ON FERMAT'S SIMPLE THEOREM

JACK CHERNICK

1. **Introduction.** Fermat's simple theorem may be stated as follows: *If a is any integer prime to m, and if m is prime, then*

$$a^{m-1} \equiv 1 \pmod{m}. \tag{1}$$

The question naturally arises, "Do there exist composite integers for which the same congruence holds?" For particular values of a the existence of such numbers has long been established.* In 1910, R. D. Carmichael† treated the congruence (1) in the stricter sense indicated. He established several criteria which may be condensed into the following theorem:

THEOREM 1. *Fermat's theorem holds for composite integers if and only if m may be expressed as a product of distinct odd primes $p_1, \cdots, p_n$, $(n>2)$, and $m-1 \equiv 0 \pmod{p_i-1}$ where i ranges from 1 to n.*

Carmichael listed several such m with $n=3$ and one with $n=4$. Many others have since been found by P. Poulet.‡ It is our purpose to continue the study of these numbers in the present paper.

Fermat's theorem is sometimes stated thus: *If m is any prime and a any integer, then*

$$a^m \equiv a \pmod{m}. \tag{2}$$

The congruences (1) and (2) are likewise equivalent if m is composite, as is easily shown by the use of Theorem 1.

Despite the apparent promise of Fermat's theorem of yielding a complete and practical test for primes, no modification of it has as yet achieved this goal. However, the recent work of D. H. Lehmer,§ based upon a list of solutions of (2) for $a=2$, now provides such a test for integers in the range 10^7 to 10^8.

2. **Proof of Theorem** 1. We present a short, independent proof of Theorem 1. Let m be a composite number for which (1) holds. First, suppose $m=2^v$, $(v>1)$. But $a^{2^{v-1}} \equiv 1 \pmod{2^v}$ will not hold for

---

* Dickson, *History of the Theory of Numbers*, vol. 1, pp. 92–95.

† This Bulletin, vol. 16 (1910), pp. 232–238; also American Mathematical Monthly, vol. 19 (1912), pp. 22–27.

‡ D. H. Lehmer informs us that all m's under $5 \cdot 10^7$ and all, with $n=3$, under 10^8 have been tabulated by Poulet.

§ American Mathematical Monthly, vol. 43 (1936), pp. 347–354.

$a=3$ and $v\geqq 2$. Therefore m contains at least one odd prime factor.

Next, let $m=rp^v$ where v is the highest power of any odd prime contained in m. Let ω be a primitive root of p^v. Since ω is prime to p, the arithmetical progression ω, $\omega+p^v$, $\omega+2p^v$, $\cdots$ includes an infinitude of primes. Select s sufficiently large so that $x=\omega+sp^v$ is a prime greater than m. Then x is prime to m, and by (1),

$$x^{m-1} \equiv \omega^{m-1} \equiv 1 \pmod{p^v}.$$

Since ω is a primitive root of p^v, $m-1\equiv 0 \pmod{p^v-p^{v-1}}$. But $m-1=rp^v-1$ is prime to p. Hence $v=1$ only and

$$m - 1 \equiv 0 \pmod{p - 1}. \tag{3}$$

Also $p-1$ is even. Hence m is odd.

It remains to show that $n>2$. Else write $m=p_1p_2$, $(p_1>p_2)$. Then by (3),

$$p_1p_2 - 1 \equiv p_2 - 1 \equiv 0 \pmod{p_1 - 1};$$

or $p_2\geqq p_1$, a contradiction.

This completes the proof that the conditions given in Theorem 1 are necessary. Conversely, when m satisfies the stated conditions, the congruence (1) obviously follows.

We shall find it convenient henceforth to denote by F_n any composite integer of n prime factors for which Fermat's theorem holds.

3. **Properties of F_3.** A. *Theorem* 2. We shall prove the following theorem:

THEOREM 2. *Every F_3 is of the form $(2r_1h+1)(2r_2h+1)(2r_3h+1)$ where the r's are relatively prime in pairs.*

Let $F_3=p_1p_2p_3$. Set $p_i=r_ik+1$, where k is the g.c.f. of p_i-1, i running from 1 to 3. Then by Theorem 1, we have the congruential conditions

$$(r_1k + 1)(r_2k + 1)(r_3k + 1) \equiv 1 \pmod{kr_i};$$

or by simplifying,

$$k(r_1r_2 + r_1r_3 + r_2r_3) + r_1 + r_2 + r_3 \equiv 0 \pmod{r_i}. \tag{4}$$

The r's are relatively prime in pairs; for by (4), if any two have a common factor, so does the third, contrary to hypothesis. Since k must be even, we obtain Theorem 2.

Now (4) is replaceable by the single condition

$$k(r_1r_2 + r_1r_3 + r_2r_3) + r_1 + r_2 + r_3 \equiv 0 \pmod{r_1r_2r_3}. \tag{5}$$

The latter congruence is linear in k. Moreover, the coefficient of k is prime to the modulus. Hence its general solution is given by

$$k = Mr_1r_2r_3 - (r_1 + r_2 + r_3)(r_1r_2 + r_1r_3 + r_2r_3)^a,$$

where $a = \phi(r_1)\phi(r_2)\phi(r_3) - 1$.

B. *Universal forms.* For given r_i the solution of (5) affords a one-parameter expression for F_3. Thus $(r_1, r_2, r_3) = (1, 2, 3)$ gives $k = 6M$, whence

$$U_3 = (6M + 1)(12M + 1)(18M + 1)$$

yields an F_3 for every M for which the quantities in parentheses are prime. A few examples are

$7 \cdot 13 \cdot 19$,	$271 \cdot 541 \cdot 811$,	$337 \cdot 673 \cdot 1009$,
$37 \cdot 73 \cdot 109$,	$307 \cdot 613 \cdot 919$,	$601 \cdot 1201 \cdot 1801$,
$211 \cdot 421 \cdot 631$,	$331 \cdot 661 \cdot 991$,	$727 \cdot 1453 \cdot 2179$.

Similarly, $(r_1, r_2, r_3) = (1, 2, 5)$, $(1, 3, 8)$, and $(2, 3, 5)$ yield, respectively, the forms $U_3 = (10M+7)(20M+13)(50M+31)$, $(24M+13) \cdot (72M+37)(192M+97)$, and $(60M+41)(90M+61)(150M+101)$.

We shall call these forms universal. More precisely, the product U_n of n odd distinct linear factors a_iM+b_i, $(n \geqq 3)$, will be termed universal if it satisfies the set of congruences $U_n \equiv 1 \pmod{a_iM+b_i-1}$, where i ranges from 1 to n, for every integral value of M. The presence of these forms makes it easy to conjecture but no less difficult to prove the existence of an infinitude of F_n. The question whether such forms represent an infinitude of sets of primes has already been raised by L. E. Dickson.*

4. **Properties of F_n, $(n > 3)$.** When $n > 3$, similar results may be derived. If we write any F_n in the form $(r_1k+1) \cdots (r_nk+1)$, where k is the g.c.f. of $p_i - 1$, i ranging from 1 to n, it can be shown that the r's are relatively prime in sets of $n-1$. But for given r_i, the congruence of Theorem 1 is no longer readily nor necessarily solvable. Thus if $n = 4$, (4) is replaced by the quadratic congruences

$$k^2(\sum r_1r_2r_3) + k(\sum r_1r_2) + \sum r_1 \equiv 0 \pmod{r_i}, \tag{6}$$

i from 1 to 4. Let us limit the r's by $\prod_1^4 r_1 \leqq 100$. Most of the possible cases are then eliminated by the theory of quadratic residues. By solving (6) generally for the six cases that remain, there results from each one or more universal forms, as exhibited in the following table:

* Messenger of Mathematics, vol. 33 (1904), pp. 155–161.

r_i	U_4
1, 2, 3, 6	$(6M+1)(12M+1)(18M+1)(36M+1)$
1, 2, 3, 12	$(12M+7)(24M+13)(36M+19)(144M+73)$
1, 2, 4, 7	$(28M+15)(56M+29)(112M+57)(196M+99)$
1, 2, 4, 11	$(44M+15)(88M+29)(176M+57)(484M+155)$
1, 2, 4, 11	$(44M+43)(88M+85)(176M+169)(484M+463)$
1, 2, 5, 10	$(10M+7)(20M+13)(50M+31)(100M+61)$
1, 3, 4, 6	$(12M+11)(36M+31)(48M+41)(72M+61)$

When $n>4$, congruences of higher degree than (6) result. To surmount this difficulty, we have the following theorem:

THEOREM 3. *Let $p_1p_2 \cdots p_n$ be an F_n. Define k_1 as the g.c.f. of p_i-1, $r_i=(p_i-1)/k_1$, and R as the l.c.m. of r_i, i ranging from 1 to n. Then $U_n=\prod_1^n(r_iRM+p_i)$ is an universal form, with the proviso that if the r's are all odd, M be replaced by $2M$.*

By Theorem 1, $k=k_1$ is a solution of the congruence

$$\left[\prod_1^n (r_ik+1)-1\right]/k \equiv 0 \pmod{R}. \tag{7}$$

Hence any $k\equiv k_1 \pmod{R}$ is a solution of (7). Let $k=MR+k_1$. On substituting this for k_1, we obtain the form of Theorem 3. By (7), this form satisfies the congruence required for universality. Any factor r_iRM+p_i of this form is odd since RM is even and p_i is odd. No two factors r_iRM+p_i, r_jRM+p_j are equal, for if $p_i>p_j$, by definition $r_i>r_j$. Hence the form is universal.

Theorem 3 enables us to derive universal forms from given F_n. A method of obtaining such F_n in certain cases from known F_{n-1} is now shown by the next theorem:

THEOREM 4. *Let $F_{n-1}=p_1p_2 \cdots p_{n-1}$, q the l.c.m. of p_i-1, i from 1 to $n-1$, and $r=(F_{n-1}-1)/q$. If $p_n=q\pi+1$, where π is any divisor of r and p_n is a prime distinct from p_i, then $p_1p_2 \cdots p_n$ is an F_n.*

By Theorem 1, it suffices that $F_n\equiv 1 \pmod{p_i-1}$, i ranging from 1 to n. Now $F_n\equiv F_{n-1}p_n\equiv p_n\equiv 1 \pmod{q}$. Hence it remains to show that $F_n\equiv 1 \pmod{p_n-1}$. But $F_n\equiv F_{n-1}p_n\equiv F_{n-1}\equiv 1 \pmod{p_n-1}$, whence Theorem 4 follows.

As an example, take $F_3=7\cdot 13\cdot 19$. Then $q=36$, $r=48$, $p_4=37$, 73, 109, 433, or 577. By repeated application of Theorem 4, we find the interesting series

$F_3 = 5 \cdot 17 \cdot 29,\quad 7 \cdot 13 \cdot 31,$
$F_4 = 5 \cdot 17 \cdot 29 \cdot 113,\quad 7 \cdot 13 \cdot 31 \cdot 61,$
$F_5 = 5 \cdot 17 \cdot 29 \cdot 113 \cdot 337,\quad 7 \cdot 13 \cdot 31 \cdot 61 \cdot 181,$
$F_6 = 5 \cdot 17 \cdot 29 \cdot 113 \cdot 337 \cdot 673,\quad 7 \cdot 13 \cdot 31 \cdot 61 \cdot 181 \cdot 541,$
$F_7 = 5 \cdot 17 \cdot 29 \cdot 113 \cdot 337 \cdot 673 \cdot 2689,\quad 7 \cdot 13 \cdot 31 \cdot 61 \cdot 181 \cdot 541 \cdot 2161.$

The process may be continued to the limits of present-day factor tables. With the aid of Theorem 3, we can use these solutions to derive universal forms. Thus from the last of these F_n, we get

$$U_7 = (360M + 7)(720M + 13)(1800M + 31)(3600M + 61) \cdot (10800M + 181)(32400M + 541)(129600M + 2161).$$

5. **The existence of an U_n for any $n > 3$.** Theorem 4 is readily applied to U_n in place of F_n by merely omitting the condition that the p's be prime. For instance, consider $U_3 = (6M+1)(12M+1)(18M+1)$. Here $q = 36M$. Taking $\pi = 1$, we obtain

$$U_4 = (6M + 1)(12M + 1)(18M + 1)(36M + 1).$$

Similarly, we find

$$U_5 = (6M + 1)(12M + 1)(18M + 1)(36M + 1)(72M + 1),$$

provided $M \equiv 0 \pmod 2$; and

$$U_6 = (6M + 1)(12M + 1)(18M + 1)(36M + 1)(72M + 1)(144M + 1),$$

if $M \equiv 0 \pmod 4$.

This suggests the possibility of an unending series of such forms. Indeed, suppose $M = 2^{n-4}M_1$, and let

$$U_n = (6M+1)(12M+1)(18M+1)(2^2 \cdot 9M+1) \cdots (2^{n-2} \cdot 9M+1) \tag{8}$$

be an universal form. Then

$$U_{n+1} = (6M + 1)(12M + 1)(18M + 1)(2^2 \cdot 9M + 1) \cdots (2^{n-1} \cdot 9M + 1)$$

is universal if

$$U_n \equiv 1 \pmod{2^{n-1} \cdot 9M}, \tag{9}$$

since, by Theorem 4, $q = 2^{n-2} \cdot 9M$ and we may thus take $\pi = 2$. By Theorem 1, we already know that (9) holds for the modulus $2^{n-2} \cdot 9M$.

When U_n is expanded in terms of M, (9) becomes

$$1 + M(6 + 12 + 18 + 36 + \cdots + 2^{n-2} \cdot 9) + KM^2 \equiv 1 \pmod{2^{n-1} \cdot 9M}, \tag{10}$$

where K is a polynomial in M. The second term in the left-hand member sums to $2^{n-1} \cdot 9M$. Hence (10) reduces to

$$KM \equiv 0 \pmod{2^{n-1} \cdot 9}. \tag{11}$$

Conversely (11) implies (9). Since (9) holds for the modulus $2^{n-2} \cdot 9M$, it follows similarly that (11) holds for the modulus $2^{n-2} \cdot 9$ with $M = 2^{n-4} M_1$. Hence (11) will be true for the given modulus if $M = 2^{n-3} M_1$. This supplies a proof by induction that (8) is a universal form for every $n \geqq 4$.

If, in addition,* M is divisible by every prime p where $3 < p \leqq n$, we satisfy the necessary condition given by Dickson† for the form (8) to represent at least one set of n primes. The proof of the sufficiency of this condition still remains a challenge to the ingenuity of number theorists.

NEW YORK, N. Y.

RINGS AS GROUPS WITH OPERATORS

C. J. EVERETT, JR.

1. **Introduction.** A module M $(0, a, b, \cdots)$ is a commutative group, additively written. Every correspondence of M onto itself, or part of itself, such that $a \to a'$, $b \to b'$ implies $a+b \to a'+b'$ defines an *endomorphism* of M. An endomorphism may be regarded as an operator θ on M subject to the postulates (i) $\theta a = a'$ is uniquely defined as an element of M, (ii) $\theta(a+b) = \theta a + \theta b$, $(a, b \in M)$. In particular, there exist a null operator 0 $(0M = 0)$ and a unit operator ϵ $(\epsilon a = a, a \in M)$. Designate by Ω_M the set of all such operators, $0, \epsilon, \alpha, \beta, \cdots$. It is well known that if operations of $\oplus$ and $\odot$ be defined in Ω_M by $(\theta+\eta)a = \theta a + \eta a$ and $(\theta\eta)a = \theta(\eta a)$, $(a \in M)$, Ω_M forms a ring with unit element ϵ (*endomorphism ring* of M).‡ The equation $\theta = \eta$ means $\theta a = \eta a$ (all $a \in M$). A ring $R(M)$ is called a ring over M in case M is the additive group of $R(M)$. Correspondence of a set P onto a set Q (many-one) is written $P \sim Q$; if specifically one-one, $P \cong Q$. Corresponding operations in P, Q preserved under the map are indicated in parentheses; for example, $P \sim Q$ $(+)$. If a set T has the property that TP is defined in P, TQ in Q, and if, under a correspondence $P \sim Q$, $p \to q$ implies $tp \to tq$ $(t \in T, p \in P, q \in Q)$, we write $P \sim Q$ (T) (T-operator correspondence). If R is a ring, the two-sided ideal N of elements z of R such that $zr = 0$ (all $r \in R$), is called the left annulling ideal of R.

---

* For example, replace $6M$ in (8) by $2^w n! M$, $(w \geqq n-3)$.

† Loc. cit., p. 156.

‡ van der Waerden, *Moderne Algebra*, vol. 1, 2d edition, p. 146.