Eureka No 11, Jan 1949

Sloane 1350 1351

—A Problem in
ebra

TON

electing members of itself
oard sisting of president,
M.P. here are N of them
the same board there are
ich makes just one election.
ing elected by two boards
r, for any five M.P.'s the
cted by the board whose
d men respectively, whose
whose secretary is the fifth
the board whose president
is the man elected by the
and fourth men respectively,

ith that of the board whose
t the second, and secretary
fficers are the third, fourth

M.P. B such that any board
-president (not necessarily
etary.

three members of a board
of president and secretary
.

members always make the
which office on the board,

r he serves as two members
d if define the product
lected by the board whose
en the M.P.'s form a group.

I forum
to bore 'em.
ne

sinorum.

# A Note on Fermat's Last Theorem and the Mersenne Numbers

By C. B. Haselgrove

The object of this paper is to establish a connection between Fermat's Last Theorem and some numbers which are of the same type as the Mersenne Numbers but which are more general in nature. A table of these numbers, which we shall call the *Associated Mersenne Numbers*, can be found at the end of this paper. The method that we shall use is the classical method of the theory of equations which we shall apply to the theory of congruences. We shall assume that the reader is familiar with the elementary theory of congruences as given in works such as Hardy and Wright: *An Introduction to the Theory of Numbers*. Almost all the theorems of the theory of equations may be taken over into the theory of congruences by merely replacing the equality signs by congruence signs. In particular, this is true of the theorem that any symmetric function of the roots, with integral coefficients, can be expressed as a polynomial function of the coefficients with integral coefficients. The proof of this result in the theory of congruences is the same as in the theory of equations except for the replacement of all the equality signs by congruence signs.

It is well known that if $p$ is a prime of the form $(nr + 1)$ the congruence:

$$x^n \equiv 1 \pmod{p} \quad \ldots \quad \ldots \quad \ldots \quad (1)$$

has $n$ distinct roots which are the residues which $r^{th}$ powers may take (mod $p$). For by a theorem due to Fermat we have $a^{nr} \equiv a^{p-1} \equiv 1 \pmod{p}$ provided that $p$ does not divide $a$. For if $x$ is a root of the congruence (1) the congruence $a^r \equiv x$ has at most $r$ roots. Also the congruence (1) has at most $n$ roots. If it has fewer than $n$ roots we arrive at a contradiction since $a$ can take $nr$ different values (mod $p$). Let the roots of the congruence (1) be $x_1, x_2, \ldots x_n$. Then, as we have stated above, any polynomial symmetric function of the $x_i$ with integral coefficients can be expressed as a polynomial function of the coefficients with integral coefficients. This function of the coefficients is the same as the corresponding symmetric function of the roots of the equation

$$x^n = 1 \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad (2)$$

which we shall suppose has roots $z_1, z_2 \ldots z_n$ where $z_n = 1$. Thus we have in particular

$$\Pi\,(n_i + x_j - 1) \equiv \Pi\,(z_i + z_j - 1) \pmod{p} \quad \ldots \quad (3)$$

where $i$ and $j$ both run from 1 to $n$ on both sides of the equation. As the factors of the left-hand side of (3) are the possible values of



Entered
Extend!

$x^r + y^r - 1 \pmod{p}$, the necessary and sufficient condition that it is possible to solve the congruence

$$x^r + y^r \equiv 1 \pmod{p} \qquad \ldots \qquad \ldots \qquad (4)$$

is that $p$ should divide the right-hand side of the equation (3), which is an integer which we shall denote by $\sigma(n)$. This is the necessary and sufficient condition that the congruence

$$x^r + y^r \equiv z^r \pmod{p} \qquad \ldots \qquad \ldots \qquad (5)$$

can be solved with $xyz$ not divisible by $p$. For if we can solve (4) we can certainly solve (5) by taking $z \equiv 1$. Also, if we can solve (5) we can solve (4) by finding $a$, so that $az \equiv 1 \pmod{p}$ and then multiplying both sides of the congruence (5) by $a^r$. Hence, if $x$, $y$ and $z$ are three positive integers such that:

$$x^r + y^r = z^r \qquad \ldots \qquad \ldots \qquad \ldots \qquad (6)$$

and if $p$ is a prime of the form $(nr + 1)$ then either $p$ divides $xyz$ or divides $\sigma(n)$. Thus, $p$ divides $xyz\sigma(n)$. It now remains to determine the factors of the numbers $\sigma(n)$.

Consider the product

$$a_k(n) = \prod (z_i^k + z_i - 1) \quad i = 0, 1, \ldots n - 1 \quad \ldots \qquad (7).$$

Then $a_k(n)$ is an integer since the product on the right-hand side of (7) is a symmetric function of the roots of the equation (2). Further, if $n$ is a prime we have:

$$\prod_{k=1}^{n-1} a_k(n) = \prod_{i=1}^{n} \prod_{k=1}^{n-1} (z_i^k + z_i - 1).$$

Now if $z_i \neq 1$, $z_i^k$ runs through all the $z_j \neq 1$. If $z_i = 1$, $z_i^k + z_i - 1 = 1$ for all $k$. Hence the product equals

$$\prod_{i=1}^{n} \prod_{j=1}^{n} (z_i + z_j - 1)$$

since the product of those terms with $z_i = 1$ or $z_j = 1$ is 1.

Thus

$$\sigma(n) = \prod_{k=1}^{n-1} a_k(n) \qquad \ldots \qquad \ldots \qquad \ldots \qquad (8).$$

Also for composite $n$ we see that $a_k(n)$ divides $\sigma(n)$. Thus by studying the properties of the numbers $a_k(n)$, which we shall call the *Associated Mersenne Numbers*, we can obtain information about the numbers $\sigma(n)$. Suppose that the roots of the equation

$$z^k + z - 1 = 0 \qquad \ldots \qquad \ldots \qquad \ldots \qquad (9)$$

are $b_1, b_2 \ldots b_k$, where $k \geqslant 2$. Then since $\prod (b - z_i) = b^n - 1$ we have

$$a_k(n) = \prod (1 - b_j^n) \text{ where } j \text{ runs from } 1 \text{ to } k \quad \ldots \qquad \ldots \qquad (10)$$

This expresses $a_k(n)$ as a symmetric function of the roots of the equation (9). We shall now state some results that can be deduced from (10); proofs will not be given here as they involve the theory of the Galois Imaginaries. For an account of this theory see ref. 1.

(I) If $n$ divides $m$ then $a_k(n)$ divides $a_k(m)$.

(II) If $p$ and $q$ are primes and if $p$ divides $a_k(q)$ then $q$ divides $p^K - 1$ where K is the lowest common multiple of 1, 2, . . . $k$.

(III) If $p$ is a prime then $p$ divides $a_k(p^K - 1)$, and the residues of $a_k(n)$ (mod $p$), as a function of $n$, repeat with period $p^K - 1$.

(IV) There is a linear recurrence formula for $a_k(n)$ regarded as a function of $n$. For example, we have:

(i) $a_1(n) = 2^n - 1. \quad a_1(n) = 2a_1(n-1) + 1.$

(ii) $a_2(n) = -a_2(n-1) + a_2(n-2) + 1 - (-1)^n.$

(iii) $a_3(n) = a_3(n-1) - a_3(n-2) + 3a_3(n-3) - a_3(n-4) + a_3(n-5) - a_3(n-6).$

The result (I) is a trivial consequence of the formula (10), for the quotient $a_k(m)/a_k(n)$ is clearly a symmetric polynomial function of the roots of (9) and so is an integer.

The linear recurrence formulae may easily be proved by multiplying out the product for $a_k(n)$. This expresses $a_k(n)$ as the sum of the $n^{th}$ powers of certain quantities which may be regarded as the roots of an equation with integral coefficients. It is shown in books on algebra (e.g. ref. 2) that such an expression satisfies a linear recurrence relation with the same coefficients as the equation.

The results (II) and (III) may easily be proved by means of the Galois Imaginaries which enable us to solve the congruence $z^k + z - 1 \equiv 0 \pmod{p}$. The relation (II) shows the analogy between the numbers $a_k(n)$ and the Mersenne Numbers which satisfy the relation (II) with $k = 1$, K $= 1$.

As the sign of the numbers $a_k(n)$ is irrelevant to the subject, we have tabulated them as if they were positive numbers. There is something to be said for modifying the definitions so that they are necessarily positive. The tables have been constructed by using the linear recurrence formulae. The relations (I), (II) and (III) form a very useful check on the accuracy of the calculations. There are several very interesting relations between the numbers $a_k(n)$ which there is no space to discuss here. For example, $a_k(n) = a_l(n)$ if $kl \equiv 1 \pmod{n}$. It would be very interesting to study under what conditions $a_k(p)$ is prime, but the author has not the time at his disposal to carry out any of the laborious calculations necessary. It is possible that the numbers may provide a useful test for the primality of the Mersenne Numbers and other related numbers. The numbers $a_2(n)$ have already been used for this purpose by Lucas (ref. 3).

type #1

1350 1351


REFERENCES

1. L. E. Dickson, *Linear Groups*, Chapters I–V.
2. Durell and Robson, *Advanced Algebra*, Vol. II, Chapter XI.
3. Hardy and Wright, *Theory of Numbers*, pp. 147 and 243.


TABLE OF THE ASSOCIATED MERSENNE NUMBERS

| $n$ | $k = 1$ | $k = 2$ | $k = 3$ |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 1 |
| 2 | 3 | 1 | 3 |
| 3 | 7 | 4 | 1 |
| 4 | 15 | 5 | 3 |
| 5 | 31 | 11 | 11 |
| 6 | 63 | 16 | 9 |
| 7 | 127 | 29 | 8 |
| 8 | 255 | 45 | 27 |
| 9 | 511 | 76 | 37 |
| 10 | 1023 | 121 | 33 |
| 11 | 2047 | 199 | 67 |
| 12 | 4095 | 320 | 117 |
| 13 | 8191 | 521 | 131 |
| 14 | 16383 | 841 | 192 |
| 15 | 32767 | 1364 | 341 |
| 16 | 65535 | 2205 | 459 |
| 17 | 131071 | 3571 | 613 |
| 18 | 262143 | 5776 | 999 |
| 19 | 524287 | 9349 | 1483 |

## Remark on the Motion of Tops in reply to Query

DEAR "SUCRA",

Though with great success
At first I steadily precess,
This later changes to nutation—
A thing you'll find by computation—
And now please let the matter drop.

*Signed*,
Yours,
A mathematic
TOP.

P.S.—For further reference, Lamb,
The latter part of his Dynam.



E.I

By D.

ELECTRONICS has only recen
machines. It was first used i
integrator and calculator mad
this was under construction i
an equivalent performance co
incorporated high-speed mem
constructed in various places
memories usually consisting
cathode-ray tubes.

E.D.S.A.C. (the electroni
is a small machine of this
laboratory under the direct
consider briefly its mode of

The machine has five pa

(*a*) A memory unit,
(*b*) A computor or arithn
(*c*) A control unit,
(*d*) An input unit, and
(*e*) An output unit (see

(*a*) Numbers, expressed
form of supersonic bursts o
in a tube. The waves are
vibrating quartz crystal, a
are converted into electric
to generate waves again.
many balls in the air at t
juggle with 576 digits, and s
of 16 tubes, it can hold 10
these numbers can be rea

(*b*) The computor cons
*accumulator*. Numbers fr
subtracted from, the nu
together and added to c
accumulator. In additio
replace any number in the
elementary operations of
be speedily carried out.

(*c*) The control "look
held in the memory, and
then executes. The orde
control number, which i