ACTA ARITHMETICA
XXI (1972)

Some modular results on the Euler and Bernoulli polynomials

by

JOHN BRILLHART (Tucson, Ariz.)

Dedicated to the memory of Waclaw 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 $B_n(x) \pmod p$, where p is an odd prime. The next results deal with the irreducibility over the rational field R 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 R respectively for $n \leqslant 26$, $n \neq 5$, and $n \leqslant 22$, $n \neq 11$.

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

$$E_n(x) = \sum_{s=0}^{n} \binom{n}{s} 2^{-s} C_s x^{n-s}, \qquad n \geqslant 0, \tag{1}$$

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

The Bernoulli polynomials have the explicit form

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

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: $E_0 = 1$, $E_2 = -1, \ldots$; $E_{2m+1} = 0$, $m \geqslant 0$. 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* $\pmod p$

respectively as the Legendre symbol

$$\left(\frac{(-1)^m E_{2m}}{p}\right) = +1 \text{ or } -1.$$

Proof. It was proved in [2], p. 52, (10), that

$$D\big(e(x)\big) = (-1)^m E_{2m} a^2, \quad a \neq 0. \tag{2}$$

From this equation the result immediately follows from the theorem of Stickelberger [10]: If an nth degree polynomial $f(x)$ has s irreducible factors (mod p), where p is an odd prime not dividing $D\big(f(x)\big)$, then the Legendre symbol $\left(\frac{D}{p}\right) = (-1)^{n-s}$. Q.E.D.

COROLLARY. *The only odd primes p for which $e(x)$ can be irreducible* (mod p) *are those p, not dividing $D\big(e(x)\big)$, for which* $\left(\frac{(-1)^m E_{2m}}{p}\right) = -1$.

If we let $e_1(x) = 2^{2m+1}E_{2m+1}(x)/(2x-1)$ and recall ([2], p. 53) the equation $D\big(e_1(x)\big) = (-1)^m(2m+1)E_{2m}b^2$, $b \neq 0$, $m \neq 2$, we can also use Stickelberger's theorem to obtain

THEOREM 2. *If an odd prime p does not divide $D\big(e_1(x)\big)$, then $e_1(x)$ has an even or odd number of irreducible factors* (mod p) *respectively as the Legendre symbol*

$$\left(\frac{(-1)^m(2m+1)E_{2m}}{p}\right) = +1 \text{ or } -1.$$

We can also derive two theorems of a similar kind for $B_n(x)$ from the formulas ([2], p. 62)

$$D\big(2^m B_{2m}(x)\big) = (-1)^m D_{2m} a^2 \quad \text{when} \quad a \neq 0,$$

where D_s is the rational number $D_s = 2(1-2^{s-1})B_s$, and

$$D\big(2B_{2m+1}(x)\big) = (-1)^{m+1}(2^{2m-1}-1)^3[(4m+2)B_{2m}]^7 b^2, \quad b \neq 0.$$

3. Two irreducibility theorems. In preparing for the proofs of the theorems given below, we first establish in general how the polynomial $E_{p^n+1}(x)$, $n \geqslant 1$, factors (mod p).

If p is an odd prime, we have from (1) (using [6])

$$E_{p^n+1}(x) = \sum_{s=0}^{p^n+1} \binom{p^n+1}{s} 2^{-s} C_s x^{p^n+1-s} \equiv x^{p^n+1} - x^{p^n}/2 + xC_{p^n}/2^{p^n} \pmod p.$$

But

$$C_{p^n} = [2^{p^n+1}(1-2^{p^n+1})B_{p^n+1}]/(p^n+1)^{\dagger} \equiv 4(-3)B_2/2 = -1 \pmod p$$

by Kummer's congruence.

Hence,

$$2E_{p^n+1}(x) \equiv 2x^{p^n+1} - x^{p^n} - x \pmod p.$$

Further, setting

$$F(x) = -2(x+1)^{p^n+1}E_{p^n+1}\big(1/(x+1)\big),$$

we obtain

$$F(x) \equiv (x+1)^{p^n} + (x+1) - 2 \equiv x(x^{p^n-1}+1) \pmod p. \tag{3}$$

If $p^n - 1 = 2^a k$, $2 \nmid k$, $a \geqslant 1$, then the binomial on the right side factors as

$$x^{p^n-1}+1 \equiv \prod_{d|k} Q_{2^{a+1}d}(x) \pmod p,$$

where $Q_m(x)$ is the mth cyclotomic polynomial. Also, it is well-known if $p \nmid m$ that

$$Q_m(x) \equiv \prod_{i=1}^{f} P_i(x) \pmod p, \tag{4}$$

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 $f = \varphi(m)/e$, φ 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 $n_1, n_2, \ldots, n_{(p-1)/2}$ are the quadratic non-residues of p, then the factorization*

$$2E_{p+1}(x) \equiv x(x-1)\prod_{s=1}^{(p-1)/2}[(1-n_s)x^2 - 2x + 1] \pmod p$$

is complete (mod p).

Proof. Taking $n = 1$ in (3) we find

$$F(x) \equiv x[(x^2)^{(p-1)/2}+1] \equiv x\prod_{s=1}^{(p-1)/2}(x^2 - n_s) \pmod p,$$

where we have used Euler's Criterion.

Transforming back with the formula $2E_{p+1}(x) = -x^{p+1}F\left(\frac{1}{x} - 1\right)$, 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*

$$2E_{p^2+1}(x) \equiv x(x-1)\prod_{s=1}^{(p^2-1)/4} G_s(x) \pmod p,$$

where the $G_s(x)$ are distinct quartic polynomials, which are irreducible (mod p).

Proof. Taking $n = 2$ in (3) we find

$$F(x) \equiv x(x^{p^2-1}+1) \equiv x\prod_{d|k} Q_{2^{a+1}d}(x) \pmod p,$$

where $p^2-1 = 2^a k$, $2\nmid k$. Now for each $d|k$, $p^2 \not\equiv 1 \pmod{2^{a+1}d}$, but $p^4 \equiv 1 \pmod{2^{a+1}d}$. 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):

$$E_{2m}(x)/x(x-1) \equiv x^{2m-1}\left[1+\left(1+\frac{1}{x}\right)^{2m-1}\right] \pmod 2, \tag{5}$$

so again the factorization rests on the modular factorization of a binomial, $z^{2m-1}+1$, where $z = 1+\dfrac{1}{x}$. Hence,

$$z^{2m-1}+1 \equiv \prod_{d|(2m-1)} Q_d(z) \pmod 2,$$

where $Q_d(z)$ 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 $E_{8m}(x)/x(x-1)$ is irreducible over R.*

Proof. Let $e(x) = E_{8m}(x)/x(x-1)$. 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

$$e(x) \equiv x^{8m-1}\left[1+\left(1+\frac{1}{x}\right)^{8m-1}\right] \pmod 2.$$

But

$$z^{8m-1}+1 \equiv (1+z)Q_p(z) \equiv (1+z)P_1(z)P_2(z) \pmod 2,$$

where $P_1(z)$ and $P_2(z)$ are irreducible (mod 2) with odd degree $(p-1)/2$. Transforming back (and losing the factor $1+z$) we obtain

$$e(x) \equiv x^{(p-1)/2}P_1\left(1+\frac{1}{x}\right)\cdot x^{(p-1)/2}P_2\left(1+\frac{1}{x}\right) \pmod 2.$$

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.

THEOREM 4. *If a prime $p \equiv 3 \pmod 8$ has 2 as a primitive root, and $2^{p-1} \not\equiv 1 \pmod{p^2}$, then $E_{p^2+1}(x)/x(x-1)$ is irreducible over R.*

Proof. Let $e(x) = E_{p^2+1}(x)/x(x-1)$. The condition $2^{p-1} \not\equiv 1 \pmod{p^2}$ implies 2 is a primitive root of p^2 (and in fact all higher powers of p; see Nagell [7]). From Lemma 2 we know $e(x)$ factors into a product of irreducible quartics (mod p). Thus, if $e(x)$ were reducible over R, the degree of each factor would be a multiplie of 4.

On the other hand, we have from (5) that

$$e(x) \equiv x^{p^2}\left[1+\left(1+\frac{1}{x}\right)^{p^2}\right] \pmod 2.$$

But

$$z^{p^2}+1 \equiv (1+z)Q_p(z)Q_{p^2}(z) \pmod 2,$$

where $Q_p(z)$ and $Q_{p^2}(z)$ are irreducible (mod 2), since 2 is a primitive root of both p and p^2. Transforming back we obtain

$$e(x) \equiv x^{p-1}Q_p\left(1+\frac{1}{x}\right)\cdot x^{p(p-1)}Q_{p^2}\left(1+\frac{1}{x}\right) \pmod 2.$$

Hence, if $e(x)$ were reducible over R, it would factor into irreducible factors of degree $p-1$ and $p(p-1)$. But the condition $p \equiv 3 \pmod 8$ implies $4\nmid(p-1)$, which contradicts the conclusion of the first part of the proof. (Note: the extra 2 in the modulus of $p \equiv 3 \pmod 8$, beyond what is needed to establish the contradiction, is present so that 2 can be a primitive root of p). Q.E.D.

Comment. It is worth mentioning that no prime $p \equiv 3 \pmod 8$ is known $< 2^{31}$ for which $2^{p-1} \equiv 1 \pmod{p^2}$. (See [3].) The primes of this form < 100 having 2 as a primitive root are 3, 11, 19, 59, 67, and 83.

We conclude this section with the following result.

THEOREM 5. *If p is an odd prime, then*

$$E_{p-1}(2k-1) \equiv 0 \pmod p \quad \text{and} \quad E_{p-1}(2k) \equiv 2 \pmod p, \qquad k = 1, 2, \ldots, (p-1)/2.$$

Proof (Carlitz). From the identity

$$E_n(x+1)+E_n(x) = 2x^n, \quad n \geqslant 0,$$

we conclude that

$$E_{p-1}(x+1)-E_{p-1}(x-1) = 2[x^{p-1}-(x-1)^{p-1}].$$

Hence,

$$E_{p-1}(p-2) \equiv E_{p-1}(p-4) \equiv \ldots \equiv E_{p-1}(1) = 0 \pmod p$$

and

$$E_{p-1}(p-1) \equiv E_{p-1}(p-3) \equiv \ldots \equiv E_{p-1}(2) = 2 \pmod{p}. \quad \text{Q.E.D.}$$

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

THEOREM ([4], p. 475). *If a prime p is $\equiv 3 \pmod 4$, then $E_p(x)/(x-\frac{1}{2})$ is irreducible over R.*

THEOREM ([2], 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 ([4], p. 475). *If $2m = k(p-1)p^t$, $t \geqslant 0$, $1 \leqslant k < p$, where p is an odd prime, then $B_{2m}(x)$ is irreducible over R.*

THEOREM ([2], p. 59). *If $2m-1$ is a prime having 2 as a primitive root, then $B_{2m+1}(x)/x(x-\frac{1}{2})(x-1)$ 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 $n \leqslant 26$, $n \neq 5$, except in the 10 cases: $n = 9, 13, 15$–$18, 21, 22, 25, 26$, which 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 $f(x) = a_0x^n + \ldots + a_n$, $a_i \in I$, 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 $f(x) \pmod p$.

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

If we now have the complete factorizations of $f(x)$ modulo various primes p_i, $p_i \nmid a_0$, we then know a set of integers in which the degrees of the factors of $f(x)$ over I must lie, namely $F = \bigcap_i \mathscr{D}(f(x), p_i)$. 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 $\mathscr{D}(e(x), p) = \{2, 4, 6, \ldots, p-1\}$. Also, $S_2(e) = \{(p-1)/2, (p-1)/2\}$, where $(p-1)/2$ is odd, so $\mathscr{D}(e(x), 2) = \{(p-1)/2, p-1\}$. Thus, $F = \mathscr{D}(e(x), p) \cap \mathscr{D}(e(x), 2) = \{p-1\}$. In Theorem 4 we had

with $e(x) = E_{p^2+1}(x)/x(x-1)$ that $S_p(e) = \{4, 4, \ldots, 4\}$, so

$$\mathscr{D}(e(x), p) = \{4, 8, 12, \ldots, p^2-1\}$$

and $S_2(e) = \{p-1, p(p-1)\}$, so

$$\mathscr{D}(e(x), 2) = \{p-1, p(p-1), p^2-1\},$$

where $4 \nmid (p-1)$. Thus

$$F = \mathscr{D}(e(x), p) \cap \mathscr{D}(e(x), 2) = \{p^2-1\}.$$

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. Stauduhar 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 $E_n(x) = \sum_{s=0}^{n} c(n, s)x^s$, $n \geqslant 2$. Then with the starting values $c(2, 2) = 1$, $c(2, 1) = -1$, and $c(2, 0) = 0$ we compute in general

$$c(n+2, s) = (n+1)(n+2)c(n, s-2)/s(s-1), \quad 2 \leqslant s \leqslant n+2,$$

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

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 $n+2 = 2^a k$, k odd. Since $E_n'(x) = nE_{n-1}(x)$, we can compute the coefficients $b(n+1, s)$ of the intermediate polynomial of odd degree by differentiating $E_{n+2}(x)$, i.e.

$$b(n+1, s-1) = s \cdot c(n+2, s)/k, \quad 1 \leqslant s \leqslant n+2.$$

(Here the b's are integers, which differ from the actual (fractional) coefficients of $E_{n+1}(x)$ by the factor 2^a.) 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 n 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 1

n	Degrees and moduli	n	Degrees and moduli
9	(1, 1, 6; 13), (4, 4; 17)	18	(8, 8; 11), (5, 5, 6; 23)
13	mod 7	21	(10, 10; 11), (2, 2, 16; 17)
15	mod 19	22	mod 17
16	(7, 7; 11), (4, 5, 5; 13)	25	(5, 5, 14; 3), (4, 20; 17)
17	(6, 10; 7), (1, 1, 14; 11)	26	(4, 20; 3), (12, 12; 23)

The case of the Bernoulli polynomials for $n \leqslant 22$, $n \neq 11$, 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 $B_{14}(x)$ has been shown by L. Carlitz in [5]. To obtain $B_{17}(x)$, 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 $B_n(x)$ are fractions, whose denominators are not just powers of 2. The factorizations that settle this case are $(4, 10; 7)$ 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

[1] E. Berlekamp, *Algebraic Coding Theory*, New York 1968, pp. 146–150.
[2] J. Brillhart, *On the Euler and Bernoulli polynomials*, Journ. für Math. 234 (1969), pp. 45–64.
[3] — J. Tonascia, and P. Weinberger, *On the Fermat quotient*, Proceedings of the 1969 Atlas Symposium on Computers in Number Theory at Oxford.

[4] L. Carlitz, *Note on irreducibility of the Bernoulli and Euler polynomials*, Duke Math. Journ. 19 (1952), pp. 475–481.
[5] — *The irreducibility of the Bernoulli polynomial* $B_{14}(x)$, Math. Comp. 19 (1965), pp. 667–670.
[6] L. E. Dickson, *History of the Theory of Numbers*, vol. 1, New York 1966, p. 270.
[7] T. Nagell, *Introduction to Number Theory*, New York 1951, p. 107.
[8] N.E. Nörlund, *Vorlesungen über Differenzenrechnung*, New York 1954, Chapter 2.
[9] J. J. Schäffer, *The equation* $1^p + 2^p + 3^p + \ldots + n^p = m^q$, Acta Math. 95 (1956), pp. 155–189.
[10] G. Voronoï, *Sur une propriété du discriminant des fonctions entières*, Verhandlungen des dritten internationalen Mathematiker-Kongresses in Heidelberg 1904, Leipzig 1905, pp. 186–189.

Received on 5. 7. 1971 (188)