A COLORING PROOF OF A GENERALISATION OF FERMAT'S LITTLE THEOREM

C. J. SMYTH

Department of Electronic Systems Engineering, University of Essex, Colchester CO4 3SQ, United Kingdom

Before stating the main result of this note, I ask the reader to fill in the missing formula in the following table:

	$(a, n) = 1$	all integers a
$n = p$ prime	$a^{p-1} \equiv 1 \pmod p$	$a^p \equiv a \pmod p$
n composite	$a^{\phi(n)} \equiv 1 \pmod n$	?

(Here ϕ is Euler's totient function: $\phi(n) = n\prod_{p|n}(1 - \frac{1}{p})$).

The answer to this question seems little-known to mathematicians, even to number theorists. The reason for this seems to be its non-appearance in most of the standard reference books. The missing result is a beautiful one:

$$(1) \qquad \sum_{d|n} a^d \mu\left(\frac{n}{d}\right) \equiv 0 \pmod n$$

(μ being the Möbius function defined by $\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \prod_{p \text{ prime}} (1 - p^{-s})$). Its history is chronicled in Dickson [**1**, pp. 82–86]. Gauss' proof of the result, but only for a prime, was published posthumously in 1863. It was not until 1880–83 that four independent proofs for all a were published by Kantor, Weyr, Lucas and Pellet (for precise references see [**1**]; see also [**5**]).

Let $\theta_1, \theta_2, \ldots, \theta_D$ be the zeros of a monic polynomial with integer coefficients, and put

$$(2) \qquad S_n = \theta_1^n + \theta_2^n + \cdots + \theta_D^n.$$

Then the result

$$(3) \qquad S_p \equiv S_1 \pmod p$$

proved by Schönemann [**4**] in 1839 is a generalisation of

$$(4) \qquad a^p \equiv a \pmod p$$

to which, of course, (3) reduces if $D = 1$.

The result I will prove is the following:

$$(5) \qquad \sum_{d|n} S_d \mu\left(\frac{n}{d}\right) \equiv 0 \pmod n$$

generalising both (1) and (3).

In 1872 Petersen [**3**] proved Fermat's Little Theorem (4) by the following argument (for $a > 0$): Suppose one has p boxes, arranged in a circle, to be colored with a colors. There are a^p colorings in all, and a colorings with every box the same color. The $a^p - a$ remaining colorings can be arranged in sets of p, since the p rotations of any one of these colorings are all distinct. Hence $p|(a^p - a)$.

Thue [**6**] in 1910 published a proof of (1) by generalising this idea. (His proof is neatly summarised in [**1**, p. 82]. Thue uses (1) to prove $a^{\phi(n)} \equiv 1 \pmod n$ for $(a, n) = 1$.) Here we will prove (5), by generalising a bit further. Our result is:

THEOREM. *Let $a_1, a_2, a_3, \ldots$ be an infinite sequence of non-negative integers. Suppose we are given n boxes, arranged in a circle. In some of the spaces between adjacent boxes, a barrier or* *partition is placed, the number of such partitions ranging from* 1 *to* n. *Suppose that a group of* j *boxes between two partitions must be painted the same color, from a palette of* a_j *different colors. Then the total number* s_n^* *of such "partition-colorings" of the boxes satisfies*

$$(6^*) \qquad s_n^* = a_1 s_{n-1}^* + a_2 s_{n-2}^* + \cdots + a_{n-1} s_1^* + n a_n \quad (n = 1, 2, \ldots),$$

$$(5^*) \qquad \sum_{d|n} s_d^* \mu\left(\frac{n}{d}\right) \equiv 0 \pmod n.$$

Note that the coloring does not always specify the partition: when there is only one partition, all n boxes are colored alike, in a_n possible colors, but we count $n\, a_n$ total partition-colorings, taking into account the n possible positions for the partition.

Before proving the theorem, we show how (5) follows from it. Let

$$\begin{aligned} P(x) &= (x - \theta_1)(x - \theta_2) \cdots (x - \theta_D) \\ &= x^D - a_1 x^{D-1} - a_2 x^{D-2} - \cdots - a_{D-1} x - a_D, \end{aligned}$$

say. Then, as Newton showed, the S_n defined by (2) satisfy

$$(6) \qquad S_n = a_1 S_{n-1} + a_2 S_{n-2} + \cdots + a_{n-1} S_1 + n a_n \quad (n = 1, 2, \ldots),$$

where we put $a_k = 0$ for $k > D$. This follows straight from the fact that

$$D + \sum_{n=1}^{\infty} S_n z^n = \sum_{j=1}^{D} \frac{1}{1 - \theta_j z} = P'(z^{-1}) / (z P(z^{-1})).$$

Since $\{S_n\}$ is uniquely specified by (6), we have from the Theorem that $S_n = s_n^*$ and so (5) holds, when $a_1, \ldots, a_D$ are non-negative.

If any a_i in (7) are negative, we can still verify (5), as follows: fix n, and put

$$a_i = a_i^+ - k_i n \quad (i = 1, \ldots, D),$$

where the a_1^+ are positive, and the k_i integers. Define $S_1^+, S_2^+, \ldots, S_n^+$ by

$$(6^+) \qquad S_j^+ = a_1^+ S_{j-1}^+ + \cdots + a_{j-1}^+ S_1^+ + j a_j^+ \quad (j = 1, \ldots, n).$$

Then $\sum_{d|n} S_d^+ \mu(\frac{n}{d}) \equiv 0 \pmod n$. But $S_j \equiv S_j^+ \pmod n$ for $j = 1, \ldots, n$ by (6^+) and so (5) follows for arbitrary integers a_i.

Proof of the theorem. Label the boxes $B_0, B_2, \ldots, B_{n-1}$, going around clockwise. Suppose, for a particular partition-coloring that, starting from B_0, the first complete group of boxes between partitions goes from B_t to $B_{t+u-1 \pmod n}$. Then by removing this group of u boxes, and closing up the gap (leaving a partition there), we obtain an associated partition-coloring of $n - u$ boxes, if $u < n$. (If $u = n$ we know already that we obtain $n\, a_n$ possible colorings.)

Conversely, any partition-coloring of $n - u$ boxes, $u < n$, can be used to construct a partition-coloring of n boxes, by inserting a group of u boxes, followed by a partition, immediately after the first partition found, on proceeding from B_0 clockwise. Thus this correspondence is 1–1, and, since the inserted group of u boxes can be colored in a_u ways,

$$s_n^* = \sum_{u=1}^{n-1} a_u s_{n-u}^* + n a_n$$

which is (6^*).

We now show that there are integers r_n divisible by n such that

$$(7) \qquad s_n^* = \sum_{d|n} r_d,$$

from which $n|r_n = \sum_{d|n} s_d^* \mu(\frac{n}{d})$, and hence (5*) follows immediately by Möbius inversion (see, e.g., [2, p. 234]).

We define r_n to be the number of partition-colorings of n boxes which are distinct from all their rotations. Then clearly $n|r_n$. Further, the partition-colorings of n boxes which have the property that rotation by d places, but not fewer, produces the same coloring are obtained in the following way: Take any of the r_d colorings of d boxes referred to above, and repeat the pattern n/d times, with a partition between each pattern, to obtain a coloring of n boxes. There are r_d such colorings, and so the total number s_n^* colorings is given by (7). This completes the proof of the theorem.

I would like to thank Professor David Boyd for useful discussions concerning this topic, and Professor A. Schinzel for providing reference [5]. This note was written while the author was at James Cook University, Townsville, Australia.

References

1. L. E. Dickson, History of the Theory of Numbers, Vol. 1, Chelsea, New York, 1971.
2. G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, 4th ed., Oxford University Press, 1960.
3. J. Petersen, Tidsskrift for Mathematik (3), 2, 1972, 64–65 (Danish).
4. T. Schönemann, J. Für Math. (Crelle), 19 (1839), p. 290, 31 (1846), p. 288.
5. T. Szele, Une généralisation de la congruence de Fermat, Mat. Tidsskr, B. 1948, 57–59 (1948).
6. A. Thue, Ein Kombinatorischer Beweis eines Satzes von Fermat, in Selected Mathematical Papers of Axel Thue, Universitelsforlaget, 1977 (originally Kra. Vidensk. Selsk, Skrifter. I. Mat. Nat. Kl. 1910, No. 3).

SOME REMARKS ON FUNCTIONS WITH ONE-SIDED DERIVATIVES

A. D. Miller* and R. Výborný
University of Queensland, St. Lucia, 4067 Queensland, Australia

An important theorem in introductory calculus relates the monotonicity of a function to the sign of its derivative: If f is continuous on the closed interval $[a, b]$ and differentiable on the open interval (a, b), then f is monotonic increasing (decreasing) if and only if $f' \geqslant 0$ ($\leqslant 0$) on (a, b). (A simple corollary to this result states that f is constant on $[a, b]$ if and only if $f' = 0$ on (a, b).) Most standard proofs of the sufficiency part of this theorem use the classical Mean Value Theorem of Calculus.

Despite the simple geometrical interpretation of the Mean Value Theorem, namely, the chord of the graph of f must be parallel to the tangent at some intermediate point, experience in teaching elementary calculus courses shows that whereas students find the above monotonicity theorem geometrically plausible, they often have difficulty in grasping the meaning of the Mean Value Theorem. It is interesting to note that the usual textbook proof of the Mean Value Theorem is due to Bonnet, and first appeared in print in 1868. For a detailed historical account of the Mean Value Theorem see [2]. Surprisingly, it does not seem generally known that a few years later Scheeffer [6] in an investigation of the uniqueness of the anti-derivative introduced an idea which is able to provide an alternative, simple and intuitive approach to the above monotonicity result. In this note we wish to revive this idea. However, our main aim is to prove the monotonicity result but requiring only conditions on one-sided derivatives. In doing this we refine the remark of Knight [5].

THEOREM 1. *Let f be a continuous function on $[a, b]$. If for each $x \in (a, b)$ one of the one-sided*

*Now at Centre for Mathematical Analysis, Australian National University, Canberra, A.C.T. 2600, Australia.