EXPOSITIONAL DIOPHANTINE EQUATION

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 a result is obtained on two finite numbers with unequal logarithms, which result is applied to solving a kind of diophantine equations.

Contents

1. Function in module 1
2. Unequal Logarithms on Two Numbers 3

In this paper \( p, p_i \) are primes, \( m, m', m'' \) are great enough. all numbers that are indicated by letters are integers unless further indication. \( C, C', C_i \) are constants, \( C(z), C'(z), C_i(z) \) are constants independent of \( z \).

1. Function in module

Definition 1.1. Define

\[ [a]_q := \{ a + kq : \forall k \} \]

\[ [a = b]_q : [a]_q = [b]_q \]

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

\[ [a + b]_q = [a]_q + [b]_q \]

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

\[ [a + c]_q[b + d]_q' = [a]_q[b]_q' + [c]_q[d]_q', (q, q') = 1 \]

\[ [ka]_q[kb]_q' = k[a]_q[b]_q', (q, q') = 1 \]

\[ [a^k]_q[k^k]_q' = ([a]_q[b]_q')^k, (q, q') = 1 \]

Definition 1.2. Function of \( x \in \mathbb{Z} \): \( c + \sum_{i=1}^m c_i x^i \) is called power-analytic (i.e power series).

Define \( F(z), Z(z) \) is power-analytic functions of \( z \).
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)

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

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

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

$n$ is sufficiently great. $e$ is the generating element in mod $p$

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

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

then

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

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

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

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

\[ [x/y] = a : x/y - 1 < a < x/y \]

\[ y = T(x, q) : [y = x]_q, 0 \leq y < q \]

Definition 1.8.

\[ [i = a]_{p^m} : [a^2 = -1]_{p^m}, 4 | p - 1 \]
2. Unequal Logarithms on Two Numbers

Definition 2.1.

\[ x \to a \]

means the variable \( x \) gets value \( a \).

Theorem 2.2. If

\[ qa + b < q^2, a, b > 0, (a, b) = (a, q) = (b, q) = (a^2 - b^2, q) = 1 \]

then

\[ [\text{lm}(a) \neq \text{lm}(b)]_{q^3} \]

Proof. Presume

\[ (rlm(a) - rlm(b), q^m) = q^q, q^2r|q' \]
\[ r := P(q), d := (q^m, x - x', y - y') \]
\[ v := [-Q^{m'}(q)]_q^m [-1]_{\Pi(p_i, -1), p_i|q} \]

considering

\[ |ax - by| = ax' - by' =: q'z q'q \]
\[ 0 \leq x, x' < q' + r; 0 \leq y, y' < qr \]
\[ [(x, y) = (x', y') = (b, a)]_r \]

Checking the freedom and determination of variables and the symmetry between \((x, y), (x', y')\) we can find two distinct points \((x, y), (x', y')\) satisfy these conditions. Then

\[ |ax - by - ax' + by'| < q'q \]

hence

\[ ax - by = ax' - by' \]

Make

\[ (x, y, x', y') \rightarrow (x, y, x', y') + dC : (ax - by, p_i^m) = (p_i^m, d), (p_i^m, d)|q' \]

We have for some \( k, k' \)

\[ [k - k' = (x' - x)/b]_q^m \]
\[ k : k' = x - y + d(x - y)^2 : x' - y' + d(x' - y')^2 \]

Then

\[ [x + kb = x' + k'b, y + ka = y' + k'a]_q^m \]
\[ [b^{2v}(x + kb)^2 - a^{2v}(y + ka)^2 = b^{2v}(x' + k'b)^2 - a^{2v}(y' + k'a)^2]_q^m \]

and

\[ [x - y + k(b - a) = 0]_{d^2} \]

Use the identity

\[ u^2(x + s) - u^2(y + t)^2 = (x + s - y - t)u^2x^2 - u^2y^2 + (ux - wy)^2(s + t) \]
\[ + \frac{2xy(us - wt)(w - u)}{x - y} + u^2 s^2 - w^2 t^2 \]

and make

\[ (u, w, x, y, s, t) \rightarrow (b^v, a^v, x, y, kb, ka), (b^v, a^v, x', y', k'b, k'a) \]
to get
\[
[(x - y + k(b - a))\frac{b^2x^2 - a^2y^2}{x - y} + \frac{k(b^v x - a^v y)^2(b + a)}{x - y}]
\]
\[
= (x' - y' + k'(b - a))\frac{b^2x'^2 - a^2y'^2}{x' - y'} + \frac{k'(b^v x' - a^v y')^2(b + a)}{x' - y'}
\]
then
\[
\frac{k(b^v x - a^v y)^2(b + a)}{x - y} = \frac{k'(b^v x' - a^v y')^2(b + a)}{x' - y'}
\]
\[
[x - y = x' - y']\frac{dqq}{(d^5,d^4r,dqq',p_m)}
\]
It’s invalid, unless
\[
qr|d
\]
\[
x - x' = y - y' = 0
\]
It’s invalid.
If \((q',p^m)\) is great enough, then
\[
a^{p_{i-1}} = b^{p_{i-1}}
\]
It’s invalid.

**Theorem 2.3.** 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\(p,q > 36\).

**Proof.** Make logarithm on \(a, b\) in mod \(c^q\). It’s a condition sufficient for a controversy. Prove on the module \((a^2 - b^2, c)^m\) or the other part of module. \(\square\)