Some modular results on the Euler and Bernoulli polynomials

by

JOHN BRILLHART (Tucson, Ariz.)

Dedicated to the memory of Wacław Sierpiński

1. Introduction. In this paper we will be concerned primarily with the Euler polynomials $E_n(x)$, although the Bernoulli polynomials $B_n(x)$ will be considered briefly in Sections 2 and 4.

The first results we give have to do with determining the parity of the number of irreducible factors of $E_n(x)$ and $E_n(x) \pmod{p}$, where $p$ is an odd prime. The next results deal with the irreducibility over the rational field $\mathbb{Q}$ of the members of two particular classes of Euler polynomials. The final results consist of showing $E_n(x)$ and $B_n(x)$ with their linear factors removed are irreducible over $\mathbb{Q}$ respectively for $n \leq 26$, $n \neq 5$, and $n \leq 22$, $n \neq 11$.

2. Parity theorems. The Euler polynomials can be given about the origin in Nörlund’s notation [8] as

$$E_n(x) = \sum_{s=0}^{n} \binom{n}{s} 2^{-s} C_s x^{n-s}, \quad n \geq 0,$$

where $C_{s-1} = 2^s (1 - 2^s) B_s / s$ and $B_s$ is the Bernoulli number, $B_0 = 1$, $B_1 = -1/2$, $B_2 = 1/6$, $B_3 = 0$, $B_{2n+1} = 0$, $m > 0$.

The Bernoulli polynomials have the explicit form

$$B_n(x) = \sum_{s=0}^{n} \binom{n}{s} B_s x^{n-s}, \quad n \geq 0,$$

where $B_s$ is again the Bernoulli number.

We will also use the notation $e(x) = E_{2m}(x) / x(x-1)$, as well as $E_n$ for the Euler number: $E_0 = 1$, $E_2 = -1$, $E_4 = 1/6$; $E_{2m+1} = 0$, $m \geq 0$. We then have

**Theorem 1.** If an odd prime $p$ does not divide the discriminant $D(e(x))$, then $e(x)$ has an even or odd number of irreducible factors (mod $p$)
respectively as the Legendre symbol
\[ \left( \frac{-1}{p} \right) \equiv 1 \text{ or } -1. \]

Proof. It was proved in [2], p. 52, (10) that
\[ D(2) = (-1)^{m} E_{2m} a^{2}, \quad a \neq 0. \]
From this equation the result immediately follows from the theorem of Stieckelberger [10]: If an \( n \)th degree polynomial \( f(x) \) has \( a \) irreducible factors (mod \( p \)), where \( p \) is an odd prime not dividing \( D(f(x)) \), then the Legendre symbol \( \left( \frac{D}{p} \right) = (-1)^{a-1} \). Q.E.D.

Corollary. The only odd primes \( p \) for which \( 2 \) can be irreducible (mod \( p \)) are those \( p \), not dividing \( D(2) \), for which
\[ \left( \frac{-1}{p} \right) = 1. \]
If we let \( e_{1}(x) = 2^{m+1} E_{2m+1} (x)/(2x-1) \) and recall ([2], p. 53) the equation \( D(e_{1}(x)) = (-1)^{m} (2m+1) E_{2m} b^{2}, \quad b \neq 0, \quad m \neq 2 \), we can also use Stieckelberger’s theorem to obtain
Theorem 2. If an odd prime \( p \) does not divide \( D(e_{1}(x)) \), then \( e_{1}(x) \) has an even or odd number of irreducible factors (mod \( p \)) respectively as the Legendre symbol
\[ \left( \frac{-1}{p} \right) \equiv 1 \text{ or } -1. \]
We can also derive two theorems of a similar kind for \( B_{n}(x) \) from the formulas ([2], p. 62)
\[ D(2^{m} B_{m}(x)) = (-1)^{m} D_{m} a^{2} \quad \text{when} \quad a \neq 0, \]
where \( D_{m} \) is the rational number \( D_{m} = 2(1 - 2^{m-1}) B_{m} \), and
\[ D(2 B_{2m+1}(x)) = (-1)^{m+1} (2^{2m+1} - 1)^{2} [(4m+2) B_{2m}] b^{2}, \quad b \neq 0. \]
3. Two irreducibility theorems. In preparing for the proofs of the theorems given below, we first establish in general how the polynomial \( E_{a_{1}+1}(x) \), \( n \geq 1 \), factors (mod \( p \)).
If \( p \) is an odd prime, we have from (1) (using [6])
\[ E_{p^{n+1}}(x) = \sum_{z=0}^{p^{n+1}} \left( \begin{array}{c} p^{n+1} \hline z \end{array} \right) 2^{-z} C_{z} \varphi^{p^{n+1} - z} \equiv \varphi^{p^{n+1} - x} - \varphi^{p^{n+1} - x} + 2 + x \varphi^{p^{n+1}} (mod p). \]
But
\[ \varphi^{p^{n+1} - x} = (1 - 2^{p^{n+1} - 1} B_{p^{n+1}})(p^{n+1}) = 2 - 3 B_{2}/2 = -1 (mod p) \]
by Kummer’s congruence.

Hence,
\[ 2 E_{p^{n+1}}(x) = 2 x^{p^{n+1} - x^{p^{n+1}} - x (mod p)}. \]
Further, setting
\[ F(x) = -2(x+1)^{p^{n+1}} E_{p^{n+1}}(x + 1), \]
we obtain
\[ F(x) = (x+1)^{p^{n+1}} (x+1) - 2 = x^{p^{n+1} + 1} (mod p). \]
If \( p^{n+1} = 2^{k}, \quad 2 \nmid k, \quad a \geq 1 \), then the binomial on the right side factors as
\[ x^{2^{k-1}+1} = \prod_{d \mid k} Q_{d^{a}}(x) (mod p), \]
where \( Q_{d}(x) \) is the \( d \)th cyclotomic polynomial. Also, it is well-known if \( p \nmid m \) that
\[ Q_{m}(x) = \prod_{i=1}^{f} P_{i}(x) (mod p), \]
where the \( P_{i}(x) \) are distinct and irreducible (mod \( p \)), and are all of degree \( e \), where \( e \) is the order of \( p \) (mod \( m \)) and \( f = \varphi(m)/e \), \( \varphi \) the Euler function. The factorization is thus complete.
It will be of use to go further than the above development in the cases \( n = 1 \) and 2. Accordingly we have
Lemma 1. If \( p \) is an odd prime and \( a_{1}, a_{2}, \ldots, a_{n-1} \) are the quadratic non-residues of \( p \), then the factorization
\[ 2 E_{p+1}(x) = x(x-1) \prod_{a=1}^{(p-1)/2} [(1-a) x^{2} - 2 a + 1] (mod p) \]
is complete (mod \( p \)).
Proof. Taking \( n = 1 \) in (3) we find
\[ F(x) = x [x^{2} - 2^{m-1} + 1] = x \prod_{a=1}^{(p-1)/2} (x^{2} - a_{2}) (mod p), \]
where we have used Euler’s Criterion.
Transforming back with the formula \( 2 E_{p+1}(x) = -x^{p+1} F \left( \frac{x}{x} - 1 \right) \), we obtain the required factorization, where the quadratic factors are clearly irreducible (mod \( p \)). Q.E.D.

Lemma 2. If \( p \) is an odd prime, then
\[ 2 E_{p+1}(x) = x(x-1) \prod_{a=1}^{(p-1)/2} G_{a}(x) (mod p), \]
where the $Q_s(x)$ are distinct quartic polynomials, which are irreducible (mod $p$).

Proof. Taking $a = 2$ in (3) we find
\[ \mathcal{P}(a) = x(2x^3 + 1) = x \prod_{d|x} \mathcal{Q}_{x+1,d}(\text{mod } p), \]
where $p^2 - 1 = 2^k, k \geq 2$. Now for each $d | k$, $p^2 \not\equiv 1 \pmod{2^{s+1}}$, but $p^2 \equiv 1 \pmod{2^{s+1}d}$. Hence, $e = 4$ for each $d$, and the result is proved, since transforming back yields distinct, irreducible, quartic factors (mod $p$). Q.E.D.

To conclude these preliminaries, we recall how $E_{2m}(x)$ factors (mod 2) (see [2], pp. 53–54):
\[ E_{2m}(x)x(x-1) = x^{2m-1} \left[ 1 + \left( 1 + \frac{1}{x} \right)^{2m-1} \right] \pmod{2}, \tag{5} \]
so again the factorization rests on the modular factorization of a binomial, $x^{2m-1} + 1$, where $x = 1 + \frac{1}{x}$. Hence,
\[ x^{2m-1} + 1 = \prod_{d|(2m-1)} Q_d(x) \pmod{2}, \]
where $Q_d(x)$ may possibly factor further (mod 2) as described in (4).

**Theorem 3.** If $p = 8m - 1$ is a prime for which 2 has the order $(p-1)/2$ (mod $p$), then $E_{2m}(x)x(x-1)$ is irreducible over $R$.

Proof. Let $e(x) = E_{2m}(x)x(x-1)$. By Lemma 1 we know that $e(x)$ factors into a product of irreducible quadratics (mod $p$). Hence, if $e(x)$ were reducible over $R$, the degree of each factor would be even.

On the other hand, we have by (5) that
\[ e(x) = x^{2m-1} \left[ 1 + \left( 1 + \frac{1}{x} \right)^{2m-1} \right] \pmod{2}. \]
But
\[ x^{2m-1} + 1 = (1 + x)Q_p(x)(1 + x)P_1(x)P_2(x) \pmod{2}, \]
where $P_1(x)$ and $P_2(x)$ are irreducible (mod 2) with odd degree $(p-1)/2$. Transforming back (and losing the factor $1 + x$) we obtain
\[ e(x) = x^{(p-1)/2}P_1 \left( 1 + \frac{1}{x} \right), P_2(x) \left( 1 + \frac{1}{x} \right) \pmod{2}. \]

From this factorization we conclude if $e(x)$ were reducible over $R$, it would have two factors of odd degree $(p-1)/2$, which contradicts the conclusion of the first part of the proof. Q.E.D.
and
\[ E_{p-1}(p-1) = E_{p-1}(p-3) = \ldots = E_{p-1}(2) = 2 \mod p. \]
Q.E.D.

4. Further irreducibility results. In two previous papers the following irreducibility theorems for Euler and Bernoulli polynomials have been proved:

**Theorem** ([A], p. 475). If a prime \( p \) is \( 3 \mod 4 \), then \( E_p(x)/x(x-1) \) is irreducible over \( R \).

**Theorem** ([B], p. 55). If \( 2m-1 \) is a prime having 2 as a primitive root, then \( E_{2m}(x)/x(x-1) \) is irreducible over \( R \).

**Theorem** ([C], p. 475). If \( 2m = k(p-1)t \), \( t \geq 0 \), \( 1 < k < p \), where \( p \) is an odd prime, then \( B_{2m}(x) \) is irreducible over \( R \).

**Theorem** ([D], p. 59). If \( 2m-1 \) is a prime having 2 as a primitive root, then \( B_{2m+1}(x)/x(x-1) \) is irreducible over \( R \).

When the first two of these theorems are combined with Theorems 3 and 4 of this paper, we find that \( E_n(x) \) with its linear factors removed is irreducible for \( n \leq 26 \), \( n \geq 5 \), except in the 10 cases: \( n = 9, 13, 15-18, 21, 22, 25, 26 \), the theorems don’t cover. Before establishing the irreducibility in these cases, we first consider a general procedure for showing irreducibility by combining modular factorization information.

Let \( f(x) = a_0 x^n + \ldots + a_n \), \( a_i \in I \), the integers, and suppose \( p \) is a prime, \( p \nmid a_0 \).

We can easily determine a set of integers which contains the degrees of the factors of \( f(x) \) over \( I \) from the degrees of the irreducible factors of \( f(x) \mod p \).

Let \( E_p(f) = \{d_1, \ldots, d_k\} \) be the set of degrees of the irreducible factors of \( f(x) \mod p \). We then define the degree set \( D(f(x), p) \) of \( f(x) \) with respect to \( p \) to be the set of sums of the elements in each of the non-empty subsets of \( E_p(f) \).

If we now have the complete factorizations of \( f(x) \) modulo various primes \( p_1, p_2, \ldots, p_n \), we then know a set of integers in which the degrees of the factors of \( f(x) \) over \( I \) must lie, namely \( F = \bigcap D(f(x), p_i) \). As soon as enough \( p_i \) have been discovered so that \( F = \{n\} \), we know \( f(x) \) is irreducible over \( I \). (I am grateful to R. Graham for first pointing out this simple procedure to me.)

It is clear Theorems 3 and 4 were proved by using this procedure. In Theorem 3 we had with \( e(x) = E_{p+1}(x)/x(x-1) \) that \( S_p(e) = \{2, 2, \ldots, 2\} \), so \( D(e(x), p) = \{2, 4, 6, \ldots, p-1\} \). Also, \( S_2(e) = \{p-1)/2 \}, \) \( (p-1)/2 \) is odd, so \( D(e(x), 2) = (p-1)/2, p-1 \). Thus, \( F = D(e(x), p) \cap D(e(x), 2) = \{p-1\} \). In Theorem 4 we had with \( e(x) = E_{p+2}(x)/x(x-1) \) that \( S_p(e) = \{4, 4, \ldots, 4\} \), so \( D(e(x), p) = \{4, 8, 12, \ldots, p^2-1\} \) and \( S_4(e) = \{p-1, (p-1)/2 \} \), so \( D(e(x), 2) = \{p-1, p(p-1), p^2-1\} \), where \( 4 \nmid (p-1) \). Thus, \( F = D(e(x), p) \cap D(e(x), 2) = \{p^2-1\} \).

To obtain the modular factorizations needed to show the irreducibility of the 10 undecided cases of \( E_n(x) \), we have used a modular factorization program, written by R. Stadthar for the CDC 6400, which is based on the powerful algorithm of E. Berlekamp [1]. To obtain the polynomials themselves as input for this program, it was necessary to devise a simple means of calculating a table of \( E_n(x) \) with respect to the various prime moduli which would be used in the factoring program. This calculation was carried out by Dr. W. F. Lunnon on the Atlas Computer at the Atlas Computer Laboratory, Didcot, England. Using the following algorithm, the first 100 Euler polynomials were computed modulo each prime \( < 100 \).

**Algorithm:** Let \( E_n(x) = \sum_{s=0}^{n} c(n, s) x^s, \) \( n \geq 0 \). Then with the starting values \( c(2, 2) = 1, c(2, 1) = -1, \) and \( c(2, 0) = 0 \) we compute in general

\[
c(n+2, s) = (n+1)(n+2)c(n, s-2)/s(s-1), \quad 2 \leq s \leq n+2, \]

\[
c(n+2, 1) = -\sum_{s=2}^{n+2} c(n+2, s) \quad \text{and} \quad c(n+2, 0) = 0.
\]

Thus, starting with \( n = 2 \), we first compute the coefficients of the next Euler polynomial of even degree. Since this polynomial also has integer coefficients, the exact division serves as a check on the arithmetic.

Now let \( n+2 = 2^k k \), \( k, \) odd. Since \( E_e(x) = n E_{n+2}(x) \), we can compute the coefficients \( b(n+1, s) \) of the intermediate polynomial of odd degree by differentiating \( E_{n+2}(x) \), i.e.

\[
b(n+1, s-1) = s \cdot c(n+2, s)/k, \quad 1 \leq s \leq n+2.
\]

(Here the \( b \)'s are integers, which differ from the actual (fractional) coefficients of \( E_{n+2}(x) \) by the factor \( 2^k \).) Finally, each of the polynomials is reduced modulo each odd prime \( < 100 \) (none of these primes divides the leading coefficient of the generated polynomials, since this coefficient is 1 when \( a \) is even and a power of 2 otherwise).

We should remark that the program written by Dr. Lunnon of necessity employed multiple precision calculation, since the coefficients
of \( E_n(x) \) generally grow in size with \( n \). It would have been more efficient to bypass this multiple precision calculation by computing the polynomials directly modulo \( p \) from the recursion, if this were possible. However, it was not clear how to do this.

In the following table we list the information obtained from the factoring program which shows the irreducibility of the \( E_n(x) \) under consideration. The degrees of the irreducible factors are given first, followed (after the semi-colon) by the modulus. In case the respective polynomial was found to be irreducible (mod \( p \)), the entry reads “mod \( p \”).

<table>
<thead>
<tr>
<th>( n )</th>
<th>Degrees and moduli</th>
<th>( \sigma )</th>
<th>Degrees and moduli</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>(1, 4, 13), (4, 4, 17)</td>
<td>18</td>
<td>(8, 11), (5, 5, 23)</td>
</tr>
<tr>
<td>13 mod 7</td>
<td>21</td>
<td>(30, 10, 11), (2, 2, 16, 17)</td>
<td></td>
</tr>
<tr>
<td>16 mod 11</td>
<td>23</td>
<td>(5, 14, 3), (4, 20, 17)</td>
<td></td>
</tr>
<tr>
<td>16 (7, 11)</td>
<td>25</td>
<td>(4, 20, 3), (12, 13, 23)</td>
<td></td>
</tr>
</tbody>
</table>

The case of the Bernoulli polynomials for \( n \leq 23, n \neq 11 \), is much simpler, since the last two theorems given at the beginning of this section cover all the cases except \( n = 14 \) and 17. The irreducibility of \( B_n(x) \) has been shown by L. Carlitz in [5]. To obtain \( B_n(x) \), a calculation was carried out by hand, rather than make a table of \( B_n(x) \) similar to the one made for \( E_n(x) \). To construct such a table is only slightly more complicated than for \( E_n(x) \), the complication arising from the fact that in general the coefficients of \( E_n(x) \) are fractions, whose denominators are not just powers of 2. The factorizations that settle this case are (4, 19, 7) and (7, 7, 11).

Acknowledgements. The author would like to thank Dr. W.F. Lunnon and the directors of the Atlas Computer Laboratory for their kind assistance in carrying out the calculation described above. He would also like to thank J. Schäffer for pointing out to him that the factorization of \( B_{11}(x) \), asserted to be new in [2], had previously appeared in a somewhat different form in his paper ([9], p. 171). Finally, he would like to thank R. Stauduhar for the use of his modular factoring program.

References