Canad. Math. Bull. Vol. **24** (3), 1981

A NOTE ON DIRICHLET'S THEOREM

BY
R. A. SMITH

A well-known theorem of Dirichlet asserts that for any pair of positive integers k and n which are relatively prime, there exists an infinity of primes $p \equiv k \pmod{n}$. In 1949, Selberg [5] gave a rather complicated non-analytic proof of this result. Although a simple-minded non-analytic proof of this result is highly desirable, no such proof seems to exist except for special cases. Such a proof was given in 1903 by Birkhoff and Vandiver [1] for the special case $k = 1$; variations of this proof have been given by Rotkiewicz [4] and Estermann [2]. The combinatorial nature of these proofs (for $k = 1$) unfortunately distract from the underlying simplicity of the idea of the proof. The following is an arithmetic interpretation of Birkhoff and Vandiver's argument.

To show the existence of infinitely many primes $p \equiv 1 \bmod n$, it suffices to show there exists infinitely many primes p for which the congruence

$$X^n \equiv 1 \bmod p$$

is solvable with an integer of order n mod p. This can be accomplished as follows.

For any $n \geq 1$, let F_n denote the nth cyclotomic polynomial. As is well-known, $F_n \in \mathbb{Z}[X] - \mathbb{Z}$ and

$$X^n - 1 = \prod_{d|n} F_d(X). \tag{1}$$

For any prime p and any non-zero integer $z \in \mathbb{Z}$, let $\operatorname{ord}_p(z)$ denote the unique integer $\nu \geq 0$ defined by $z = p^\nu y$ where $y \in \mathbb{Z}$ and $(y, p) = 1$. Thus, for any $x \in \mathbb{Z}$, $x \neq \pm 1$ (1) implies

$$\operatorname{ord}_p(x^n - 1) = \sum_{d|n} \operatorname{ord}_p F_d(x). \tag{2}$$

By the Möbius Inversion Formula, (2) can be rewritten as

$$\operatorname{ord}_p F_n(x) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \operatorname{ord}_p(x^d - 1). \tag{3}$$

By a well-known theorem (cf. [3], p. 82), there exists infinitely many primes p

Received by the editors November 15, 1979.

such that

$$F_n(X) \equiv 0 \bmod p \tag{4}$$

is solvable in $\mathbb{Z}$. Fix such a prime $p > n$ and choose an integer x satisfying (4). Then by (1), $x^n \equiv 1 \bmod p$. If f is the order of $x \bmod p$, then clearly f divides n. Thus it suffices to show that $f = n$. We prove this as follows.

Since $\operatorname{ord}_p(x^d - 1) = 0$ if f does not divide d, then (3) becomes

$$\begin{aligned} \operatorname{ord}_p F_n(x) &= \sum_{\substack{d \mid n \\ f \mid d}} \mu\left(\frac{n}{d}\right) \operatorname{ord}_p(x^d - 1) \\ &= \sum_{d \mid m} \mu\left(\frac{m}{d}\right) \operatorname{ord}_p(x^{df} - 1) \end{aligned} \tag{5}$$

where $m = n/f$. For any integer $d \geq 1$ relatively prime to p, then

$$\operatorname{ord}_p(x^{df} - 1) = \operatorname{ord}_p(x^f - 1). \tag{6}$$

To see this, let $x^f = 1 + tp^s$, where $(t, p) = 1$ and $s = \operatorname{ord}_p(x^f - 1) \geq 1$. Since $(d, p) = 1$, then clearly $x^{df} = 1 + t_1 p^s$ where $(t_1, p) = 1$, as required.

Since $(m, p) = 1$, then (5) and (6) imply

$$\begin{aligned} \operatorname{ord}_p F_n(x) &= \operatorname{ord}_p(x^f - 1) \sum_{d \mid m} \mu\left(\frac{m}{d}\right) \\ &= \operatorname{ord}_p(x^f - 1) \begin{cases} 1 & \text{if } m = 1 \\ 0 & \text{if } m > 1. \end{cases} \end{aligned}$$

Since $\operatorname{ord}_p F_n(x) \geq 1$, then $m = 1$, i.e., $n = f$ as required.

References

1. G. D. Birkhoff and H. S. Vandiver, *On the integral divisors of* $a^n - b^n$, Ann. of Math. **5** (1903/1904), 173–180.

2. T. Estermann, *Note on a paper of A. Rotkiewicz*, Acta Arith. **8** (1963), 465–467.

3. T. Nagell, *Introduction to Number Theory*, John Wiley and Sons, New York (1951).

4. A. Rotkiewicz, *Démonstration arithmétique de l'existence d'une infinité de nombres premiers de la forme* $nk + 1$, L'Enseignement Math. (2) **7** (1961), 277–280.

5. A. Selberg, *An elementary proof of Dirichlet's Theorem about primes in an arithmetic progression*, Ann. of Math. (2) **50** (1949), 297–304.

University of Toronto,
Toronto, Canada,
M5S 1A1.