BULLETIN OF THE

AMERICAN MATHEMATICAL SOCIETY.

NOTE ON FERMAT'S NUMBERS.

BY DR. J. C. MOREHEAD AND MR. A. E. WESTERN.

(Read before the Chicago Section of the American Mathematical Society, April 9, 1909.)

In June, 1658, Fermat wrote to Sir Kenelm Digby a letter,* in which, after referring to certain theorems proved by him, which he might propose to Viscount Brouncker and John Wallis, in order to give them something to do, he said that, instead of these theorems, he would submit to them, as problems, some theorems which he admitted he could not prove, though he was convinced of their truth. The first of these problems was to prove that $2^{2^n} + 1$ is a prime, and he gave as examples the numbers corresponding to $n = 1, 2, 3, 4$, which in fact are primes. Fermat challenged his English friends to furnish a proof of this proposition, which was certainly very beautiful, and which he believed was true. He added that perhaps the proof would give the key to penetrate all the mystery of prime numbers.†

As is well known, the theorem is untrue for many values of n.‡ In 1905 Dr. Morehead read before the AMERICAN MATHEMATICAL SOCIETY a "Note on Fermat's numbers,"‡ which stated the result of a calculation proving that $F_7 = 2^{128} + 1$ is composite. Mr. Western had independently performed the same calculation, and communicated the result almost simul-

*Pierre de Fermat, Œuvres, Paris, 1896, vol. 2, p. 405 (in Latin); vol. 3, p. 315 (French translation).

†That Fermat attached great importance to this theorem is further evidenced by the fact that he referred to it in six other letters and papers written between 1640 and 1659. Cf. Œuvres, vol. 1, p. 131; vol. 2, pp. 206, 207, 212, 309, 434.

‡W. W. R. Ball, Mathematical Recreations and Problems, 2d ed., 1892, p. 26. *Proc. Lond. Math. Soc.*, Series 2, vol. 1 (1904), p. 175. BULLETIN, vol. 11, p. 543, and vol. 12, p. 449.

taneously to the London Mathematical Society;* and it was found that the two calculations were in exact agreement. There is therefore no doubt that F_7 is composite, but the actual factors are unknown. The authors have since carried out a similar calculation for F_8, each doing a half of the whole work. As this is probably by far the largest calculation in connection with the theory of numbers which has been yet performed, some particulars of the methods employed may be of interest.

The test employed by the authors in the case both of F_7 and F_8 depends on the following theorem:

If $a^x \equiv 1 \pmod{p}$ *is true when* $x = p - 1$, *but is not true when* x *is any factor of* $p - 1$, *then* p *is prime.*

This theorem appears to have been first given by Lucas in 1876, and is called by him the reciprocal of Fermat's theorem.† The proof is very simple; if p is composite, then $\phi(p) < p - 1$; and if the assumption of the theorem is satisfied, then $a^x \equiv 1 \pmod{p}$ for both $x = \phi(p)$ and $x = p - 1$, and therefore also for $x = \delta$, the greatest common divisor of $\phi(p)$ and $p - 1$, which contradicts the assumption. Therefore, under the conditions of the theorem, p cannot be composite.

Applying this to the case of Fermat's numbers, and taking $a = 3$, it is clear that if F_n is prime,

$$3^{\frac{1}{2}(F_n - 1)} \equiv -1 \pmod{F_n},$$

for $F_n \equiv -1 \pmod{3}$, and so 3 is a quadratic non-residue of F_n. And since $\frac{1}{2}(F_n - 1)$ is a power of 2, no value of x less than $\frac{1}{2}(F_n - 1)$ will make

$$3^x \equiv -1 \pmod{F_n}.$$

Therefore by Lucas's theorem, if

$$3^{\frac{1}{2}(F_n - 1)} \equiv -1 \pmod{F_n},$$

F_n is prime, and if not, F_n is composite.

The index of 3 in this congruence may be reduced; for

$$-1 \equiv 2^{2^n} \pmod{F_n},$$

and we therefore obtain, by successive extractions of the square root,

$$3^{2^{(2^n - n - 1)}} \equiv 2^x \pmod{F_n},$$

Proc. Lond. Math. Soc., ser. 2, vol. 3, p. xxi.

† Lucas, Théorie des Nombres; Paris, 1891, p. 441.

where x is odd. Now

$$2 \equiv 2^{2^{n-1}}(2^{2^{n-1}} - 1)^2 \pmod{F_n},$$

and so

$$(A) \qquad 3^{2^{(2^n-n-2)}} \equiv \pm 2^y(2^{2^n-1} \pm 1) \pmod{F_n},$$

where y may be taken to be between 0 and 2^{n-1}.

Applying this criterion to F_8, it is necessary to calculate the residue of the 2^{246}th power of 3 (mod F_8).

Mr. Western's method was as follows. Having obtained

$$3^{2^t} \equiv \Sigma a_n x^n \pmod{F_8} \quad (n = 0, 1, \cdots, 7),$$

where $x = 2^{32}$, and $a_0, a_1, \cdots, a_7$, are positive or negative numbers less than $\frac{1}{2}x$ (*i. e.* containing at most 10 digits), the residue on the right is squared; since $x^8 \equiv -1$, we obtain

$$3^{2^{t+1}} \equiv \Sigma A_n x^n \pmod{F_8},$$

where

$$A_0 = a_0^2 - 2a_1a_7 - 2a_2a_6 - 2a_3a_5 - a_4^2,$$

$$A_1 = 2(a_0a_1 - a_2a_7 - a_3a_6 - a_4a_5), \quad \text{etc.};$$

thus division by F_8 is performed simultaneously with the operation of squaring. The numbers $A_0, A_1, \cdots$ are each less than $2x^2$ (and generally less than x^2); each A is then divided by x, giving

$$A_r = b_r + xc_r,$$

where

$$|b_r| < \tfrac{1}{2}x, \quad |c_r| < 2x,$$

and then

$$3^{2^{t+1}} \equiv (b_0 - c_7) + (b_1 + c_0)x + \cdots + (b_7 + c_6)x^7.$$

The coefficients in this are then adjusted, so as to make each of them numerically less than $\frac{1}{2}x$, and we finally get

$$3^{2^{t+1}} \equiv \Sigma a'_n x^n \pmod{F_8}.$$

The whole process is then repeated. The calculations of A_r, b_r, c_r, were wholly performed on a 10-figure arithmometer, and the b_r and c_r alone were written down.

In such a calculation as this, in which a single error would vitiate all the subsequent work, care must be taken to detect any mistakes in each stage, before proceeding to the next stage. The test employed by Mr. Western was

$$\sum a' \equiv (a_0 + a_1 + a_2 + a_3)^2 - (a_4 + a_5 + a_6 + a_7)^2 + 2(a_0 + a_1 + a_2 + a_3)(a_4 + a_5 + a_6 + a_7) - 4a_3(a_5 + a_7) - 4a_6(a_2 + a_3) - 4a_7(a_1 + a_2) - 2(c_7 + d) \pmod{k},$$

where d is the multiplier of x^8 carried forward from the last term $(b_7 + c_6)x^7$ to the first term, and k is any factor of $x - 1$. The values of k used were 3, 5, and 17.

Dr. Morehead expressed the residue of $3^{2^{126}}$, calculated by Mr. Western, in the form $ax + b$, where $x = 2^{128}$ and $|a|$, $|b| < \frac{1}{2}x$; then squaring and replacing x^2 by -1, he obtained

$$3^{2^{127}} \equiv 2abx + (b - a)(b + a) \pmod{F_8}.$$

The products $2ab$, $(b - a)(b + a)$ were then calculated and expressed, by division by x, in the forms $\alpha x + \alpha'$, $\beta x + \beta'$ respectively, so that

$$2abx + (b - a)(b + a) = (\alpha x + \alpha')x + \beta x + \beta' \equiv (\alpha' + \beta)x + \beta' - \alpha \pmod{F_8},$$

$\alpha, \alpha', \beta, \beta'$ having been so adjusted that $|\alpha' + \beta|$, $|\beta' - \alpha| < \frac{1}{2}x$. Thus was obtained

$$3^{2^{127}} \equiv a'x + b' \pmod{F_8},$$

and, by repetition of this process, the residues of

$$3^{2^{128}}, 3^{2^{129}}, \cdots, 3^{2^{246}}.*$$

The test formula (A) shows that if F_8 were prime we should have, in the residue of $3^{2^{246}}$, $|a| = |b|$. This residue was found to be

(107 2093 3158 0550 8180 4331 6350 5866 1999 4098)x

+ (34 1778 3881 0697 6545 8021 2127 5588 1034 4254),

and therefore F_8 is composite.

This result is especially interesting as completing a chain of

* The part of the calculation carried out by Dr. Morehead was checked at each stage by applying the test

$$-ab + b^2 - a^2 \equiv 4a' + b' - \alpha \pmod{9},$$

and similar tests for the moduli 11, 19, 41, 101. Two 8-figure calculating machines were used together for the greater part of the calculation and checking at each stage.

five composite Fermat numbers, F_5, F_6, F_7, F_8, F_9, following the first five (and only known) Fermat primes, 3, 5, 17, 257, 65537, and as leaving F_{10}(a 309-place number) the smallest Fermat number whose status is unknown. All the Fermat numbers $F_5, \cdots, F_{12}$, except F_{10}, are now known to be composite.

If ζ is a primitive 2^{n+1}th root of 1, so that $\zeta^{2^n} = -1$, F_n is the norm of $2 - \zeta$ in the field of ζ. Accordingly the problem of factoring F_n is the same as that of factoring $2 - \zeta$. It is possible that Fermat may have observed this, and may have assumed that it was improbable that $2 - \zeta$ could have complex factors of the form

$$a_0 + a_1\zeta + \cdots + a_{2^n-1}\zeta^{2^n-1}.$$

In fact, when $n \geqq 2$, the field contains an infinite number of units, and so $2 - \zeta$ can be expressed in an infinite number of ways as the product of two complex numbers of the field, one of these being a unit, and the other having F_n as its norm. But whether, for any value of n, $2 - \zeta$ can be expressed as the product of two actual numbers of the field, neither being a unit, is not known. It seems probable that the prime factors of $2 - \zeta$, if any, are always ideals.

Actual complex numbers containing the complex factors of known factors of Fermat's numbers may be easily found; for instance, ζ being a primitive 64th root of 1, and p being 641, the smaller factor of F_5,

$$p = 1 + 2^7 + 2^9.$$

But $2 \equiv \zeta \pmod{\pi}$, π being one of the prime factors of p in the field of ζ, so

$$1 + \zeta^7 + \zeta^9 \equiv 0 \pmod{\pi}.$$

The norm of $1 + \zeta^7 + \zeta^9$ is 193.641, as shown by Reuschle,* who states that the prime factors of 641 are ideal.

Again the smaller factor of F_6 is

$$p = 274{,}177 = 1 - 2^8 - 2^{12} + 2^{14} + 2^{18},$$

so ζ being as before, and π being a prime factor of p in the field of ζ, we have $4 \equiv \zeta \pmod{\pi}$, and so,

$$1 - \zeta^4 - \zeta^6 + \zeta^7 + \zeta^9 \equiv 0 \pmod{\pi}.$$

* Tafeln complexer Primzahlen, p. 455.

The norm of the number on the left is found to be p. It seems impracticable to determine whether or not p has actual prime factors in the field of 128th roots of 1, but this is very improbable, as the class number in that field is a multiple of 21,121.*

The use of complex numbers appears to be of no assistance in the problem of determining whether F_n is prime or composite.

AN EXTENSION OF CERTAIN INTEGRABILITY CONDITIONS.

BY PROFESSOR J. EDMUND WRIGHT.

SUPPOSE there are n functions $a_1, a_2, \cdots, a_n$ of n independent variables $x_1, x_2, \cdots, x_n$, satisfying the conditions

$$\frac{\partial a_p}{\partial x_q} - \frac{\partial a_q}{\partial x_p} = 0$$

for all values of p and q. It is well known that the functions a must all be first derivatives of a single function V. Similarly, if there are $\frac{1}{2}n(n+1)$ functions a_{pq} such that $a_{pq} = a_{qp}$, satisfying the relations

$$\frac{\partial a_{pq}}{\partial x_r} = \frac{\partial a_{pr}}{\partial x_q}$$

for all values of p, q, r, then the a's must be second derivatives of a single function.

The following question arises in connection with an application of the theory of invariants of quadratic differential forms:

Suppose there are $n(n+1)$ functions H_{pq}, K_{pq} such that $H_{pq} = H_{qp}$, $K_{pq} = K_{qp}$, satisfying the conditions

$$\frac{\partial}{\partial x_r}(H_{pq}) + K_{pq}\frac{\partial Y}{\partial x_r} = \frac{\partial}{\partial x_p}(H_{qr}) + K_{qr}\frac{\partial Y}{\partial x_p},$$

for all values of p, q, r; Y being a given function of the variables; what are the conditions on the functions H, K?

We first consider the case of $2n$ functions $a_1, a_2, \cdots, a_n; b_1, b_2, \cdots, b_n$, satisfying the conditions

* Reuschle, Tafeln, p. 461.