make $M_p$ prime are 2, 3, 5, 7, 13, 17, 19, 31, 67, 127 and 257. Comparison of this list with the correct data recorded in the top line of the table presented below shows that Mersenne made five mistakes. $p = 67$ and 257 do not yield prime values for $M_p$, and $p = 61, 89$ and 107 were not included in his list of special primes.

With reference to explicit factoring, attention should be called to a valuable paper by Professor D. H. Lehmer entitled "On the Factors of $2^n - 1". His investigations on 76 numbers unveiled eleven factors which fall within Mersenne's range. Incidentally two of his new factors confirmed the present writer's final residues for $M_{167}$ and $M_{229}$.

$\begin{array}{c|c}
p & \text{Prime} & \text{Composite and fully factored} & \text{Two or more prime factors found} & \text{Only one prime factor known} & \text{Composite but no factor known} \\
2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127 & \text{Prime} & \text{Composite and fully factored} & \text{Two or more prime factors found} & \text{Only one prime factor known} & \text{Composite but no factor known} \\
11, 29, 37, 41, 43, 47, 53, 59, 67, 71, 73, 79, 113 & \text{Prime} & \text{Composite and fully factored} & \text{Two or more prime factors found} & \text{Only one prime factor known} & \text{Composite but no factor known} \\
151, 163, 173, 179, 181, 223, 233, 239, 251 & \text{Prime} & \text{Composite and fully factored} & \text{Two or more prime factors found} & \text{Only one prime factor known} & \text{Composite but no factor known} \\
83, 97, 131, 167, 191, 211, 229 & \text{Prime} & \text{Composite and fully factored} & \text{Two or more prime factors found} & \text{Only one prime factor known} & \text{Composite but no factor known} \\
101, 103, 109, 137, 139, 149, 157, 193, 199, 227, 241, 257 & \text{Prime} & \text{Composite and fully factored} & \text{Two or more prime factors found} & \text{Only one prime factor known} & \text{Composite but no factor known} \\
\end{array}$


NEW TYPES OF CONGRUENCES INVOLVING BERNOULLI NUMBERS AND FERMAT'S QUOTIENT

BY H. S. VANDIVER

DEPARTMENT OF APPLIED MATHEMATICS, UNIVERSITY OF TEXAS

Communicated January 17, 1948

In another paper the writer gave the relation

$$\begin{align*}
(mb + k)^n &= \sum_{a=1}^{s} \binom{r}{a} (-1)^{s-1} \frac{S_a(m, k, a)}{a}; \quad r > n; \\
\end{align*}$$

(1)

where we define the Bernoulli numbers $b_a$ by means of the recursion formula $(b + 1)^n = b_n$; $n > 1$, the left-hand member being expanded in full and $b$, substituted for $b^r$, and the left-hand member of (1) is interpreted in the same way;

$$\begin{align*}
S_a(m, k, a) &= \sum_{i=0}^{a-1} (im + k)^n; \quad 0^0 = 1,
\end{align*}$$

$m$ and $k$ are any integers with $m \neq 0$. In the present paper we shall employ (1) as well as other known relations to obtain various congruences. The principal results proved seem to be (5), (6b), (7) and (20).
By the well-known Bernoulli summation formula we also have

\[(b + k)^n = nS_{n-1}(k) + b_n,\]  

(2)

where

\[S_{n-1}(k) = S_{n-1}(1, 0, k).\]

Set in (1), \(r = p - 1\) we have, if \(n < p - 1\), \(p\) being an odd prime,

\[(mb + k)^n = \sum_{a=1}^{p-1} \binom{p - 1}{a} (-1)^{a-1} S_n(m, k, a).\]  

(3)

It is known that

\[\binom{p - 1}{a} = (-1)^a \pmod{p},\]  

(3a)

so that from (3) we obtain

\[(mb + k)^n = -\sum_{a=1}^{p-1} \frac{S_n(m, k, a)}{a} \pmod{p}.\]  

(4)

For a particular \(a = i\), the corresponding term on the right may be written

\[-\sum_{i=1}^{p-1} k^n + (k + m)^n + \ldots (k + (i - 1)m)^n = C.\]

Now collect the terms in the right-hand member of (4) involving each particular \(m\)th power, we find

\[C = \sum_{s=0}^{p-2} \frac{1}{s + 1} + \frac{1}{s + 2} + \ldots + \frac{1}{p - 1}.\]

But also

\[1 + \frac{1}{2} + \ldots + \frac{1}{p - 1} = 1 + 2^{p-2} + \ldots + (p - 1)^{p-2} \equiv 0 \pmod{p},\]  

(4a)

since \(p\) is odd. The last result gives

\[-\left(\frac{1}{s + 1} + \frac{1}{s + 2} + \ldots + \frac{1}{p - 1}\right) \equiv 1 + \frac{1}{2} + \ldots + \frac{1}{s},\]

so that (4) may be written, \(n < p - 1,\)

\[(mb + k)^n \equiv \sum_{a=1}^{p-2} \frac{(ma + k)^n R_a \pmod{p}},\]  

(5)

where

\[R_a = 1 + \frac{1}{2} + \ldots + \frac{1}{a}.\]
For $k = 0, m = 1$, this becomes
\[ b_n \equiv \sum_{a=1}^{p-2} a^n R_a \pmod{p}. \] (5a)

Also, (5) gives for $g$ any integer, $0 < g < p$, for $mg + k \not\equiv 0 \pmod{p}$,
\[
\sum_{n=0}^{p-2} (mg + k)^{n+p-2}(mb + k)^n
\equiv \sum_{a=1}^{p-1} R_a \sum_{n=0}^{p-2} (ma + k)^n (mg + k)^{p-2-n}
\equiv -(mg + k)^{p-2} R_g + \sum_{a=1}^{p-1} R_a \frac{(ma + k)^{p-1} - (mg + k)^{p-1}}{m(a - g)},
\]
or
\[
\sum_{n=0}^{p-2} (mg + k)^{n+p-2}(mb + k)^n \equiv -(mg + k)^{p-2} R_g, \quad (5b)
\]
modulo $p$, by Fermat's theorem, provided $mg + k \not\equiv 0 \pmod{p}$. For $m = 1, k = 0$ this reduces to
\[
\sum_{n=0}^{p-2} g^{-n} b_n \equiv -R_g \pmod{p},
\]
which for $g = 1$ becomes
\[
b_0 + b_1 + \ldots + b_{p-2} \equiv -1 \pmod{p}. \quad (6a)
\]

Taking the relation (5a) for $n = 0, 1, \ldots, p - 2$ in turn introducing powers of the integers $m$, prime to $p$, similarly to the procedure in the proof of (5b) we obtain
\[
\sum_{n=0}^{p-2} g^{-n} m^n b_n \equiv -R_a \pmod{p},
\]
where $am \equiv g \pmod{p}; \quad a < p$.

Now take (5a) again and let $p = 1 + cm$ and put $n, n + c, \ldots, n + (m - 1)c$, in turn in this congruence, and add, we obtain if $n < c$
\[
\sum_{i=0}^{m-1} b_{n+ic} \equiv m \sum_{r} r^n R_r \pmod{p},
\]
where $r$ ranges over the distinct solutions in the set 1, 2, \ldots, $p - 1$ of $x^c \equiv 1 \pmod{p}$. The relation (7) has a type of analogy with the relation
\[
\frac{\sum r^n}{p} \equiv -cn \sum_{k=0}^{m-1} \frac{b_{kc+n}}{kc+n} \pmod{p},
\]
(8)
with $e$ and $n$ even. Set $\mu_k \equiv k/m \pmod{p}; 0 < \mu_k < p$. Then

$$(mb + k)^n = m^n \left( b + \frac{k}{m} \right)^n \equiv m^n (b + \mu_k)^n$$

$$\equiv m^n (b_n + n(0^{n-1} + 1^{n-1} + \ldots + (\mu_k - 1)^{n-1})) \pmod{p},$$
on applying (2). This gives

$$\frac{(mb + k)^n - m^n b_n}{n} = m^n (0^{n-1} + 1^{n-1} + \ldots + (\mu_k - 1)^{n-1}),$$
modulo $p$. Setting $n = 1, 2, \ldots, p - 1$, in turn we obtain by adding, since

$$1 + (ma) + (ma)^2 + \ldots + (ma)^{p-2} \equiv \frac{(ma)^{p-1} - 1}{ma - 1} \pmod{p},$$
unless $ma - 1 \equiv 0 \pmod{p},$

$$\sum_{i=1}^{p-1} \frac{(mb + k)^i - m^ib_i}{i} \equiv m \text{ or } 0 \pmod{p}, \quad (9)$$
according as $\mu_1 \geq \mu_k$ or $\mu_1 < \mu_k$. In particular the right-hand member is $m$ if $k = 1$. Using the known relations,

$$S_n(p) \equiv pb_n \pmod{p},$$

$0 < g < p$, the first congruence following involving $p$ terms on the left, we have

$$g^{p-2}(1 + 1 + 1 + \ldots + 1) \equiv pb_{g^{p-2}} \pmod{p^2},$$
$$g^{p-3}(1 + 2 + \ldots + p - 1) \equiv pb_{g^{p-3}} \pmod{p^2},$$
and we obtain by addition

$$pg^{p-2} + \sum_{a=1}^{p-1} \frac{a^{p-1} - g^{p-1}}{a - g} \equiv - \frac{R_g}{g} \pmod{p^2},$$
employing (6), and if we write, with $(a, p) = 1,$

$$q(a) = \frac{a^{p-1} - 1}{p},$$
then the above gives

$$g^{p-2} + \sum_{\substack{a=1 \atop a \neq g}}^{p-1} \frac{q(a) - q(g)}{a - g} \equiv - \frac{R_p}{g} \pmod{p}. $$
Now modulo $p$,
\[ g^{p-2} + \sum_{a=1}^{p-1} \frac{q(a)}{a - g} - \sum_{a=1}^{p-1} \frac{q(g)}{a - g} \equiv \sum_{a=1}^{p-1} \frac{q(a) - q(g)}{a - g} g^{p-2} + g^{p-2} . \]

using
\[ \sum_{a=1}^{p-1} \frac{1}{a - g} \equiv \sum_{a=1}^{p-1} (a - g)^{p-2} \equiv g^{p-2} \pmod{p}, \]

hence
\[ \frac{1 - q(g)}{g} + \sum_{a=1}^{p-1} \frac{q(a)}{a - g} \equiv -R \pmod{p}, \tag{9a} \]

which for $g = 1$ gives
\[ \sum_{a=1}^{p-1} \frac{q(a)}{a - 1} \equiv -2 \pmod{p}. \]

We now obtain another formula related to (5b). Employing¹ (relation (4))
\[ (b(m, k) + m)^{n+1} - b_{n+1}(m, k) = m(n + 1)k^{p-2}, \]

and setting $n = p - 2$, we have after employing (3a),
\[ \sum_{i=0}^{p-2} (-1)^i b_i(m, k)m^{p-1-i} = -mk^{p-2}, \]

modulo $p$, where $(mb + k)^s = b_s(m, k)$.

We shall now modify some of the ideas in a certain proof² of (8) to obtain new types of congruences involving the Bernoulli numbers and Fermat's quotient. We have⁴
\[ \left( 1 - \frac{m^n}{nm^{n-1}} \right) b_n = \sum_{k=1}^{m-1} \sum_{i=1}^{[kp/m]} i^{n-1} \pmod{p}, \tag{10} \]

where $[x]$ is the greatest integer in $x$, $m > 1$, $n > 1$, $(m, p) = 1$. For $n = 1$ we shall now show that
\[ (m - 1)b_1 = \sum_{k=1}^{m-1} \sum_{i=1}^{[kp/r]} i^{n-1} \pmod{p}. \tag{10a} \]

We have for $(k, m) = 1$, $(m, p) = 1$.
\[ pk = r_k + m \left\lfloor \frac{pk}{m} \right\rfloor; \quad 0 < r_k < m. \]
Set $k = 1, 2, 3, \ldots, m - 1$ in turn and add we have since $pk_1 \equiv pk_2 (\mod m)$ only if $k_1 = k_2$ and therefore the r's range in some order over 1, 2, \ldots, $m - 1$,

$$m \sum_{k=1}^{m-1} \left\lfloor \frac{pk}{m} \right\rfloor + m \frac{m-1}{2} \equiv 0 \pmod{p},$$

or

$$m \sum_{k=1}^{m-1} \left\lfloor \frac{pk}{m} \right\rfloor \equiv b_1(m - 1) \pmod{p}.$$

Now take (10) with (10a), put $n = 1, 2, \ldots, p - 1$, in turn and add, after multiplying each relation in turn by $\frac{g^{k-1-n}}{p-1}$, we find

$$\frac{m^{p-1} - 1}{m^{p-2}} b_{p-1} - \frac{(m - 1)}{2} + \sum_{s=2}^{p-2} g^{p-1-s} \frac{1 - m^s}{sm^{s-1}} b_s \equiv -g^{p-2} \alpha(g, m) \pmod{p}, \quad (11)$$

since in (10) and (10a) when we add we have on the right

$$\sum_{k=1}^{m-1} \sum_{i=1}^{\left[\frac{kp}{m}\right]} g^{i^p-2} + ig^{i^p-3} + i^2 g^{i^p-4} + \ldots + i^{p-2},$$

or, if $0 < g < p$,

$$\sum_{k=1}^{m-1} \sum_{i=1}^{\left[\frac{kp}{m}\right]} \frac{g^{i^p-1} - g^{i^p-1}}{i - g} + g^{p-2}(p - 1) \alpha(g, m),$$

where $g^{p-2}$ occurs $\alpha(g, m)$ times in the right-hand member of (10) and (10a). Now (11) is satisfied identically for $m = 1$. It may also be written

$$(m^{p-1} - 1)b_{p-1} - \frac{m - 1}{2m} + \sum_{s=2}^{p-2} m^{p-1-s} \frac{1 - g^{p-1-s}}{sm^{s-1}} b_s \equiv -g^{p-2} \alpha(g, m) \pmod{p} \quad (11a)$$

Set $g = 1, m = 1, 2, \ldots, p - 1$ and add, we have, since for $m < p$, that $\alpha(1, m) = m - 1$,

$$(S_{p-1}(p) - p + 1)b_{p-1} + \sum_{s=1}^{p-2} b_s \equiv 0 \pmod{p}, \quad (12)$$

since

$$S_a(p) \equiv 0 \pmod{p}$$

for $a < p - 1$. Now we can write

$$S_{p-1}(p) \equiv pb_{p-1}(\mod p^2). \quad (13)$$
Using (13) and \( pb_{p-1} \equiv -1 \pmod{p} \), together with
\[
b_{p-1} \equiv 1 + \frac{(p - 1)!}{p} \pmod{p},
\]
we obtain the known formula
\[
\sum_{s=1}^{p-2} \frac{b_s}{s} \equiv W \pmod{p},
\]
where \( W \) is the Wilson quotient
\[
\frac{(p - 1)! + 1}{p}.
\]
On using this in connection with (11a) for \( m < p \) we have another known result
\[
-q(m) + \sum_{s=1}^{p-2} \frac{b_s}{sm^s} \equiv W \pmod{p}.
\]
Multiplying this last congruence through by \( a' \) gives, if \( t \) is in the range 1, 2, 3, \ldots, \( p - 2 \),
\[
\sum_{a=1}^{p-1} a'q(a) \equiv - \frac{b_t}{t} \pmod{p}.
\]
The relation (15) is an analogous theorem to (6). If \( m > 1, (m, p) = 1 \), \( p \) prime and odd, then it is known that
\[
\frac{(m^n - 1)b_n}{n} \equiv \sum' (-1)^{n-1} f_{n-1}(\rho) \pmod{p}
\]
where
\[
f_k(x) = 0^k + 1^kx + 2^kx^2 + \ldots + (p - 1)^kx^{p-1}
\]
with \( 0^p = 1 \). In this relation set \( n = 2, 3, \ldots, p - 1 \), together with the relation
\[
0 \equiv r^{p-2} \sum' \rho + \rho^2 + \ldots + \rho^{p-1}
\]
and add these \( p - 1 \) congruences, we obtain, if \( r < p \), the symbol \( \sum' \) indicating summation over all the distinct \( m \)th roots of unity excepting unity,
\[
\sum_{s=1}^{p-2} \sum' \rho^s(r^{p-2} + r^{p-3}s + \ldots + s^{p-2}) \pmod{p}
\]
\[
\begin{align*}
\equiv & \frac{\rho^{p-2}(\rho - 1)^p}{1 - \rho^p} + \sum' \frac{s_{1}^{\rho-1} - r^{p-1}}{s_{1} - r} + (1 - \rho^p) \\
\equiv & \sum' \frac{\rho^{p-2}}{\rho^p - 1},
\end{align*}
\]
modulo \( p \), so we obtain, if we set
\[
\beta(m, r) = \sum' \frac{\rho^i}{(\rho^p - 1)},
\]
for \( m > 1, 0 < r < p \),
\[
-q(m) + \sum_{n=2}^{p-2} \frac{1 - m^n}{n} \rho^{p-1-n} b_n \equiv r^{p-2} \beta(m, r) \text{(mod } p) .
\]
But by (15) we also have
\[
-\frac{r^{p-2}}{2} = q(r) + \sum_{n=2}^{p-2} \frac{\rho^{p-1-n} b_n}{n} \equiv W \text{(mod } p).
\]
Now (18) may be written
\[
-q(m) + \sum_{n=2}^{p-2} \frac{r^{p-1-n} b_n}{n} - \sum_{n=2}^{p-2} \frac{m^n \rho^{p-1-n} b_n}{n} \equiv r^{p-2} \beta(m, r),
\]
modulo \( p \), which with (19) gives, if \( m > 1, 0 < r < p \),
\[
-q(m) + q(r) + \frac{r^{p-2}}{2} + W - \sum_{n=2}^{p-2} \frac{m^n \rho^{p-1-n} b_n}{n} \equiv r^{p-2} \beta(m, r),
\]
modulo \( p \). For \( r = 1 \) in particular this takes the form
\[
-q(m) + W + \frac{1}{2} - \sum_{n=2}^{p-2} \frac{m^n b_n}{n} \equiv \beta(m, 1).
\]
Note that there is a certain type of analogy between (6b) and (20) with \( b_n \) corresponding to \( b_n/n \).

2 This relation is certainly one of the simplest the author has ever noted concerning the Bernoulli numbers. I have failed to find it in the literature, but do not imagine it could be new. Another proof may be obtained of it by the use of (2) by setting \( n = p \) and \( k = p - 1 \) therein.
3 These Proceedings, 31, 59, 312–314 (1945).
5 This relation is well known; for a recent proof, cf., Vandiver, Duke Math. Jour., 8, 578 (1941).
7 Included in a result due to Frobenius, Berlin Sitzungsberichte, 827 (1910). The latter theorem was generalized by Vandiver, Trans. Amer. Math. Soc., 51, 515 (1942).