The Irreducibility of the Bernoulli Polynomial $B_{14}(x)$

By L. Carlitz

1. Put

$$B_n(x) = (B + x)^n = \sum_{r=0}^{n} \binom{n}{r} B_r x^{n-r},$$

where B_r is defined by means of

$$B_0 = 1, \qquad (B + 1)^n = B^n \qquad (n > 1).$$

For n odd, $n > 1$, it is familiar that $B_n(x)$ has the linear factors $x, x - \frac{1}{2}, x - 1$. For n even no factors with rational coefficients are known and it seems plausible that $B_n(x)$ is irreducible (with respect to the rational field). The writer has proved [1] that $B_n(x)$ is irreducible for

$$n = kp^r(p - 1) \qquad (1 \leqq k < p, r \geqq 0),$$

where p is an odd prime, and also for $n = 2^r, r \geqq 1$. McCarthy [2] has proved the irreducibility of $B_n(x)$ for $n = (kp + k + 1)(p - 1)$ when $k < p$.

It is noted in [1] that for even values of $n \leqq 50$ the irreducibility of $B_n(x)$ remains in doubt for $n = 14, 26, 34, 37$. The irreducibility of $B_{14}(x)$ has been verified in the Duke University Computing Laboratory by R. Carlitz.

The purpose of the present note is to give a proof of the irreducibility of $B_{14}(x)$ that uses a minimum of computation. While the result is special, the method is of a rather general nature and may perhaps be of use in proving more comprehensive results.

2. Using the notation of Nörlund [2, Ch. 2] we put

$$(1) \qquad P(x) = 2^{14}B_{14}\left(\frac{x+1}{2}\right) = \sum_{r=0}^{7} \binom{14}{2r} D_{2r} x^{14-2r},$$

where

$$D_{2r} = (2 - 2^{2r})B_{2r}.$$

By the Staudt-Clausen theorem the denominator of D_{2r} is odd; moreover, if p is an odd prime and $r > 0$,

$$pD_{2r} \equiv \begin{cases} -1 \pmod p & (p - 1 \mid 2r), \\ 0 \pmod p & (p - 1 \nmid 2r). \end{cases}$$

We first take $p = 3$. Then

$$-3P(x) \equiv \sum_{r=0}^{6} \binom{14}{2r} x^{2r} \qquad (\text{mod } 3).$$

It is easily verified that

$$\binom{14}{2} \equiv \binom{14}{12} \equiv 1, \quad \binom{14}{4} \equiv \binom{14}{10} \equiv -1, \quad \binom{14}{6} \equiv \binom{14}{8} \equiv 0 \pmod 3,$$

Received February 18, 1965. Supported in part by NSF grant GP-1593.

so that

$$(2) \qquad -3P(x) \equiv x^{12} - x^{10} - x^4 + x^2 + 1 \pmod 3.$$

Here we have made use of the familiar result that if

$$n = n_0 + n_1 p + n_2 p^2 + \cdots \qquad (0 \leqq n_j < p),$$
$$r = r_0 + r_1 p + r_2 p^2 + \cdots \qquad (0 \leqq r_j < p),$$

then

$$\binom{n}{r} \equiv \binom{n_0}{r_0}\binom{n_1}{r_1}\binom{n_2}{r_2}\cdots \pmod p,$$

where p is a prime.

Next we verify that

$$(3) \qquad \begin{aligned} x^{12} - x^{10} - x^4 + x^2 + 1 &\equiv (x^3 - x)^4 + (x^3 - x)^2 + 1 \\ &\equiv [(x^3 - x)^2 - 1]^2 \equiv (x^3 - x - 1)^2(x^3 - x + 1)^2 \pmod 3. \end{aligned}$$

The polynomials $x^3 - x \pm 1$ are irreducible (mod 3) since clearly neither has a linear factor. (The irreducibility is a special case of the irreducibility (mod p) of $x^p - x - k$, where k is any integer not divisible by p.)

It is evident from (1) that

$$(4) \qquad P(x) = Q(x^2),$$

where $Q(y)$ is a polynomial of degree 7 in y. Since

$$(x^3 - x - 1)(x^3 - x - 1) = x^2(x^2 - 1)^2 - 1,$$

it follows from (2) and (3) that

$$(5) \qquad -3Q(y) \equiv (y(y-1)^2 - 1)^2 \equiv (y^3 - y^2 - y - 1)^2 \pmod 3.$$

Also it is easily verified that $y^3 + y^2 + y - 1$ is irreducible (mod 3).

3. We now take $p = 13$. Then we find that

$$(6) \qquad P(x) \equiv x^{14} + \binom{14}{2} D_{12}x^2 + D_{14} \pmod{13}.$$

By Kummer's congruence [3, Ch. 14]

$$\frac{B_{14}}{14} \equiv \frac{B_2}{2} \equiv \frac{1}{12} \equiv -1 \pmod{13},$$

so that

$$D_{14} = (2 - 2^{14})B_{14} \equiv 2 \pmod{13}.$$

By the Staudt-Clausen theorem

$$13D_{12} \equiv -1 \pmod{13}.$$

Thus (6) becomes

$$(7) \qquad P(x) \equiv x^{14} - \tfrac{1}{2}x^2 + 2 \pmod{13}.$$

If a is a rational integer, (7) gives

$$P(a) \equiv \tfrac{1}{2}a^2 + 2 \equiv \tfrac{1}{2}(a+3)(a-3) \pmod{13}.$$

Also, since

$$P'(x) \equiv x^{13} - x \pmod{13},$$

it follows that 3 and -3 are zeros of $P(x)$ of multiplicity two.

In terms of $Q(y)$, as defined by (4), we have

$$(8) \qquad Q(y) \equiv (y+4)^2 Q_1(y) \pmod{13},$$

where $Q_1(y)$ is a polynomial of degree 5 in y that has no linear factors. We shall now prove that $Q_1(y)$ has no quadratic factors (mod 13). For assume that

$$(9) \qquad Q(a+\theta) = 0 \qquad (\theta^2 \in \mathrm{GF}(13),\ \theta \notin \mathrm{GF}(13)),$$

where a is some rational integer and θ is a number of $\mathrm{GF}(13^2)$ that is not in GF(13). Then by (7)

$$Q(a+\theta) = (a+\theta)^7 - \tfrac{1}{2}(a+\theta) + 2 = 0,$$

so that

$$(a+\theta)^7 = \tfrac{1}{2}a - 2 + \tfrac{1}{2}\theta.$$

Squaring both sides of this equation we get, since

$$(a+\theta)^{14} = (a+\theta)(a+\theta^{13}) = (a+\theta)(a-\theta),$$

$$a^2 - \theta^2 = (\tfrac{1}{2}a - 2)^2 + \tfrac{1}{2}(a-4)\theta + \tfrac{1}{4}\theta^2.$$

This evidently implies $a = 4$, $\theta^2 = 5$. The quadratic $y^2 + 5y - 2$ has the roots $4 \pm \sqrt{5}$ and is irreducible over GF(13). Thus if (9) holds $Q(y)$ must be divisible by $y^2 + 5y - 2$; it is however readily verified that this is not the case.

It follows at once from the above discussion that $Q_1(y)$ is irreducible (mod 13).

4. Returning to (1) we find that

$$P(x) \equiv (x^7 - x)^2 \pmod{7}.$$

By Kummer's congruence

$$\frac{B_{14}}{14} \equiv \frac{B_2}{2} \equiv 3 \pmod{7},$$

so that the numerator of B_{14} is divisible by 7 but not by 7^2. Since

$$D_{14} = (2 - 2^{14})B_{14},$$

the same is true of D_{14}. Hence $P(x)$ is a polynomial with coefficients that are integral (mod 7) and with constant term divisible by 7 but not by 7^2; moreover $P(-x) = P(x)$. Now assume a factorization

$$(10) \qquad P(x) = P_1(x)P_2(x)\cdots P_k(x)$$

where the $P_j(x)$ are normalized irreducibles with rational coefficients that are integral (mod p). Exactly one of the $P_j(x)$, say $P_1(x)$, has constant term divisible by 7. Replacing x by $-x$ in (10) we infer that $P_1(-x) = P_1(x)$ and therefore

$P_1(x) = Q_1(x^2)$. Hence the reducibility of $P(x)$ over the rational field implies the reducibility of $Q(x)$.

On the other hand, by (5) and (8),

$$\begin{cases} -3Q(y) \equiv (y^3 + y^2 + y - 1)^2 & \pmod 3, \\ Q(y) \equiv (y + 4)^2 Q_1(y) & \pmod{13}, \end{cases}$$

where the factors on the right are irreducible for the respective moduli. Since $Q_1(y)$ is of degree 5, it follows that $Q(y)$ is irreducible over the rationals. Therefore, by the preceding paragraph, $P(x)$ is also irreducible.

5. We remark that

$$2B_{14}(x) \equiv (x^3 + x + 1)^2(x^3 + x^2 + 1)^2 \pmod 2;$$

the cubics $x^3 + x + 1$, $x^3 + x^2 + 1$ are irreducible (mod 2). We have also

$$-5B_{14}(x) \equiv (x^5 - x)^2 \pmod 5.$$

It can be verified that

$$Q(y) \equiv y^7 - 3y^6 - 3y^2 + 4y - 4 \pmod{11}$$

and that $Q(y)$ has no linear factors (mod 11). However the complete factorization of $Q(y)$ (mod 11) has not been obtained.

We observe that for an arbitrary prime $p > 3$, the polynomial

$$P_{2p}(x) = 2^{2p}B_{2p}\left(\frac{x+1}{2}\right) = \sum_{r=0}^{p} \binom{2p}{2r} D_{2r} x^{2p-2r}$$

has coefficients integral (mod p); indeed

$$P_{2p}(x) \equiv (x^p - x)^2 \pmod p.$$

Moreover the constant term D_{2p} is divisible by p and not by p^2. It follows, exactly as in the special case $p = 7$, that to prove the irreducibility over the rationals of $P_{2p}(x)$ it suffices to prove the irreducibility of $Q_p(y)$, where

$$Q_p(x^2) = P_{2p}(x).$$

Duke University,
Durham, North Carolina

1. L. Carlitz, "Note on irreducibility of the Bernoulli and Euler polynomials," *Duke Math. J.*, v. 19, 1952, pp. 475–481. MR **14,** 163.

2. P. J. McCarthy, "Irreducibility of certain Bernoulli polynomials," *Amer. Math. Monthly* v. 68, 1961, pp. 352–353. MR **23,** #A1625.

3. N. Nielsen, *Traité Élémentaire des Nombres de Bernoulli*, Paris, 1923.

4. N. E. Nörlund, *Vorlesungen über Differenzenrechnung*, Berlin, 1924.