COLLOQUIUM MATHEMATICUM

VOL. LXVIII 1995 FASC. 2

A NOTE ON THE INTEGER SOLUTIONS OF HYPERELLIPTIC EQUATIONS

BY

MAOHUA LE (ZHANJIANG)

1. Introduction. Let $\mathbb{Z}$, $\mathbb{N}$, $\mathbb{Q}$ denote the sets of integers, positive integers and rational numbers respectively. Let $m, n \in \mathbb{N}$ with $m \geq 2$, $n \geq 2$ and $mn \geq 6$. Let $f(x) = a_0x^m + \ldots + a_{m-1}x + a_m \in \mathbb{Z}[x]$ with $a_0 \neq 0$, and let $H = \max(|a_0|, \ldots, |a_m|)$. There are many papers concerning the solutions (x, y) of the hyperelliptic equation

$$f(x) = y^n, \quad x, y \in \mathbb{Z}. \tag{1}$$

Let $e_1, \ldots, e_s$ be the multiplicities of distinct zeros of $f(x)$ with $e_1 \geq \ldots \ldots \geq e_s$. In [5], LeVeque proved that if (1) has infinitely many solutions (x, y), then either $\{n/\gcd(e_1, n), \ldots, n/\gcd(e_s, n)\} = \{2, 2, 1, \ldots, 1\}$ or
$\{t, 1, \ldots, 1\}$ with $t \in \mathbb{N}$. In [1], Baker proved that if $n = 2$ and $f(x)$ has at least three simple zeros, then all solutions (x, y) of (1) satisfy

$$\max(|x|, |y|) < \exp\exp\exp(m^{10m^3} H^{m^2}); \tag{2}$$

if $n > 2$ and $f(x)$ has at least two simple zeros, then

$$\max(|x|, |y|) < \exp\exp((5n)^{10} m^{10m^3} H^{m^2}).$$

Afterwards, Sprindžuk [10] improved Baker's bound (2) showing that if $n = 2$, $a_0 = 1$ and $f(x)$ has at least three simple zeros, then

$$\max(|x|, |y|) \ll \exp(|D|^{(8+\varepsilon)(6m^3+12m^2)} (\log H)^{1+\varepsilon}), \quad \varepsilon > 0,$$

where D is the discriminant of $f(x)$ and the positive constant implied by $\ll$ only depends on ε and m and is effectively computable.

In this note, using some elementary methods, we prove the following result, related to the main theorem of [11].

THEOREM. *If* $m \equiv 0 \pmod{n}$, $a_0 = 1$, $a_1, \ldots, a_m$ *are not all zeros and the first nonzero coefficient is coprime with* n, *then* (1) *has only finitely many*

1991 *Mathematics Subject Classification*: 11D41, 05A19.

Supported by the National Natural Science Foundation of China.

solutions (x, y). *Moreover, all solutions of* (1) *satisfy* $|x| < (4mH)^{2m/n+1}$ *and* $|y| < (4mH)^{2m^2/n^2+m/n+1}$.

Now we give two applications of the above theorem. Let $m_1, \ldots, m_s \in \mathbb{N}$ with $1 \le m_1 < \ldots < m_s$. In [9], Rotkiewicz and Złotkowski proved that the equation

$$x^{m_s} + x^{m_{s-1}} + \ldots + x^{m_1} + 1 = y^z, \quad x, y, z \in \mathbb{N},$$

under some conditions has only finitely many solutions (x, y, z). By the Theorem, we have:

COROLLARY 1. *If* $n \ge 2$ *and* $m_s \equiv 0 \pmod n$, *then all solutions* (x, y) *of the equation*

$$x^{m_s} \pm x^{m_{s-1}} \pm \ldots \pm x^{m_1} \pm 1 = y^n, \quad x, y \in \mathbb{N}, \tag{3}$$

satisfy $x < (4m_s)^{2m_s/n+1}$ *and* $y < (4m_s)^{2m_s^2/n^2+m_s/n+1}$.

Let $k \in \mathbb{N}$ with $k > 2$, and let $\zeta_k = e^{2\pi\sqrt{-1}/k}$. Then

$$\Phi_k(x) = x^{\varphi(k)} + a_1 x^{\varphi(k)-1} + \ldots + a_{\varphi(k)} = \prod_{\substack{1 \le l \le k \\ \gcd(l,k)=1}} (x - \zeta_k^l) \in \mathbb{Z}[x] \tag{4}$$

is called the kth *cyclotomic polynomial*, where $\varphi(k)$ is Euler's function of k. In [6], Ljunggren proved that if k is an odd prime, then

$$\Phi_k(x) = y^2, \quad x, y \in \mathbb{N},\ x > 1,\ y > 1, \tag{5}$$

has only one solution $(k, x, y) = (5, 3, 11)$. For a general k, we have:

COROLLARY 2. *Let d be the greatest square-free factor of k, and let* $m = \varphi(d)$. *Then all solutions* (x, y) *of* (5) *satisfy*

$$x < \exp\left(\frac{d}{k}(m+1)(m^{1/2} + \log 4m)\right),$$
$$y < \exp\left(\frac{d}{k}(m^2+m+1)(m^{1/2} + \log 4m)\right).$$

Moreover, if $k/d \ge (m+1)(m^{1/2} + \log 4m)/\log 2$, *then* (5) *has no solution* (x, y).

2. Lemmas

LEMMA 1. *Let* $F(z) = \sum_{k=0}^{\infty} \alpha_k z^k$ *be a power series with real coefficients and* $\alpha_0 > 0$. *For any* $n \in \mathbb{N}$ *with* $n > 1$ *and any* $k \in \mathbb{Z}$ *with* $k \ge 0$, *let*

$$\beta_0 = 1, \quad \beta_k = \sum \left(\prod_{i=0}^{r_1+\ldots+r_k-1} \left(\frac{1}{n} - i\right)\right)\left(\prod_{j=1}^{k} \frac{(\alpha_j/\alpha_0)^{r_j}}{r_j!}\right), \quad k > 0, \tag{6}$$

where the summation is over all solutions $(r_1, \ldots, r_k)$ *of the equation*

$$r_1 + 2r_2 + \ldots + kr_k = k, \quad r_1, \ldots, r_k \in \mathbb{Z},\ r_1, \ldots, r_k \ge 0. \tag{7}$$

If there exists a positive number M *such that* $\max_{k\in\mathbb{N}} |\alpha_k/\alpha_0| \le M$, *then*

$$(F(z))^{1/n} = \alpha_0^{1/n} G(z) = \alpha_0^{1/n} \sum_{k=0}^{\infty} \beta_k z^k, \quad |z| < \frac{1}{2M}. \tag{8}$$

Proof. By [8], we have

$$\begin{aligned}\sum \frac{(r_1 + \ldots + r_k)!}{r_1! \ldots r_k!} &= \sum_{l=1}^{k} \sum_{\Omega:\, r_1+\ldots+r_k = l} \frac{(r_1 + \ldots + r_k)!}{r_1! \ldots r_k!} \\ &= \sum_{l=1}^{k} \binom{k-1}{l-1} = 2^{k-1},\end{aligned} \tag{9}$$

where the summation $\sum_{\Omega}$ is over all solutions $(r_1, \ldots, r_k)$ of (7) which satisfy the condition Ω. Hence, by (6), if $\max_{k\in\mathbb{N}} |\alpha_k/\alpha_0| \le M$, then the convergence radius R of $G(z) = \sum_{k=0}^{\infty} \beta_k z^k$ satisfies

$$R = \lim_{k\to\infty} \frac{1}{|\beta_k|^{1/k}} \ge \frac{1}{2M}.$$

This implies that $G(z)$ is convergent for $|z| < 1/(2M)$.

Let u, v be variables with $v = F(u)$, and let $G(u) = H(v) = H(F(u))$. Let $D_u = d/du$, $D_v = d/dv$, and let $D_u^k F(u) = f_k$, $D_u^k G(u) = g_k$ and $D_v^k H(v) = h_k$ for any $k \in \mathbb{N}$. By di Bruno's formula (cf. [8]), we have

$$g_k = \sum k! h_{r_1+\ldots+r_k} \left(\prod_{j=1}^{k} \frac{1}{r_j!} \left(\frac{f_j}{j!} \right)^{r_j} \right), \quad k \in \mathbb{N}. \tag{10}$$

Put $u = z$, $v = F(z)/\alpha_0$ and $G(z) = H(v) = v^{1/n}$. Since

$$f_k|_{z=0} = k!\alpha_k, \quad g_k|_{z=0} = k!\beta_k, \quad h_k|_{z=0} = h_k|_{v=1} = \prod_{i=0}^{k-1} \left(\frac{1}{n} - i \right), \quad k \in \mathbb{N},$$

we get (6) by (10). Since $G(z)$ is convergent for $|z| < 1/(2M)$, we obtain (7) immediately. The lemma is proved.

LEMMA 2. *If* $n > 1$, $m \equiv 0 \pmod n$, $a_0 = 1$, $a_i = 0$ $(1 \le i \le s-1)$, $a_s \ne 0$ *and* $\gcd(a_s, n) = 1$, *then*

$$(f(x))^{1/n} = \sum_{k=0}^{\infty} \beta_k x^{m/n-k}, \quad |x| > 2H, \tag{11}$$

where the coefficients β_k $(k = 0, 1, \ldots)$ *satisfy*

(i)

$$\beta_0 = 1, \quad \beta_k = \sum{}' \Bigg(\prod_{i=0}^{r_s+\ldots+r_m-1}\Big(\frac{1}{n}-i\Big)\Bigg)\Bigg(\prod_{j=s}^{m}\frac{a_j^{r_j}}{r_j!}\Bigg), \quad k>0, \tag{12}$$

where the summation $\sum'$ *is over all solutions* $(r_s, \ldots, r_m)$ *of the equation*

$$sr_s + \ldots + mr_m = k, \qquad r_s, \ldots, r_m \in \mathbb{Z},\ r_s, \ldots, r_m \ge 0. \tag{13}$$

(ii) *For any* $k \in \mathbb{N}$, $|\beta_k| < 2^{k-1}H^k$.
(iii) *If* $\beta_k \ne 0$, *then* $|\beta_k| \ge 1/(k!n^k)$.
(iv) *For any* $q \in \mathbb{N}$, $\beta_{qs} \ne 0$.

Proof. Put $\alpha_i = a_i$ $(i = 0, 1, \ldots, m)$ and $\alpha_j = 0$ $(j > m)$. Since $a_l = 0$ $(1 \le l \le s-1)$, by Lemma 1, we get

$$(F(z))^{1/n} = G(z) = \sum_{k=0}^{\infty}\beta_k z^k, \qquad |z| < 1/(2H), \tag{14}$$

where β_k $(k = 0, 1, \ldots)$ satisfy (12). Put $z = 1/x$. Since $m \equiv 0 \pmod{n}$, (14) yields (11) and (i). From (9) and (12), (ii) is clear. Since $(r_s + \ldots + r_m)! \equiv 0 \pmod{r_s! \ldots r_m!}$, we get (iii) by (12).

For any $q \in \mathbb{N}$, from (12) we get

$$\beta_{qs} = \frac{a_s^q}{q!n^q}\prod_{i=0}^{q-1}(1-ni) + I, \tag{15}$$

where

$$I = \sum_{\Omega:\,(r_s, r_{s+1}, \ldots, r_m)\ne(q,0,\ldots,0)}{}' \Bigg(\prod_{i=0}^{r_s+\ldots+r_m-1}\Big(\frac{1}{n}-i\Big)\Bigg)\Bigg(\prod_{j=s}^{m}\frac{a_j^{r_j}}{r_j!}\Bigg), \tag{16}$$

where the summation $\sum'_{\Omega}$ is over all solutions $(r_s, \ldots, r_m)$ of (13) which satisfy the condition Ω. Let p be a prime factor of n, $\lambda = \operatorname{ord}_p n$, and let $\delta_k = \operatorname{ord}_p k!$ for any $k \in \mathbb{N}$. Since $\gcd(a_s, n) = 1$, we have

$$a_s^q(1-n)\ldots\frac{1-n(q-1)}{q!n^q} = \frac{a}{b} \in \mathbb{Q},$$

where $a, b \in \mathbb{Z}$ satisfy $a \ne 0$, $b > 0$ and $b \equiv 0 \pmod{p^{\lambda q+\delta_q}}$. On the other hand, since every solution $(r_s, \ldots, r_m)$ of (13) with $(r_s, r_{s+1}, \ldots, r_m) \ne (q, 0, \ldots, 0)$ satisfies $0 < r_s + \ldots + r_m < q$, we see from (16) that $I = a'/b' \in \mathbb{Q}$, where $a', b' \in \mathbb{Z}$ satisfy $\gcd(a', b') = 1$, $b' > 0$ and $b' \not\equiv 0 \pmod{p^{\lambda q+\delta_q}}$. Therefore, by (15), we get $\beta_{qs} \ne 0$. The lemma is proved.

3. Proof of Theorem. Let (x, y) be a solution of (1) with $|x| \ge (4mH)^{2m/n+1}$. Since $a_i = 0$ $(1 \le i \le s-1)$ and $a_s \ne 0$, we have

$$(17)\qquad 0<\left||x|^{m-s}-H\frac{|x|^{m-s}-1}{|x|-1}\right|\le|y^n-x^m|=\Big|\sum_{k=s}^{m}a_kx^{m-k}\Big|$$
$$\le H\frac{|x|^{m-s+1}-1}{|x|-1}<2H|x|^{m-s}.$$

Notice that $m\equiv 0 \pmod n$. We see from (17) that $y\ne x^{m/n}$. Then

$$|y^n-x^m|>|x|^{(n-1)m/n}$$

and

$$(18)\qquad 1\le s\le m/n$$

by (17).

By Lemma 2, we see from (11) that

$$(19)\qquad y=S_1+S_2,$$

where

$$(20)\qquad S_1=\sum_{k=0}^{m/n}\beta_kx^{m/n-k},$$

$$(21)\qquad S_2=\sum_{k=m/n+1}^{\infty}\beta_k/x^{k-m/n}.$$

From (12) and (20), $S_1=a''/b''\in\mathbb{Q}$, where $a'',b''\in\mathbb{Z}$ satisfy $\gcd(a'',b'')=1$, $b''>0$ and $n^{m/n}(m/n)!\equiv 0 \pmod{b''}$. Hence, by (19), we have either

$$(22)\qquad |y-S_1|=|S_2|\ge\frac{1}{n^{m/n}(m/n)!}$$

or

$$(23)\qquad |y-S_1|=|S_2|=0.$$

By Stirling's theorem,

$$(24)\qquad t!<\sqrt{2\pi t}\,(t/e)^te^{1/(12t)},\qquad t\in\mathbb{N}.$$

By (21), (24) and Lemma 2(ii), if $|x|\ge(4mH)^{2m/n+1}$, then

$$(25)\qquad |S_2|\le\sum_{k=m/n+1}^{\infty}|\beta_k/x^{k-m/n}|<\sum_{k=1}^{\infty}(2^{m/n}H^{m/n+1}/|x|)^k$$
$$=\frac{2^{m/n}H^{m/n+1}}{|x|-2^{m/n}H^{m/n+1}}<\frac{1}{n^{m/n}(m/n)!}.$$

This implies that (22) is impossible.

On the other hand, there exists a multiple of s among the integers $m/n+1,\dots,m/n+s$. Hence, by Lemma 2(iv), there exists $t\in\mathbb{N}$ such that

$m/n+1 \le t \le m/n+s$, $\beta_t \ne 0$ and $\beta_i = 0$ $(m/n+1 \le i \le t-1)$. Then, by (18) and Lemma 2(iii), we have

$$\left|\frac{\beta_t}{x^{t-m/n}}\right| \ge \frac{1}{(2m/n)!n^{2m/n}|x|^{t-m/n}}, \tag{26}$$

and by (21) and Lemma 2(ii),

$$\begin{aligned}\left|\sum_{k=t+1}^{\infty}\frac{\beta_k}{x^{k-m/n}}\right| &< \frac{1}{|x|^{t-m/n}}\sum_{k=1}^{\infty}\left(\frac{2^{2m/n}H^{2m/n+1}}{|x|}\right)^k \\ &= \frac{2^{2m/n}H^{2m/n+1}}{|x|^{t-m/n}(|x|-2^{2m/n}H^{2m/n+1})}.\end{aligned} \tag{27}$$

The combination of (26) and (27) yields $|S_2| \ne 0$ for $|x| \ge (4mH)^{2m/n+1}$, which contradicts (23). Thus, $|x| < (4mH)^{2m/n+1}$, and by (19), (20) and (25), $|y| < (4mH)^{2m^2/n^2+m/n+1}$. This completes the proof.

4. Proof of Corollaries 1 and 2. Since $H = 1$ for (3), Corollary 1 follows immediately from the Theorem.

Now we deal with the equation (5). It is a well known fact that if d is the greatest square-free factor of k, then $\Phi_k(x) = \Phi_d(x^{k/d})$. Let $\Phi_d(X) = X^m + b_1X^{m-1} + \ldots + b_m \in \mathbb{Z}[X]$, where $m = \varphi(d)$. Then (5) can be written as

$$\Phi_d(x^{k/d}) = y^2, \quad x, y \in \mathbb{N},\ x > 1,\ y > 1. \tag{28}$$

When $d = 1$ or 2, since $k/d > 1$, from (28) we get

$$x^{k/d} \pm 1 = y^2, \quad x, y \in \mathbb{N},\ x > 1,\ y > 1. \tag{29}$$

By [3] and [4], the equation (29) has only one solution $(x, y, k/d) = (2, 3, 3)$ with $k/d > 1$.

When $d > 2$, we have $2 \mid m$. Notice that $b_1 = -\mu(d) = \pm 1$ by Theorem 7·4·4 of [2] and $\max(|b_1|, \ldots, |b_m|) < e^{m^{1/2}}$ by [7]. We see from the Theorem that all solutions of (28) satisfy

$$\begin{aligned} x^{k/d} &< \exp((m+1)(m^{1/2} + \log 4m)), \\ y &< \exp((m^2+m+1)(m^{1/2} + \log 4m)). \end{aligned} \tag{30}$$

On the other hand, since $x \ge 2$, (30) is impossible for $k/d \ge (m+1)(m^{1/2} + \log 4m)/\log 2$. Corollary 2 is proved.

REFERENCES

[1] A. Baker, *Bounds for the solutions of the hyperelliptic equation*, Proc. Cambridge Philos. Soc. 65 (1969), 439–444.

[2] L.-K. Hua, *Introduction to Number Theory*, Springer, Berlin, 1982.
[3] C. Ko, *On the diophantine equation $x^2 = y^n + 1$, $xy \neq 0$*, Sci. Sinica 14 (1964), 457–460.
[4] V. A. Lebesgue, *Sur l'impossibilité, en nombres entiers, de l'équation $x^m = y^2+1$*, Nouv. Ann. Math. (1) 9 (1850), 178–181.
[5] W. J. LeVeque, *On the equation $y^m = f(x)$*, Acta Arith. 9 (1964), 209–219.
[6] W. Ljunggren, *Noen setninger om ubestemte likninger av formen $(x^n-1)/(x-1) = y^q$*, Norsk. Mat. Tidsskr. 25 (1943), 17–20.
[7] H. L. Montgomery and R. C. Vaughan, *The order of magnitude of mth coefficients of cyclotomic polynomials*, Glasgow Math. J. 27 (1985), 143–159.
[8] J. Riordan, *Introduction to Combinatorial Analysis*, Wiley, 1958.
[9] A. Rotkiewicz and W. Złotkowski, *On the diophantine equation $1 + p^{\alpha_1} + \ldots + p^{\alpha_k} = y^2$*, in: Number Theory, Vol. II (Budapest 1987), North-Holland, Amsterdam, 1990, 917–937.
[10] V. G. Sprindžuk, *Hyperelliptic diophantine equation and class numbers of ideals*, Acta Arith. 30 (1976), 95–108 (in Russian).
[11] P. G. Walsh, *A quantitative version of Runge's theorem on diophantine equations*, Acta Arith. 62 (1992), 157–172.

DEPARTMENT OF MATHEMATICS
ZHANJIANG TEACHER'S COLLEGE
P.O. BOX 524048
ZHANJIANG, GUANGDONG
P.R. CHINA

Reçu par la Rédaction le 26.4.1993