第26卷第6期 华东交通大学学报 Vol.26 No.6
2009年12月 Journal of East China Jiaotong University Dec.,2009

文章编号:1005-0523(2009)06-0098-03

素数原根的两个猜想

周 娟[1],周尚超[2]

(华东交通大学 1.软件学院; 2.基础科学学院,江西 南昌 330013)

摘要:应用计算机编程,对素数原根进行了研究,通过对100亿以下素数进行了验证,得出了两个猜想:(1) 若 p 和 $q=4p+1$ 都是素数,则 q 的最小原根为2;(2) 若 p 和 $q=2p+1$ 都是素数,当 $p=1(\mathrm{mod}\ 4)$ 时,2是 q 的最小原根,而当 $p=3(\mathrm{mod}\ 4)$ 时,2不是 q 的最小原根。在验证这两个猜想的过程中,还发现对于 p 和 $2^k p+1$ 都为素数时,2不是 $2^k p+1$ 的最小原根($k>2$)。

关 键 词:素数;原根;算法

中图分类号:O157 **文献标识码**:A

素数是除了1和它本身外不能被其它数整除的数。素数在数论中起着关键的作用,前10个素数是2,3,5,7,11,13,17,19,23,29。令 p 为素数,如果 a 与 p 互素,则 $a^{(p-1)}=1(\mathrm{mod}\ p)$。如果 $a^t=1(\mathrm{mod}\ p)$,且 t 是最小的,则称 t 是 a 的指数$(\mathrm{mod}\ p)$,如果 a 的指数为 $p-1$,则称 a 为 p 的原根。例如 $p=7, 2^3=1(\mathrm{mod}\ 7)$,2的指数为3$(\mathrm{mod}\ 7)$,显然不满足 $t=p-1$,所以2不是7的原根。又例如 $p=11, 2^{10}=1\ 024=1(\mathrm{mod}\ 11)$,如果2的指数为 t,则由以下引理1,$t=2,5$,或10,$2^2=4, 2^5=32$,可以看出对于11的原根来说,2和5都不是可取的指数,而可取的指数是10,即2是11的原根。原根是数论中重要的概念,在多数数论书中都列出部分素数的最小原根。蔺大正[1]对最小原根进行了分析,提出了几个猜想。

引理1[2~4] 若 a 对模 p 的指数是 t,则 t 整除 $p-1$。

引理2 若 $q=4p+1$ 是素数,则 a 是 q 的原根的充要条件是 $a^{2p}=-1(\mathrm{mod}\ q)$。

根据引理1,a 的指数是2,4,p,2p,4p,如果 a 的指数是 p,则 $a^{2p}=1(\mathrm{mod}\ q)$,$a$ 的指数显然不会是2和4。

根据引理2,对 $q=4p+1$ 是素数,只要计算出 $2^{2p}=-1(\mathrm{mod}\ q)$,就能说明2是原根了。同样对 $q=2p+1$ 是素数,当 $p=1(\mathrm{mod}\ 4)$,$2^p=-1(\mathrm{mod}\ q)$,就能说明2是原根,当 $p=3(\mathrm{mod}\ 4)$,$2^p=1(\mathrm{mod}\ q)$,就能说明2不是是原根。对 $q=2^k p+1$ 是素数($k>2$),计算出 $2^{(k-1)}p==1(\mathrm{mod}\ q)$,说明2不是原根。

1 计算方法

用C语言编程,编制了以下几个函数

(1) 用筛法计算小于0.1亿的素数,并将素数保存在数组prime[]中,程序如下

```
int  prime[784990];
bool PR[10000004];
void PRIME(int M)
{int i,j,k,i2;
for(i=0,j=1;i<=M;i+=2,j+=2){PR[i]=0;PR[j]=1;}
PR[2]=1;PR[1]=0;
for(i=3;i<=3163;i+=2)
{if(PR[i])
  {i2=i+i; k=i2+i; while(k<=M){PR[k]=0;k+=i2;}}
```

收稿日期:2009-09-20

作者简介:周 娟(1977-),女,云南昆明人,硕士,助教,研究方向为软件理论、数据结构和计算方法。

```
}
k=2;prime[1]=2;prime[2]=3;
for(i=5;i<=M;i++)if(PR[i]){prime[++k]=i;}
pr("%d\n",k);        //664579
prime[0]=k;
}
```

(2) 素数判断函数

```
int Isp(__int64 q)
{int p=(int)sqrt(q)+3,i;

for(i=2;prime[i]<=p;i++)
{if(q%prime[i]==0)return 0;}
return 1;
}
```

(3) 计算 n 次幂的函数

```
__int64 mul(__int64 a,__int64 b)
{
__int64 c=0;
while(b)
{
  if(b&1){c+=a;if(c>=q)c-=q;}
  a=a+a;if(a>=q)a-=q;
  b/=2;
}
return c;
}
__int64 pow(__int64 m)
{--int64 c=2,d=1;   // c^m
  while(m>1)
  {
   if(m&1){//d=d*c%q;
     d=mul(d,c);
     m--;}
   else {c=mul(c,c);//c=c*c%q;
   m/=2;}
  }
  c=mul(c,d);//c=c*d%q;
  return c;
}
```

2　计算结果及猜想

对小于 100 亿的每个素数 q,如果 $q=2^kp+1$,且 p 是素数,则计算 $b=2^{(q-1)/2}\bmod q$。若 $b=1$,说明 2 不是 q 的原根,若 $b=q-1$,则 $2^{(q-1)}=1 \bmod q$,2 是 q 的原根。计算结果如下。

(1) 若 $q=4p+1<100$ 亿,q 和 p 都是素数,则 2 是 q 的最小原根。

(2) 若 $q=2p+1<100$ 亿,q 和 p 都是素数,且 $p=1(\bmod 4)$,则 2 是 q 的最小原根。

(3) 若 $q=2p+1<100$ 亿，q 和 p 都是素数，且 $p=3(\mathrm{mod}\ 4)$，则 2 不是 q 的最小原根。

(4) 若 $q=2^k p+1<100$ 亿，q 和 p 都是素数，且 $k>2$，则 2 不是 q 的最小原根。

以 4 亿个数为 1 个区间，算出的结果列于表 1，每行第一列表示 4 亿个数的区间，第 2 列表示这个区间 $2^k p+1$ 型素数的个数，第 3 列表示原根为 2 的 $2p+1$ 型素数的个数，第 4 列表示原根为 2 的 $4p+1$ 型素数的个数，第 5 列为原根不为 2 的素数的个数。

表 1 原根为 2 的 $2^k p+1$ 型素数的个数

区 间	素数个数	原根为 2 的 $2p+1$ 型素数的个数	原根为 2 的 $4p+1$ 型素数的个数	原根不为 2 的素数个数
$(0, 4.0\times10^8]$	1 635 504	391 351	407 199	444 883
$(4\times10^8, 8\times10^8]$	1 395 891	335 179	347 640	377 291
$(8\times10^8, 1.2\times10^9]$	1 322 377	318 465	329 096	356 177
$(1.2\times10^9, 1.6\times10^9]$	1 279 305	307 950	318 703	344 137
$(1.6\times10^9, 2.0\times10^9]$	1 247 637	300 312	311 737	334 993
$(2.0\times10^9, 2.4\times10^9]$	1 223 476	294 185	305 080	329 339
$(2.4\times10^9, 2.8\times10^9]$	1 204 110	290 635	300 239	322 810
$(2.8\times10^9, 3.2\times10^9]$	1 188 425	286 706	296 557	318 501
$(3.2\times10^9, 3.6\times10^9]$	1 173 890	282 727	292 629	314 929
$(3.6\times10^9, 4.0\times10^9]$	1 160 723	279 959	290 067	310 934
$(4.0\times10^9, 4.4\times10^9]$	1 149 155	277 303	286 354	308 188
$(4.4\times10^9, 4.8\times10^9]$	1 140 921	275 583	284 296	305 839
$(4.8\times10^9, 5.2\times10^9]$	1 131 635	272 995	281 885	303 409
$(5.2\times10^9, 5.6\times10^9]$	1 123 369	270 976	280 102	300 718
$(5.6\times10^9, 6.0\times10^9]$	1 116 452	269 625	278 432	298 955
$(6.0\times10^9, 6.4\times10^9]$	1 109 576	267 910	276 194	297 083
$(6.4\times10^9, 6.8\times10^9]$	1 101 388	266 155	274 502	294 395
$(6.8\times10^9, 7.2\times10^9]$	1 095 767	264 844	273 100	293 105
$(7.2\times10^9, 7.6\times10^9]$	1 091 037	263 621	272 529	291 510
$(7.6\times10^9, 8.0\times10^9]$	1 087 522	263 353	270 883	290 761
$(8.0\times10^9, 8.4\times10^9]$	1 082 804	261 964	270 213	288 700
$(8.4\times10^9, 8.8\times10^9]$	1 077 686	260 723	268 977	287 931
$(8.8\times10^9, 9.2\times10^9]$	1 071 567	258 289	267 540	286 676
$(9.2\times10^9, 9.6\times10^9]$	1 069 163	258 267	266 952	285 703
$(9.6\times10^9, 1.0\times10^{10}]$	1 064 146	257 600	264 901	284 641

根据计算结果提出下面 2 个猜想。

猜想 1 若 p 和 $q=4p+1$ 都是素数，则 q 的最小原根为 2。

猜想 2 若 p 和 $q=2p+1$ 都是素数，当 $p=1(\mathrm{mod}\ 4)$ 时，2 是 q 的最小原根，而当 $p=3(\mathrm{mod}\ 4)$ 时，2 不是 q 的最小原根。

参考文献：

[1] 华罗庚.数论[M].北京:科学出版社,1981.1-76.

[2] 刘汝佳,黄 亮.算法艺术与信息学竞赛[M].北京:清华大学出版社,2004.216-228.

[3] 闵嗣鹤,严士健.初等数论[M].北京:高等教育出版社,2004.120-130.

[4] 蔺大正.从计算看素数的最小原根[J].数学的实践与认识,1992,(3):91-95.

(下转第 130 页)

The Development of Jiangxi Real Estate in the Global Financial Crisis

YANG Lu, SHI Huan-ping

(School of Economics and Management, East China Jiaotong University, Nanchang 330013, China)

Abstract: This paper discusses the development of the real estate industry after the outbreak of the global financial crisis in Jiangxi Province. Since the financial crisis, the real estate market of Jiangxi has experienced two periods, one is downturn period, from September 2008 to February 2009; the other is rebounded period, from March 2009 till now. This article firstly uses some indicators such as sales of commercial residential building, as-built area, the average price, investment of real estate and its growth to illustrate the changes in the real estate market in Jiangxi Province after the outbreak of the global financial crisis. Then, the reasons why the real estate market gets warm afterwards are analyzed. Finally, the author puts forward some personal advice for the development of Jiangxi real estare.

Key words: financial crisis; real estate; rebound

(责任编辑:王全金 吴泽九)

(上接第 100 页)

Two Conjecture for Primitive Root of Prime Number

ZHOU Juan[1], ZHOU Shang-chao[2]

(East China Jiaotong University 1. School of Software; 2. School of Basic Science. Nanchang 330013, China)

Abstract: The primitive root of prime number have been studied by application of computer programming. Two conjectures are obtained on basis of the verification on the prime numbers below 10 billion: (1) For any prime p and q, if $q = 4p + 1$, then 2 is the least primitive root of q. (2) For any prime p and q, $q = 2p + 1$, if $p = 1 \pmod 4$, then 2 is the least primitive root of q, if $p = 3 \pmod 4$, then 2 is not the least primitive root of q. In the course of the verification on these two conje ctures, the autcor found that for any prime p and q, if $q = 2^k p + 1$, $k > 2$, then 2 is not the least primitive root of q.

Key words: prime; primitive root; algorithm

(责任编辑:刘棉玲 吴泽九)