not very uncommon to need just the power of two 2^b; for example the startvalue for the Newton method.

```
int mp_2expt(mp_int *a, int b);
```

It is faster than doing it by shifting 1 with `mp_mul_2d`.

3.5.2 Polynomial Basis Operations

Strictly speaking the organization of the integers within the mp_int structures is what is known as a "polynomial basis". This simply means a field element is stored by divisions of a radix. For example, if $f(x) = \sum_{i=0}^{k} y_i x^k$ for any vector $\vec{y}$ then the array of digits in $\vec{y}$ are said to be the polynomial basis representation of z if $f(\beta) = z$ for a given radix β.

To multiply by the polynomial $g(x) = x$ all you have todo is shift the digits of the basis left one place. The following function provides this operation.

```
int mp_lshd (mp_int * a, int b);
```

This will multiply a in place by x^b which is equivalent to shifting the digits left b places and inserting zeroes in the least significant digits. Similarly to divide by a power of x the following function is provided.

```
void mp_rshd (mp_int * a, int b)
```

This will divide a in place by x^b and discard the remainder. This function cannot fail as it performs the operations in place and no new digits are required to complete it.

3.5.3 AND, OR, XOR and COMPLEMENT Operations

While AND, OR and XOR operations compute arbitrary-precision bitwise operations. Negative numbers are treated as if they are in two-complement representation, while internally they are sign-magnitude however.

```
int mp_or  (mp_int * a, mp_int * b, mp_int * c);
int mp_and (mp_int * a, mp_int * b, mp_int * c);
int mp_xor (mp_int * a, mp_int * b, mp_int * c);
int mp_complement(const mp_int *a, mp_int *b);
int mp_signed_rsh(mp_int * a, int b, mp_int * c, mp_int * d);
```

The function `mp_complement` computes a two-complement $b =\sim a$. The function `mp_signed_rsh` performs sign extending right shift. For positive numbers it is equivalent to `mp_div_2d`.

3.5.4 Bit Picking

```
int mp_get_bit(mp_int *a, int b)
```

Pick a bit: returns `MP_YES` if the bit at position b (0-index) is set, that is if it is 1 (one), `MP_NO` if the bit is 0 (zero) and `MP_VAL` if $b < 0$.

3.6 Addition and Subtraction

To compute an addition or subtraction the following two functions can be used.

```
int mp_add (mp_int * a, mp_int * b, mp_int * c);
int mp_sub (mp_int * a, mp_int * b, mp_int * c)
```

Which perform $c = a \odot b$ where $\odot$ is one of signed addition or subtraction. The operations are fully sign aware.

3.7 Sign Manipulation

3.7.1 Negation

Simple integer negation can be performed with the following.

```
int mp_neg (mp_int * a, mp_int * b);
```

Which assigns $-a$ to b.

3.7.2 Absolute

Simple integer absolutes can be performed with the following.

```
int mp_abs (mp_int * a, mp_int * b);
```

Which assigns $|a|$ to b.

3.8 Integer Division and Remainder

To perform a complete and general integer division with remainder use the following function.

```
int mp_div (mp_int * a, mp_int * b, mp_int * c, mp_int * d);
```

This divides a by b and stores the quotient in c and d. The signed quotient is computed such that $bc + d = a$. Note that either of c or d can be set to **NULL** if their value is not required. If b is zero the function returns **MP_VAL**.

Chapter 4

Multiplication and Squaring

4.1 Multiplication

A full signed integer multiplication can be performed with the following.

```
int mp_mul (mp_int * a, mp_int * b, mp_int * c);
```

Which assigns the full signed product ab to c. This function actually breaks into one of four cases which are specific multiplication routines optimized for given parameters. First there are the Toom-Cook multiplications which should only be used with very large inputs. This is followed by the Karatsuba multiplications which are for moderate sized inputs. Then followed by the Comba and baseline multipliers.

Fortunately for the developer you don't really need to know this unless you really want to fine tune the system. mp_mul() will determine on its own[1] what routine to use automatically when it is called.

```
int main(void)
{
   mp_int number1, number2;
   int result;

   /* Initialize the numbers */
   if ((result = mp_init_multi(&number1,
                               &number2, NULL)) != MP_OKAY) {
      printf("Error initializing the numbers.  %s",
             mp_error_to_string(result));
      return EXIT_FAILURE;
   }
```

[1]Some tweaking may be required but `make tune` will put some reasonable values in `bncore.c`

```
   /* set the terms */
   mp_set_i32(&number, 257);
   mp_set_i32(&number2, 1023);

   /* multiply them */
   if ((result = mp_mul(&number1, &number2,
                        &number1)) != MP_OKAY) {
      printf("Error multiplying terms.  %s",
             mp_error_to_string(result));
      return EXIT_FAILURE;
   }

   /* display */
   printf("number1 * number2 == %" PRIi32, mp_get_i32(&number1));

   /* free terms and return */
   mp_clear_multi(&number1, &number2, NULL);

   return EXIT_SUCCESS;
}
```

If this program succeeds it shall output the following.

```
number1 * number2 == 262911
```

4.2 Squaring

Since squaring can be performed faster than multiplication it is performed it's own function instead of just using mp_mul().

```
int mp_sqr (mp_int * a, mp_int * b);
```

Will square a and store it in b. Like the case of multiplication there are four different squaring algorithms all which can be called from mp_sqr(). It is ideal to use mp_sqr over mp_mul when squaring terms because of the speed difference.

4.3 Tuning Polynomial Basis Routines

Both of the Toom-Cook and Karatsuba multiplication algorithms are faster than the traditional $O(n^2)$ approach that the Comba and baseline algorithms use. At $O(n^{1.464973})$ and $O(n^{1.584962})$ running times respectively they require considerably less work. For example, a 10000-digit multiplication would take roughly 724,000 single precision multiplications with Toom-Cook or 100,000,000 single precision multiplications with the standard Comba (a factor of 138).

So why not always use Karatsuba or Toom-Cook? The simple answer is that they have so much overhead that they're not actually faster than Comba until

you hit distinct "cutoff" points. For Karatsuba with the default configuration, GCC 3.3.1 and an Athlon XP processor the cutoff point is roughly 110 digits (about 70 for the Intel P4). That is, at 110 digits Karatsuba and Comba multiplications just about break even and for 110+ digits Karatsuba is faster.

Toom-Cook has incredible overhead and is probably only useful for very large inputs. So far no known cutoff points exist and for the most part I just set the cutoff points very high to make sure they're not called.

To get reasonable values for the cut-off points for your architecture, type

```
make tune
```

This will run a benchmark, computes the medians, rewrites `bncore.c`, and recompiles `bncore.c` and relinks the library.

The benchmark itself can be fine-tuned in the file `etc/tune_it.sh`.

The program `etc/tune` is also able to print a list of values for printing curves with e.g.: `gnuplot`. type `./etc/tune -h` to get a list of all available options.

Chapter 5

Modular Reduction

Modular reduction is process of taking the remainder of one quantity divided by another. Expressed as (5.1) the modular reduction is equivalent to the remainder of b divided by c.

$$a \equiv b \pmod{c} \tag{5.1}$$

Of particular interest to cryptography are reductions where b is limited to the range $0 \le b < c^2$ since particularly fast reduction algorithms can be written for the limited range.

Note that one of the four optimized reduction algorithms are automatically chosen in the modular exponentiation algorithm mp_exptmod when an appropriate modulus is detected.

5.1 Straight Division

In order to effect an arbitrary modular reduction the following algorithm is provided.

```
int mp_mod(mp_int *a, mp_int *b, mp_int *c);
```

This reduces a modulo b and stores the result in c. The sign of c shall agree with the sign of b. This algorithm accepts an input a of any range and is not limited by $0 \le a < b^2$.

5.2 Barrett Reduction

Barrett reduction is a generic optimized reduction algorithm that requires pre–computation to achieve a decent speedup over straight division. First a μ value must be precomputed with the following function.

```
int mp_reduce_setup(mp_int *a, mp_int *b);
```

Given a modulus in b this produces the required μ value in a. For any given modulus this only has to be computed once. Modular reduction can now be performed with the following.

```
int mp_reduce(mp_int *a, mp_int *b, mp_int *c);
```

This will reduce a in place modulo b with the precomputed μ value in c. a must be in the range $0 \le a < b^2$.

```
int main(void)
{
   mp_int   a, b, c, mu;
   int      result;

   /* initialize a,b to desired values, mp_init mu,
    * c and set c to 1...we want to compute a^3 mod b
    */

   /* get mu value */
   if ((result = mp_reduce_setup(&mu, b)) != MP_OKAY) {
      printf("Error getting mu.  %s",
             mp_error_to_string(result));
      return EXIT_FAILURE;
   }

   /* square a to get c = a^2 */
   if ((result = mp_sqr(&a, &c)) != MP_OKAY) {
      printf("Error squaring.  %s",
             mp_error_to_string(result));
      return EXIT_FAILURE;
   }

   /* now reduce 'c' modulo b */
   if ((result = mp_reduce(&c, &b, &mu)) != MP_OKAY) {
      printf("Error reducing.  %s",
             mp_error_to_string(result));
      return EXIT_FAILURE;
   }

   /* multiply a to get c = a^3 */
   if ((result = mp_mul(&a, &c, &c)) != MP_OKAY) {
      printf("Error reducing.  %s",
             mp_error_to_string(result));
      return EXIT_FAILURE;
   }

   /* now reduce 'c' modulo b  */
```

```
   if ((result = mp_reduce(&c, &b, &mu)) != MP_OKAY) {
      printf("Error reducing.  %s",
             mp_error_to_string(result));
      return EXIT_FAILURE;
   }

   /* c now equals a^3 mod b */

   return EXIT_SUCCESS;
}
```

This program will calculate $a^3 \bmod b$ if all the functions succeed.

5.3 Montgomery Reduction

Montgomery is a specialized reduction algorithm for any odd moduli. Like Barrett reduction a pre–computation step is required. This is accomplished with the following.

```
int mp_montgomery_setup(mp_int *a, mp_digit *mp);
```

For the given odd moduli a the precomputation value is placed in mp. The reduction is computed with the following.

```
int mp_montgomery_reduce(mp_int *a, mp_int *m, mp_digit mp);
```

This reduces a in place modulo m with the pre–computed value mp. a must be in the range $0 \le a < b^2$.

Montgomery reduction is faster than Barrett reduction for moduli smaller than the "comba" limit. With the default setup for instance, the limit is 127 digits (3556–bits). Note that this function is not limited to 127 digits just that it falls back to a baseline algorithm after that point.

An important observation is that this reduction does not return $a \bmod m$ but $aR^{-1} \bmod m$ where $R = \beta^n$, n is the n number of digits in m and β is radix used (default is 2^{28}).

To quickly calculate R the following function was provided.

```
int mp_montgomery_calc_normalization(mp_int *a, mp_int *b);
```

Which calculates $a = R$ for the odd moduli b without using multiplication or division.

The normal modus operandi for Montgomery reductions is to normalize the integers before entering the system. For example, to calculate $a^3 \bmod b$ using Montgomery reduction the value of a can be normalized by multiplying it by R. Consider the following code snippet.

```
int main(void)
{
   mp_int   a, b, c, R;
   mp_digit mp;
   int      result;

   /* initialize a,b to desired values,
    * mp_init R, c and set c to 1....
    */

   /* get normalization */
   if ((result = mp_montgomery_calc_normalization(&R, b)) != MP_OKAY) {
      printf("Error getting norm.  %s",
             mp_error_to_string(result));
      return EXIT_FAILURE;
   }

   /* get mp value */
   if ((result = mp_montgomery_setup(&c, &mp)) != MP_OKAY) {
      printf("Error setting up montgomery.  %s",
             mp_error_to_string(result));
      return EXIT_FAILURE;
   }

   /* normalize ‘a’ so now a is equal to aR */
   if ((result = mp_mulmod(&a, &R, &b, &a)) != MP_OKAY) {
      printf("Error computing aR.  %s",
             mp_error_to_string(result));
      return EXIT_FAILURE;
   }

   /* square a to get c = a^2R^2 */
   if ((result = mp_sqr(&a, &c)) != MP_OKAY) {
      printf("Error squaring.  %s",
             mp_error_to_string(result));
      return EXIT_FAILURE;
   }

   /* now reduce ‘c’ back down to c = a^2R^2 * R^-1 == a^2R */
   if ((result = mp_montgomery_reduce(&c, &b, mp)) != MP_OKAY) {
      printf("Error reducing.  %s",
             mp_error_to_string(result));
      return EXIT_FAILURE;
   }

   /* multiply a to get c = a^3R^2 */
```

```
   if ((result = mp_mul(&a, &c, &c)) != MP_OKAY) {
      printf("Error reducing.  %s",
             mp_error_to_string(result));
      return EXIT_FAILURE;
   }

   /* now reduce 'c' back down to c = a^3R^2 * R^-1 == a^3R */
   if ((result = mp_montgomery_reduce(&c, &b, mp)) != MP_OKAY) {
      printf("Error reducing.  %s",
             mp_error_to_string(result));
      return EXIT_FAILURE;
   }

   /* now reduce (again) 'c' back down to c = a^3R * R^-1 == a^3 */
   if ((result = mp_montgomery_reduce(&c, &b, mp)) != MP_OKAY) {
      printf("Error reducing.  %s",
             mp_error_to_string(result));
      return EXIT_FAILURE;
   }

   /* c now equals a^3 mod b */

   return EXIT_SUCCESS;
}
```

This particular example does not look too efficient but it demonstrates the point of the algorithm. By normalizing the inputs the reduced results are always of the form aR for some variable a. This allows a single final reduction to correct for the normalization and the fast reduction used within the algorithm.

For more details consider examining the file *bn_mp_exptmod_fast.c*.

5.4 Restricted Diminished Radix

"Diminished Radix" reduction refers to reduction with respect to moduli that are amenable to simple digit shifting and small multiplications. In this case the "restricted" variant refers to moduli of the form $\beta^k - p$ for some $k \geq 0$ and $0 < p < \beta$ where β is the radix (default to 2^{28}).

As in the case of Montgomery reduction there is a pre–computation phase required for a given modulus.

```
void mp_dr_setup(mp_int *a, mp_digit *d);
```

This computes the value required for the modulus a and stores it in d. This function cannot fail and does not return any error codes. After the pre–computation a reduction can be performed with the following.

```
int mp_dr_reduce(mp_int *a, mp_int *b, mp_digit mp);
```

This reduces a in place modulo b with the pre–computed value mp. b must be of a restricted diminished radix form and a must be in the range $0 \le a < b^2$. Diminished radix reductions are much faster than both Barrett and Montgomery reductions as they have a much lower asymptotic running time.

Since the moduli are restricted this algorithm is not particularly useful for something like Rabin, RSA or BBS cryptographic purposes. This reduction algorithm is useful for Diffie-Hellman and ECC where fixed primes are acceptable.

Note that unlike Montgomery reduction there is no normalization process. The result of this function is equal to the correct residue.

5.5 Unrestricted Diminished Radix

Unrestricted reductions work much like the restricted counterparts except in this case the moduli is of the form $2^k - p$ for $0 < p < \beta$. In this sense the unrestricted reductions are more flexible as they can be applied to a wider range of numbers.

```
int mp_reduce_2k_setup(mp_int *a, mp_digit *d);
```

This will compute the required d value for the given moduli a.

```
int mp_reduce_2k(mp_int *a, mp_int *n, mp_digit d);
```

This will reduce a in place modulo n with the pre–computed value d. From my experience this routine is slower than mp_dr_reduce but faster for most moduli sizes than the Montgomery reduction.

5.6 Combined Modular Reduction

Some of the combinations of an arithmetic operations followed by a modular reduction can be done in a faster way. The ones implemented are:

Addition $d = (a + b) \ mod \ c$

```
int mp_addmod(const mp_int *a, const mp_int *b, const mp_int *c, mp_int *d);
```

Subtraction $d = (a - b) \ mod \ c$

```
int mp_submod(const mp_int *a, const mp_int *b, const mp_int *c, mp_int *d);
```

Multiplication $d = (ab) \ mod \ c$

```
int mp_mulmod(const mp_int *a, const mp_int *b, const mp_int *c, mp_int *d);
```

Squaring $d = (a^2) \ mod \ c$

```
int mp_sqrmod(const mp_int *a, const mp_int *b, const mp_int *c, mp_int *d);
```

Chapter 6

Exponentiation

6.1 Single Digit Exponentiation

```
mp_err mp_expt_n(const mp_int *a, int b, int *c)
```

This function computes $c = a^b$.

6.2 Modular Exponentiation

```
int mp_exptmod (mp_int * G, mp_int * X, mp_int * P, mp_int * Y)
```

This computes $Y \equiv G^X \pmod{P}$ using a variable width sliding window algorithm. This function will automatically detect the fastest modular reduction technique to use during the operation. For negative values of X the operation is performed as $Y \equiv (G^{-1} \bmod P)^{|X|} \pmod{P}$ provided that $gcd(G, P) = 1$.

This function is actually a shell around the two internal exponentiation functions. This routine will automatically detect when Barrett, Montgomery, Restricted and Unrestricted Diminished Radix based exponentiation can be used. Generally moduli of the a "restricted diminished radix" form lead to the fastest modular exponentiations. Followed by Montgomery and the other two algorithms.

6.3 Modulus a Power of Two

```
int mp_mod_2d(const mp_int *a, int b, mp_int *c)
```

It calculates $c = a \ mod \ 2^b$.

6.4 Root Finding

```
mp_err mp_root_n(const mp_int *a, int b, mp_int *c)
```

This computes $c = a^{1/b}$ such that $c^b \leq a$ and $(c+1)^b > a$. Will return a positive root only for even roots and return a root with the sign of the input for odd roots. For example, performing $4^{1/2}$ will return 2 whereas $(-8)^{1/3}$ will return -2.

This algorithm uses the "Newton Approximation" method and will converge on the correct root fairly quickly.

The square root $c = a^{1/2}$ (with the same conditions $c^2 \leq a$ and $(c+1)^2 > a$) is implemented with a faster algorithm.

```
int mp_sqrt (mp_int * a, mp_digit b, mp_int * c)
```

Chapter 7

Logarithm

7.1 Integer Logarithm

A logarithm function for positive integer input `a, base` computing $\lfloor \log_b x \rfloor$ such that $(\log_b x)^b \leq x$.

```
mp_err mp_log_n(const mp_int *a, int base, int *c)
```

7.1.1 Example

```
#include <stdlib.h>
#include <stdio.h>
#include <errno.h>

#include <tommath.h>

int main(int argc, char **argv)

   mp_int x, output;
   int base;
   int e;

   if (argc != 3)
      fprintf(stderr,"Usage %s base x\n", argv[0]);
      exit(EXIT_FAILURE);

   if ((e = mp_init_multi(&x, &output, NULL)) != MP_OKAY)
      fprintf(stderr,"mp_init failed: \"%s\"\n",
                     mp_error_to_string(e));
              exit(EXIT_FAILURE);

   errno = 0;
```

```
base = (int)strtoul(argv[1], NULL, 10);

if (errno == ERANGE)
   fprintf(stderr,"strtoul(1) failed: input out of range\n");
   exit(EXIT_FAILURE);

if ((e = mp_read_radix(&x, argv[2], 10)) != MP_OKAY)
   fprintf(stderr,"mp_read_radix failed: \"%s\"\n",
                  mp_error_to_string(e));
   exit(EXIT_FAILURE);

if ((e = mp_log_n(&x, base, &output)) != MP_OKAY)
   fprintf(stderr,"mp_log_n failed: \"%s\"\n",
                  mp_error_to_string(e));
   exit(EXIT_FAILURE);


if ((e = mp_fwrite(&output, 10, stdout)) != MP_OKAY)
   fprintf(stderr,"mp_fwrite failed: \"%s\"\n",
                  mp_error_to_string(e));
   exit(EXIT_FAILURE);

putchar('\n');

mp_clear_multi(&x, &output, NULL);
exit(EXIT_SUCCESS);
```

Chapter 8

Prime Numbers

8.1 Trial Division

```
int mp_prime_is_divisible (mp_int * a, int *result)
```

This will attempt to evenly divide a by a list of primes[1] and store the outcome in "result". That is if $result = 0$ then a is not divisible by the primes, otherwise it is. Note that if the function does not return **MP_OKAY** the value in "result" should be considered undefined[2].

8.2 Fermat Test

```
int mp_prime_fermat (mp_int * a, mp_int * b, int *result)
```

Performs a Fermat primality test to the base b. That is it computes $b^a \bmod a$ and tests whether the value is equal to b or not. If the values are equal then a is probably prime and *result* is set to one. Otherwise *result* is set to zero.

8.3 Miller-Rabin Test

```
int mp_prime_miller_rabin (mp_int * a, mp_int * b, int *result)
```

Performs a Miller-Rabin test to the base b of a. This test is much stronger than the Fermat test and is very hard to fool (besides with Carmichael numbers). If a passes the test (therefore is probably prime) *result* is set to one. Otherwise *result* is set to zero.

Note that is suggested that you use the Miller-Rabin test instead of the Fermat test since all of the failures of Miller-Rabin are a subset of the failures of the Fermat test.

[1] Default is the first 256 primes.

[2] Currently the default is to set it to zero first.

8.3.1 Required Number of Tests

Generally to ensure a number is very likely to be prime you have to perform the Miller-Rabin with at least a half-dozen or so unique bases. However, it has been proven that the probability of failure goes down as the size of the input goes up. This is why a simple function has been provided to help out.

```
int mp_prime_rabin_miller_trials(int size)
```

This returns the number of trials required for a low probability of failure for a given "size" expressed in bits. This comes in handy specially since larger numbers are slower to test. For example, a 512-bit number would require 18 tests for a probability of 2^{-160} whereas a 1024-bit number would only require 12 tests for a probability of 2^{-192}. The exact values as implemented are listed in table 8.1.

bits	Rounds	Error
80	-1	Use deterministic algorithm for size ¡= 80 bits
81	37	2^{-96}
96	32	2^{-96}
128	40	2^{-112}
160	35	2^{-112}
256	27	2^{-128}
384	16	2^{-128}
512	18	2^{-160}
768	11	2^{-160}
896	10	2^{-160}
1024	12	2^{-192}
1536	8	2^{-192}
2048	6	2^{-192}
3072	4	2^{-192}
4096	5	2^{-256}
5120	4	2^{-256}
6144	4	2^{-256}
8192	3	2^{-256}
9216	3	2^{-256}
10240	2	2^{-256}

Table 8.1: Number of Miller-Rabin rounds as implemented

You should always still perform a trial division before a Miller-Rabin test though.

A small table, broke in two for typographical reasons, with the number of rounds of Miller-Rabin tests is shown below. The numbers have been compute with a PARI/GP script listed in appendix A. The first column is the number of bits b in the prime $p = 2^b$, the numbers in the first row represent the probability

that the number that all of the Miller-Rabin tests deemed a pseudoprime is actually a composite. There is a deterministic test for numbers smaller than 2^{80}.

bits	$\mathbf{2^{-80}}$	$\mathbf{2^{-96}}$	$\mathbf{2^{-112}}$	$\mathbf{2^{-128}}$	$\mathbf{2^{-160}}$	$\mathbf{2^{-192}}$
80	31	39	47	55	71	87
96	29	37	45	53	69	85
128	24	32	40	48	64	80
160	19	27	35	43	59	75
192	15	21	29	37	53	69
256	10	15	20	27	43	59
384	7	9	12	16	25	38
512	5	7	9	12	18	26
768	4	5	6	8	11	16
1024	3	4	5	6	9	12
1536	2	3	3	4	6	8
2048	2	2	3	3	4	6
3072	1	2	2	2	3	4
4096	1	1	2	2	2	3
6144	1	1	1	1	2	2
8192	1	1	1	1	2	2
12288	1	1	1	1	1	1
16384	1	1	1	1	1	1
24576	1	1	1	1	1	1
32768	1	1	1	1	1	1

Table 8.2: Number of Miller-Rabin rounds. Part I

bits	2^{-224}	2^{-256}	2^{-288}	2^{-320}	2^{-352}	2^{-384}	2^{-416}
80	103	119	135	151	167	183	199
96	101	117	133	149	165	181	197
128	96	112	128	144	160	176	192
160	91	107	123	139	155	171	187
192	85	101	117	133	149	165	181
256	75	91	107	123	139	155	171
384	54	70	86	102	118	134	150
512	36	49	65	81	97	113	129
768	22	29	37	47	58	70	86
1024	16	21	26	33	40	48	58
1536	10	13	17	21	25	30	35
2048	8	10	13	15	18	22	26
3072	5	7	8	10	12	14	17
4096	4	5	6	8	9	11	12
6144	3	4	4	5	6	7	8
8192	2	3	3	4	5	6	6
12288	2	2	2	3	3	4	4
16384	1	2	2	2	3	3	3
24576	1	1	2	2	2	2	2
32768	1	1	1	1	2	2	2

Table 8.3: Number of Miller-Rabin rounds. Part II

Determining the probability needed to pick the right column is a bit harder. Fips 186.4, for example has 2^{-80} for 512 bit large numbers, 2^{-112} for 1024 bits, and 2^{128} for 1536 bits. It can be seen in table 8.2 that those combinations follow the diagonal from $(512, 2^{-80})$ downwards and to the right to gain a lower probabilty of getting a composite declared a pseudoprime for the same amount of work or less.

If this version of the library has the strong Lucas-Selfridge and/or the Frobenius-Underwood test implemented only one or two rounds of the Miller-Rabin test with a random base is necesssary for numbers larger than or equal to 1024 bits.

This function is meant for RSA. The number of rounds for DSA is $\lceil -log_2(p)/2 \rceil$ with p the probability which is just the half of the absolute value of p if given as a power of two. E.g.: with $p = 2^{-128}$, $\lceil -log_2(p)/2 \rceil = 64$.

This function can be used to test a DSA prime directly if these rounds are followed by a Lucas test.

See also table C.1 in FIPS 186-4.

8.4 Strong Lucas-Selfridge Test

```
int mp_prime_strong_lucas_selfridge(const mp_int *a, int *result)
```

Performs a strong Lucas-Selfridge test. The strong Lucas-Selfridge test together with the Rabin-Miler test with bases 2 and 3 resemble the BPSW test. The single internal use is a compile-time option in `mp_prime_is_prime` and can be excluded from the Libtommath build if not needed.

8.5 Frobenius (Underwood) Test

```
int mp_prime_frobenius_underwood(const mp_int *N, int *result)
```

Performs the variant of the Frobenius test as described by Paul Underwood. The single internal use is in `mp_prime_is_prime` for `MP_8BIT` only but can be included at build-time for all other sizes if the preprocessor macro `LTM_USE_FROBENIUS_TEST` is defined.

It returns `MP_ITER` if the number of iterations is exhausted, assumes a composite as the input and sets `result` accordingly. This will reduce the set of available pseudoprimes by a very small amount: test with large datasets (more than 10^{10} numbers, both randomly chosen and sequences of odd numbers with a random start point) found only 31 (thirty-one) numbers with $a > 120$ and none at all with just an additional simple check for divisors $d < 2^8$.

8.6 Primality Testing

Testing if a number is a square can be done a bit faster than just by calculating the square root. It is used by the primality testing function described below.

```
int mp_is_square(const mp_int *arg, int *ret);
```

```
int mp_prime_is_prime (mp_int * a, int t, int *result)
```

This will perform a trial division followed by two rounds of Miller-Rabin with bases 2 and 3 and a Lucas-Selfridge test. The Lucas-Selfridge test is replaced with a Frobenius-Underwood for `MP_8BIT`. The Frobenius-Underwood test for all other sizes is available as a compile-time option with the preprocessor macro `LTM_USE_FROBENIUS_TEST`. See file `bn_mp_prime_is_prime.c` for the necessary details. It shall be noted that both functions are much slower than the Miller-Rabin test and if speed is an essential issue, the macro `LTM_USE_ONLY_MR` switches both functions, the Frobenius-Underwood test and the Lucas-Selfridge test off and their code will not even be compiled into the library.

If t is set to a positive value t additional rounds of the Miller-Rabin test with random bases will be performed to allow for Fips 186.4 (vid. p. 126ff) compliance. The function `mp_prime_rabin_miller_trials` can be used to determine the number of rounds. It is vital that the function `mp_rand()` has a cryptographically strong random number generator available.

One Miller-Rabin tests with a random base will be run automatically, so by setting t to a positive value this function will run $t + 1$ Miller-Rabin tests with random bases.

If t is set to a negative value the test will run the deterministic Miller-Rabin test for the primes up to 3317044064679887385961981. That limit has to be checked by the caller.

If a passes all of the tests *result* is set to one, otherwise it is set to zero.

8.7 Next Prime

```
int mp_prime_next_prime(mp_int *a, int t, int bbs_style)
```

This finds the next prime after a that passes mp_prime_is_prime() with t tests but see the documentation for mp_prime_is_prime for details regarding the use of the argument t. Set *bbs_style* to one if you want only the next prime congruent to 3 mod 4, otherwise set it to zero to find any next prime.

8.8 Random Primes

```
int mp_prime_rand(mp_int *a,    int t,
                  int     size, int flags);
```

This will generate a prime in a using t tests of the primality testing algorithms. See the documentation for mp_prime_is_prime for details regarding the use of the argument t. The variable *size* specifies the bit length of the prime desired. The variable $flags$ specifies one of several options available (see fig. 8.1) which can be OR'ed together.

The function mp_prime_rand() is suitable for generating primes which must be secret (as in the case of RSA) since there is no skew on the least significant bits.

Note: This function replaces the deprecated mp_prime_random and mp_prime_random_ex functions.

Flag	Meaning
LTM_PRIME_BBS	Make the prime congruent to 3 modulo 4
LTM_PRIME_SAFE	Make a prime p such that $(p-1)/2$ is also prime. This option implies LTM_PRIME_BBS as well.
LTM_PRIME_2MSB_OFF	Makes sure that the bit adjacent to the most significant bit Is forced to zero.
LTM_PRIME_2MSB_ON	Makes sure that the bit adjacent to the most significant bit Is forced to one.

Figure 8.1: Primality Generation Options

Chapter 9

Random Number Generation

9.1 PRNG

`int mp_rand_digit(mp_digit *r)`

This function generates a random number in `r` of the size given in `r` (that is, the variable is used for in- and output) but not more than `MP_MASK` bits.

`int mp_rand(mp_int *a, int digits)`

This function generates a random number of `digits` bits.

The random number generated with these two functions is cryptographically secure if the source of random numbers the operating systems offers is cryptographically secure. It will use `arc4random()` if the OS is a BSD flavor, Wincrypt on Windows, or `/dev/urandom` on all operating systems that have it.

Chapter 10

Input and Output

10.1 ASCII Conversions

10.1.1 To ASCII

```
int mp_to_radix (mp_int *a, char *str, size_t maxlen, size_t *written, int radix);
```

This stores a in `str` of maximum length `maxlen` as a base-`radix` string of ASCII chars and appends a `NUL` character to terminate the string.

Valid values of `radix` line in the range $[2, 64]$.

The exact number of characters in `str` plus the `NUL` will be put in `written` if that variable is not set to `NULL`.

If `str` is not big enough to hold a, `str` will be filled with the least-significant digits of length `maxlen-1`, then `str` will be `NUL` terminated and the error `MP_VAL` is returned.

Please be aware that this function cannot evaluate the actual size of the buffer, it relies on the correctness of `maxlen`!

```
int mp_radix_size (mp_int * a, int radix, int *size)
```

This stores in "size" the number of characters (including space for the NUL terminator) required. Upon error this function returns an error code and "size" will be zero.

If `LTM_NO_FILE` is not defined a function to write to a file is also available.

```
int mp_fwrite(const mp_int *a, int radix, FILE *stream);
```

10.1.2 From ASCII

```
int mp_read_radix (mp_int * a, char *str, int radix);
```

This will read the base-"radix" NUL terminated string from "str" into a. It will stop reading when it reads a character it does not recognize (which happens to

include th NUL char... imagine that...). A single leading − sign can be used to denote a negative number.

If LTM_NO_FILE is not defined a function to read from a file is also available.

```
int mp_fread(mp_int *a, int radix, FILE *stream);
```

10.2 Binary Conversions

Converting an mp_int to and from binary is another keen idea.

```
size_t mp_ubin_size(mp_int *a);
```

This will return the number of bytes (octets) required to store the unsigned copy of the integer a.

```
int mp_to_unsigned_bin(mp_int *a, unsigned char *b, size_t maxlen, size_t *len);
```

This will store a into the buffer b of size `maxlen` in big–endian format storing the number of bytes written in `len`. Fortunately this is exactly what DER (or is it ASN?) requires. It does not store the sign of the integer.

```
int mp_from_ubin(mp_int *a, unsigned char *b, size_t size);
```

This will read in an unsigned big–endian array of bytes (octets) from b of length `size` into a. The resulting big-integer a will always be positive.

For those who acknowledge the existence of negative numbers (heretic!) there are "signed" versions of the previous functions.

```
int mp_sbin_size(mp_int *a);
int mp_from_sbin(mp_int *a, unsigned char *b, size_t size);
int mp_to_sbin(mp_int *a, unsigned char *b, size_t maxsize, size_t *len);
```

They operate essentially the same as the unsigned copies except they prefix the data with zero or non–zero byte depending on the sign. If the sign is zpos (e.g. not negative) the prefix is zero, otherwise the prefix is non–zero.

The two functions `mp_unpack` (get your gifts out of the box, import binary data) and `mp_pack` (put your gifts into the box, export binary data) implement the similarly working GMP functions as described at `http://gmplib.org/manual/Integer-Import-and-Export.html` with the exception that `mp_pack` will not allocate memory if `rop` is `NULL`.

```
int mp_unpack(mp_int *rop, size_t count, mp_order order, size_t size,
              mp_endian endian, size_t nails, const void *op, size_t maxsize);
int mp_pack(void *rop, size_t *countp, mp_order order, size_t size,
              mp_endian endian, size_t nails, const mp_int *op);
```

The function `mp_pack` has the additional variable `maxsize` which must hold the size of the buffer `rop` in bytes. Use

```
/* Parameters "nails" and "size" are the same as in mp_pack */
size_t mp_pack_size(mp_int *a, size_t nails, size_t size);
```

To get the size in bytes necessary to be put in `maxsize`).

To enhance the readability of your code, the following enums have been wrought for your convenience.

```
typedef enum
   MP_LSB_FIRST = -1,
   MP_MSB_FIRST =  1
 mp_order;
typedef enum
   MP_LITTLE_ENDIAN  = -1,
   MP_NATIVE_ENDIAN  =  0,
   MP_BIG_ENDIAN     =  1
 mp_endian;
```

Chapter 11

Algebraic Functions

11.1 Extended Euclidean Algorithm

```
int mp_exteuclid(mp_int *a, mp_int *b,
                 mp_int *U1, mp_int *U2, mp_int *U3);
```

This finds the triple U1/U2/U3 using the Extended Euclidean algorithm such that the following equation holds.

$$a \cdot U1 + b \cdot U2 = U3 \tag{11.1}$$

Any of the U1/U2/U3 parameters can be set to **NULL** if they are not desired.

11.2 Greatest Common Divisor

```
int mp_gcd (mp_int * a, mp_int * b, mp_int * c)
```

This will compute the greatest common divisor of a and b and store it in c.

11.3 Least Common Multiple

```
int mp_lcm (mp_int * a, mp_int * b, mp_int * c)
```

This will compute the least common multiple of a and b and store it in c.

11.4 Jacobi Symbol

```
int mp_jacobi (mp_int * a, mp_int * p, int *c)
```

This will compute the Jacobi symbol for a with respect to p. If p is prime this essentially computes the Legendre symbol. The result is stored in c and can take on one of three values $\{-1, 0, 1\}$. If p is prime then the result will be -1 when a is not a quadratic residue modulo p. The result will be 0 if a divides p and the result will be 1 if a is a quadratic residue modulo p.

11.5 Kronecker Symbol

```
int mp_kronecker (mp_int * a, mp_int * p, int *c)
```

Extension of the Jacoby symbol to all $\{a, p\} \in \mathbb{Z}$.

11.6 Modular square root

```
int mp_sqrtmod_prime(mp_int *n, mp_int *p, mp_int *r)
```

This will solve the modular equatioon $r^2 = n \ mod \ p$ where p is a prime number greater than 2 (odd prime). The result is returned in the third argument r, the function returns **MP_OKAY** on success, other return values indicate failure.

The implementation is split for two different cases:

1. if $p \ mod \ 4 == 3$ we apply Handbook of Applied Cryptography algorithm 3.36 and compute r directly as $r = n^{(p+1)/4} \ mod \ p$
2. otherwise we use Tonelli-Shanks algorithm

The function does not check the primality of parameter p thus it is up to the caller to assure that this parameter is a prime number. When p is a composite the function behaviour is undefined, it may even return a false-positive **MP_OKAY**.

11.7 Modular Inverse

```
int mp_invmod (mp_int * a, mp_int * b, mp_int * c)
```

Computes the multiplicative inverse of a modulo b and stores the result in c such that $ac \equiv 1 \pmod{b}$.

11.8 Single Digit Functions

For those using small numbers (*snicker snicker*) there are several "helper" functions

```
int mp_add_d(mp_int *a, mp_digit b, mp_int *c);
int mp_sub_d(mp_int *a, mp_digit b, mp_int *c);
int mp_mul_d(mp_int *a, mp_digit b, mp_int *c);
```

```
int mp_div_d(mp_int *a, mp_digit b, mp_int *c, mp_digit *d);
int mp_mod_d(mp_int *a, mp_digit b, mp_digit *c);
```

These work like the full mp_int capable variants except the second parameter b is a mp_digit. These functions fairly handy if you have to work with relatively small numbers since you will not have to allocate an entire mp_int to store a number like 1 or 2.

The functions `mp_incr` and `mp_decr` mimic the postfix operators `++` and `--` respectively, to increment the input by one. They call the full single-digit functions if the addition would carry. Both functions need to be included in a minimized library because they call each other in case of a negative input, These functions change the inputs!

```
int mp_incr(mp_int *a);
int mp_decr(mp_int *a);
```

The division by three can be made faster by replacing the division with a multiplication by the multiplicative inverse of three.

```
int mp_div_3(const mp_int *a, mp_int *c, mp_digit *d);
```

Chapter 12

Little Helpers

It is never wrong to have some useful little shortcuts at hand.

12.1 Function Macros

To make this overview simpler the macros are given as function prototypes. The return of logic macros is `MP_NO` or `MP_YES` respectively.

`int mp_iseven(mp_int *a)`

Checks if $a = 0 mod 2$

`int mp_isodd(mp_int *a)`

Checks if $a = 1 mod 2$

`int mp_isneg(mp_int *a)`

Checks if $a < 0$

`int mp_iszero(mp_int *a)`

Checks if $a = 0$. It does not check if the amount of memory allocated for a is also minimal.

Other macros which are either shortcuts to normal functions or just other names for them do have their place in a programmer's life, too!

12.1.1 Renamings

```
#define mp_mag_size(mp) mp_unsigned_bin_size(mp)


#define mp_raw_size(mp) mp_signed_bin_size(mp)
```

```
#define mp_read_mag(mp, str, len) mp_read_unsigned_bin((mp), (str), (len))

 #define mp_read_raw(mp, str, len) mp_read_signed_bin((mp), (str), (len))

#define mp_tomag(mp, str) mp_to_unsigned_bin((mp), (str))

#define mp_toraw(mp, str)         mp_to_signed_bin((mp), (str))
```

12.1.2 Shortcuts

```
#define mp_to_binary(M, S, N)  mp_to_radix((M), (S), (N), 2)

#define mp_to_octal(M, S, N)   mp_to_radix((M), (S), (N), 8)

#define mp_to_decimal(M, S, N) mp_to_radix((M), (S), (N), 10)

#define mp_to_hex(M, S, N)     mp_to_radix((M), (S), (N), 16)
```

Appendices

Appendix A

Computing Number of Miller-Rabin Trials

The number of Miller-Rabin rounds in the tables **??**, **??**, and **??** have been calculated with the formula in FIPS 186-4 appendix F.1 (page 117) implemented as a PARI/GP script.

```
log2(x) = log(x)/log(2)

fips_f1_sums(k, M, t) =
   local(s = 0);
   s = sum(m=3,M,
          2^(m-t*(m-1)) *
          sum(j=2,m,
             1/ ( 2^( j + (k-1)/j ) )
          )
        );
   return(s);


fips_f1_2(k, t, M) =
   local(common_factor, t1, t2, f1, f2, ds, res);

   common_factor = 2.00743 * log(2) * k * 2^(-k);
   t1 = 2^(k - 2 - M*t);
   f1 = (8 * ((Pi^2) - 6))/3;
   f2 = 2^(k - 2);
   ds = t1 + f1 * f2 * fips_f1_sums(k, M, t);
   res = common_factor * ds;
   return(res);
```

```
fips_f1_1(prime_length, ptarget)=
   local(t, t_end, M, M_end, pkt);

   t_end = ceil(-log2(ptarget)/2);
   M_end = floor(2 * sqrt(prime_length-1) - 1);

   for(t = 1, t_end,
      for(M = 3, M_end,
         pkt = fips_f1_2(prime_length, t, M);
         if(pkt <= ptarget,
            return(t);
         );
      );
   );
```

To get the number of rounds for a 1024 bit large prime with a probability of 2^{-160}:

```
? fips_f1_1(1024,2^(-160))
%1 = 9
```

Index

mp_2expt, 26
mp_abs, 28
mp_add, 27
mp_add_d, 56
mp_addmod, 38
mp_and, 27
mp_clamp, 14
mp_clear, 11
mp_clear_multi, 12
mp_cmp, 22
mp_cmp_d, 23
mp_cmp_mag, 21
mp_cnt_lsb, 17
mp_complement, 27
mp_copy, 17
mp_count_bits, 17
mp_div, 28
mp_div_2, 25
mp_div_2d, 26
mp_div_3, 57
mp_div_d, 56
mp_dr_reduce, 37
mp_dr_setup, 37
MP_EQ, 21
mp_error_to_string, 9
mp_exch, 17
mp_expt_n, 39
mp_exptmod, 39
mp_exteuclid, 55
mp_fread, 52
mp_from_ubin, 52
mp_fwrite, 51
mp_gcd, 55
mp_get_bit, 27
mp_get_i32, 18
mp_get_i64, 18
mp_get_l, 19
mp_get_ll, 20
mp_get_mag_u32, 18
mp_get_mag_u64, 18
mp_get_mag_ul, 19
mp_get_mag_ull, 20
mp_get_u32, 18
mp_get_u64, 18
mp_get_ul, 19
mp_get_ull, 20
mp_grow, 15
MP_GT, 21
mp_init, 10
mp_init_copy, 12
mp_init_multi, 12
mp_init_set, 20
mp_init_set_int, 20
mp_init_size, 13
mp_int, 10
mp_invmod, 56
mp_is_square, 47
mp_iseven, 59
mp_isneg, 59
mp_isodd, 59
mp_iszero, 59
mp_jacobi, 55
mp_kronecker, 56
mp_lcm, 55
mp_log_n, 41
mp_lshd, 26
MP_LT, 21
mp_mag_size, 59
MP_MEM, 9
mp_mod, 33
mp_mod_2d, 39
mp_mod_d, 56
mp_montgomery_calc_normalization, 35
mp_montgomery_reduce, 35

mp_montgomery_setup, 35
mp_mul, 29
mp_mul_2, 25
mp_mul_2d, 26
mp_mul_d, 56
mp_neg, 27
MP_NO, 9
MP_OKAY, 9
mp_or, 27
mp_pack, 52
mp_prime_fermat, 43
mp_prime_frobenius_underwood, 47
mp_prime_is_divisible, 43
mp_prime_is_prime, 47
mp_prime_miller_rabin, 43
mp_prime_next_prime, 48
mp_prime_rabin_miller_trials, 44
mp_prime_rand, 48
mp_prime_strong_lucas_selfridge, 46
mp_radix_size, 51
mp_rand, 49
mp_rand_digit, 49
mp_raw_size, 59
mp_read_mag, 59
mp_read_radix, 51
mp_read_raw, 60
mp_read_signed_bin, 52
mp_reduce, 34
mp_reduce_2k, 38
mp_reduce_2k_setup, 38
mp_reduce_setup, 33
mp_root_n, 39
mp_rshd, 26
mp_set, 18
mp_set_i32, 18
mp_set_i64, 18
mp_set_l, 19
mp_set_ll, 20
mp_set_u32, 18
mp_set_u64, 18
mp_set_ul, 19
mp_set_ull, 20
mp_shrink, 14
mp_signed_bin_size, 52
mp_sqr, 30
mp_sqrt, 40
mp_sqrtmod_prime, 56
mp_sub, 27
mp_sub_d, 56
mp_to_binary, 60
mp_to_decimal, 60
mp_to_hex, 60
mp_to_octal, 60
mp_to_radix, 51
mp_to_signed_bin, 52
mp_to_ubin, 52
mp_tomag, 60
mp_toraw, 60
mp_ubin_size, 52
mp_unpack, 52
MP_VAL, 9
mp_xor, 27
MP_YES, 9
mp_zero, 14