TOKYO J. MATH.
VOL. 4, No. 2, 1981

On Existence of Infinitely Many Prime Divisors in a Given Set

Hiroshi KOBAYASHI

Ebina Highschool
(Communicated by K. Katayama)

There are some problems in number theory which is concerned with existence of infinitely many primes in a given set, e.g., Dirichlet's theorem on arithmetic progressions or existence of Fermat primes.

We consider a rather loose problem which is concerned with existence of infinitely many prime divisors of elements of a given set.

Let M be a set of rational integers. We call M of type I if the set of prime divisors of M is an infinite set. Otherwise M is said to be of type II.

We assert that if M is an infinite set of type II, and a is a non-zero rational integer, the set $M+a=\{t+a|t\in M\}$ is of type I.

We need the following lemma which is known as Siegel's theorem. (cf. (1) p. 127)

LEMMA. *Let K be a field of finite type over $\boldsymbol{Q}$, and R a subring of K of finite type over $\boldsymbol{Z}$. Let C be a projective non-singular curve of genus $\geqq 1$ defined over K, and let φ be a non-constant function in $K(C)$. Then there is only a finite number of points $P\in C_k$ which are not poles of φ and satisfies $\varphi(P)\in R$.*

THEOREM. *Let M be a set of rational integers of type II, a be a non-zero rational integer, and m be a rational integer not less than 3. Let $(b_t)_{t\in M}$ be a family of rational integers with index set M. Set $N=\{a+b_t^m\cdot t|t\in M\}$. If N is an infinite set, then N is of type I.*

PROOF. If the set of prime divisors of M is $\{p_1, \cdots, p_n\}$, m-th roots of all elements of M are contained in the ring $R=\boldsymbol{Z}[\zeta, p_1^{1/m}, \cdots, p_n^{1/m}]$ (where $\zeta=\exp((\pi/m)i)$) which is of finite type over $\boldsymbol{Z}$, and is a subring of a finite extention field K of $\boldsymbol{Q}$. Put

Received December 19, 1980

$$k_t = b_t \cdot t^{1/m}, \qquad x_t = (a + k_t^m)^{-1/m}, \qquad y_t = k_t \cdot x_t$$

for every $t \in M$ for which $a + b_t^m \cdot t \neq 0$ holds. Here the power $1/m$ means any chosen m-th root: for example we can specify

$$t^{1/m} = \begin{cases} \text{positive } m\text{-th root of } t & \text{when } t > 0 \\ 0 & \text{when } t = 0 \\ |t|^{1/m} \cdot \zeta & \text{when } t < 0 \end{cases}$$

Assume N is of type II. Then all x_t's and y_t's are contained in a finite extention L of K, so that points $P_t(x_t, y_t)$ are L-rational points of the curve C of equation $ax^m + y^m = 1$ which is the affine part of the non-singular projective curve $ax_1^m + x_2^m = x_0^m$ whose genus is $\geqq 1$.

Since N is an infinite set, we have infinite number of P_t's on C, but the function $\varphi(x, y) = y/x$ takes values $k_t \in R$ at each P_t, which is a contradiction by Siegel's theorem.

COROLLARY 1. *If M is an infinite set of type II, and a is a non-zero integer, then $M + a$ is of type I.*

COROLLARY 2. *The set of all Fermat numbers has infinitely many prime divisors.*

Reference

[1] S. LANG, Diophantine Geometry, Interscience Publishers, a division of John Wiley & Sons, New York, 1962.

Present Address:
Ebina Highschool
589 Nakashinden, Ebina-shi
Kanagawa 243