

原

Miller-Rabin素性测试算法详解

2017年05月24日 14:54:09

Nicetomeetu-

阅读数 5413

文章标签:

Miller-Rabin素性测试算法

csdn

数论

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。
本文链接：https://blog.csdn.net/ECNU_LZJ/article/details/72675595

看了一些别人的博客，发现里面涉及到的公式没有证明，于是就打算自己写一篇比较详细的讲解。

先看两个引理及其证明(建议把证明搞懂)。

PS：以下图片均为作者用wps制作，如想使用请附上作者博客链接，谢谢O(∩_∩)O。

引理 1(费马定理) 设 p 是素数， a 为整数，且 $(a, p) = 1$ ，则 $a^{p-1} \equiv 1(\text{mod } p)$ 。

证明:考虑 $1, 2, 3, \dots, (p-1)$ 这 $p-1$ 个数字，给它们同时乘上 a ，得到 $a, 2a, 3a, \dots, (p-1)a$ 。

$\because a \neq b(\text{mod } p), (c, p) = 1$

$\therefore ac \neq bc(\text{mod } p)$

$\therefore 1 \times 2 \times 3 \times \dots \times (p-1) \equiv a \cdot 2a \cdot 3a \times \dots \times (p-1)a (\text{mod } p)$

$\therefore (p-1)! \equiv (p-1)! a^{p-1} (\text{mod } p)$

$\because ((p-1)!, p) = 1$

$\therefore a^{p-1} \equiv 1(\text{mod } p)$ http://blog.csdn.net/ECNU_LZJ

引理 2(二次探测定理) 如果 p 是一个素数，且 $0 < x < p$ ，则方程 $x^2 \equiv 1(\text{mod } p)$ 的解

为 $x = 1, p-1$ 。

证明: 易知 $x^2 - 1 \equiv 0(\text{mod } p)$

$\therefore (x+1)(x-1) \equiv 0(\text{mod } p)$

$\therefore p \mid (x-1)(x+1)$

$\because p$ 为质数

$\therefore x = 1$ 或者 $x = p-1$

看完了上面的引理，那就可以正式开始Miller-Rabin算法的讲解了。

背景:

素性测试(即测试给定的数是否为素数)是近代密码学中的一个非常重要的课题。虽然Wilson定理(对于给定的正整数 n ， n 是素数的充要条件为 $(n-1)! \equiv -1(\text{mod } n)$)给出数的充要条件，但根据它来素性测试所需的计算量太大，无法实现对较大整数的测试。目前，尽管高效的确定性的素性算法尚未找到，但已有一些随机算法可用于素性测试分解。下面描述的Miller-Rabin素性测试算法就是一个这样的算法。

算法:

首先要知道费马定理只是 n 是素数的必要条件。即费马定理不成立， n 一定是合数；费马定理成立， n 可能是素数。接下来我们开始Miller-Rabin算法的分析过程。

假设 n 是奇素数，则 $n-1$ 必为偶数。令 $n-1=2^q \cdot m$ 。

随机选取整数 $a(0 < a < n)$ ，由费马定理， $(a^{2^q \cdot m} = a^{n-1}) \equiv 1(\text{mod } n)$ 。由二次探测定理可知： $a^{2^{q-1} \cdot m} \equiv 1(\text{mod } n)$ 或 $a^{2^{q-1} \cdot m} \equiv n-1(\text{mod } n)$ 。若 $a^{2^{q-1} \cdot m} \equiv 1(\text{mod } n)$ 成立，则再次由二次探测定理可知： $a^{2^{q-2} \cdot m} \equiv 1(\text{mod } n)$ 或 $a^{2^{q-2} \cdot m} \equiv n-1(\text{mod } n)$ ，……。如此反复应用二次探测定理，直到某一步 $a^m \equiv 1(\text{mod } n)$ 或 $a^m \equiv n-1(\text{mod } n)$ 。总之，若 n 是素数，则 $a^m \equiv 1(\text{mod } n)$ ，或存在 $0 \leq r \leq q-1$ ，使 $a^{2^r \cdot m} \equiv n-1(\text{mod } n)$ 。

所以该算法过程为

- 给定奇数 n ，为了判断是否为素数，首先测试 $a^{2^q \cdot m} \equiv 1(\text{mod } n)$ 是否成立。若不成立，则 n 一定为合数；若成立，则继续运行算法做进一步的测试。
- 考察下面的 **Miller 序列**：

$$a^m(\text{mod } n), a^{2^m}(\text{mod } n), a^{4^m}(\text{mod } n), \dots, a^{2^{q-1} \cdot m}(\text{mod } n)$$

若 $a^m \equiv 1(\text{mod } n)$ ，或者存在某个整数 $0 \leq r \leq q-1$ ，使 $a^{2^r \cdot m} \equiv n-1(\text{mod } n)$ 成立，则称 n 通过 **Miller 测试**。

由上面的分析可知，素数一定通过 Miller 测试。所以，如果 n 不能通过 Miller 测试，则 n 一定是合数；如果 n 能通过 Miller 测试，则 n 很可能是素数。这就是 **Miller-Rabin 算法**。

可以证明 Miller-Rabin 算法给出的错误结果的概率小于等于 $\frac{1}{4}$ 。若反复测试 k 次，则错


误概率可降低至 $(\frac{1}{4})^k$ 。这是一个很保守的估计，实际使用的效果要好得多。


如果仔细看的话，应该能看懂大致原理了，数论基础好的甚至都可以开始写代码了吧，哈哈。


示例代码如下：


```
1 typedef long long int ll;
2
3 ll mod_mul(ll a, ll b, ll mod)
4 {
5     ll res = 0;
6     while (b)
7     {
8         if (b & 1)
9             res = (res + a) % mod;
10        a = (a + a) % mod;
11        b >>= 1;
12    }
13    return res;
14 }
15
16 ll mod_pow(ll a, ll n, ll mod)
17 {
18     ll res = 1;
19     while (n)
20     {
21         if (n & 1)
22             res = mod_mul(res, a, mod);
23         a = mod_mul(a, a, mod);
24         n >>= 1;
25     }
26     return res;
27 }
28
```


```
29 // Miller-Rabin随机算法检测n是否为素数
30 bool Miller_Rabin(ll n)
31 {
32     if (n == 2)
33         return true;
34     if (n < 2 || !(n & 1))
35         return false;
36     ll m = n - 1, k = 0;
37     while (!(m & 1))
38     {
39         k++;
40         m >>= 1;
41     }
42     for (int i = 1; i <= 20; i++) // 20为Miller-Rabin测试的迭代次数
43     {
44         ll a = rand() % (n - 1) + 1;
45         ll x = mod_pow(a, m, n);
46         ll y;
47         for (int j = 1; j <= k; j++)
48         {
49             y = mod_mul(x, x, n);
50             if (y == 1 && x != 1 && x != n - 1)
51                 return false;
52             x = y;
53         }
54         if (y != 1)
55             return false;
56     }
57     return true;
58 }
```


3















【吐血推荐】15年老股民悟出的买卖规律，没想到震惊无数被套散户。

股管家·顶新



想对作者说点什么

- 素数判定Miller_Rabin 算法详解

素数判定Miller_Rabin 算法详解上次说好的要把素数判定和大致分解（见另一篇博文）的快速随机化算法解决了，于... 博文 来自： JUST CODE

阅读数 1万+
- Miller-Rabin素数检测算法

今天看了一下Miller-Rabin素数检测的算法，总结了一下，希望这篇博客对你们有帮助。先说几个理论基础：1.费马...

博文 阅读数 4431
- Miller-Rabin素性测试算法详解——定理

代码图片来自：https://blog.csdn.net/ECNU_LZJ/article/details/72675595两个引理证明过程：代码不是完整的一... 博文 来自： Source_Roc

阅读数 590
- 素数判定之Miller-Rabin算法

费马小定理P为素数时，二次探测原理所以结合起来对于p-1，将其分解，因为p为素数，所以一定是奇数（2被特判... 博文 来自： 这里RevollA，_(;3...

阅读数 166
- 人脸识别主要算法原理

Miller_Rabin算法详解

提示： Miller-Rabin质数测试小Hi： 这种质数算法是基于费马小定理的一个扩展，首先我们要知道什么是费马小定理...

博文 来自： 老子（道家）

Miller-Rabin素数测试算法

知识点系列之---Miller-Rabin素数测试

博文 来自： forever_dreams的...

Miller_Rabin素性测试学习小记

问题给出一个正整数n，判断它是不是质数。有一个简单暴力的方法：试除法，从2枚举到n--√n\sqrt{n}，如果有一...

博文 来自： qq_36551189的博客
- 3016






- https://blog.csdn.net/ECNU_LZJ/article/details/72675595

3/8

【BZOJ3667】Rabin-Miller算法
【题目链接】[点击打开链接](#)【思路要点】Pollard's rhoPollard's rhoPollard's\rho算法模板...
pollard-rho&miller-rabin
今天学习pollard-rho和miller-rabin。前置：不管怎么说大力筛一遍2,3,5,7,11,13,17都是错不了的！Miller-rabin%...

Miller-Rabin素性测试算法详解——定理 - Source_Roc - CSDN博客
[数论] Miller_Rabin素性测试 - 烟尘的博客 - CSDN博客

女孩子千万不要让男票发现这传奇！开局一条龙吸引力太大了！
贪玩游戏 · 顶新

Miller-Rabin学习笔记
为什么要学习Miller-Rabin?之前一直认为素性测试可以使用费马小定理的逆命题，虽说会有一定的概率判错，多选几... 博文 来自: [hanjinbo的博客](#)
Python Miller-Rabin素性检测算法 - cuit2016123070的..._CSDN博客

素性测试的Miller-Rabin算法完全解析 (C语言实现、Python实现)

【学习笔记】Miller-Rabin素数测试
【算法简介】MillerRabinMillerRabinMillerRabin素数测试是一种判断一个数是否是质数的方式。其单次测试的时间... 博文 来自: [cz_xuyixuan的博客](#)



StanleyClinton
131篇文章
排名:千里之外
[关注](#)



阿明
87篇文章
排名:千里之外
[关注](#)



sdau_fangshifeng
367篇文章
排名:千里之外
[关注](#)



RevollA
273篇文章
排名:千里之外
[关注](#)

Miller-Rabin概率素数测试算法 - 72 73 76 89 82 84 89..._CSDN博客

Rabin-Miller素性测试算法 - hcancientmoon的专栏 - CSDN博客

[数论] Miller_Rabin素性测试
文章目录问题引入算法思想参考代码问题引入给定一个数aaa，要求判断aaa是否为素数如果aaa为一个很小的数，我... 博文 来自: [烟尘的博客](#)

Python Miller-Rabin素性检测算法
概念：Miller-Rabin算法常用来判断一个大整数是否是素数，如果该算法判定一个数是合数，则这个数肯定是合数。... 博文 来自: [cuit2016123070的...](#)

C++实现的Miller-Rabin素性测试程序 - 海鸟Blog - CSDN博客

Miller-Rabin 素性测试 - weixin_30596023的博客 - CSDN博客

素性测试的Miller-Rabin算法完全解析（C语言实现、Python实现）
因为文中存在公式，只能用图片方式上传了！以下为C语言源代码：#include<stdio.h>typedeflonglongunsi... 博文 来自: [heshiip的专栏](#)

95后宝妈，为减肥连吃一个月，7天瘦8磅，现在体重不过百
争霸减肥 · 猎媒

Miller-Rabin素数测试算法 - forever_dreams的博客 - CSDN博客

求助：Rabin-Miller算法
下面是我在网上找的一个利用Rabin-Miller算法测试一个数是否是一个素数的程序，但我实在看不明白函数 bool Witnes... 论坛
素数判定的一些讨论（Miller-Rabin算法）
很久没有写博客了。。。最近军训加开学，感觉刷题速度有降低，要补一补。回归正题，正式进入数论阶段，讨论一... 博文 来自: [哇-WA 的博客](#)

| | | |
|--|----------|---------------------------|
| <div><div>Miller-Rabin素数检测算法笔记</div><div>本文内容主要参考《程序员的数学思维修炼》一书中对素数和余数的讲解及这篇博文:Miller-Rabin素数测试学习笔记...</div></div> | 阅读数 1503 | |
| <div><div>Rabin-Miller算法的设计与实现</div><div>一：说明：Rabin-Miller算法是用来测试一个数是否是一个素数的，以下是它的设计与实现。二：原理1：费马小定...</div></div> | 阅读数 2328 | 来自： 不知道是谁的博客 |
| <div><div>Miller-Rabin素性测试与二次探测</div><div>算法简介首先是一些概念：费马小定理：对于素数p和任意整数a，有$ap \equiv a \pmod p$$a^p \equiv a \pmod p$.反之，对于一个数...</div></div> | 阅读数 1003 | 来自： 小豪之家 |
| <div><div>陈小龙坦言：这游戏不充钱都能当全服大哥，找到充值入口算我输！</div><div>贪玩游戏 · 顶新</div></div> | | 来自： Mercury |
| <div><div>Rabin-Miller素性测试算法</div><div>Th1如果a^2</div></div> | 阅读数 1497 | 来自： hcancientmoon的... |
| <div><div>Miller-Rabin概率素数测试算法</div><div>本文首先鸣谢以下资料文章：资料1资料2资料3下面我们开始正文，从源头开始真正的梳理一下素数测试1.素数我们...</div></div> | 阅读数 6363 | 来自： 72 73 76 89 82 84... |
| <div><div>bzoj3667: Rabin-Miller算法</div><div>传送门：http://www.lydsy.com/JudgeOnline/problem.php?id=3667思路：首先我们说说Miller_Rabin算法我们...</div></div> | 阅读数 5 | 来自： weixin_30642869... |
| <div><div>millerrabin</div><div>概率型素性测试。可以说是历史上对费马小定理的”误“翻译起源，后逐渐发展而成。费尔马小定理:如果p是一个素...</div></div> | 阅读数 257 | 来自： wind-wing |
| <div><div>millerrabin学习笔记 数论</div><div>首先介绍一下millerrabin算法。millerrabin是一种素性测试算法，用来判断一个大数是否是一个质数。millerrabi...</div></div> | 阅读数 296 | 来自： forever_shi的博客 |
| <div><div>光绪年间132岁老人首次公开长寿秘诀，居然是因为...</div><div>好伙伴 · 猎媒</div></div> | | |
| <div><div>素数 （性质，费马小定理 millerrabin素性测试）</div><div>转载自Matrix大牛的博客把代码翻译成C++http://www.matrix67.com/blog/archives/234一个数是素数（也叫质...</div></div> | 阅读数 401 | 来自： pxlsdz的博客 |
| <div><div>Miller_Rabin算法【大素数判定】</div><div>基于费马小定理和二次探测定理#include<iostream>#include<stdlib.h>;usingnamespacestd;typedefl...</div></div> | 阅读数 103 | 来自： 追梦者 |
| <div><div>Miller-Rabin随机性素数测试算法(Miller_Rabin模板)</div><div>转载自：http://www.dxmtb.com/blog/miller-rabin/普通的素数测试我们有O(\sqrt{n})的试除算法。事实上，我们有O...</div></div> | 阅读数 7745 | 来自： Learn as if you we... |
| <div><div>Miller-Rabin算法</div><div>一.费马小定理 ifnisprimeand(a,n)equalsone,then$a^{n-1} \equiv 1 \pmod n$费马小定理只是个必要条件,符合费马小定理而...</div></div> | 阅读数 6186 | 来自： highyyy的专栏 |
| <div><div>算法基础 - 素数判定(Miller-Rabin算法)</div><div>素数判定素数不需要解释了，那么素数如何判定？最简单的算法，暴力测试，就是最简单的，从2枚举到\sqrt{n}...</div></div> | 阅读数 2926 | 来自： 累了就歇一会 |
| <div><div>陈小龙哭诉：郑州土豪怒砸2亿请他代言这款0充值传奇！真经典！</div><div>贪玩游戏 · 顶新</div></div> | | |
| <div><div>星星之火Oler：素数判断——Miller_Rabin</div><div>在这一讲中，我们来看一下如何判断一个素数常用的有种目录——普通判断——MillerRabin素数测试法算法前置：...</div></div> | 阅读数 25 | 来自： qq_43890190的博客 |
| <div><div>素性测试</div><div>所谓素性测试是检测一个数是否为素数的测试。而对素数的研究是有很长一段历史，把素数的东西写成一本书的话也...</div></div> | 阅读数 14 | 来自： nayao-net |
| <div><div>【算法编程】基于Miller-Rabin的大素数测试</div><div>基本原理：费尔马小定理:如果p是一个素数,且0则$a^{(p-1)} \equiv 1 \pmod p$。 利用费尔马小定理,对于给定的整数n,可以设计...</div></div> | 阅读数 2666 | 来自： 青峰碧陋室 |
| <div><div>素数判定MillerRabin算法</div><div>随机产生的任意大小的数，并验证其是否为素数。</div></div> | 01-01 | 下载 |




种一颗牙需要多少钱呢

种一颗牙需要多少钱


4003162126


Miller Rabin算法


首先介绍一下费马小定理定义:假如p是质数, 且gcd(a,p)=1, 那么a^(p-1)≡1 (mod p)当p为素数a^(p-1)=1(mod p)...





3














阅读数 671

来自: [LuRiCheng的博客](#)



Nicetomeetu-

关注

TA的个人主页 >

原创152

粉丝28

喜欢23

评论31

等级: 博客5

访问: 6万+

积分: 2137

排名: 3万+

勋章: 恒



Web前端开发

最新文章

EOJ 3486 二分+哈希

BZOJ - 4428 记忆化搜索

HDU 5952 Counting Cliques 爆搜

HDU 6181 Two Paths 次短路

HDU 6168 Numbers 思维

分类专栏



=====动态规划=====

40篇



ACM-基础dp

24篇



ACM-区间dp

6篇



ACM-数位dp

12篇



ACM-树形dp

1篇

展开

归档

2018年7月

1篇

2017年10月

1篇

2017年9月

1篇

2017年8月

23篇

2017年7月

17篇

2017年6月

14篇









| | |
|---------|-----|
| 2017年5月 | 11篇 |
| 2017年4月 | 10篇 |
| ... | ... |
| 展开 | |

热门文章

- Miller-Rabin素性测试算法详解
阅读数 5395
- 判断最小生成树的唯一性
阅读数 5087
- Windows环境下创建动态链接库(Visual Studio版)
阅读数 2213
- wxPython：图标、菜单、加速键、消息框
阅读数 1808
- Windows环境下创建并使用动态链接库 (CodeBlocks版)
阅读数 1343

最新评论

- POJ 2449 A* + spf...
qq_36666115： 非常的好！！！！
- 判断最小生成树的唯一性
weixin_43100196： 啊啊啊啊啊啊啊啊
- 判断最小生成树的唯一性
weixin_43100196： 请问大佬，一个带权连通图中，权值最小的边一定在任何最小生成树中的 ...
- POJ 1182 食物链 并查集+...
qq_14938523： “如果等于1，代表y被x吃，如果为2，代表x吃y”这不是同一个意思吗
- EOJ 2069 二分图匹配模板
sinat_39409536： eoj2069应该是在是在poj3041的基础上加强了数据，用模板匈牙利会超时emm ...

 腾讯云

学生服务器

体验套餐10元/月

1核2G·1M带宽
50GB存储

立即抢购



程序人生



CSDN资讯

- QQ客服 kefu@csdn.net
- 客服论坛 400-660-0108
- 工作时间 8:30-22:00

关于我们 招聘 广告服务 网站地图


百度提供站内搜索 京ICP备19004658号

©1999-2019 北京创新乐知网络技术有限公司

网络110报警服务 经营性网站备案信息

北京互联网违法和不良信息举报中心

中国互联网举报中心 家长监护 版权申诉

 3



