MERSENNE-FORM AND FERMAT-FORM NUMBER CONGRUENCES

R. R. SEEBER, IBM, Poughkeepsie, N. Y.

This note gives congruences for Mersenne-form and Fermat-form numbers, the principal results being given by Theorem 2 and by (6) and (10) of Table 1; both (6) and (10) are similar in form to Wilson's Theorem.

All results after Theorem 2 are given in tabular form. Tables 2 and 3 give subsidiary statements, not all new, some of which are required for Table 1 proofs.

We define Mersenne-form and Fermat-form numbers by

$$M(n) = 2^n - 1, \tag{1}$$

and

$$F(n) = 2^n + 1. \tag{2}$$

Here and in what follows the letters denote nonnegative integers unless further restricted.

The proofs depend on a theorem given by an anonymous writer [1]. He employed nth roots of unity and the irreducibility of the associated cyclotomic equation to prove:

THEOREM 1. *If n is a prime, then the sums of the numbers $1, 2, 3, \cdots, n-1$ taken t at a time, for a fixed t, $0 \leqq t < n$, when divided by n give each of the residues $1, 2, 3, \cdots, n-1$ an equal number of times, $D(n-1, t)$, and the residue zero one more time or one less time according as t is even or odd.*

REMARK. $D(n-1, t)$ is given by $\left(\binom{n-1}{t} - (-1)^t\right)/n$.

Also since $2^n \equiv 1 \pmod{M(n)}$, we have

$$2^{kn+m} \equiv 2^m \pmod{M(n)}. \tag{3}$$

Expanding the products gives, for $n > 1$,

$$M(1)M(2) \cdots M(n-1) = \sum_{t=0}^{n-1} (-1)^{n-1-t} A(n-1, t) \tag{4}$$

and

$$F(1)F(2) \cdots F(n-1) = \sum_{t=0}^{n-1} A(n-1, t), \tag{5}$$

where $A(n-1, t)$ is the sum of all those terms of the complete product in (5) that can be formed by selecting t of the powers of 2 and $n-1-t$ of the 1's.

We see that the terms in the sum $A(n-1, t)$ are powers of 2, some of which may equal or exceed 2^n. By virtue of (3) we may reduce these to powers less than n but greater than or equal to zero, thus forming the new set of coefficients

$B(n-1, t)$ where

$$B(n-1, t) \equiv A(n-1, t) (\text{mod } M(n)).$$

But the exponents in the powers of 2 in the sums $B(n-1, t)$ were thus derived exactly in conformity with Theorem 1. Hence, if n is prime, we have:

$$\begin{aligned} B(n-1, t) &= 2^0(D(n-1, t) + (-1)^t) + D(n-1, t)(2^1 + 2^2 + \cdots + 2^{n-1}) \\ &= D(n-1, t)(2^0 + 2^1 + 2^2 + \cdots + 2^{n-1}) + (-1)^t \equiv (-1)^t (\text{mod } M(n)). \end{aligned}$$

This gives:

THEOREM 2. $A(n-1, t) \equiv (-1)^t$ (mod $M(n)$) *if n is prime.*

This theorem is somewhat more than we need to prove (6) and (10), which now follow from (4) and (5), respectively.

Also, since $A(n, t) = 2^n A(n-1, t-1) + A(n-1, t)$ for $0 < t < n$, we have by Theorem 2 and (3):

COROLLARY. $A(n, t) \equiv 0$ (mod $M(n)$) *for* $0 < t < n$ *if n is prime.*

TABLE 1. Congruences

$(1) M(n) = 2^n - 1$; $(2) F(n) = 2^n + 1$.

Ref. No.	*Congruences*	*Conditions*	*Refs. for Proofs*
(6)	$M(1)M(2) \cdots M(n-1)$ $\equiv (-1)^{n-1}n$ (mod $M(n)$)	if n is a prime.	Th. 2
(7)	$M(1)M(2) \cdots M(n-1) \equiv \pm n$ (mod $M(n)$)	only if n is a prime.	(15), (20)
(8)	$M(1)M(2) \cdots M(n-1) \equiv 0$ (mod $M(n)$)	iff $n=6$.	Ref. [3]
(9)	$M(1)M(2) \cdots M(n-1)$ $\equiv (n/2)M(n/2)$ (mod $M(n)$)	if $n = 2^{k+1}$.	(17)
(10)	$F(1)F(2) \cdots F(n-1) \equiv 1$ (mod $M(n)$)	if n is an odd prime.	Th. 2
(11)	$F(1)F(2) \cdots F(n-1) \equiv 0$ (mod $M(n)$)	iff $n = 2^{k+1}$.	(10), (15), (21)
(12)	$F(1)F(2) \cdots F(n-1) \equiv F(n/2)$ (mod $M(n)$)	if $n/2$ is an odd prime.	(10), (16)
(13)	$M(1)M(2) \cdots M(n-1)$ $\equiv \pm F(1)F(2) \cdots F(n-1)$ (mod $F(n)$)	if $n = 4(k+1) \pm 1$.	(4), (5)

The converse of (6) is included in (7), and (8) was given by Zsigmondy [3]. We return later for the proofs of (7), (9), (11), (12), and (13).

In Table 2 we give quotients and remainders for divisions of M's and F's. We need only the remainders but also give the quotients for the proofs. Let $Q(x, y)$ be the quotient and $R(x, y)$ be the remainder on dividing x into y in the usual way, i.e.,

$$y = xQ(x, y) + R(x, y), \qquad 0 \leqq R(x, y) < x. \tag{14}$$

By dividing $M(5)$ into $M(12)$ in binary, it is easy to "see" the derivation of (15). (Compare [2].)

TABLE 2. Quotients and Remainders

(1) $M(n) = 2^n - 1$; (2) $F(n) = 2^n + 1$; (14) $y = xQ(x, y) + R(x, y)$, $0 \leqq R(x, y) < x$.

Ref. No.	x	y	$Q(x, y)$	$R(x, y)$	Conditions
(15)	$M(b)$	$M(a)$	$\left(\sum_{i=0}^{Q(b,a)-1} 2^{bi}\right) 2^{R(b,a)}$	$M(R(b, a))$	$b > 0$
(16a)	$M(b)$	$F(a)$	$\left(\sum_{i=0}^{Q(b,a)-1} 2^{bi}\right) 2^{R(b,a)}$	$F(R(b, a))$	$\begin{cases} b > 2 \text{ or} \\ b = 2 \text{ and } R(b, a) = 0 \end{cases}$
(16b)	$M(b)$	$F(a)$	$\left(\sum_{i=0}^{Q(2,a)-1} 2^{2i}\right) 2 + 1$	0	$b = 2$ and $R(b, a) = 1$
(16c)	$M(b)$	$F(a)$	$F(a)$	0	$b = 1$
(17a)	$F(b)$	$M(a)$	$\left(\sum_{i=0}^{Q(2b,a)-1} 2^{2bi}\right) 2^{R(2b,a)}M(b)$	$M(R(b, a))$	$R(2b, a) < b, b > 0$
(17b)	$F(b)$	$M(a)$	$\left(\sum_{i=0}^{Q(2b,a)-1} 2^{2bi}\right) \begin{matrix} 2^{R(b,a)+b}M(b) \\ +M(R(b,a)) \end{matrix}$	$\begin{matrix} M(b - R(b, a))2^{R(b,a)} \\ = M(b) - M(R(b, a)) > 0 \end{matrix}$	$0 < b \leqq R(2b, a)$
(17c)	$F(b)$	$M(a)$	$M(a - 1)$	1	$a > 0, b = 0$
(17d)	$F(b)$	$M(a)$	0	0	$a = b = 0$
(18a)	$F(b)$	$F(a)$	$\left(\sum_{i=0}^{Q(2b,a)-1} 2^{2bi}\right) 2^{R(2b,a)}M(b)$	$F(R(b, a))$	$R(2b, a) < b, b > 0$
(18b)	$F(b)$	$F(a)$	$\left(\sum_{i=0}^{Q(2b,a)-1} 2^{2bi}\right) 2^bM(b) + 1$	0	$R(2b, a) = b, b > 0$
(18c)	$F(b)$	$F(a)$	$\left(\sum_{i=0}^{Q(2b,a)-1} 2^{2bi}\right) \begin{matrix} 2^{R(b,a)+b}M(b) \\ +M(R(b,a)) \end{matrix}$	$\begin{matrix} M(b-R(b, a))2^{R(b,a)}+2 \\ =F(b)-M(R(b, a))>0 \end{matrix}$	$0 < b < R(2b, a)$
(18d)	$F(b)$	$F(a)$	2^{a-1}	1	$a > 0, b = 0$
(18e)	$F(b)$	$F(a)$	1	0	$a = b = 0$
(19)	$F(b) - M(R(b, a))$	$F(b)$	1	$M(R(b, a)) > 0$	$0 < b < R(2b, a)$

$$10000100 = (2^5 + 1)2^2 = \left(\sum_{i=0}^{Q(5,12)-1} 2^{5i}\right) 2^{R(5,12)}$$

```
        10000100
11111)111111111111
      11111
          11111
          11111
             11 = M(2) = M(R(5, 12)).
```

In similar fashion we may derive (16), (17), and (18); however, the proofs in each case, including (19), follow directly by seeing that (14) is satisfied for the given conditions.

TABLE 3. Highest Common Divisors

(1) $M(n)=2^n-1$; (2) $F(n)=2^n+1$; (14) $y=xQ(x,y)+R(x,y)$, $0\leqq R(x,y)<x$.

Ref. No.	x	y	(x, y)	*Conditions*	*Refs. for Proofs*
(20)	$M(b)$	$M(a)$	$M((b,a))$	$b>0$.	(15)
(21a)	$F(b)$	$M(a)$	$F(b)$	$a=0$.	(15), (16)
(21b)	$F(b)$	$M(a)$	$F((b,a))$	$a>0$, $b>0$, $R(2(b,a),a)=0$.	(17), (18)
(21c)	$F(b)$	$M(a)$	1	Otherwise than for (21a) and (21b).	
(22a)	$F(b)$	$F(a)$	$F(0)$	$a=b=0$.	(16), (18)
(22b)	$F(b)$	$F(a)$	$F((b,a))$	$a>0$, $b>0$, $R(2(b,a),a)>0$, $R(2(b,a),b)>0$.	(19)
(22c)	$F(b)$	$F(a)$	1	Otherwise than for (22a) and (22b).	

In (20), (21), and (22) of Table 3 we give highest common divisors for M's and F's. By considering the remainders in successive steps of Euclid's algorism, we see that their possible forms are given in the remainders column of Table 2. A little consideration shows that divisors in all cases will have to be of form $F(u)$ or $M(v)$. Then Table 2 is used to identify the divisors that will leave a zero remainder for both arguments of (x, y).

Returning to Table 1, consider the proof of (7). Assume n is composite with

$$n = \prod_{i=1}^{k} p_i^{s_i} \tag{23}$$

where the p_i are distinct primes and $q_i=p_i^{s_i}$. Since $q_i|n$, $M(q_i)|M(n)$ by (15); and $M(q_i)|M(1)M(2)\cdots M(n-1)\pm n$ for $i=1, 2, \cdots, k$. If $k>1$, then $q_i<n$ and $M(q_i)$ is among the factors $M(1)$, $M(2)$, $\cdots$, $M(n-1)$; hence, $M(q_i)|n$ also. Since n is a common multiple of all the $M(q_i)$, it is a multiple of their least common multiple. Since the q_i are coprime, the $M(q_i)$ are also coprime by (15). Hence the least common multiple of the $M(q_i)$ is their product, and we have $M(q_1)M(q_2)\cdots M(q_k)|q_1q_2\cdots q_k$. But this is impossible since $M(q_i)>q_i$ for $q_i>1$. Thus for $k>1$, n cannot be composite.

If $k=1$, then $n=q_1=p_1^{s_1}$ and $s_1>1$. Since $p_1|n$, $M(p_1)|M(n)$ by (15); and $M(p_1)|M(1)M(2)\cdots M(n-1)\pm n$. Now $p_1<n$ and $M(p_1)$ is among the factors $M(1)$, $M(2)$, $\cdots$, $M(n-1)$; hence, $M(p_1)|n$ also. Since $M(p_1)>1$, we must have $M(p_1)=p_1^t$ where $0<t\leqq s_1$ and $p_1|M(p_1)$. This is false for $p_1=2$. If $p_1>2$, then $p_1|M(p_1-1)$ by Fermat's Theorem. But p_1 cannot divide both $M(p_1)$ and $M(p_1-1)$ since $(M(p_1), M(p_1-1))=M((p_1, p_1-1))=1$ by (20). Hence n is not composite, which completes the proof of (7).

Next consider the proof of (9). Since

$$M(n) = M(2^{k+1}) = M(2^k)F(2^k) = M(n/2)F(n/2),$$

we must show that

$$C = M(1)M(2) \cdots M(2^k - 1)M(2^k + 1)M(2^k + 2) \cdots M(2^k + 2^k - 1) - 2^k \equiv 0 \pmod{F(2^k)}.$$

Now by (17b) we have $M(2^k + x) \equiv M(2^k) - M(x) \pmod{F(2^k)}$ if $0 < 2^k \leq R(2^{k+1}, 2^k+x)$, i.e., if $0 \leq x < 2^k$. But $M(2^k) - M(x) = F(2^k) - 2 - (F(x) - 2) = F(2^k) - F(x)$. Thus $M(2^k+x) \equiv -F(x)$ (mod $F(2^k)$ if $0 \leq x < 2^k$ and

$$C \equiv M(1)M(2) \cdots M(2^k - 1)(-1)F(1)F(2) \cdots F(2^k - 1) - 2^k \pmod{F(2^k)}$$

or $C \equiv (-1)^1 M(2)M(4) \cdots M(2^{k+1}-2) - 2^k \pmod{F(2^k)}$. This telescoping is repeated, giving $C \equiv (-1)^2 (M(2^k))^1 M(4)M(8) \cdots M(2^{k+1}-4) - 2^k$ and finally $C \equiv (-1)^k (M(2^k))^k - 2^k \pmod{F(2^k)}$. Since this expression is divisible by $M(2^k)+2 = F(2^k)$, thus $C \equiv 0 \pmod{F(2^k)}$, thereby completing the proof of (9).

Now consider the proof of (11). The first part follows immediately since $M(2^{k+1}) = F(2^0)F(2^1) \cdots F(2^k)$. If n is not a power of 2, it is either an odd prime or has an odd prime divisor p; both of these cases lead to contradictions. In the former case, $F(1)F(2) \cdots F(n-1) \equiv 1 \pmod{M(n)}$ by (10). In the latter case with $n = pm$, we have $M(p) \mid M(n)$ by (15) and thus $M(p) \mid F(1)F(2) \cdots F(n-1)$. But by (21c), $(F(x), M(p)) = 1$ for $0 < x < n$, since $p > 0$ and $R(2(x, p), p) > 0$. Thus $M(p) \nmid F(1)F(2) \cdots F(n-1)$, completing the proof of (11).

To prove (12), it is only necessary to show that

$$F(1)F(2) \cdots F(n/2 - 1)F(n/2 + 1)F(n/2 + 2) \cdots F(n - 1) \equiv 1 \pmod{M(n/2)}, \tag{24}$$

since $M(n) = F(n/2)M(n/2)$ with $n/2$ an odd prime. By (16a), $F(n/2+x) \equiv F(x) \pmod{M(n/2)}$, since $n/2 > 2$ for $0 < x < n/2$. Also $F(1)F(2) \cdots F(n/2-1) \equiv 1 \pmod{M(n/2)}$ by (10). Hence (24) is satisfied and (12) is proved.

Finally, to prove (13), we observe, first, that $2^{kn+m} \equiv (-1)^k 2^m \pmod{F(n)}$, which is similar to (3); and, second, that $A(x, x-t) = 2^{x(x+1)/2-(x+1)t} A(x, t)$, which follows from symmetry considerations in the definition of $A(x, t)$. Now applying (4) and (5), we have (13) directly.

As to the converses of (9), (10), (12), and (13), we can offer them only as conjectures; the conjectures have been verified by computation for $n < 35$ for the converse of (13) and for $n < 71$ for the others. For the converse (10), we see by (21) that there is no immediate proof in the manner of that for (7); obviously n must be odd. Also it appears likely that there are additional relationships similar to (9) and (12).

The author is indebted to L. Hellerman for a suggestion used in the proofs and to the referee for directing attention to reference 3.

References

1. Anonymous, Théorèmes et problèmes sur les nombres, Jour. für Math. (Crelle), 6 (1830) 100–106. See also L. E. Dickson, History of the Theory of Numbers, Vol. 1, p. 327, note 1.

2. D. Shanks, Solved and Unsolved Problems in Number Theory, Spartan, Washington, 1962, 17–19.

3. K. Zsigmondy, Zur Theorie der Potenzreste, Monatshefte Math. Phys., 3 (1892) 265–284. See also Dickson, History, p. 386, note 44.