unites them, and to make them known individually, luminously and completely." Therefore let us cultivate geometry which has its own advantages, and this without wishing to make it equal in all points to its rival. Besides, if we should be tempted to neglect it, it would soon find, as it once has done, in the applications of mathematics the means of reviving and developing itself anew. It is like the giant Antæus, who regained his strength whenever he touched his mother earth.

NOTE ON FERMAT'S NUMBERS.

BY DR. J. C. MOREHEAD.

(Read before the American Mathematical Society, April 29, 1905.)

How many primes are contained in the form

$$F_n = 2^{2^n} + 1$$

is a famous question in the theory of numbers. Fermat showed that F_0, F_1, $\cdots$, F_4 are primes, and stated that he believed F_n to be prime for every value of n. This statement of Fermat was generally accepted as correct until Euler showed in 1732 that F_5 has the factor 641. In the period 1878–1903 factors were found of eight other Fermat numbers, viz.,

$$F_6, \quad F_9, \quad F_{11}, \quad F_{12}, \quad F_{18}, \quad F_{23}, \quad F_{36}, \quad F_{38}.$$

In the present note we add to the list the tenth composite case, F_7, identified by applying Pepin's criterion:* "The necessary and sufficient condition that F_n be prime is

$$P_n = \alpha^{\frac{1}{2}(F_n-1)} + 1 \equiv 0 \pmod{F_n},$$

α being any quadratic non-residue of F_n." Taking the non-residue $\alpha = 3$, I have found by a lengthy computation just completed that

* *Comptes rendus*, vol. 85 (1878), p. 329.

$$P_7 \equiv 110\ 780\ 954\ 395\ 540\ 516\ 579\ 111\ 562\ 860\ 048\ 860\ 421 \mod F_7.$$

Hence F_7 is necessarily composite.*

This result is of especial interest and importance in the theory of Fermat's numbers, as the following considerations will make clear. Euler showed that the factors of F_n are of the form $2^{n+1}q + 1$, which led to his factoring F_5; and Lucas showed that the factors must have the form

$$Q_n = 2^{n+2}q + 1.$$

Now $F_0, \cdots, F_3$ are primes for the sufficient reason that $Q_n > \sqrt{F_n}$; and 193 is the only prime $Q_4 < \sqrt{F_4}$. But as soon as Q_n has any range of values, we have $F_5, F_6, \cdots$ composite. Thus the fact that $F_0, \cdots, F_4$ are primes gives no ground for inferring that there are other primes of the form F_n. No one has proved the existence of a single prime F_n after F_4. This was the main feature of interest in the result of the computation I carried out for F_7 — there was the possibility that F_7 would turn out to be a prime. Besides, on account of the increasing difficulty of applying any known necessary and sufficient criterion to the higher Fermat's numbers, F_7 was looked upon as the last chance for determining a Fermat prime, — at least until essentially different criteria, or more powerful methods of computation are devised. A similar computation for F_8, if practicable at all, would involve at least eight times the labor of the computation for F_7.

The number F_6 was first shown to be composite by a method † somewhat similar to that which I have now applied to F_7. But all known factors of F_n were obtained by the direct method of testing as possible factors primes of the form Q_n. I have devised a means of investigating these possible factors Q_n, based

* On page 13 of Klein's Vorträge über ausgewählte Fragen der Elementargeometrie it is asserted that F_7 is composite. It is highly probable that this is a misprint, as a careful search through the entire literature on this subject has failed to reveal any other reference to this fact. In particular, cf. Hermes' paper, presented by Klein himself, in *Gött. Nachrichten*, 1894, p. 170; Lucas, Récréations Mathématiques, II (1896), pp 234, 235; Bachmann, Encyk. der Math. Wiss., I, p. 577; Cunningham and Western, *Proc. Lond. Math. Soc.* (2), vol. I (1904), p. 175.

† Lucas, Récréations Mathématiques, II, pp. 234, 235; *Amer. Journ. of Math.*, vol. I (1878), p. 238; *Comptes rendus*, vol. 85 (1878), p. 138.

on an extensive table of values of a pair of numerical functions. Although the table is only partially completed, I have shown by this method that, aside from those already known, there are no factors under 524,288,000 of any F_n, $n > 16$, as against the limit 100,000,000 given by Cunningham and Western.* Incidentally, this method shows four errors in a list of forty-five numbers of the form Q_n studied by Seelhoff.†

NEW HAVEN, CONN.,
June 15, 1905.

SIMPLY TRANSITIVE PRIMITIVE GROUPS WHICH ARE SIMPLE GROUPS.

BY PROFESSOR H. L. RIETZ.

(Read before the Chicago Section of the American Mathematical Society, April 22, 1905).

IN the papers published by several writers ‡ relating to the existence of simple groups of odd composite order, much use is made of the fact that, if such a group existed, it could be represented as a simply transitive primitive substitution group. But this work has thus far led to no simple groups.

In working on this problem, it appeared well to examine some simply transitive primitive groups which are simple groups of even order, but upon examining the literature of primitive groups with a view to finding groups of this type, I find only two such groups. It therefore seems worth while to call attention to a system of groups of this type. This will be done by proving the following theorem:

There is a simple group G of composite order corresponding to every prime number $p > 11$ (where $p = 2q + 1$, q being a prime number) which can be represented as a simply transitive primitive group of degree

$$1 + \kappa p \quad \left(\frac{(p-2)! - 1}{p} \equiv \kappa > 1 \right).$$

---

* *Proc. Lond. Math. Soc.* (2), vol. 1 (1904), p. 175.

†*Zeitschrift für Math. u. Phys.*, vol. 31, p. 380. The present range of my table covers only eighteen numbers of Seelhoff's list.

‡ Miller, *Proc. Lond. Math. Soc.*, vol. 33, pp. 6–10. Burnside, *Proc. Lond. Math. Soc.*, vol. 33, pp. 162–185. Rietz, *Amer. Journ. Math.*, vol. 26, pp. 1–30.