MODULAR LOGARITHMS UNEQUAL

WU SHENGPING

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 the result that two finite numbers is with unequal logarithms in a corresponding module is proven, which result is applied to solving a kind of high degree diophantine equation.

CONTENTS

1. Function in module 1
2. Unequal Logarithms of Two Numbers 2

In this paper p, p_i are primes. m, m' are great enough. All numbers that are indicated by Latin letters are integers unless with further indication. $C(z)$ mean constant independent of z. $F(z)$ means variable F is the function dependent of z. The formula $a << b$ means that b is far greater than a.

1. FUNCTION IN MODULE

Theorem 1.1. *Define the congruence class in the form:*

$$[a]_q := [a + kq]_q, \forall k$$

$$[a = b]_q : [a]_q = [b]_q$$

$$[x]_{qq'} = [a]_q[b]_{q'} : [x = b]_q, [x = b]_{q'}, (q, q') = 1$$

then

$$[a + b]_q = [a]_q + [b]_q$$

$$[ab]_q = [a]_q \cdot [b]_q$$

$$[a + c]_q[b + d]_{q'} = [a]_q[b]_{q'} + [c]_q[d]_{q'}, (q, q') = 1$$

$$[ka]_q[kb]_{q'} = k[a]_q[b]_{q'}, (q, q') = 1$$

$$[a^k]_q[b^k]_{q'} = ([a]_q[b]_{q'})^k, (q, q') = 1$$

Definition 1.2. Function of $x \in \mathbf{Z}$: $c + \sum_{i=1}^m c_i x^i$ is called power-analytic (i.e power series), it's denoted by $P(x)$.

Date: Sep 23, 2018.
2010 *Mathematics Subject Classification.* 11Y40,11D41.
Key words and phrases. Diophantine equation, Discrete logarithm.

Theorem 1.3. *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 1.4. *(Modular Logarithm) Define*

$$[lm_a(x) := y]_{p^{m-1}(p-1)} : [a^y = x]_{p^m}$$

$$[E := \sum_{i=0}^{n} \frac{p^i}{i!}]_{p^m}$$

n is sufficiently great. then

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

$$[lm_E(px+1) = \sum_{i=1}^{n} \frac{(-1)^{i+1} p^{i-1}}{i} x^i]_{p^{m-1}}$$

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

$$Q(q) := \prod_i [p_i]_{p_i^m}, \forall p_i : p_i | q$$

Define

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

e is the generating element in mod p and meets

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

To prove the theorem, one can contrast the coefficients of E^x and $E^{lm(1+px)}$ to those of real exponents of $exp(px)$ and $exp(log(px+1))$.

Definition 1.5. $P(q)$ is the product of all the distinct prime factors of q.

Definition 1.6.

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

Definition 1.7.

$$y := \overline{[x]}_q : [y = x]_q, -q/2 < y \leq q/2$$

2. Unequal Logarithms of Two Numbers

Theorem 2.1. *If*

$$a + P(q)b \leq q$$

$$a > b > 0$$

$$P^2(q) | q$$

$$(a,b) = (a,q) = (b,q) = (a-b,q) = 1$$

then

$$[lm(a) \neq lm(b)]_{q/P(q)}$$

Proof. Define

$$r := P(q)$$
$$[v+1 := 1 - p_i^m]_{p_i^m(p_i-1)}, v > 0, p_i | q$$

Presume

$$q' = \prod_i (a^{v+1} - b^{v+1}, p_i^m), q | q'$$

Set

$$0 \le x, x' < q'$$
$$0 \le y, y' < q'r + r$$
$$d := (x - x', q^m)$$
$$l := \prod_i [\frac{a^{v+1}}{b^{v+1}}]_{p_i^m}$$

Consider

$$[lax - by = lax' - by' = q'rU]_{q'^2} \tag{2.1}$$
$$(x, y, x', y') = (b, a, b, a)$$

After checking the freedom and determination of variables and the symmetry between $(x, y), (x', y')$, and with the Drawer Principle, we can find two *distinct* points $(x, y), (x', y')$ satisfying these conditions.

Make for some z

$$[lax - kby = lax' - kby']_{p_i^m}$$
$$[k = \frac{u}{b(by - by')} := 1 + q^2 z/d]_{p_i^m}$$
$$K := \frac{\overline{[u^{p_i-1}]}_{p_i^m}}{b^{p_i-1}(by - by')^{p_i-1}}$$

Therefore

$$[l^{p_i-1}(ax - ax')^{p_i-1} = K(by - by')^{p_i-1}]_{p_i^m}$$
$$[a^{p_i-1}(ax - ax')^{p_i-1} = Kb^{p_i-1}(by - by')^{p_i-1}]_{p_i^m}$$
$$[a^{p_i-1}(ax - ax')^{p_i-1} = \overline{[u^{p_i-1}]}_{p_i^m}]_{p_i^m}$$

Because

$$|a^{p_i-1}(ax - ax')^{p_i-1} - \overline{[u^{p_i-1}]}_{p_i^m}| < p_i^m$$

then

$$Z^{p_i-1} := a^{p_i-1}(ax - ax')^{p_i-1} = \overline{[u^{p_i-1}]}_{p_i^m}$$

Vary m on this formula

$$Z^{p_i-1} = \overline{[u^{p_i-1}]}_{p_i^{m'}}, m' << m$$

Hence

$$\overline{[\overline{[u]}_{p_i^{m'}}^{p_i-1}]}_{p_i^{m'}} = \overline{[\overline{[u]}_{p_i^m}^{p_i-1}]}_{p_i^m}$$
$$\overline{[\overline{[u]}_{p_i^m}^{p_i-1}]}_{p_i^{m'}} = \overline{[\overline{[u]}_{p_i^m}^{p_i-1}]}_{p_i^m}$$

Then

$$\overline{[u]}_{p_i^m}^{p_i-1} << p_i^m$$
$$Z^{p_i-1} = \overline{[u]}_{p_i^m}^{p_i-1}$$

$$Z = \overline{[u]}_{p_i^m}$$

This means

$$[a^2(x-x') = kb^2(y-y')]_{p_i^m}$$

It's invalid unless

$$q'|d$$

So that

$$[ax-by = ax'-by']_{q'^2}$$
$$|(ax-by)-(ax'-by')| < q'^2$$
$$ax-by = ax'-by'$$
$$x-x' = y-y' = 0$$

It's invalid.

If (q', p_i^m) is great enough then

$$a^{p_i-1} = b^{p_i-1}$$

It's invalid. □

On this proof, we can easily find if $(l-1, p_i^m) = (q'/r, p_i^m)$ then $(d, p_i^m) \neq (q', p_i^m)$. Or, make

$$(X, Y, X', Y') = (x, y, x', y') + rz'(kb, a, kb, a)$$

to set

$$[laX - kbY = 0]_{p_i^m}$$

then

$$(laX - bY - (laX' - bY'), p_i^m) = (q'^2/r, p_i^m)$$

if

$$(lax - by - (lax' - by'), p_i^m) = (q'^2, p_i^m)$$

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 $p > 8, q > 2$.

Proof. Make logarithm on a, b in mod c^q. The conditions are sufficient for a controversy. Prove on the module $(a-b, c)^m$ or the other part of module. □

The People's Republic of China.