A research on the theory of residue of higher degree

Team members

Yanjie Jing Tao Gu

Teacher

Hongliang Shi

School

No.2 Secondary School Attached to East China Normal University

Statement

When we participated in the national competition, we were told that all of the results have been discussed in some professional books on number theory, and there have been far better methods to solve them. We didn't know it when we were doing the study. These results and proofs are all got by ourselves.

Abstract

In this paper, we first discussed some properties of the symbol $\left(\frac{a}{p}\right)_k$ to make the following discussion more convenient. Then we used the methods of elementary number theory to discuss some basic properties of residue of higher degree on condition that the degree k is an odd prime, 2^n, p^n and any positive integer.

Key word: residue of higher degree

Introduction

The conception of quadratic residue comes from the problem of solving quadratic congruence. A general quadratic congruence to a particular modulo $ax^2+bx+c\equiv 0(\mathrm{mod}\ p)$ can always be converted into the basic two terms congruence $x^2\equiv a(\mathrm{mod}\ p)$. As for the solvability of it, Euler once got a effective criterion. To be convenient, Legendre introduced the symbol $\left(\frac{a}{p}\right)$. So, the problem is to calculate the symbol $\left(\frac{a}{p}\right)$. Early in a former paper, Euler raised a conjecture. Both Legendre and Gauss realized the importance of the conjecture for calculating the value of Legendre symbol. The

conjecture was finally completely proved by Gauss. That is the famous law of quadratic reciprocity. Thus, the problem of calculating Legendre symbol has been completely solved. But solving congruence equation of higher degree, even the most basic two terms congruence, is a really difficulty in elementary number theory. In this paper, we discussed some basic properties of two terms congruence equation $x^k \equiv a(\mathrm{mod}\ p)$ and some related problems with theories of congruence. Although most of these conclusions can be easily got with algebraic number theory, we mainly used elementary methods.

Definition First we suppose that $(a, p) = 1$. If $x^k \equiv a(\mathrm{mod}\ p)$ has solutions, we call a is the residue of k degree modulo p, otherwise we call a the non-residue of k degree modulo p. For convenience, we introduced the symbol $\left(\frac{a}{p}\right)_k$. We denote $\left(\frac{a}{p}\right)_k = 1$, it represents that a is the residue modulo p of degree k; If $\left(\frac{a}{p}\right)_k = -1$, it represents that a is the non-residue modulo p of degree k. If $k = 2$, then it is quadratic residue, which we are familiar with. And at this time we can omit k, and briefly symbol it as $\left(\frac{a}{p}\right)$. If $(a, p) > 1$, we denote $\left(\frac{a}{p}\right)_k = 0$. This condition is special, we didn't discuss it in this paper.

Main results

In this paper, we always postulate p as a prime. The conclusion when $p = 2$ is commonly known,（we always have $\left(\frac{a}{2}\right)_k = 1$）.Thus, we always postulate p as an odd prime.

1. Properties of the symbol $\left(\frac{a}{p}\right)_k$

First, we will discuss some properties of the symbol $\left(\frac{a}{p}\right)_k$ to make the following discussion more convenient.

Obviously, we have $\left(\frac{1}{p}\right)_k = 1$, $\left(\frac{a^k}{p}\right)_k = 1$, and if $a \equiv b(\mathrm{mod}\ p)$, $\left(\frac{a}{p}\right)_k = \left(\frac{b}{p}\right)_k$.

It is easy to popularize the following Euler criterion：

Theorem 1 If $p \equiv 1(\bmod k)$, then we have

(1)$\left(\frac{a}{p}\right)_k = 1 \Leftrightarrow a^{\frac{p-1}{k}} \equiv 1(\bmod p)$; (2)$\left(\frac{a}{p}\right)_k = -1 \Leftrightarrow \sum_{n=1}^{k-1} a^{\frac{p-1}{k}n} \equiv -1(\bmod p)$.

Proof ： If $p \equiv 1(\bmod k)$, if $x^k \equiv a(\bmod p)$ has solution $x \equiv x_1(\bmod p)$,

then $(x_1^k)^{\frac{p-1}{k}} \equiv a^{\frac{p-1}{k}} (\bmod p)$, that is $a^{\frac{p-1}{k}} \equiv x_1^{p-1} \equiv 1(\bmod p)$.

On the contrary, if $a^{\frac{p-1}{k}} \equiv 1(\bmod p)$, we can know

$$0 \equiv x^{p-1} - 1 = \left(x^k\right)^{\frac{p-1}{k}} - a^{\frac{p-1}{k}} + a^{\frac{p-1}{k}} - 1 \equiv \left(x^k\right)^{\frac{p-1}{k}} - a^{\frac{p-1}{k}} = (x^k - a)\sum_{i=1}^{\frac{p-1}{k}} \left(x^k\right)^{i-1} a^{\frac{p-1}{k}-(i-1)} (\bmod p)$$

.

Hence there must exist solutions to $x^k - a \equiv 0(\bmod p)$. And we can also know that there

are k solutions to $x^k - a \equiv 0(\bmod p)$.

If $p \equiv 1(\bmod k)$, we have $a^{p-1} - 1 = (a^{\frac{p-1}{k}} - 1)\sum_{n=0}^{k-1} a^{\frac{p-1}{k}n} \equiv 0(\bmod p)$

If$\left(\frac{a}{p}\right)_k = -1$, $a^{\frac{p-1}{k}} - 1 \not\equiv 0(\bmod p)$, so $\sum_{n=1}^{k-1} a^{\frac{p-1}{k}n} \equiv -1(\bmod p)$.

On the contrary, if$\sum_{n=1}^{k-1} a^{\frac{p-1}{k}n} \equiv -1(\bmod p)$, we can know $a^{\frac{p-1}{k}} - 1 \not\equiv 0(\bmod p)$, thus

$\left(\frac{a}{p}\right)_k = -1$.

In quadratic residue there is $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$, this is not surely tenable in residue of

higher degree, next we will proof ：

Theorem 2 $\forall a, b$, if$\left(\frac{a}{p}\right)_k, \left(\frac{b}{p}\right)_k$ don't both equal -1, $\left(\frac{a}{p}\right)_k \left(\frac{b}{p}\right)_k = \left(\frac{ab}{p}\right)_k$ is always

tenable.

Proof ： If $\left(\frac{a}{p}\right)_k = 1$, $\left(\frac{b}{p}\right)_k = 1$, assume that solutions of $x^k \equiv a(\bmod p)$ are

$x \equiv x_1(\bmod p)$,solutions of $x^k \equiv b(\bmod p)$ are $x \equiv x_2(\bmod p)$,

then $(x_1x_2)^k = x_1^k x_2^k \equiv ab(\mathrm{mod}\, p)$, that is $x^k \equiv ab(\mathrm{mod}\, p)$ also has solution, that is $\left(\frac{ab}{p}\right)_k = 1$. Here $\left(\frac{a}{p}\right)_k\left(\frac{b}{p}\right)_k = \left(\frac{ab}{p}\right)_k$ is tenable.

If $\left(\frac{a}{p}\right)_k = 1, \left(\frac{b}{p}\right)_k = -1$, assume the solution to $x^k \equiv a(\mathrm{mod}\, p)$ is $x \equiv x_1(\mathrm{mod}\, p)$, if $x^k \equiv ab(\mathrm{mod}\, p)$ has solution, assume the solution is $x \equiv x_2(\mathrm{mod}\, p)$, that is $x_2^k \equiv ab(\mathrm{mod}\, p)$. We say a^{-1} as the solution to $x \cdot a \equiv 1(\mathrm{mod}\, p)$.

Therefore $1 \equiv (x_1^{-1} \cdot x_1)^k = (x_1^{-1})^k \cdot x_1^k \equiv a \cdot (x_1^{-1})^k (\mathrm{mod}\, p)$, $(x_1^{-1})^k \equiv a^{-1}(\mathrm{mod}\, p)$. We can know from $x_2^k \equiv ab(\mathrm{mod}\, p)$ that $a^{-1} \cdot x_2^k \equiv a^{-1}ab \equiv b(\mathrm{mod}\, p)$. Because there is no solution to $x^k \equiv b(\mathrm{mod}\, p)$, so there is also no solution to $x^k \equiv a^{-1} \cdot x_2^k (\mathrm{mod}\, p)$. Neither is $(x_2^{-1} \cdot x)^k \equiv a^{-1}(\mathrm{mod}\, p)$ or $x_2^{-1} \cdot x \equiv x_1^{-1}(\mathrm{mod}\, p)$. But we have It is a contradiction $x^k \equiv ab(\mathrm{mod}\, p)$, Hence $\left(\frac{ab}{p}\right)_k = -1$. Hence $\left(\frac{a}{p}\right)_k\left(\frac{b}{p}\right)_k = \left(\frac{ab}{p}\right)_k$.

If $\left(\frac{a}{p}\right)_k = -1, \left(\frac{b}{p}\right)_k = -1$, we cannot decide whether $\left(\frac{ab}{p}\right)_k = 1$ or $\left(\frac{ab}{p}\right)_k = -1$. For example：if $k = 3$ and $p = 19$， we can know $\left(\frac{2}{19}\right)_3 = -1, \left(\frac{4}{19}\right)_3 = -1$ and $\left(\frac{2\times 4}{19}\right)_3 = \left(\frac{8}{19}\right)_3 = 1 = \left(\frac{2}{19}\right)_3 \times \left(\frac{4}{19}\right)_3$, in this condition $\left(\frac{a}{p}\right)_k\left(\frac{b}{p}\right)_k = \left(\frac{ab}{p}\right)_k$ is tenable. But we can also know $\left(\frac{2}{19}\right)_3 = -1, \left(\frac{5}{19}\right)_3 = -1$ and $\left(\frac{2\times 5}{19}\right)_3 = \left(\frac{10}{19}\right)_3 = -1 \neq \left(\frac{2}{19}\right)_3 \times \left(\frac{4}{19}\right)_3$, in this condition $\left(\frac{a}{p}\right)_k\left(\frac{b}{p}\right)_k = \left(\frac{ab}{p}\right)_k$ is not tenable. Hence, $\left(\frac{a}{p}\right)_k\left(\frac{b}{p}\right)_k = \left(\frac{ab}{p}\right)_k$ is not always tenable.

2. The solvability of $x^k \equiv a(\mathrm{mod}\, p)$

If k is an odd prime

If k is an odd prime, we have $(p-x)^k \equiv (-x)^k = -x^k \pmod p$. That means the first half of complete residue system modulo p is corresponding to the second half of complete residue system modulo p. So we only need to discuss the first half part of complete residue system modulo p here.

2.1.1 If $k = 3$

We have the following conclusions

Theorem 3 If $p \equiv -1 \pmod 3$, there is always $\left(\frac{a}{p}\right)_3 = 1$, if $p \equiv 1 \pmod 3$, there are only $\frac{p-1}{3}$ a in the complete residue system modulo p make $\left(\frac{a}{p}\right)_3 = 1$ tenable.

Proof: If $p \equiv 1 \pmod 3$, according to Euler **criterion**, for every a, There are 3 solutions to $x^3 \equiv a \pmod p$. For different a, the solution could not be the same. Hence there are only $\frac{p-1}{3}$ a make $\left(\frac{a}{p}\right)_3 = 1$ in a complete residue system modulo p.

If $p \equiv -1 \pmod 3$,we have $(3, p-1) = 1$. Therefore there is a solution to $3u + v(p-1) = 1$. We say them as u_0, v_0.

Then $a^1 = a^{3u_0 + v_0(p-1)} = \left(a^{u_0}\right)^3 \cdot \left(a^{v_0}\right)^{p-1} \equiv \left(a^{u_0}\right)^3 \pmod p$. Hence, there always exists solution to $x^3 \equiv a \pmod p$. Thus the theorem is tenable.

Thus, theorem **3** is tenable.

If $p \equiv 1 \pmod 3$,we also have following conclusions:

Corollary 1 If x_1, x_2 satisfy $x_1^3 \equiv 1 \pmod p$, $x_2^3 \equiv 1 \pmod p$, and also $x_1 \not\equiv x_2 \pmod p$, $x_1 \not\equiv 1 \pmod p$, $x_2 \not\equiv 1 \pmod p$, then $x_1^2 \equiv x_2 \pmod p$.

Proof : It is easy to know from above that, x_1, x_2 are two different solutions to $x^2 + x + 1 \equiv 0 \pmod p$. From $x_1^3 \equiv 1 \pmod p$ we have $(x_1^2)^3 = (x_1^3)^2 \equiv 1 \pmod p$

So x_1^2 also satisfy $x_1^3 \equiv 1(\mathrm{mod}\ p)$. Also, because $x^2 + x + 1 \equiv 0(\mathrm{mod}\ p)$ only has two solutions, $x_1^2 \equiv 1(\mathrm{mod}\ p), x_1^2 \equiv x_1(\mathrm{mod}\ p)$ are all impossible. Hence, $x_1^2 \equiv x_2(\mathrm{mod}\ p)$.

Corollary 2 If x satisfy $x^3 \equiv 1(\mathrm{mod}\ p)$, and also $x \not\equiv 1(\mathrm{mod}\ p)$, then $(x+1)^3 \equiv -1(\mathrm{mod}\ p)$, and also $(x-1)^3 \equiv (x+2)^3(\mathrm{mod}\ p)$.

Proof : If x satisfies $x^3 \equiv 1(\mathrm{mod}\ p)$ and $x \not\equiv 1(\mathrm{mod}\ p)$, x satisfies $x^2 + x + 1 \equiv 0(\mathrm{mod}\ p)$, so $(x+1)^3 = x^3 + 3x^2 + 3x + 1 \equiv 1 + 3(-1) + 1 = -1(\mathrm{mod}\ p)$

Also $(x+2)^3 - (x-1)^3 = (x+2-x+1)(x^2 + 4x + 4 + x^2 + x - 2 + x^2 - 2x + 1)$

$= 3(3x^2 + 3x + 3) \equiv 0(\mathrm{mod}\ p)$, that is $(x-1)^3 \equiv (x+2)^3(\mathrm{mod}\ p)$

Corollary 3 If there is $x_1^3 \equiv 1(\mathrm{mod}\ p)$, $x_2^3 \equiv 1(\mathrm{mod}\ p)$, and $x_1 \not\equiv x_2(\mathrm{mod}\ p)$, $x_1 \not\equiv 1(\mathrm{mod}\ p)$, $x_2 \not\equiv 1(\mathrm{mod}\ p)$, $1 \le x_1 < x_2 \le p-1$, then $x_1 + x_2 = p - 1$.

Proof : From Corollary 1, there is $x_1 + x_2 \equiv x_1 + x_1^2 \equiv -1(\mathrm{mod}\ p)$.

If $x_1, x_2 \ge \frac{p-1}{2}$, then according to Corollary 2, $(x_1+1)^3 \equiv -1(\mathrm{mod}\ p)$, $(x_2+1)^3 \equiv -1(\mathrm{mod}\ p)$. Because $x_1 + 1, x_2 + 1, > \frac{p-1}{2}$, so $p - (x_1+1), p - (x_2+1) \le \frac{p-1}{2}$, also $\left(p - (x_1+1)\right)^3 \equiv 1(\mathrm{mod}\ p), \left(p - (x_2+1)\right)^3 \equiv 1(\mathrm{mod}\ p)$, this is contradictory to $x^2 + x + 1 \equiv 0(\mathrm{mod}\ p)$ only has solutions x_1, x_2, and $x_1, x_2 \ge \frac{p-1}{2}$, thus there is $1 \le x_1 < \frac{p-1}{2}, 1 < x_2 \le p-1$,

Thus $x_1 + x_2 < \frac{p-1}{2} + p - 1 = \frac{3(p-1)}{2}$, thus $x_1 + x_2 = p - 1$.

2. 1. 2 If k is an odd prime and $k > 3$

We can reach similar conclusions:

Theorem 4 If $p \not\equiv 1(\mathrm{mod}\, k)$, $\left(\frac{a}{p}\right)_k = 1$ is tenable; if $p \equiv 1(\mathrm{mod}\, k)$, there are $\frac{p-1}{k}$

a in complete residue system modulo p make $\left(\frac{a}{p}\right)_k = 1$ tenable.

Proof : If $p \equiv 1(\bmod k)$, according to Euler criterion, for every a, There are k solutions to $x^k \equiv a(\bmod p)$. For different a, the solution could not be the same. Hence there are only $\frac{p-1}{k}$ a make $\left(\frac{a}{p}\right)_k = 1$ in a complete residue system modulo p.

If $p \not\equiv 1(\bmod k)$,we have $(k, p-1) = 1$. Therefore there is a solution to $uk + v(p-1) = 1$. We say them as u_0, v_0.

Then $a^1 = a^{u_0 k + v_0 (p-1)} = \left(a^{u_0}\right)^k \cdot \left(a^{v_0}\right)^{p-1} \equiv \left(a^{u_0}\right)^k (\bmod p)$. Hence, there always exists solution to $x^k \equiv a(\bmod p)$. Thus the theorem is tenable.

We can also popularize this Corollary:

Corollary 4 If x_i ($i = 1, 2, \ldots, k-1$) meet $x_i^k \equiv 1(\bmod p)$ ($i = 1, 2, \ldots, k-1$) and $x_i \not\equiv 1(\bmod p)$. $\forall i \neq j$ ($i, j = 1, 2, \ldots, k-1$), $x_i \not\equiv x_j (\bmod p)$. Then $\forall i, j$ ($i, j = 1, 2, \ldots, k-1$), $\exists n$ ($n = 1, 2, \ldots, k-1$), $\ni x_i^n \equiv x_j (\bmod p)$.

Proof : It is easy to know from above that x_i are the $k-1$ solutions to $\sum_{i=1}^{k} x^{k-i} \equiv 0(\bmod p)$. From $x_i^k \equiv 1(\bmod p)$ there is $(x_i^2)^k = (x_i^k)^2 \equiv 1(\bmod p)$, $(x_i^3)^k = (x_i^k)^3 \equiv 1(\bmod p)$, ..., $(x_i^{k-1})^k = (x_i^k)^{k-1} \equiv 1(\bmod p)$, so $x_i^2, x_i^3, \ldots\ldots, x_i^{k-1}$ also satisfy $x^k \equiv 1(\bmod p)$. Also because $\sum_{i=1}^{k} x^{k-i} \equiv 0(\bmod p)$ only has $k-1$ solutions, $\forall i \in [2, k-1]$ and $i \in Z$, $x_1^i \equiv 1(\bmod p)$ and to $\forall i, j \in [2, k-1]$, $i, j \in Z$ and $i \neq j$, $x_1^i \equiv x_1^j (\bmod p)$ are all impossible, thus $\forall i, j$ ($i, j = 1, 2, \ldots, k-1$), $\exists n$ ($n = 1, 2, \ldots, k-1$), $\ni x_i^n \equiv x_j (\bmod p)$.

Corollary 5 If x_i ($i = 1, 2, \ldots, k-1$) meet $x_i^k \equiv 1(\bmod p)$ ($i = 1, 2, \ldots, k-1$)and

$x_i \not\equiv 1(\mathrm{mod}\, p)$. $\forall i \neq j$ $(i, j = 1,2,\ldots, k-1)$, $x_i \not\equiv x_j(\mathrm{mod}\, p)$. then we have

$\sum_{i=1}^{k-1} x_i \equiv -1(\mathrm{mod}\, p)$, $\sum_{i,j=1}^{k-1} x_i x_j \equiv 1(\mathrm{mod}\, p)$, ..., $\sum_{j=1}^{k-1} \frac{\prod_{i=1}^{k-1} x_i}{x_j} \equiv -1(\mathrm{mod}\, p)$,

$\prod_{i=1}^{k-1} x_i \equiv 1(\mathrm{mod}\, p)$.

Proof : It is easy to know from above that x_i are the $k-1$ solutions to

$\sum_{i=1}^{k} x^{k-i} \equiv 0(\mathrm{mod}\, p)$. Therefore $\prod_{i=1}^{k-1}(x - x_i) = x^{k-1} - \sum_{i=1}^{k-1} x_i \cdot x^{k-2} + \sum_{1 \le i, j \le k-1} x_i x_j \cdot x^{k-3} -$ ...

$-\sum_{j=1}^{k-1} \frac{\prod_{i=1}^{k-1} x_i}{x_j} + \prod_{i=1}^{k-1} x_i \cdot x \equiv \sum_{i=1}^{k-1} x^i (\mathrm{mod}\, p)$. Hence $\sum_{i=1}^{k-1} x_i \equiv -1(\mathrm{mod}\, p)$,

$\sum_{i,j=1}^{k-1} x_i x_j \equiv 1(\mathrm{mod}\, p)$, ..., $\sum_{j=1}^{k-1} \frac{\prod_{i=1}^{k-1} x_i}{x_j} \equiv -1(\mathrm{mod}\, p)$, $\prod_{i=1}^{k-1} x_i \equiv 1(\mathrm{mod}\, p)$.

2. 2 If $k = 2^n$

If $k = 2^n$, because $(p - x)^{2^n} \equiv (-x)^{2^n} = x^{2^n}$, that is the first half of complete residue system of 2^n degree modulo p is corresponding to the second half of complete residue system of 2^n degree modulo p. So we only need to discuss the first half part of complete residue system modulo p here.

So we only need to discuss the first half part of complete residue system of 2^n degree modulo p here.

1. 2. 1 If $n = 1, k = 2$

This is the quadratic residue that we are familiar with. Theories of it is already quite perfect, here we will add some more.

Theorem 5 : To $\forall$ x_1, x_2, $x_1 \not\equiv x_2(\mathrm{mod}\, p)$, and $1 \le x_1 < x_2 \le \frac{p-1}{2}$, there is $x_1^2 \not\equiv x_2^2(\mathrm{mod}\, p)$. If $p \equiv -1(\mathrm{mod}\, 4)$, to $\forall$ x_1, x_2, $x_1 \not\equiv x_2(\mathrm{mod}\, p)$,and also, we all

have $x_1^2 \not\equiv -x_2^2 (\mathrm{mod}\, p)$. If $p \equiv 1(\mathrm{mod}\, 4)$, to $\forall\ x_1$, $\exists\ x_2$, and also $x_1 \not\equiv x_2 (\mathrm{mod}\, p)$, make $x_1^2 \equiv -x_2^2 (\mathrm{mod}\, p)$ tenable.

Proof : Assume $\exists\ x_1, x_2$, and also $x_1 \not\equiv x_2 (\mathrm{mod}\, p)$, make $x_1^2 \equiv x_2^2 (\mathrm{mod}\, p)$ tenable, then $p \mid x_2^2 - x_1^2 = (x_2 + x_1)(x_2 - x_1)$, take $1 \le x_1 < x_2 \le p-1$, then $1 \le x_2 - x_1 < p-1$, $1 \le x_2 + x_1 < 2(p-1)$, so $x_2 + x_1 = p$. Also because $(p-x)^2 = (-x)^2 = x^2$, so $p = 2x_2 = 2x_1$, this is contradictory to that p is an odd prime. Hence, there is no x_1, x_2 , $x_1 \not\equiv x_2 (\mathrm{mod}\, p)$, make $x_1^2 \equiv x_2^2 (\mathrm{mod}\, p)$ tenable. Assume $\exists\ x_1, x_2$, and $x_1 \not\equiv x_2 (\mathrm{mod}\, p)$, make $x_1^2 \equiv -x_2^2 (\mathrm{mod}\, p)$ tenable, then $p \mid x_2^2 + x_1^2$, because p is an odd prime, $p \equiv 1(\mathrm{mod}\, 4)$; on the contrary, if $p \equiv 1(\mathrm{mod}\, 4)$, $\frac{p-1}{2} \equiv 0(\mathrm{mod}\, 2)$. If there is $\left(\frac{a}{p}\right) = 1$, then there is $a^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\, p)$, and also $(-a)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\, p)$, that is $\left(\frac{-a}{p}\right) = 1$. Proof is finished.

From above we can know that , if $p \equiv -1(\mathrm{mod}\, 4)$, absolute value of quadratic residue modulo p can range through the first part of complete residue system modulo p, but the opposite numbers are not its residue at the same time . And if $p \equiv 1(\mathrm{mod}\, 4)$, absolute value of quadratic residue modulo p cannot range through the first part of complete residue systemmodulo p, but the opposite numbers are among residue modulo p. Because $\left(\frac{n^2}{p}\right) = 1$, we can have the following corollary：

Corollary 6 If $p \equiv -1(\mathrm{mod}\, 4)$, $\left(\frac{-n^2}{p}\right) = -1$. If $p \equiv 1(\mathrm{mod}\, 4)$时, $\left(\frac{-n^2}{p}\right) = 1$. that is $\left(\frac{-n^2}{p}\right) = (-1)^{\frac{p-1}{2}}$. Specially, if $n = 1$, there is $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Theorem 6 If $p \equiv -1(\mathrm{mod}\,4)$, $a \equiv \left(\frac{p+1}{4}\right)^n (\mathrm{mod}\, p)(n \in N) \Rightarrow \left(\frac{a}{p}\right) = 1$; if

$p \equiv 1(\mathrm{mod}\,4)$, $a \equiv \left(\frac{p-1}{4}\right)^n$ or $-\left(\frac{p-1}{4}\right)^n (\mathrm{mod}\, p)\ (n \in N) \Rightarrow \left(\frac{a}{p}\right) = 1$.

Proof : If $p \equiv -1(\mathrm{mod}\,4)$, $\left(\frac{p+1}{2}\right)^2 = \frac{p+1}{4}(p+1) \equiv \frac{p+1}{4}(\mathrm{mod}\, p)$, that

is $x^2 \equiv \frac{p+1}{4}(\mathrm{mod}\, p)$ must have solution. If $\left(\frac{a}{p}\right) = 1$, $\left(\frac{a^n}{p}\right) = \left(\frac{a}{p}\right)^n = 1$, that

is $\left(\frac{p+1}{4}\right)^n \left(n \in N^*\right)$ is also quadratic residue modulo p, also 1 is quadratic residue modulo

p, thus $\left(\frac{p+1}{4}\right)^n \left(n \in N\right)$ are all the quadratic residue modulo p.

If $p \equiv 1(\mathrm{mod}\,4)$, $\left(\frac{p-1}{2}\right)^2 = \frac{p-1}{4}(p-1) \equiv -\frac{p-1}{4}(\mathrm{mod}\, p)$, that

is $x^2 \equiv -\frac{p-1}{4}(\mathrm{mod}\, p)$ must has solution. According to Theorem1. 1. 1（2）,

$x^2 \equiv \frac{p-1}{4}(\mathrm{mod}\, p)$ also has solution. If $\left(\frac{a}{p}\right) = 1$, $\left(\frac{a^n}{p}\right) = \left(\frac{a}{p}\right)^n = 1$, that

is $\left(\frac{p-1}{4}\right)^n$,$-\left(\frac{p-1}{4}\right)^n \left(n \in N^*\right)$ is also quadratic residue modulo p, also ,1, -1 is

quadratic residue modulo p. Thus, $\left(\frac{p-1}{4}\right)^n$,$-\left(\frac{p-1}{4}\right)^n \left(n \in N\right)$ are all the quadratic

residue of p.

But whether $a \equiv \left(\frac{p+1}{4}\right)^n (\mathrm{mod}\, p)\left(n \in N\right)$、 $a \equiv \left(\frac{p-1}{4}\right)^n$ or

$-\left(\frac{p-1}{4}\right)^n (\mathrm{mod}\, p)\ \left(n \in N\right)$ is also the necessary condition of $\left(\frac{a}{p}\right) = 1$ when

$p \equiv -1(\mathrm{mod}\,4)$、 $p \equiv 1(\mathrm{mod}\,4)$时$\left(\frac{a}{p}\right) = 1$, this is still a conclusion that we have not

proved in this paper.

Theorem 7 $\left(\frac{3}{p}\right)=1\Leftrightarrow p\equiv 1$ or $-1(\mathrm{mod}12)$, $\left(\frac{5}{p}\right)=1\Leftrightarrow p\equiv 1$ or $-1(\mathrm{mod}10)$,

$\left(\frac{7}{p}\right)=1\Leftrightarrow p\equiv 1$ or -1, 3 or -3, 9 or $-9(\mathrm{mod}28)$.

Proof : If $a=3$,we can know $\left(\frac{p}{3}\right)=1\Leftrightarrow p\equiv 1(\mathrm{mod}3)$. According to law of quadratic reciprocity, $\left(\frac{p}{3}\right)\left(\frac{3}{p}\right)=(-1)^{\frac{3-1}{2}\cdot\frac{p-1}{2}}=(-1)^{\frac{p-1}{2}}$. Therefore $\left(\frac{3}{p}\right)=1\Leftrightarrow\begin{cases}\left(\frac{p}{3}\right)=1\\ \frac{p-1}{2}\equiv 0(\mathrm{mod}2)\end{cases}$

or $\begin{cases}\left(\frac{p}{3}\right)=-1\\ \frac{p-1}{2}\equiv 1(\mathrm{mod}2)\end{cases}$. $\begin{cases}p\equiv 1(\mathrm{mod}3)\\ p\equiv 1(\mathrm{mod}4)\end{cases}$ or $\begin{cases}p\equiv -1(\mathrm{mod}3)\\ p\equiv -1(\mathrm{mod}4)\end{cases}$. Hence $p\equiv 1(\mathrm{mod}12)$ or

$p\equiv -1(\mathrm{mod}12)$.

If $a=5$,we can know $\left(\frac{p}{5}\right)=1\Leftrightarrow p\equiv 1(\mathrm{mod}5)$ or $p\equiv -1(\mathrm{mod}5)$. According to law of quadratic reciprocity, $\left(\frac{p}{5}\right)\left(\frac{5}{p}\right)=(-1)^{\frac{5-1}{2}\cdot\frac{p-1}{2}}=1$. Therefore $\left(\frac{5}{p}\right)=1\Leftrightarrow\left(\frac{p}{5}\right)=1$.

$p\equiv 1(\mathrm{mod}5)$ or $p\equiv -1(\mathrm{mod}5)$. In addition, $p\equiv 1(\mathrm{mod}2)$. Hence, $p\equiv 1(\mathrm{mod}10)$ or

$p\equiv -1(\mathrm{mod}10)$.

If $a=7$, we can know $\left(\frac{p}{7}\right)=1\Leftrightarrow p\equiv 1(\mathrm{mod}7)$ or $p\equiv -3(\mathrm{mod}7)$ or $p\equiv 2(\mathrm{mod}7)$.

According to law of quadratic reciprocity, $\left(\frac{p}{7}\right)\left(\frac{7}{p}\right)=(-1)^{\frac{7-1}{2}\cdot\frac{p-1}{2}}=(-1)^{\frac{p-1}{2}}$. Therefore

$\left(\frac{7}{p}\right)=1\Leftrightarrow\begin{cases}\left(\frac{p}{7}\right)=1\\ \frac{p-1}{2}\equiv 0(\mathrm{mod}2)\end{cases}$ or $\begin{cases}\left(\frac{p}{7}\right)=-1\\ \frac{p-1}{2}\equiv 1(\mathrm{mod}2)\end{cases}$.

$\begin{cases}p\equiv 1or-3or2(\mathrm{mod}7)\\ p\equiv 1(\mathrm{mod}4)\end{cases}$ or $\begin{cases}p\equiv -1or3or-2(\mathrm{mod}7)\\ p\equiv -1(\mathrm{mod}4)\end{cases}$.

Hence $p \equiv 1(\mathrm{mod}\,28)$ or $p \equiv -1(\mathrm{mod}\,28)$ or $p \equiv 3(\mathrm{mod}\,28)$ or $p \equiv -3(\mathrm{mod}\,28)$ or $p \equiv 9(\mathrm{mod}\,28)$ or $p \equiv -9(\mathrm{mod}\,28)$.

We can get a further conclusion according to the discussion above.

Theorem 8 Postulate a to be an odd prime , then:

If $a \equiv -1(\mathrm{mod}\,4)$, $p \equiv \pm\left(\frac{a-1}{2}\right)^n (\mathrm{mod}\,4a) \Rightarrow \left(\frac{a}{p}\right) = 1, n \in N$.

If $a \equiv 1(\mathrm{mod}\,4)$, $p \equiv \pm\left(\frac{a-1}{4}\right)^n (\mathrm{mod}\,2a) \Rightarrow \left(\frac{a}{p}\right) = 1, n \in N$.

Proof: If $a \equiv -1(\mathrm{mod}\,4)$, according to law of quadratic reciprocity, we have

$\left(\frac{a}{p}\right)\left(\frac{p}{a}\right) = (-1)^{\frac{a-1}{2}\frac{p-1}{2}} = \left((-1)^{\frac{a-1}{2}}\right)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}}$. So

$\left(\frac{a}{p}\right) = 1 \Leftrightarrow \begin{cases} \left(\frac{p}{a}\right) = 1 \\ p \equiv 1(\mathrm{mod}\,4) \end{cases}$ or $\begin{cases} \left(\frac{p}{a}\right) = -1 \\ p \equiv -1(\mathrm{mod}\,4) \end{cases}$. According to Theorem 6, if

$a \equiv -1(\mathrm{mod}\,4)$, $p \equiv \left(\frac{a+1}{4}\right)^n (\mathrm{mod}\,a)(n \in N) \Rightarrow \left(\frac{p}{a}\right) = 1$. According to Theorem 5,

$p \equiv -\left(\frac{a+1}{4}\right)^n (\mathrm{mod}\,a)(n \in N) \Rightarrow \left(\frac{p}{a}\right) = -1$, so $\begin{cases} p \equiv \left(\frac{a+1}{4}\right)^n (\mathrm{mod}\,a)(n \in N) \\ p \equiv 1(\mathrm{mod}\,4) \end{cases}$ or

$\begin{cases} p \equiv -\left(\frac{a+1}{4}\right)^n (\mathrm{mod}\,a)(n \in N) \Rightarrow \left(\frac{p}{a}\right) = 1 \\ p \equiv -1(\mathrm{mod}\,4) \end{cases}$. $a \not\equiv -1(\mathrm{mod}8)$, $\frac{a+1}{4} \equiv 1(\mathrm{mod}\,2)$,

$\pm\left(\frac{a+1}{4}\right)^n \equiv 1(\mathrm{mod}\,2)$, $\begin{cases} p \equiv \left(\frac{a+1}{4}\right)^n (\mathrm{mod}\,a) \\ p \equiv \left(\frac{a+1}{4}\right)^n (\mathrm{mod}\,4) \end{cases}$ or $\begin{cases} p \equiv -\left(\frac{a+1}{4}\right)^n (\mathrm{mod}\,a) \\ p \equiv -\left(\frac{a+1}{4}\right)^n (\mathrm{mod}\,4) \end{cases}$.

Hence $p \equiv \left(\frac{a+1}{2}\right)^n (\mathrm{mod}\,4a)$ or $p \equiv -\left(\frac{a+1}{2}\right)^n (\mathrm{mod}\,4a) \Rightarrow \left(\frac{a}{p}\right) = 1$.

If $a \equiv 1(\bmod 4)$, $\left(\frac{a}{p}\right)\left(\frac{p}{a}\right) = (-1)^{\frac{a-1}{2}\frac{p-1}{2}} = \left((-1)^{\frac{a-1}{2}}\right)^{\frac{p-1}{2}} = 1$. So $\left(\frac{a}{p}\right) = 1 \Leftrightarrow \left(\frac{p}{a}\right) = 1.$

According to Theorem 6, if $a \equiv 1(\bmod 4)$, $p \equiv \left(\frac{a-1}{4}\right)^n$ or

$-\left(\frac{a-1}{4}\right)^n (\bmod a)$ $(n \in N) \Rightarrow \left(\frac{p}{a}\right) = 1$. So $p \equiv \left(\frac{a-1}{4}\right)^n$ or

$-\left(\frac{a-1}{4}\right)^n (\bmod a)$ $(n \in N) \Rightarrow \left(\frac{a}{p}\right) = 1$. $p \equiv 1(\bmod 2)$, $a \not\equiv 1(\bmod 8)$, so

$\frac{a-1}{4} \equiv 1(\bmod 2)$, $\pm\left(\frac{a-1}{4}\right)^n \equiv 1(\bmod 2)$. $\begin{cases} p \equiv \pm\left(\frac{a-1}{4}\right)^n (\bmod a) \\ p \equiv 1(\bmod 2) \end{cases}$.

$\begin{cases} p \equiv \pm\left(\frac{a-1}{4}\right)^n (\bmod a) \\ p \equiv \pm\left(\frac{a-1}{4}\right)^n (\bmod 2) \end{cases}$. Hence, $p \equiv \pm\left(\frac{a-1}{4}\right)^n (\bmod 2a)$.

2.2 $n \geq 2$

About the solvability of $x^{2^n} \equiv a(\bmod p)$ when $n \geq 2$, we have following conclusions:

Theorem 9 If $p \equiv -1(\bmod 4)$, there is $\left(\frac{a}{p}\right)_{2^n} = \left(\frac{a}{p}\right)$.

Proof : According to Theorem 1. 2. 1(1), if $p \equiv -1(\bmod 4)$, absolute value of quadratic residue modulo p can range through the first part of complete residue system modulo p, and the residue of 4 degree modulo p is the quadratic residue modulo p of quadratic residue modulo p, so the residue of 4 degree modulo p is the quadratic residue modulo the first half of complete residue system modulo p. And it is quadratic residue modulo p, that is $\left(\frac{a}{p}\right)_4 = \left(\frac{a}{p}\right)$.

In the same way there is $\left(\frac{a}{p}\right)_8 = \left(\frac{a}{p}\right)_4$, $\left(\frac{a}{p}\right)_{16} = \left(\frac{a}{p}\right)_8$, ..., $\left(\frac{a}{p}\right)_{2^n} = \left(\frac{a}{p}\right)_{2^{n-1}}$.

By induction, there is, $\left(\frac{a}{p}\right)_{2^n} = \left(\frac{a}{p}\right)$.

If $p \equiv 1(\mathrm{mod}\,4)$, opposite numbers in residue modulo p always exist at the same time.

But there is $x^2 \equiv (-x)^2 (\mathrm{mod}\ p)$, so when n increases, the opposite numbers in residue of 2^{n-1} degree will become the same value in the residue of 2^n degree, but this will not absolutely cause the opposite numbers in residue of higher degree to disappear. Following will be the proof :

Theorem 10 If $\forall\ 1 \le x_1 \le \frac{p-1}{2}$ there is $1 \le x_2 \le \frac{p-1}{2}$ make $x_1^{2^n} \equiv -x_2^{2^n} (\mathrm{mod}\ p)$ tenable. Then we have $p \equiv 1(\mathrm{mod}\,2^{n+1})$.

Also, if $p \equiv 1(\mathrm{mod}\,2^{n+1})$, $\forall\ 1 \le x_1 \le \frac{p-1}{2}$ there is $1 \le x_2 \le \frac{p-1}{2}$ make $x_1^{2^n} \equiv -x_2^{2^n} (\mathrm{mod}\ p)$ tenable.

Proof : If $x_1^{2^n} \equiv -x_2^{2^n} (\mathrm{mod}\ p)$, Then we can assume $p = 2^m t + 1$ and t is an odd number. Then $\left(x_1^{2^n}\right)^t \equiv \left(-x_2^{2^n}\right)^t = -\left(x_2^{2^n}\right)^t (\mathrm{mod}\ p)$, $x_1^{2^n t} \equiv -x_2^{2^n t} (\mathrm{mod}\ p)$. Suppose $m \le n$, then $x_1^{2^n t} = \left(x_1^{2^m t}\right)^{2^{n-m}} \equiv 1(\mathrm{mod}\ p)$, $x_2^{2^n t} = \left(x_2^{2^m t}\right)^{2^{n-m}} \equiv 1(\mathrm{mod}\ p)$. It is contradictory to $x_1^{2^n t} \equiv -x_2^{2^n t} (\mathrm{mod}\ p)$. Therefore $m \ge n+1$, $p \equiv 1(\mathrm{mod}\,2^{n+1})$.

On the contrary, if $p \equiv 1(\mathrm{mod}\,2^{n+1})$, if there is $x_1^{2^n} \equiv a(\mathrm{mod}\ p)$, then according to Euler criterion, which we will popularize later, there is $a^{\frac{p-1}{2^n}} \equiv 1(\mathrm{mod}\ p)$, and because $p \equiv 1(\mathrm{mod}\,2^{n+1})$, so $\frac{p-1}{2^n} \equiv 0(\mathrm{mod}\,2)$, so $(-a)^{\frac{p-1}{2^n}} = a^{\frac{p-1}{2^n}} \equiv 1(\mathrm{mod}\ p)$, that is $x_1^{2^n} \equiv -a(\mathrm{mod}\ p)$ also has solution, that is $\exists x_2$ that satisfies $x_1^{2^n} \equiv -x_2^{2^n} (\mathrm{mod}\ p)$.

Now we assume $1 \le x_1 \le \frac{p-1}{2}$, $x_1^{2^n} \equiv -x_2^{2^n} (\mathrm{mod}\ p)$. If $\frac{p-1}{2} \le x_2 \le p-1$, then $(p-x_2)^{2^n} \equiv (-x_2)^{2^n} = x_2^{2^n} (\mathrm{mod}\ p)$, $x_1^{2^n} \equiv -x_2^{2^n} \equiv -(p-x_2)^{2^n} (\mathrm{mod}\ p)$, and $1 \le p - x_2 \le \frac{p-1}{2}$, that is there always exists x_2 $1 \le x_2 \le \frac{p-1}{2}$, meet $x_1^{2^n} \equiv -x_2^{2^n} (\mathrm{mod}\ p)$.

Proof is finished.

2. 3 If k is q^n (q is an odd prime)

Similar to the discussion about $k=2^n$ above, we can conclude some properties when $k=q^n$. The properties have some differences when the index is odd or even. The condition when $n=1, k=q^n$ has been discussed in 1. 1. Here we always postulate $n\geq 2$.

Theorem 11 If $p \not\equiv 1(\mathrm{mod}\, q)$, then $\left(\frac{a}{p}\right)_{q^n}=1$.

Proof : If $p \not\equiv 1(\mathrm{mod}\, q)$, according to theorem **1. 3. 1(1)**, residue of q degree modulo p equal complete residue system modulo p, and residue of q^2 degree modulo p equal residue of q^2 degree of residue of q^2 degree modulo p, that is residue of q degree of complete residue system modulo, it is still complete residue system modulo p. By conduction, we can know that residue of q^n degree modulo p equal complete residue system modulo p. That is $\left(\frac{a}{p}\right)_{q^n}=\left(\frac{a}{p}\right)_{q}=1$

Theorem 12 If $p\equiv 1(\mathrm{mod}\, q^n)$ but $p \not\equiv 1(\mathrm{mod}\, q^{n+1})$, if $m\geq n$, there is $\left(\frac{a}{p}\right)_{q^m}=\left(\frac{a}{p}\right)_{q^n}$.

Proof : If $p\equiv 1(\mathrm{mod}\, q^n)$ but $p \not\equiv 1(\mathrm{mod}\, q^{n+1})$, if x_1, x_2 satisfy $x_1^{q^n} \not\equiv x_2^{q^n} (\mathrm{mod}\, p)$ but $x_1^{q^{n+1}} \equiv x_2^{q^{n+1}} (\mathrm{mod}\, p)$, that is $\left(x_1^{q^n}\right)^q \equiv \left(x_2^{q^n}\right)^q (\mathrm{mod}\, p)$, assume $x_1^{q^n} \equiv a x_2^{q^n} (\mathrm{mod}\, p)$, because $x_1^{q^n} \not\equiv x_2^{q^n} (\mathrm{mod}\, p)$, so $a \not\equiv 1(\mathrm{mod}\, p)$, then $\left(x_1^{q^n}\right)^q \equiv \left(a x_2^{q^n}\right)^q = a^q \left(x_2^{q^n}\right)^q (\mathrm{mod}\, p)$, and because $\left(x_1^{q^n}\right)^q \equiv \left(x_2^{q^n}\right)^q (\mathrm{mod}\, p)$, so $a^q \equiv 1(\mathrm{mod}\, p)$, in the same way, assume $x_2^{q^n} \equiv b x_1^{q^n} (\mathrm{mod}\, p)$, there is $b^q \equiv 1(\mathrm{mod}\, p)$, also, there is $(a^m)^q \equiv 1(\mathrm{mod}\, p)$, $(b^m)^q \equiv 1(\mathrm{mod}\, p)$, here $m \in N$

and $1 \le m \le q-1$, among a^m, b^m there are at least $q-1$ numbers aren't congruent to each other, thus, to $\forall a$,there is $a^q \equiv 1 (\mathrm{mod}\, p)$. But here $x_1^{q^n} \equiv 1 \equiv x_2^{q^n} (\mathrm{mod}\, p)$, it's a contradixtion, thus $\left(x_1^{q^n}\right)^q \not\equiv \left(x_2^{q^n}\right)^q (\mathrm{mod}\, p)$.

In residue of q^n degree, the numbers that aren't congruent to each other are still not congruent to each other after multiply itself q times. Hence, the theorem is tenable.

2. 4 If k is a positive integer which is not smaller than 2

Now we popularize k to a positive integer that is not smaller than 2. Assume $k = \prod_{i=1}^{n} p_i^{m_i}$,

it is easy to know that the necessary condition of $\left(\frac{a}{p}\right)_k = 1$ is to $\forall i \in [1,n]$ and $i \in Z$,

$\left(\frac{a}{p}\right)_{p_i^{m_i}} = 1$. Otherwise , if $\left(\frac{a}{p}\right)_{p_j^{m_j}} = -1$, that is

$x^{p_j^{m_j}} \equiv a (\mathrm{mod}\, p)$ has no solutions, then $x^k = (x^q)^{p_j^{m_j}} \equiv a (\mathrm{mod}\, p)$ also has no solution.

Here $q = \frac{\prod_{i=1}^{n} p_i^{m_i}}{p_j^{m_j}}$.

Next we will proof that it is also its sufficient condition.

Theorem 13 The sufficient and necessary condition of

$\left(\frac{a}{p}\right)_k = 1$ is to $\forall i \in [1,n]$ and $i \in Z$, $\left(\frac{a}{p}\right)_{p_i^{m_i}} = 1$.

Proof ： The necessarity has already been proved. Now we will proof the sufficiency.
First we need to proof a lemma.

Lemma If $\left(\frac{a}{p}\right)_{k_1} = 1$, $\left(\frac{a}{p}\right)_{k_2} = 1$, that is $x^{k_1} \equiv a (\mathrm{mod}\, p)$, $x^{k_2} \equiv a (\mathrm{mod}\, p)$ all

have solution, and $(k_1, k_2) = 1$. Then $\left(\frac{a}{p}\right)_{k_1 k_2} = 1$, that is $x^{k_1 k_2} \equiv a (\mathrm{mod}\, p)$ also has

solution.

Proof ： If $(k_1, k_2) = 1$时, $mk_1 + nk_2 = 1$ must have solution, we can assume they are

m_1, m_2, and $s = \alpha(p-1) + m_1$, $t = \beta(p-1) + n_1$, here α, β are positive integers

make $s,t>0$, because $x^{k_1}\equiv a(\mathrm{mod}\ p)$ has solution, so

$x^{k_1k_2t}\equiv a^{k_2t}\equiv a^{k_2n_1}(\mathrm{mod}\ p)$ also has solution, in the same way,

$x^{k_1k_2s}\equiv a^{k_1s}\equiv a^{k_1m_1}(\mathrm{mod}\ p)$ also has solution, thus

$(x^{s+t})^{k_1k_2}=x^{k_1k_2t}x^{k_1k_2s}\equiv a^{k_2n_1}a^{k_1m_1}=a^{k_1m_1+k_2n_1}=a(\mathrm{mod}\ p)$, that is $x^{k_1k_2}\equiv a(\mathrm{mod}\ p)$ has solution.

The lemma is easy to be popularized：if $\left(\frac{a}{p}\right)_{k_1}=1$, $\left(\frac{a}{p}\right)_{k_2}=1$, ……, $\left(\frac{a}{p}\right)_{k_n}=1$,

and $k_1,k_2,\ldots\ldots,k_n$ are relatively primes to each other, $k=\prod_{i=1}^{n}k_i$, then $\left(\frac{a}{p}\right)_{k}=1.$

Now back to the original problem, because $p_1^{m_1}, p_2^{m_2},\ldots\ldots, p_n^{m_n}$ are relatively primes to each other , thus the theorem is tenable.

Acknowledgements

We would like to thank Mr. Shi for guiding us when we work with this problem. He also provided some references. We thank our classmate Zhuohe Liu for helping us check the paper carefully and tipeset the paper. We also thank our classmate Sunshine Lee for teaching us some basic skills of programming, which provide much help for our research.

References

[1] G.H.Hardy, E.M.Wright. An Introduction to the Theory of Numbers [M]. Posts & Telecom Press. 2008.

[2] Chengdong Pan, Chengbiao Pan. Elementary Number Theory [M]. Peking University Press. 2004.

[3] Loo-keng Hua. Guidance of Number Theory [M]. Beijing: Science Press, 1979.