Open Access Library Journal
2026, Volume 13, e11159
ISSN Online: 2333-9721
ISSN Print: 2333-9705

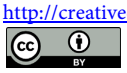
Method of Discriminating a Class of Special Prime Numbers

Zhongqi Zhou

Hubei Coal Geology Bureau, Wuhan, China
Email: zhouzongqi1058@163.com

How to cite this paper: Zhou, Z.Q. (2026) Method of Discriminating a Class of Special Prime Numbers. *Open Access Library Journal*, **13**: e11159.
https://doi.org/10.4236/oalib.1115937

Received: August 23, 2026
Accepted: September 20, 2026
Published: September 23, 2026



Abstract

It is very difficult to find a new Wieferich prime number. This paper uses Eisenstein congruence formula and Sun Zhihong congruence theorem to a method to determine Wieferich prime number. The Fermat quotient and Euler quotient are also studied in the paper.

Subject Areas

Integral Equation, Number Theory

Keywords

Wieferich Prime Number, Detemination Method, Sufficient and Necessary Conditions, Fermat Quotient, Euler Quotient

1. 引言

满足同余式

$$2^{p-1} \equiv 1 \left(\mathrm{mod}\ p^2\right)$$

的素数 p 叫作伟伊列治(Wieferich)素数，1909 年 Wieferich 证明了如下一个困难的定理：

如果费马猜想(现已成为定理)的第一种情形对于素数 p 不成立，则必有上面的同余式，所以伟伊列治素数是一种特别的素数，在正整数集中，这种素数是很少的。Lehmer (1981)证明了：在 6×10^9 以内只有素数 1093 和 3511 满足以上同余式。后来 J. knauer 和 J. Richstein 运用互联网把计算扩大到 1.25×10^{15} 均未发现新的伟伊列治素数，到目前为止，仍然只知道仅有以上两个伟伊列治素数，所以寻找更大的伟伊列治素数是一件非常困难的事情，也是一件十分有意义的事情。

2. 定义

1. 设 p 为素数， $a\in Z$ ， $(p,a)=1$ ，则称 $q_p(a)=\dfrac{a^{p-1}-1}{p}$ 为 a 对素数 p 的 Fermat 商[1]。
2. 设 $m>2$ 为整数， $a\in Z$ ， $(m,a)=1$ ，则称 $q_m(a)=\dfrac{a^{\varphi(m)}-1}{m}$ 为 a 对整数 m 的 Euler 商。

3. 引理

引理 1：Wolstenholme 定理[2]若 $p\geq 5$ 为素数，则

$$\sum_{k=1}^{p-1}\frac{1}{k}\equiv 0\left(\mathrm{mod}\ p^2\right).$$

引理 2：(孙智宏)设 p 为奇素数， a 为正整数，则[1]

$$\frac{a^p-a}{p}\equiv\sum_{k=1}^{p-1}\frac{1}{k}\left[\frac{ka}{p}\right](\mathrm{mod}\ p).$$

引理 3：(Eisenstein)设 p 为奇素数，则[1]

$$\frac{2^{p-1}-1}{p}\equiv\frac{1}{2}\sum_{k=1}^{p-1}\frac{(-1)^{k-1}}{k}(\mathrm{mod}\ p).$$

4. 伟伊列治素数的推广

我们将伟伊列治素数进行推广：

满足同余式

$$q_p(2)=\frac{2^{p-1}-1}{p}\equiv Z\left(\mathrm{mod}\ p\right)$$

的素数 p 叫作 Z 素数，$0\leq Z<p$ ， $Z\in N$ 。当 $Z=0$ 时， p 为 0 素数，也称为伟伊列治素数，任何一种 Z 素数都是非常稀少的：

在 1.25×10^{15} 以内只有 1093,3511 为 0 素数(伟伊列治素数)；

在 1×10^{10} 以内只有 3,29,37,3373,2001907169 为 1 素数；

在 1.5×10^{9} 以内只有 7,71,379,2659 为 2 素数；

在 1.6×10^{9} 以内只有 5,13,19,173,5501 为 3 素数；

在 1×10^{10} 以内只有 2633 为 4 素数；

在 10^8 以内只有 11,2152849 为 5 素数；

在 10^8 以内只有 31,89 为 6 素数；

在 2.5×10^{9} 以内只有 233,118417283 为 7 素数；

在 10^8 以内只有 59,1733 为 8 素数；

……

对于任一奇素数 p，都有 $q_p(2)\equiv Z\left(\mathrm{mod}\ p\right)$，所以，任一奇素数都属于某一 Z 素数，而一奇素数不会同时属于两类 Z 素数。本文利用 Eisenstein 同余

式、孙智宏同余式等定理得出了一种 Z 素数的判定方法。

5. 定理

定理 1：(Z 素数的判定方法)

设 $q_p(2)\equiv Z(\bmod p)$， p 为奇素数， p 为 Z 素数的充分必要条件为

$$-\frac{1}{2}\sum_{k=1}^{\frac{p-1}{2}}\frac{1}{k}\equiv q_p(2)\equiv Z(\bmod p).$$

证：必要条件：

根据引理 2，当 $a=2$ 时，

$$\frac{a^p-a}{p}\equiv\frac{2\left(2^{p-1}-1\right)}{p}\equiv\sum_{k=1}^{p-1}\frac{1}{k}\left[\frac{2k}{p}\right]\equiv\sum_{k=\frac{p+1}{2}}^{p-1}\frac{1}{k}(\bmod p).$$

当 p 为 Z 素数时，因

$$\frac{2^{p-1}-1}{p}\equiv Z(\bmod p)$$

$$\frac{\left(2^{p-1}-1\right)}{p}\equiv\frac{1}{2}\sum_{k=\frac{p+1}{2}}^{p-1}\frac{1}{k}\equiv Z(\bmod p)$$

再根据引理 1 可得

$$-\frac{1}{2}\sum_{k=1}^{\frac{p-1}{2}}\frac{1}{k}\equiv-\frac{1}{2}\sum_{k=1}^{p-1}\frac{1}{k}+\frac{1}{2}\sum_{k=\frac{p+1}{2}}^{p-1}\frac{1}{k}\equiv Z(\bmod p).$$

充分条件：

若 $-\frac{1}{2}\sum_{k=1}^{\frac{p-1}{2}}\frac{1}{k}\equiv Z(\bmod p)$，则 $\frac{1}{2}\sum_{k=1}^{\frac{p-1}{2}}\frac{1}{k}=\sum_{k=1}^{\frac{p-1}{2}}\frac{1}{2k}\equiv-Z(\bmod p)$，

根据引理 1 可知， $\sum_{k=1}^{\frac{p-1}{2}}\frac{1}{2k-1}\equiv\sum_{k=1}^{p-1}\frac{1}{k}-\sum_{k=1}^{\frac{p-1}{2}}\frac{1}{2k}\equiv Z(\bmod p)$，根据引理 3，可推得

$$\sum_{k=1}^{p-1}\frac{(-1)^{k-1}}{k}\equiv\sum_{k=1}^{\frac{p-1}{2}}\frac{1}{2k-1}+\left(-\sum_{k=1}^{\frac{p-1}{2}}\frac{1}{2k}\right)\equiv\frac{2\left(2^{p-1}-1\right)}{p}\equiv 2Z(\bmod p).$$

由上可得 $q_p(2)=\frac{2^{p-1}-1}{p}\equiv Z(\bmod p)$ 此说明 p 为 Z 素数。

推论： p 为伟伊列治素数，当且仅当 $\sum_{k=1}^{\frac{p-1}{2}}\frac{1}{k}\equiv 0(\bmod p)$。

定理 2：设 $p>3$ 为奇素数，则

$$-\frac{2}{3}\sum_{k=1}^{\left[\frac{p-1}{3}\right]}\frac{1}{k}\equiv q_p(3)(\bmod p).$$

证：根据引理 2 知：$\frac{a^p-a}{p}\equiv\sum_{k=1}^{p-1}\frac{1}{k}\left[\frac{ka}{p}\right]\left(\mathrm{mod}\,p\right)$ 当 $a=3$ 时可得

$$\frac{3^p-3}{p}\equiv\sum_{k=\left[\frac{p-1}{3}\right]+1}^{p-\left(\left[\frac{p-1}{3}\right]+1\right)}\frac{1}{k}+\sum_{k=p-\left[\frac{p-1}{3}\right]}^{p-1}\frac{2}{k}\left(\mathrm{mod}\,p\right).$$

因 $\frac{1}{a}+\frac{1}{p-a}\equiv 0\left(\mathrm{mod}\,p\right)$，所以 $\sum_{k=\left[\frac{p-1}{3}\right]+1}^{p-\left(\left[\frac{p-1}{3}\right]+1\right)}\frac{1}{k}\equiv 0\left(\mathrm{mod}\,p\right)$。

$\frac{3^p-3}{p}\equiv\sum_{k=p-\left[\frac{p-1}{3}\right]}^{p-1}\frac{2}{k}\left(\mathrm{mod}\,p\right)$。

根据引理 1 有

$$-\frac{3^p-3}{2p}\equiv-\sum_{k=p-\left[\frac{p-1}{3}\right]}^{p-1}\frac{1}{k}\equiv\sum_{k=1}^{p-1}\frac{1}{k}-\sum_{k=p-\left[\frac{p-1}{3}\right]}^{p-1}\frac{1}{k}\equiv\sum_{k=1}^{\left[\frac{p-1}{3}\right]}\frac{1}{k}\left(\mathrm{mod}\,p\right).$$

所以 $-\frac{2}{3}\sum_{k=1}^{\left[\frac{p-1}{3}\right]}\frac{1}{k}\equiv q_p\left(3\right)\left(\mathrm{mod}\,p\right).$

定理 3：

设 $n=a_1a_2\cdots a_i$，$a_j\in N$，$j=1,2,\cdots,i$。$m>2$，$\left(m,n\right)=1$，则

$$q_m\left(n\right)=q_m\left(a_1\right)+q_m\left(a_2\right)+\cdots+q_m\left(a_i\right)\left(\mathrm{mod}\,m\right).$$

证：$\left(a_1^{\varphi(m)}-1\right)\left(a_2^{\varphi(m)}-1\right)=\left(a_1a_2\right)^{\varphi(m)}-1-\left(a_1^{\varphi(m)}-1\right)-\left(a_2^{\varphi(m)}-1\right)$，

故 $q_m\left(a_1a_2\right)-q_m\left(a_1\right)-q_m\left(a_2\right)=\frac{\left(a_1^{\varphi(m)}-1\right)\left(a_2^{\varphi(m)}-1\right)}{m}\equiv 0\left(\mathrm{mod}\,m\right).$

即
$$q_m\left(a_1a_2\right)\equiv q_m\left(a_1\right)+q_m\left(a_2\right)\left(\mathrm{mod}\,m\right). \tag{1}$$

根据(1)可得

$q_m\left(\left(a_1a_2\right)a_3\right)\equiv q_m\left(a_1a_2\right)+q_m\left(a_3\right)\equiv q_m\left(a_1\right)+q_m\left(a_2\right)+q_m\left(a_3\right)\left(\mathrm{mod}\,m\right).$

同理可得

$$q_m\left(a_1a_2\cdots a_i\right)\equiv q_m\left(a_1\right)+q_m\left(a_2\right)+\cdots+q_m\left(a_i\right)\left(\mathrm{mod}\,m\right).$$

推论 $\left(a^{\varphi(m)}\right)^k-1\equiv k\left(a^{\varphi(m)}-1\right)\left(\mathrm{mod}\,m^2\right).$

定理 4：

设 $n=\frac{a}{a_1a_2\cdots a_i}$，$a\in N$，$a_j\in N$，$j=1,2,\cdots,i$。$m>2$，$\left(m,a\times a_1a_2\cdots a_i\right)=1$，

则

$$q_m\left(n\right)=q_m\left(a\right)-q_m\left(a_1\right)-q_m\left(a_2\right)-\cdots-q_m\left(a_i\right)\left(\mathrm{mod}\,m\right).$$

证：因 $a=n\times a_1a_2\cdots a_j$，根据定理 4 知：

$$q_m\left(a\right)\equiv q_m\left(n\right)+q_m\left(a_1\right)+q_m\left(a_2\right)+\cdots+q_m\left(a_i\right)\left(\mathrm{mod}\,m\right).$$

所以 $q_m(n)\equiv q_m(a)-q_m(a_1)-q_m(a_2)-\cdots-q_m(a_i)\pmod m$。

6. 猜想

猜想 1：

设 $m>2$ 为奇数，则

$$-\frac{1}{2}\sum_{\substack{k=1\\(k,m)=1}}^{\frac{m-1}{2}}\frac{1}{k}\equiv q_m(2)\pmod m.$$

根据猜想 1

$m>2$ 为奇数，$q_m(2)\equiv 0\pmod m$，当且仅当

$$\sum_{\substack{k=1\\(k,m)=1}}^{\frac{m-1}{2}}\frac{1}{k}\equiv 0\pmod m.$$

以下给出了具有上述性质的数 m：

$m=3^r\times 1093,$ $0\le r\le 1.$

$m=3^r\times 7\times 1093,$ $0\le r\le 2.$

$m=3^r\times 13\times 1093,$ $0\le r\le 2.$

$m=3^r\times 7\times 13\times 1093,$ $0\le r\le 3.$

$m=3^r\times 3511,$ $0\le r\le 3.$

$m=3^r\times 5\times 3511,$ $0\le r\le 3.$

$m=3^r\times 13\times 3511,$ $0\le r\le 4.$

$m=3^r\times 5\times 13\times 3511,$ $0\le r\le 4.$

$m=3^r\times 1093\times 3511,$ $0\le r\le 4.$

$m=3^r\times 5\times 1093\times 3511,$ $0\le r\le 4.$

$m=3^r\times 7\times 1093\times 3511,$ $0\le r\le 5.$

$m=3^r\times 13\times 1093\times 3511,$ $0\le r\le 5.$

$m=3^r\times 5\times 7\times 1093\times 3511,$ $0\le r\le 5.$

$m=3^r\times 5\times 13\times 1093\times 3511,$ $0\le r\le 5.$

$m=3^r\times 7\times 13\times 1093\times 3511,$ $0\le r\le 6.$

$m=3^r\times 5\times 7\times 13\times 1093\times 3511,$ $0\le r\le 6.$

$m=3^r\times 13^2\times 1093\times 3511,$ $0\le r\le 5.$

$m=3^r\times 5\times 13^2\times 1093\times 3511,$ $0\le r\le 5.$

$m=3^r\times 7\times 13^2\times 1093\times 3511,$ $0\le r\le 6.$

$m=3^r\times 5\times 7\times 13^2\times 1093\times 3511,$ $0\le r\le 6.$

共 104 个 m 适合：

$$2^{\varphi(m)}\equiv 1\pmod{m^2}.$$

是否还有这样的数 m，目前不能确定。

猜想 2

设 $m>3$ 为整数，$(m,3)=1$，则

$$-\frac{2}{3}\sum_{\substack{k=1\\(k,m)=1}}^{\left[\frac{m-1}{3}\right]}\frac{1}{k}\equiv q_m(3)(\mathrm{mod}\, m).$$

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] 孙智宏. 数和数列[M]. 北京: 科学出版社, 2016: 108-109.

[2] P.里本伯姆. 博大精深的素数[M]. 北京: 科学出版社, 2007: 20.

Appendix 1. Abstract and Keywords in Chinese

一类特殊素数的判定方法

摘要：寻找新的伟伊列治素数是一件很困难的事情，本文利用 Eisenstein 同余式和孙智宏同余式等定理得出了对一类特殊素数的判定方法。本文还对 Fermat 商和 Euler 商进行了研究。

关键词：伟伊列治素数，判定方法，充分和必要条件，Fermat 商，Euler 商