ACTA ARITHMETICA
XV (1969)

The simplest proof of Vandiver's theorem

by

I. SH. SLAVUTSKY (Leningrad)

Let p be an odd prime, Q and Q_p denote the rational and p-adic fields respectively. For the first factor

$$h_1 = (-1)^{\frac{p-1}{2}} 2^{-\frac{p-3}{2}} p \cdot \prod_{\substack{1\leqslant s\leqslant p-2\\(s,2)=1}} \frac{1}{p} \sum_{a=1}^{p} a\chi^s(a)$$

of the class number of the cyclotomic field $Q\left(\exp\dfrac{2\pi i}{p}\right)$, χ be a generating character mod p, Vandiver proved the congruence

$$(1)\qquad h_1 \equiv (-1)^{\frac{p-1}{2}} 2^{-\frac{p-3}{2}} p \prod_{\substack{1\leqslant s\leqslant p-2\\(s,2)=1}} B_{p^l s+1} (\operatorname{mod} p^l),$$

where l is any positive integer, $B_k(x)$ — Bernoulli polynomials, defined by

$$e^{xt}t/(e^t-1) = \sum_{k=0}^{\infty} B_k(x)t^k/k!,$$

$B_k = B_k(0)$ — Bernoulli numbers. We indicate a short way of demonstration of (1), cf. [1], [2].

Since we are interested in dividing the algebraic number h_1 (in fact a positive integer) on p^l, we consider the character χ, which is defined by p-adic limit $\chi(a) = \lim_{l\to\infty} a^{p^l}$ so that $\chi^{p-1}(a) = 1$ for $(a,p) = 1$, $\chi(a)\in Q_p$ and $\chi(a) \equiv a^{p^l} (\operatorname{mod} p^{l+1})$ (1). Then for an odd integer s, $1\leqslant s\leqslant p-2$, we obtain

$$\sum_{a=1}^{p} a\chi^s(a) \equiv \sum_{a=1}^{p} a^{sp^l+1} = \frac{B_{sp^l+2}(p)-B_{sp^l+2}}{sp^l+2}$$
$$= B_{sp^l+1}p + \frac{(sp^l+1)sp^l}{3!} B_{sp^l-1}p^3 + \ldots \equiv B_{sp^l+1}p (\operatorname{mod} p^{l+1}).$$

(1) So defined character for another aim is used by Kubota and Leopoldt [3].

Therefore if $s \neq p-2$ by Staudt's theorem we see

$$\frac{1}{p}\sum_{a=1}^{p} a\chi^s(a) \equiv B_{sp^l+1} \pmod{p^l},$$

so that (1) is proved.

For demonstration of analogy of (1) for cyclotomic field $Q\left(\exp\frac{2\pi i}{p^n}\right)$, $n > 1$, a construction of the character with a value in algebraic completion of Q_p is required.

References

[1] H. S. Vandiver, *On the first factor of the class number of a cyclotomic field*, Bull. Amer. Math. Soc. 25 (1919), pp. 458-461.

[2] H. Hasse, *Vandiver's congruence for the relative class number of the p-th cyclotomic field*, J. of Math. Anal. and Appl. 15 (1966), pp. 87-90.

[3] T. Kubota, H.-W. Leopoldt, *Eine p-adische Theorie der Zetawerte*, J. für Math. 214/215 (1964), pp. 328-339.

Reçu par la Rédaction le 16. 1. 1968

ACTA ARITHMETICA
XV (1969)

A number-theoretic constant*

by

R. J. Miech (Los Angeles, Calif.)

Let k be a positive integer, χ be a character modulo k, $L(s, \chi)$ be the associated L-series, and $\mathfrak{L}(s)$ be the product of all the L-series modulo k. It is well known that there is a positive constant c that does not depend on k such that $\mathfrak{L}(s)$ has at most one zero in the region

$$1-\frac{c}{\log k(2+|t|)} \leqslant \sigma \leqslant 1, \quad t \text{ arbitrary.}$$

There have been several investigations about the size of c. Landau, for example, proved that one could take $c > 1/(18.52)$ for the zeta function; that is, $c > 1/(18.52)$ for $k = 1$. ([5], p. 320.) More recently Pan Cheng-tung stated that one could take $c > 1/200$ for all large k [6] and Chen Jing-run claimed that this could be improved to $c > 1/(104.5)$ [2]. The interest of both of these authors in the nature of c was based on the fact that its size plays an important role in the determination of the size of the smallest prime of an arithmetic progression.

The purpose of this paper is to prove that one can take $c > 1/20$ for all large k. I think that this result can be employed to prove that the smallest prime in the progression $kn+l$ is less than k^a where a is somewhere in the neighborhood of 200; this would be an improvement on Chen Jing-run's result that $a \leqslant 777$. However I have not yet carried out the details of the proof.

Formally, the main result of this paper is the

THEOREM. *Let $\mathfrak{L}(s)$ be defined as above. Then there is a constant d_1 such that for all $k \geqslant d_1$ $\mathfrak{L}(s)$ has at most one zero in the region*

$$1-\frac{1}{20\log k(1+|t|)} \leqslant \sigma \leqslant 1, \quad t \text{ arbitrary}.$$

Moreover, if $\mathfrak{L}(s)$ does have one zero β in this region then β is real and it is a zero of $L(s, \chi_1)$ where χ_1 is a real character modulo k.

*The preparation of this paper was sponsored in part by NSF Grant GP-5497.