HIGH DEGREE DIOPHANTINE EQUATION BY CLASSICAL NUMBER THEORY

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 obtained on two finite numbers with unequal logarithms, which result is applied to solving a kind of diophantine equations. The proof of the results is mainly in the last two sections.

Contents

1. Introduction

When the high degree diophantine equation is talked about, the most famous result is Fermat's last theorem. In this article purely algebraic method is applied to discuss unequal (modulated) logarithms of finite integers under module and a nice result on equation $c^q = a^p + b^p$ is finally obtained. In this article the ring $\mathbf{Z}/(n\mathbf{Z})$ is called "mod n" as a noun grammatically, or is called "module of n", and all numbers denoted by letters are integers.

2. Modulated Function

In this section p is a prime greater than 2 unless further indication.

Definition 2.1. Function of $x \in \mathbf{Z}$: $c + \sum_{i=1}^{m} c_i x^i$ is called power-analytic (i.e power series). Function of x: $c + \sum_{i=1}^{m} c_i e^{ix}$ is called linear exponent-analytic of bottom e. e, c, c_i, i are constant integers. m is finite positive integer.

Theorem 2.2. *Power-analytic functions modulo p are all the functions from mod p to mod p, if p is a prime. And $1, x^i, (0 < i \leq p-1, x \in \mod p)$ are linear independent vectors. For convenience 1 is always written as x^0, and x^{p-1} is different from x^0.*

Date: April 9, 2015.
2000 *Mathematics Subject Classification.* 11D41.
Key words and phrases. High degree Diophantine equation, Modulated function, Modulated logarithm, Fermat's Last Theorem.

Proof. Make matrix X of rank n:

$$X_{i,1} = 1, Xij = i^{j-1} \quad (1 \leq i \leq p, 2 \leq j \leq p)$$

The columnar vector of this matrix is the values of x^i. This matrix is Vandermonde's matrix and its determinant is not zero modulo p. The number of the distinct functions in mod p and the number of the distinct linear combinations of the columnar vectors are the same as p^p. So the theorem is valid. □

A proportion of the row vector are values of exponent function modulo p.

Theorem 2.3. *Exponent-analytic functions modulo p by a certain bottom are all the functions from mod $p-1$ to mod p, if p is a prime.*

Proof. From theorem 2.2, $p-1$ is the least positive number a for:

$$\forall x \neq 0 \bmod p (x^a = 1 \bmod p)$$

or, exists two unequal number $c, b \bmod p-1$ such that functions x^c, x^b are of $x^c = x^b \bmod p$. Hence exists e whose exponent can be any member in mod p except 0. Because the part of row vector in matrix X (as in the previous theorems) are values of exponent function, so this theorem is valid. □

Theorem 2.4. *p is a prime. The members except zero factors in mod p^n forms a group of multiplication that is generated by single element e (here called generating element of mod p^n).*

Thinking about $p+1$ that is the generating element of all the subgroups of rank p^i.

Definition 2.5. (Modulated Logarithm modulo p^m) p is a prime, e is the generating element as in the last theorem:

$$lm_e(x): \quad x \in \mathbf{Z}((x,p) = 1) \to \bmod p^{m-1}(p-1): \quad e^{lm_e(x)} = x \bmod p^m$$

It's inferred that

$$y = lm_b(x) \bmod p^{m-1}, b = e^{p-1} \bmod p.$$

Lemma 2.6.

$$lm_e(-1) = p^{m-1}(p-1)/2 \ mod \ p^{m-1}(p-1)$$

p is a prime. e is defined in mod p^m.

Lemma 2.7. *The power series expansions of $log(1+x), (|x| < 1)$ (real natural logarithm), $exp(x)$ (real natural exponent), and the series for $exp(log(1+x)), (|x| < 1)$ that generated by the previous two being substituted in are absolutely convergent.*

Definition 2.8. Because:

$$\frac{a}{p^m} = kp^n \leftrightarrow a = 0 \bmod p^{m+n}$$

$a, k \in \mathbf{Z}$, it's valid to make the rational number modulo integers, if it applies to equations. It's formally written as

$$a/p^m = 0 \bmod p^n$$

Definition 2.9. $p^i || a$ means $p^i | a$ and not that $p^j | a, j > i$.

Theorem 2.10. *p is a prime greater than 2. $x \in \mathbf{Z}$*

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

n is sufficiently great and dependent on m.

$$e^{1-p^m} := E \ mod\ p^m$$

e is the generating element.

$$lm(x) := lm_e(x) \ mod\ p^{m-1}$$

Then the following are valid

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

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

$$lm_E(x^{1-p^m}) = lm(x^{1-p^m})/lm(E) = lm(x^{1-p^m}) = lm(x) \ mod\ p^{m-1}.$$

In fact m is free to be chosen. And E is nearly $exp(p)$. If $2|x$ this theorem is also valid for $p = 2$.

Proof. To prove the theorem, One can contrast the coefficients of E^x and $E^{f(x)}$ to those of $exp(px)$ and $exp(log(px+1))$. □

Theorem 2.11. *Set $d_m : p^{d_m} || p^m/m!$. It's valid that $d_{m(>p^n)} > d_{p^n}$.*

Theorem 2.12. *(Modulated Derivative) p is a prime greater than 2. $f(x)$ is a certain power-analytic function mod p^m, $f^{(i)}(x)$ is the real derivative of i-th order, then*

$$f(x+zp) = \sum_{i=0}^{n} \frac{p^i}{i!} z^i f^{(i)}(x) \ mod\ p^m$$

n is sufficiently great. $f^{(i)}(x)$ is called modulated derivative*, which is connected to the special difference by zp. If $2|z$ this theorem is also valid for $p = 2$.*

3. Some Definitions

In this section p, p_i are prime. m, m' are sufficiently great.

Definition 3.1. $x \to a$ means the variable x gets value a.

Definition 3.2. a, b, c, d, k, p, q are integers,$(p, q) = 1$:

$$[a]_p = [a + kp]_p$$

$$[a]_p + [b]_p = [a + b]_p$$

$[a = b]_p$ means $[a]_p = [b]_p$.

$$[a]_p[b]_q = [x : [x = b]_p, [x = b]_q]_{pq}$$

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

Easy to verify:

$$[a + c]_p[b + d]_q = [a]_p[b]_q + [c]_p[d]_q$$

$$[ka]_p[kb]_q = k[a]_p[b]_q$$

$$[a^k]_p[b^k]_q = ([a]_p[b]_q)^k$$

Definition 3.3. $\varphi(x)$ is the Euler's character as the least positive integer s meeting

$$\forall y((y,x)=1\rightarrow[y^s=1]_x)$$

Definition 3.4. The complete logarithm on composite modules is complicated, but this definition is easy:

$[lm(x)]_{p_1^{n_1}p_2^{n_2}\cdots p_m^{n_m}}:=[[lm(x)]_{(p_1-1)p_1^{n_1}}]_{p_1^{n_1}}[[lm(x)]_{(p_2-1)p_2^{n_2}}]_{p_2^{n_2}}\cdots[[lm(x)]_{(p_m-1)p_m^{n_m}}]_{p_m^{n_m}}$

p_i are distinct primes. This definition will be used without detailed indication.

Definition 3.5. $P(q)$ is the product of all the distinct prime factors of q.

Definition 3.6. $Q(x):=\prod_i[p_i]_{p_i^m}$, p_i is all the prime factors of x. m is sufficiently great.

Theorem 3.7. $2|q\rightarrow 2|x$*:*

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

The method of the proof is to get result in module of powers of any prime and to synthesize them in composite module.

Definition 3.8.

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

Definition 3.9.

$$[i:i^2=-1]_{p^m},4|p-1$$

Definition 3.10.

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

4. Unequal Logarithms on Two Numbers

m is sufficiently great. p_i are primes.

Definition 4.1.

$$x\rightarrow a$$

means the variable x gets the value a.

Theorem 4.2.

$$|a|+|b|<q/P(q),|a|>|b|>0,P(q)^2|q$$
$$(a,q)=(b,q)=(a^2-b^2,q)=1$$

then

$$[lm(a)\neq lm(b)]_{q^3/P^2(q)}$$

Proof. Presume

$$[lm(a)=lm(b)]_{q^3/r^2},[a^{v+1}=b^{v+1}]_{q^3/r} \tag{4.1}$$
$$r:=P(q)$$
$$v:=\prod_i[-p_i^m]_{(p_i^m-1)p_i^m},v>0,\forall p_i|q$$

Set

$$0\leq X<qr,0\leq Y<2q,[(X,Y)=(b,-a)]_r \tag{4.2}$$
$$(X,Y)\rightarrow(x,y'),(x',y),(x,y')\neq(x',y)$$

Consider

$$[ax - by = ax' - by']_{q^2} \tag{4.3}$$

$$[ax + by' = ax' + by = qC]_{qr}, (C, q) = 1 \tag{4.4}$$

Checking the freedom of variables and the symmetry between $(x, y'), (x', y)$ we can find two distinct points $(x, y') \neq (x', y)$ satisfy the equations 4.3 and 4.4.

By the conditions 4.3

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

because

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

then

$$k := (x - x')/b = (y - y')/a, (a, b) = 1 \tag{4.5}$$

$$|k| = |y - y'|/|a| < 2q/|a| < q \tag{4.6}$$

This identity is useful

$$\sum_{n=0}^{N} nx^n = \frac{x - (N+1)x^{N+1} + Nx^{N+2}}{(x-1)^2}$$

We have

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

$$s := x + dKb, t' := y' - dKa, s' := x' + dK'b, t := y - dK'a$$

$$d := (q, x - x', y - y')$$

then

$$[s = s', t = t']_{q^m}$$

So that

$$[s^{2v+2} - t'^{2v+2} = s'^{2v+2} - t^{2v+2}]_{q^2 d}$$

$$[\sum_{n=0}^{2v+1} x^n y'^{2v+1-n}(1 + dK(\frac{nb}{x} - \frac{(2v+1-n)a}{y'})$$

$$+ \sum_{k>1} d^k K^k \sum_{i=0}^{k} C_n^i C_{2v+1-n}^{k-i} (\frac{b}{x})^i (-\frac{a}{y'})^{k-i})]_{q^2 d}$$

$$= \sum_{n=0}^{2v+1} x'^n y^{2v+1-n}(1 + dK'(\frac{nb}{x'} - \frac{(2v+1-n)a}{y})$$

$$+ \sum_{k>1} d^k K'^k \sum_{i=0}^{k} C_n^i C_{2v+1-n}^{k-i} (\frac{b}{x'})^i (-\frac{a}{y})^{k-i})]_{q^2 d}$$

Use this and inductive method on n, k

$$C_n^i C_{n-1+k-i-1}^{k-i} = C_n^i (C_{n-1+(k-1-i)-1}^{(k-1-i)} + C_{n-1+(k-1-i)-1}^{k-i})$$

$$C_n^i C_{n-1+(k-1-i)-1}^{k-i} = (C_{n-1}^{i-1} + C_{n-1}^{i}) C_{(n-1)-1+(k-i)-1}^{k-i}$$

to prove

$$[\sum_{i=0}^{k} C_n^i C_{2v+1-n}^{k-i} (\frac{b}{x})^i (-\frac{a}{y'})^{k-i} = 0]_{q^2}, k > 1$$

then

$$[\frac{(ax-by')(ax+by')}{x-y'}+dK(b-a)\frac{(ax+by')^2}{(x-y')^2}]_{q^2d}$$
$$=\frac{(ax'-by)(ax'+by)}{x'-y}+dK'(b-a)\frac{(ax'+by)^2}{(x'-y)^2}]_{q^2d}$$
$$[\frac{(ax-by')(ax+by')}{x-y'}=\frac{(ax'-by)(ax'+by)}{x'-y}]_{q^2d}$$
$$[y'/x=y/x']_{qd}$$

So that

$$[x-x'=y-y'=0]_q \tag{4.7}$$

With the conditions 4.6 and 4.7

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

This means

$$(x,y')=(x',y)$$

This contradicts to the previous condition. □

Theorem 4.3. *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 $p,q>20$.

Proof. Make logarithm on a,b in mod c^q. It's a condition sufficient for a controversy. Consider two independent modules $(a+b,c)^m$ and the other part, either of which are potentially capable a proof. □

Wuhan University, Wuhan, Hubei Province, The People's Republic of China.
E-mail address: hiyaho@126.com