附　录

在这部分给出，具体给出用 MIRACL 实现椭圆曲线上双线性 Tate 的说明。

大整数 MIRACL 在 Visual Studio 2005 上的设置安装

在 Visual C++ 8.0 的 IDE 下，由 MIRACL 提供的库文件 ms32.lib（该 .lib 文件位于，解压 MIRACL 的路径\include 中）不能够很好的运行。因此，要从新 build 一个新的 ms32.lib 文件。

首先，启动，Visual Studio 2005，然后选择新建一个工程，再选择 Win32 控制台引用程序。

将此工程命名为：miracl。解决方案名称与工程名同名。工程的存储位置，可以任意选择。然后，点击确定。

点击应用设置。

点击静态库。

使预编译头无效。

点击完成。

右键点击左边工具栏中的头文件。

点击工程，选择添加现有项。

添加 miracl.h 和 mirdef.h。

注，这两个文件可以从你所下载解压的 MIRACL 库的文件路径中查找。

右键点击左边工具栏中的源文件。

点击工程，选着添加现有项。

添加如下文件到所创建的工程 miracl 中。

mraes.c，mralloc.c，mrarth0.c，mrarth1.c，mrarth2.c，mrarth3.c，mrbits.c mrbrick.c，mrbuild.c，mrcore.c，mrcrt.c，mrcurve.c，mrdouble.c，mrebrick.c，mrec2m.c，mrgf2m.c，mrfast.c，mrflash.c，mrflsh1.c，mrflsh2.c，mrflsh3.c mrflsh4.c，mrfrnd.c，mrgcd.c，mrio1.c，mrio2.c，mrjack.c，mrlucas.c，mrmonty.c mrmuldv.c，mrpi.c，mrpower.c，mrprime.c，mrrand.c，mrround.c，mrscrt.c mrshs.c，mrshs256.c，mrshs512.c，mrsmall.c，mrsroot.c，mrstrong.c，mrxgcd.c mrzzn2.c，mrzzn2b.c，mrzzn3.c，mrecn2.c。

然后，点击 build miracl。miracl 这个库将在你之前创建工程 miracl 的文件目录中。

同样，如果愿意，可以创建一个 release 版本的 ms32.lib。

关掉这个工程。

再一次，选择一个新的工程，选着 win32 控制台应用程序。

将该新建的工程命名为 brent。

工程的存储位置，例如：d:\myprojects。

解决方案名为 brent。

点击确定。

点击应用设置，保持控制台应用，再一次禁用预编译头。

点击完成。

点击左侧工具栏中的头文件。

点击工程，选择添加现有项。

添加 miracl.h 和 mirdef.h 到工程中。

同时，添加 zzn.h 和 big.h 到该工程中。

点击左侧工具栏中的源文件。

点击工程，选择添加现有项。

添加源文件 zzn.cpp，big.h，brent.cpp 到该工程中。

点击左侧工具栏中的现有资源文件。

点击工程，选择添加现有项。

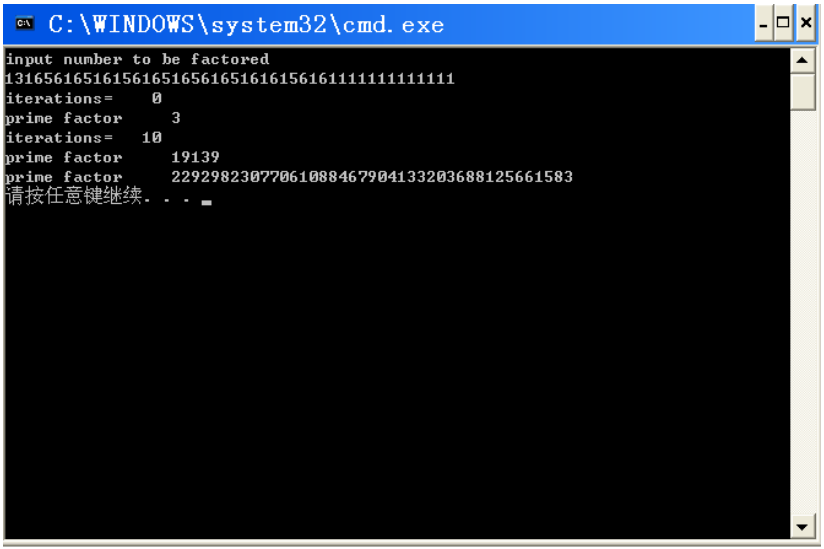
添加 miracl.lib 到工程中。

点击 build brent，调试不执行。

则文件开始运行。该程序执行大整数分解的 Brent-Pollard 算法。

注：当输入的数字为偶数时，该程序将报错。(因为，源代码中实现了这一对输入检查的功能。)

程序的执行结果见下图。



MIRACL 的架构分析

首先，允许我给出底层的架构。

miracl.h 文件给出了整个 MIRACL 所用到的宏定义，可更改的缺省定义，外部定义的函数接口结构体定义。具体可参见 MIRACL 的参考手册。

mirdef.h 文件给出了根据不同硬件环境和编译器环境给出的定义。

big.h 文件给出了大整数的定义，包含大整数初始化，以及大整数的加，减，乘，除运算，以及常用的模指数运算。

big.cpp，具体实现了 Big.h 中定义的各种运算。

注，在上文提到过的 build miracl.lib 动态链接库所用到的文件。例如：

mraes.c，mralloc.c，mrarth0.c，mrarth1.c，mrarth2.c，mrarth3.c，mrbits.c mrbrick.c，mrbuild.c，mrcore.c，mrcrt.c，mrcurve.c，mrdouble.c，mrebrick.c，mrec2m.c，mrgf2m.c，mrfast.c，mrflash.c，mrflsh1.c，mrflsh2.c，mrflsh3.c mrflsh4.c，mrfrnd.c，mrgcd.c，mrio1.c，mrio2.c，mrjack.c，mrlucas.c，mrmonty.c mrmuldv.c，mrpi.c，mrpower.c，mrprime.c，mrrand.c，mrround.c，mrscrt.c

mrshs.c，mrshs256.c，mrshs512.c，mrsmall.c，mrsroot.c，mrstrong.c，mrxgcd.c mrzzn2.c，mrzzn2b.c，mrzzn3.c，mrecn2.c。

构成了整个 MIRACL 的用于实现大数操作的核心代码。

big.h 中定义的运算，在实现上都要依靠上述底层文件的执行。但上述文件所实现的基本功能模块，在 miracl.h 中多数被定义为外部函数。具体详细说明，请单独参阅上述每一.c 文件的具体实现功能说明，在每一文件的初始部分。

zzn.h 文件定义了乘法群上的基本运算。这些基本运算包括加，减，乘，求逆运算，模指数运算。当 n 在初始化时，若被赋与一素数 p 时，则这些运算将转化为有限域 F_p 上的基本运算。

zzn.cpp 具体实现了上述在 zzn.h 中定义的函数模块。

flash.h 定义了一类特殊大数(flash number)的运算，可以看做是大数 big 的大浮点数扩充。包括浮点数的的加，减，乘，除运算，以及这类大数同大数 big 的运算。

flash.cpp 具体实现类大数的底层运算。

gf2m.h 文件定义了有限域 GF(2^m)上的代数运算。同样包括加，减，乘，求逆运算，模指数运算。该文件提供了对具体 m 值赋值运算，换句话说，该文件提供了可供用户来选定的扩域的大小。

对应的，gf2m.cpp 具体实现了 gf2m.h 定义的各种运算。

ecn.h 文件定义了椭圆曲线上的模 n 算术运算。包括椭圆曲线上的点加，点

减，标量乘运算，以及其他基本算术运算。

相应的 ecn.cpp 文件实现了相应的 ecn.h 文件定义的椭圆曲线上的模 n 算术运算。

ec2.h 文件定义了有限域 F_2^m 上的椭圆曲线上的算术运算。类似包括椭圆曲线上的点加，点减，标量乘运算，以及其他基本算术运算。

相应的 ec2.cpp 文件实现了相应的 ec2.h 文件定义的椭圆曲线上的模 n 算术运算。

crt.h 文件定义了著名的“中国剩余定理”的函数接口。

crt.cpp 文件包含了该定理实现的具体细节。

brick.h 文件定义了包含预运算的 Brick-Comb method 用来实现快速的模指数运算。

ebrick.h 文件定义了在有限域 P 上的椭圆曲线上的包含预运算的 Brickell-Etal's method 来实现模指数运算。

关于 MIRACL 其他函数功能和具体使用方法，可以参看缘代码的说明部分。由于篇幅的限制，本小节只是给出了很多人提出了 MIRACL 不能够编译运行的问题的初步回答。由于，免费版本的 MIRACL 在源代码级缺乏足够的注释信息，研究经费允许的情况下，可以购买商业版本的 MIRACL。