# GMP大数库VC使用入门教程

Winxos 2009-9-29

**GMP是GUN的一套大数库，提供了数百个基础函数，执行效率比较高，但是网上相对来说详细的教程比较少，本教程为大家介绍如何在windows ，vc6.0开发环境下，配置和使用GMP库。**

1. **编译GMP库**

直接从GMP主页上下载到的GMP源代码，在windows环境下编译起来相对比较麻烦，所以我还是推荐大家直接使用我已经编译好的库，附件中已经包含。

***（使用我编译好的库与你们自己编译的库就是一些参数不同，可能效率有点不一样，但是我们不用管这些细微的差异，主要是看看如何使用GMP库吧）***

1. **配置库**

编译好的库文件包含**gmp.h, gmp.lib**两个文件，为了以后编程的方便，建议将这两个文件放到VC系统库目录，这样以后编程的时候就可以具体调用了。

具体的做法：

将gmp.h文件放置到VC头文件目录中，在我电脑中对应的目录为

E:\Program Files\Microsoft Visual Studio\VC98\Include

将gmp.lib文件放置到VC库文件目录中，在我电脑中对应的目录为

E:\Program Files\Microsoft Visual Studio\VC98\Lib

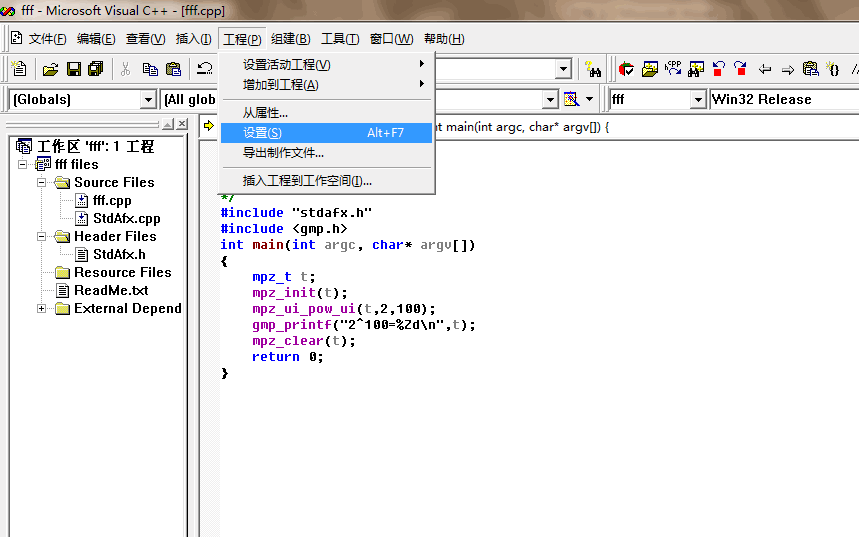
**注：如果你的VC装在不同的目录，找到对应的地方就可以了**

好了，万事具备了，可以开始编写程序了

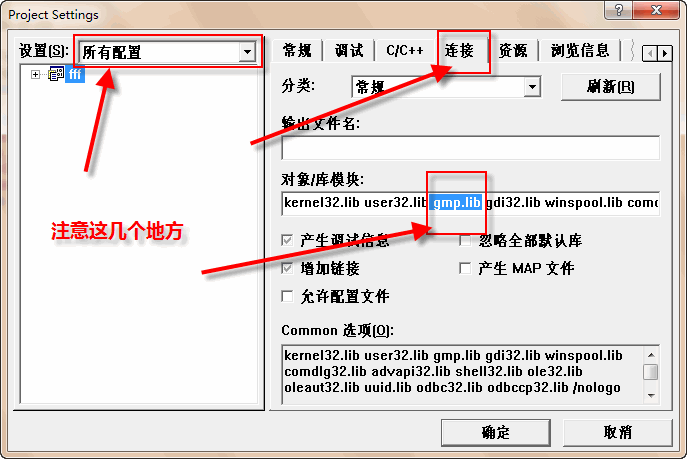
1. **编写程序**

打开VC6.0，新建一个WIN32 CONSOLE工程(默认的HELLO WORLD 就可以)，对工程进行如下设置：

**选择 工程 -> 设置** ,如下图



**弹出的对话框进行如下图设置，目的是为了添加gmp.lib库文件到工程。**



好了，确定完后就可以代码编写了。

在主程序文件输入以下代码：

/\*

GMP简单教程

winxos 2009-9-29

\*/

#include "stdafx.h" //hello world 工程默认的，如果你建立的是空工程就不需要这句

#include <gmp.h> //记得引入GMP.H的头文件

int main(int argc, char\* argv[])

{

mpz\_t t; //mpz\_t 为GMP内置大数类型

mpz\_init(t); //大数t使用前要进行初始化，以便动态分配空间

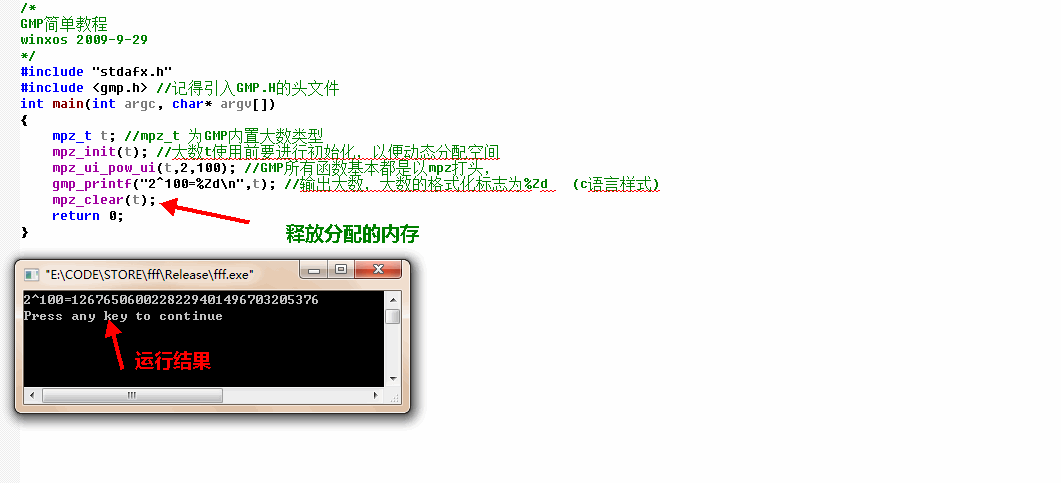
mpz\_ui\_pow\_ui(t,2,100); //GMP所有函数基本都是以mpz打头

gmp\_printf("2^100=%Zd\n",t); //输出大数，大数的格式化标志为%Zd

mpz\_clear(t);

return 0;

}

编译，运行结果如下：

是不是比较简单呢？相信您一定跃跃欲试了吧^\_^

1. **高级教程**

对于刚开始使用GMP库来说，就是不知道有哪些函数，容易被它繁多的函数吓到，到官方主页上去，就可以找到最新的帮助文档，英文的。

**实际上可以发现它的众多函数命名是比较有规律的，而且对于大数运算来说常用的函数并不多。附件中包含了常用整数函数手册。**

GMP的函数命名通常为

mpz\_funxx\_dataxx

**其中funxx表示函数功能，dataxx表示数据类型，dataxx省略通常表示数据都是大数**

举例如下：

mpz\_t t;//这是类型声明，都需要的东西

mpz\_init(t);//普通初始化，还有别的初始化方式，比如赋值初始化

mpz\_set\_ui(t,2);//赋值操作，ui表示无符号32位整数

//上面两句等同于mpz\_init\_set\_ui(t,2);

mpz\_set\_str(t, ”1234”);//从字符串赋值，跟上面是不用的赋值类型，str表示字符串

mpz\_add(t,a,b);//将大数a+b的结果赋值给t，就是t=a+b

mpz\_add\_ui(t,a,uib);//将小数uib与大数a求和结果赋值给t，就是t=a+uib

mpz\_add\_ui(t,t,1);//就是t=t+1

mpz\_sub(t,a,b);//减法

mpz\_mul(t,a,b);//乘法

gmp\_printf(“%Zd”, t);//输出t

其他的类似，请参考手册。

注：如果要熟练还是要多多的练习，应该涉及大数的问题应该不是什么问题了，不过好的算法才是王道。本篇文章意在给那些想处理大数却不知如何使用GMP库的人，winxos自己也是初学者，如果有什么错误恳请指出，一起学习。

再附上一些完整的使用GMP的C++代码。

程序一、

//梅森素数的鲁卡斯测试以及概率测试

#include <iostream>

#include <gmp>

#include <PRIMES.h> //包含了我自己定义的素数相关类，本程序调用了其产生小素数

#include <ctime>

using namespace std;

#pragma comment(lib,"gmp.lib"); //另外一种引用库的方法

int IsMersenne(int ExpP)

{

if (ExpP == 2) return 1;

mpz\_t c, b;

mpz\_init(c);

mpz\_init(b);

mpz\_ui\_pow\_ui(c, 2, ExpP);

mpz\_sub\_ui(c, c, 1); //M(p) = 2^p-1

mpz\_set\_ui(b, 4);

for (int j = 0;j < ExpP-2;j++)

{

mpz\_mul(b, b, b);

mpz\_sub\_ui(b, b, 2);

mpz\_mod(b, b, c);

}

mpz\_clear(c);

if (mpz\_cmp\_ui(b, 0) == 0)

{

mpz\_clear(b);

return 1;

}

mpz\_clear(b);

return 0;

}

int IsMersenne2(int ExpP)

{

if (ExpP == 2) return 1;

mpz\_t c;

mpz\_init(c);

mpz\_ui\_pow\_ui(c, 2, ExpP);

mpz\_sub\_ui(c, c, 1);

if (mpz\_probab\_prime\_p(c, 5))

{

return 1;

}

return 0;

}

int main()

{

time\_t a,b;

PRIMES P;

int i, ct = 0;

a=time(0);

for (i = 900;i < 1100;i++)

{

int ExpP = P.PrimeAt(i);

SetTitle(ExpP);

if (IsMersenne2(ExpP))

{

cout<<++ct<<"\t"<<ExpP<<endl;

}

}

b=time(0);

cout<<difftime(b,a)<<"秒"<<endl;

return 0;

}

程序二、

//Euler project 第二十题

int e20()

{

mpz\_t n;

int i,sum=0;

mpz\_init\_set\_ui(n,1);

for (i=2;i<=100;i++)

{

mpz\_mul\_ui(n,n,i);

}

gmp\_printf("%Zd\n",n);

while (mpz\_cmp\_ui(n,0)>0)

{

sum+=mpz\_fdiv\_ui(n,10);

mpz\_div\_ui(n,n,10);

}

printf("%d\n",sum);

mpz\_clear(n);

return 0;

}