

gqqnb的专栏

爱让一切都对了

目录视图

摘要视图

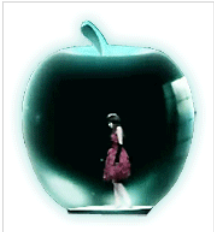
RSS 订阅

版权声明

本博客所有文章，尤其禁止将其部分或全部，以任何形式，如纯文本、图片、PDF等，张贴至百度旗下网站，包括但不限于百度百科、百度文库。

本博客所有文章，如有版权声明，则往往是知识共享-署名-相同方式共享3.0协议；若无，则认为是保留所有版权。以上两种版权，与目前的百度百科、百度文库等版权协议不符，故此禁止张贴。作者享有一切权利追究侵权事宜。

个人资料



gqqnb

访问：493154次

积分：4875

等级：BLOG > 5

排名：第4348名

原创：95篇 转载：2篇

译文：2篇 评论：101条

文章搜索

文章分类

- 版权宽松（知识共享-署名-相同方式共享） (27)
- 软件发布 (12)
- 解决方案 (26)
- C# (34)

扩展欧几里得算法是干什么用的？

2012-11-25 23:15

4525人阅读

评论(2)

收藏

举报

分类：其他 (10) 版权宽松（知识共享-署名-相同方式共享） (26)

版权声明：本文为博主原创文章，未经博主允许不得转载。

目录(?)

[+]

扩展欧几里得得**算法**（又称扩充欧几里得算法）是用来解某一类特定的不定方程的。讲解清楚需要好些预备知识，各位读者不能着急。我是花了半天时间来理解它。

不定方程

不定方程是以 x,y 为变量，形如 $ax+by=c$ ，且 a,b,x,y,c 都为整数的一类方程。例如 $4x+5y=13$ ，以不定方程来解，得 $x=-13, y=13$ 。不定方程这个名词多见于小学中学，它还有个名词叫丢番图方程，这个名称似乎在学术界更为多见。

因子

$a|b$ 表示 a 是 b 的因子， b 是 a 的倍数。

不定方程有整数解

$ax+by=c$ 有整数解，当且仅当 $\gcd(a,b)|c$ 。详情见维基百科的贝祖定理条目。

例如， $5x+14y=35$ 有没有整数解呢？

贝祖定理告诉我们有！因为 $\gcd(5,14)=1|35$ 。

Mathematica告诉我们 $x=7, y=0$ 。（你也可以手算。）

```
In[2]:= FindInstance[5 x + 14 y == 35, {x, y}, Integers]
Out[2]= {{x -> 7, y -> 0}}
```

两个不定方程（扩展欧几里得算法作用之处）

定理：若 $ax+by=g$ ，（ $g=\gcd(a,b)$ ，即 g 是 a,b 的最大公约数）有整数解 (x_1, y_1) ；则 $ax+by=c$ （ c 是 g 的倍数）有整数解 $(\frac{cx_1}{g}, \frac{cy_1}{g})$ 。读者可以测试、证明一下。

设ExtendedGCD为扩展欧几里得算法，它接受两个整数 a,b ，返回两个整数 x,y 。

若有 $ax+by=\gcd(a,b)$ ，则ExtendedGCD(a,b)可求 x,y 。

练习1

现在练习一下，使用ExtendedGCD，求 $6x+10y=2$ 的整数解。

发现 $\gcd(6,10)=2$ ，2是6和10的最大公约数，于是求 $6x+10y=2$ 的整数解可以用扩展欧几里得算法求。

以Mathematica代码为例：

- WPF (4)
- 64位 (6)
- Visual Studio (17)
- Java (8)
- sql (2)
- Windows 7 (14)
- 其他 (11)
- 测试 (5)
- 网络技术 (2)
- Linux (1)

文章存档

- 2015年02月 (1)
- 2015年01月 (2)
- 2014年12月 (2)
- 2014年10月 (1)
- 2014年07月 (1)

展开

阅读排行

- 【2012.1.24更新】不要！ (73286)
- 微信禁止模拟器登录怎么办？ (62910)
- VS2012如何添加SQL数据源？ (20554)
- 如何在Ubuntu上添加桌面图标？ (17004)
- 酷派tbl联系人读取器201 (11604)
- 在Windows里安装运行H (11231)
- 【2012.12.18更新】WP (10987)
- QQ搜集用户数据是空穴来风？ (10981)
- 错误 1 "GenerateResource" 操作失败 (10169)
- 我的文档变成英文了怎么办？ (9950)

评论排行

- 【2012.1.24更新】不要！ (24)
- 酷派tbl短信读取器发布 (9)
- "为帮助内容存储区指定值" (7)
- 【2012.12.18更新】WP (7)
- 【发布软件】Visual Studio 2012 (5)
- 酷派tbl联系人读取器201 (5)
- 如何为自定义控件设置图 (4)
- 油猴子脚本【隐藏MSDN (4)
- 在Windows里安装运行H (4)
- BeginInitInvoke、ThreadPool、Task (4)

最新评论

- 微信禁止模拟器登录怎么办？
灰色系男孩: @u012580994:换个模拟器试一下
- 微信禁止模拟器登录怎么办？
Windgodc: @weiyu1992:你好像有什么办法 可以不让微信检测出。
- 微信禁止模拟器登录怎么办？
灰色系男孩: @baidu_27813697:我可以帮你解决 加QQ 135804242 或者在CSDN留言 ...
- BeginInitInvoke、ThreadPool、Task (4)
fxfj1227: 这个测试本身就是错误的

```
In[23]:= {g, {x, y}} = ExtendedGCD[6, 10];  
x  
y
```

Out[24]= 2

Out[25]= -1

所以x=2, y=-1。6×2+10×-1=12-10=2。

练习2

求9x+8y=2的整数解。

发现gcd(9,8)=1≠2，不能直接用扩展欧几里得算法。

根据上面所说的定理，先求9x+8y=gcd(9,8)的整数解。

```
In[33]:= {g, {x, y}} = ExtendedGCD[9, 8];  
x  
y
```

Out[34]= 1

Out[35]= -1

所以9×1+8×-1=gcd(9,8)=1。

根据定理，ax+by=c有整数解 $\left(\frac{cx_1}{g}, \frac{cy_1}{g}\right)$ ，所以9x+8y=2有整数解 $\left(\frac{2 \times 1}{1}, \frac{2 \times -1}{1}\right) = (2, -2)$ 。

用来求模反元素

求a关于模n的模反元素（a<n）。egcd(a,n)={g,x,y}。若g=1，则该模反元素存在，为x；若g不等于1，则该模反元素不存在。注意，余数可以为负数的，相见维基百科。如果x为负，人们喜欢把它“正过来”，即再加上n。

练习

求540关于1769的模反元素。借助Mathematica的ExtendedGCD函数，得该模反元素为1769-95=1674。

```
In[6]:= ExtendedGCD[540, 1769]  
Out[6]= {1, {-95, 29}}
```

容易验证540*1674 mod 1769=1。

求5关于17的模反元素。

In:= ExtendedGCD[5,17]

Out:= {1, {7, -2}}

答案为7。（不用加上n了）

希望对读者有帮助。

本文依照知识共享-署名-相同方式共享3.0协议释出

作者爱让一切都对了

了。

BeginInvoke、ThreadPool、Task
gqqnb: 就是说BeginInvoke会先创建线程，然后再运行代码。但是Thread.Start()和Task...

BeginInvoke、ThreadPool、Task
gqqnb: @dear156:就是说BeginInvoke会先创建线程，然后再运行代码。但是Thread.Sta...

微信禁止模拟器登录怎么办？
baidu_27813697: 博主你好。可以电话联系吗？请求帮忙。。

精确解释Unicode
枕上雪C: 写的却是不错，最近在做敏感词，就是通过接口确认utf-8中每个的字节

BeginInvoke、ThreadPool、Task
979293886: 这是一个错误的测试。会误导人的。原因在于线程不是一开始就结束。当线程运行时间大于线程创建时间的时候那...

安装/卸载SQL时弹出命令提示符
硅谷少年: %windir%\temp%\temp%这两个文件夹都试过了，进去新建个文件再删除，都正常，不放心，还...

友情链接

Cecil&linux

顶
3

踩
0

上一篇 为什么2DES不安全？

下一篇 选择适合你的老师或材料

相关文章推荐

• POJ 2115 C Looooops 扩展欧几里得算法

• The Balance扩展欧几里得算法

• poj 1576 AB扩展欧几里得算法

• 扩展欧几里得算法

• 扩展欧几里得Extended Euclid算法求最大公约数和乘...


• 扩展欧几里得算法


• 扩展欧几里得算法

• C - Line扩展欧几里得算法

• 扩展的欧几里得算法求最大公约数的CC++ 实现

参考知识库

软件测试知识库
4723 关注 | 318 收录

算法与数据结构知识库
16343 关注 | 2320 收录

猜你在找

使用决策树算法对测试数据进行分类实战

C语言系列之 字符串压缩算法与结构体初探

使用决策树算法对测试数据进行分类实战

C语言系列之 字符串相关算法

C++ 单元测试（GoogleTest）

C语言系列之 递归算法示例与 Windows 趣味小项目

《C语言/C++学习指南》加密解密篇（安全相关算法）

C语言系列之 数组与算法实战

C语言系列之 快速排序与全排列算法

C/C++单元测试培训

查看评论

1楼 君泰的夏天 2014-07-23 17:35发表



ax+by=c有整数解，当且仅当gcd(a,c)|c。详情见维基百科的贝祖定理条目。
这里的“当且仅当gcd(a,c)”应该是“a,b”吧。

Re: gqqnb 2014-07-26 00:32发表



回复君泰的夏天：是我笔误，多谢指正。

您还没有登录,请[\[登录\]](#)或[\[注册\]](#)

* 以上用户言论只代表其个人观点，不代表CSDN网站的观点或立场

核心技术类目

全部主题

Hadoop

AWS

移动游戏

Java

Android

iOS

Swift

智能硬件

Docker

OpenStack

VPN

Spark

ERP

IE10

Eclipse

CRM

JavaScript

数据库

Ubuntu

NFC

WAP

jQuery

BI

HTML5

Spring

Apache

.NET

API

HTML

SDK

IIS

Fedora

XML

LBS

Unity

Splashtop

UML

components

Windows

Mobile

Rails

QEMU

KDE

Cassandra

CloudStack

FTC

coremail

OPhone

CouchBase

云计算

iOS6

Rackspace

Web App

SpringSide

Maemo

Compuware

大数据

aptech

Perl

Tornado

Ruby

Hibernate

ThinkPHP

HBase

Pure

Solr

Angular

Cloud Foundry

Redis

Scala

Django

Bootstrap

