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 is 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 in the form:*

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

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*

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

then

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

Date: Jan 27, 2020.
Key words and phrases. Diophantine Equation; Discrete Logarithm.

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

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

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

Define

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

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.

Definition 1.4.

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

Definition 1.5.

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

Definition 1.6.

$$_q[x] := y : [x = y]_q, 0 \leq y < q$$

2. Unequal Logarithms of Two Numbers

Theorem 2.1. *If*

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

then

$$[lm(a) \neq lm(b)]_q$$

Proof. Define

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

Set

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

Consider

$$[(x, y, x', y') = (b, a, b, a)]_r$$
$$[\beta^2 a^2 x^2 - b^2 y^2 = \beta^2 a^2 x'^2 - b^2 y'^2 =: (2, q)qN]_{q^2}, (N, q) = 1$$

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

$$(qr^n, p^m)||a^{v-1} - b^{v-1}, n \geq 0$$
$$(d, p^m)|q/r$$

Make

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

to set

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

Make

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

to set

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

hence

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

The variables of fraction z, z' meet the equation

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

It's equivalent to

$$[2(aX-\beta bY')z-2(aX'-\beta bY)z'+(1+\beta^2)(z^2-z'^2)+(a^2X^2-a^2X'^2)(1-\beta^2) = 0]_{p^m}$$

$$[(1 + \beta)(aX - aX')(z + z') + (1 - \beta^3)(aX + aX')(z - z') + (1 + \beta^2)(z^2 - z'^2)$$
$$= -(a^2X^2 - a^2X'^2)(1 - \beta^2)]_{p^m}$$

$$[(z-z'+\frac{1+\beta}{1+\beta^2}a(X-X'))(z+z'+\frac{1-\beta^3}{1+\beta^2}(aX+aX')) = \frac{\beta(1-\beta^2)}{(1+\beta^2)^2}(a^2X^2-a^2X'^2)]_{p^m}$$

In another way

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

Make by choosing a valid $z - z'$

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

then

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

It's invalid, hence

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

The case for $p = 2$ is similar.

If

$$[a^{v-1} - b^{v-1} = 0]_{p^l}$$

then

$$[a^{p-1} - b^{p-1} = 0]_{p^l}$$
$$l < C$$

Furthermore

$$q|a^{v-1} - b^{v-1} \wedge [x = x']_q = 0 \tag{2.2}$$

because if not

$$[a^v x - b^v y = a^v x' - b^v y']_{q^2}$$
$$[ax - by = ax' - by']_{q^2}$$
$$|ax - by - (ax' - by')| < q^2$$

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

therefore

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

It contradicts to the previous condition.

So that with the condition 2.1

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

Wedge with $(qr^n, p^m)|a^{v-1} - b^{v-1}$

$$(qr^{n+1}, p^m)|a^{v-1} - b^{v-1} = (qr^{n+1}, p^m)|a^{v-1} - b^{v-1} \wedge [x = x']_q$$

With the condition 2.2

$$qr|a^{v-1} - b^{v-1} = 0$$

Therefore we find the proof. □

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 $p, q > 8$.*

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

E-mail address: `hiyaho@126.com`

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