MODULAR LOGARITHM UNEQUAL

WU SHENG-PING

Abstract. The main idea of this article is simply calculating integer functions in module. The algebraic in the integer modules is studied in completely new style. By a careful construction, a result is proven that two finite numbers are with unequal logarithms in a corresponding module, and is applied to solving a kind of high degree diophantine equation.

In this paper, p is prime, C means a constant. All numbers that are indicated by Latin letters are integers unless with further indication.

1. Function in module

Theorem 1.1. *Define the congruence class* [1] *in the form:*

$$[a]_q := [a + kq]_q, \forall k \in \mathbf{Z}$$
$$[a = b]_q : [a]_q = [b]_q$$
$$[a]_q[b]_{q'} := [x]_{qq'} : [x = a]_q, [x = b]_{q'}, (q, q') = 1$$

then

$$[a + b]_q = [a]_q + [b]_q$$
$$[ab]_q = [a]_q \cdot [b]_q$$
$$[a + c]_q[b + d]_{q'} = [a]_q[b]_{q'} + [c]_q[d]_{q'}, (q, q') = 1$$
$$[ka]_q[kb]_{q'} = k[a]_q[b]_{q'}, (q, q') = 1$$

Theorem 1.2. *The integer coefficient power-analytic functions modulo p are all the functions from mod p to mod p*

$$[x^0 = 1]_p$$
$$[f(x) = \sum_{n=0}^{p-1} f(n)(1 - (x - n)^{p-1})]_p$$

Theorem 1.3. *(Modular Logarithm) Define*

$$[\mathtt{lm}_a(x) := y]_{p^{m-1}(p-1)} : [a^y = x]_{p^m}$$
$$[E := \sum_{i=0}^{m'} p^i/i!]_{p^m}$$
$$1 << m << m'$$

then

$$[E^x = \sum_{i=0}^{m'} x^i p^i/i!]_{p^m}$$

Date: Sep 1, 2024.
Key words and phrases. Diophantine Equation; Discrete Logarithm.

$$[\mathtt{lm}_E(1-xp) = -\sum_{i=1}^{m'}(xp)^i/(ip)]_{p^{m-1}}$$

$$[Q(q)\mathtt{lm}(1-xq) = -\sum_{i=1}^{m'}(xq)^i/i]_{q^m}$$

$$Q(q) := \prod_{p|q}[p]_{p^m}$$

Define

$$[\mathtt{lm}(x) := \mathtt{lm}_e(x)]_{p^{m-1}}$$

e is the generating element in mod p and meets

$$[e^{1-p^{m'}} = E]_{p^m}$$

It's proven by comparing to the Taylor expansions of real exponent and logarithm (especially on the coefficients).

Definition 1.4.

$$[\mathtt{lm}(px) := p\mathtt{lm}(x)]_{p^m}$$

Definition 1.5.

$$P(q) := \prod_{p|q} p$$

Definition 1.6.

$${}_q[x] := y : [x = y]_q, 0 \le y < q$$

2. Unequal Logarithms of Two Numbers

Theorem 2.1. *If*

$$b + a < q$$
$$a > b > 0$$
$$(a, b) = (a, q) = (b, q) = 1$$

then

$$[\mathtt{lm}(a) \neq \mathtt{lm}(b)]_q$$

Proof. Define

$$r := P(q)$$
$$\beta := \prod_{p:p|q}[(a/b)^{v_p - 1}]_{p^m}, \quad 1 << m$$
$$v_p := [p]_{p^m(p-1)}$$

Set

$$0 \le x, x' < qr + r$$
$$0 \le y, y' < qr + r$$
$$d := (x - x', q^m)$$

Consider

$$[(x, y, x', y') = (b, a, b, a)]_r$$
$$[\beta^2 a^2 x^2 - b^2 y^2 = \beta^2 a^2 x'^2 - b^2 y'^2 =: 2qrN]_{uq^2 r}, \quad u := (2, r)$$
$$[\beta a x - b y = 0]_{r^2}$$

Checking the freedom and determination of $(x,y),(x',y')$, and using the Drawer Principle, we find that there exist *distinct* $(x,y),(x',y')$ satisfying the previous conditions.

Presume

$$(qr^n,p^m)||\beta-1\wedge(d,p^m)|q/r,\quad n:=0\vee1$$

Make

$$(s,t,s',t'):=(x,y,x',y')+qZ(b,a(1\vee\beta),0,0)$$

to set

$$[\beta^2a^2s^2-b^2t^2=\beta^2a^2s'^2-b^2t'^2]_{p^m}$$

Make

$$(X,Y,X',Y'):=(s,t,s',t')+qZ'(s',-t',s,-t)$$

to set

$$[aX-bY=aX'-bY']_{p^m}$$

hence

$$[\beta^2a(X+X')=b(Y+Y')]_{p^m}$$

Try (z,z') to meet

$$[aX+bY+z-\beta z'=aX'+bY'+z'-\beta z=0]_{p^m}$$

$$[z-z'=-\frac{2}{1+\beta}(aX-aX')]_{p^m}$$

$$[z+z'=-\frac{1+\beta^2}{1-\beta}(aX+aX')]_{p^m}$$

then

$$[(aX+bY'+z-\beta z)^2=(aX'+bY+z'-\beta z')^2]_{p^m}$$

It's invalid because if

$$[aX+bY'+z-\beta z=aX'+bY+z'-\beta z'=0]_{(\beta-1,p^m)}$$

then with the identity

$$[\beta(aX+z)+(bY'-\beta z)=(aX'-\beta z')+\beta(bY+z')]_{((\beta-1)^2,p^m)}$$

it implies

$$[aX+z=bY+z']_{(\beta-1,p^m)}$$

Therefore

$$[x=x']_{(q,p^m)}\vee\neg(qr^n,p^m)||\beta-1 \tag{2.1}$$

Furthermore

$$(qr|\beta-1\wedge[x=x']_q)=0 \tag{2.2}$$

because if not,

$$[\beta ax-by=\beta ax'-by']_{q^2r}$$

$$[ax-by=ax'-by']_{q^2r}$$

$$|ax-by-(ax'-by')|<q^2r$$

$$ax-by=ax'-by'$$

Therefore

$$x-x'=0=y-y'$$

It contradicts to the previous condition.

So that with the condition 2.1

$$\neg(q,p^m)||\beta-1=[x=x']_{(q,p^m)}\wedge\neg(q,p^m)||\beta-1\vee[x\neq x']_{(q,p^m)}$$

Wedge with $(qr,p^m)|\beta-1$

$$(qr,p^m)|\beta-1=(qr,p^m)|\beta-1\wedge[x=x']_{(q,p^m)}$$

With the condition 2.2

$$(qr|\beta-1)=0$$

□

Theorem 2.2. *For prime p and positive integer q the equation $a^p+b^p=c^q$ has no integer solution (a,b,c) such that $(a,b)=(b,c)=(a,c)=1, a,b>0$ if $p,q>3$.*

Proof. Reduction to absurdity. Make logarithm on a,b in mod c^q. The conditions are sufficient for a controversy. □

References

[1] Z.I. Borevich, I.R. Shafarevich, "Number theory" , Acad. Press (1966)

E-mail address: hiyaho@126.com

Tianmen, Hubei Province, The People's Republic of China. Postcode: 431700