

## DEFINING BERNOULLI POLYNOMIALS IN $\mathbf{Z}/p\mathbf{Z}$ (A GENERIC REGULARITY CONDITION)

ANDREW GRANVILLE AND H. S. SHANK

(Communicated by William Adams)

**ABSTRACT.** We consider the problem of whether Bernoulli polynomials are uniquely defined by certain interpolation equations. This leads to an interesting characterization of regular primes, a new insight into the  $p$ -divisibility of Fermat quotients, and a generalization of Voronoi's congruences.

The Bernoulli polynomials  $B_m(x)$ ,  $m \in \{0, 1, 2, \dots\} = \mathbf{N}$ , satisfy the difference equation

$$(1) \quad F(x+1) - F(x) = mx^{m-1}$$

and the interpolation equation

$$(2) \quad F(x) = q^{m-1} \left[ F\left(\frac{x}{q}\right) + F\left(\frac{x+1}{q}\right) + \dots + F\left(\frac{x+q-1}{q}\right) \right]$$

for each integer  $q \geq 2$ , and for all real numbers  $x$ .

It is not hard to show that either (1) or (2) together with the value of  $F(0)$  completely characterize the polynomial  $F(x)$ . However, Dickey, Kairies, and Shank [2] showed that in the field  $\mathbf{Z}/p\mathbf{Z}$  this does not necessarily happen when  $q = 2$  in (2). In this note we extend their work and give explicit criteria to determine when the above characterization occurs.

Throughout we shall assume that the prime  $p$  is given and that we are considering the equations (1) and (2) only for functions  $F: \mathbf{Z}/p\mathbf{Z} \rightarrow \mathbf{Z}/p\mathbf{Z}$ . We start by observing that, as a consequence of Fermat's Little Theorem ( $x^p = x$  for all  $x \in \mathbf{Z}/p\mathbf{Z}$ ), we need only consider values of  $m$  in the range  $1 \leq m \leq p-1$ :

Let  $n$  be the least positive residue of  $m \pmod{p-1}$ . In (1) if  $p$  divides  $m$  then  $F(x) = F(0)$  for all  $x$ ; otherwise  $G(x) := F(x)/m$  satisfies  $G(x+1) - G(x) = x^{m-1} = x^{n-1}$ . In (2) we simply can replace  $q^{m-1}$  by  $q^{n-1}$ .

The Von Staudt-Clausen theorem [3,1] states that  $p$  divides the denominator of the  $m$ th Bernoulli number  $B_m$  exactly when  $p-1$  divides  $m$  (and that  $p$  divides  $pB_{p-1} + 1$ ). Thus  $B_m(x)$  is not well defined in  $\mathbf{Z}/p\mathbf{Z}$  for  $m \geq p-1$ .

---

Received by the editors October 29, 1988 and, in revised form, April 29, 1989.

1980 *Mathematics Subject Classification* (1985 Revision). Primary 11B68; Secondary 11A15.

©1990 American Mathematical Society  
0002-9939/90 \$1.00 + \$.25 per page

We adjust for this problem by instead using the function

$$C_m(x) = \frac{1}{m}[B_m(x) - B_m]$$

which, by (1), equals the sum of the  $m-1$ th powers of the nonnegative integers less than  $x$ , at each positive integer  $x$ . Our key lemma is

**Lemma 1.** *Suppose that  $p$  is a given prime and  $n$  and  $v$  are integers with  $1 \leq n \leq p-1$  and  $F(x+1) - F(x) = vx^{n-1}$  for each nonzero element  $x$  in  $\mathbf{Z}/p\mathbf{Z}$ . Then  $F(x) = vC_n(x) + F(0)$  in  $\mathbf{Z}/p\mathbf{Z}$ .*

*Proof.* Let  $G(x) = F(x) - vC_n(x)$ . By (1) we have  $G(x+1) - G(x) = 0$  for each  $x \neq 0$ . Therefore  $G(p) = G(p-1) = \dots = G(1)$  and  $G(p) = G(0) = F(0)$ , giving the result.

Taking  $n$  to be the least positive residue of  $m \pmod{p}$  in Lemma 1 gives

**Theorem 1.** *For any given prime  $p$  and integer  $m$ , the equation (1) together with the value of  $F(0)$  completely (and uniquely) characterize a function  $F: \mathbf{Z}/p\mathbf{Z} \rightarrow \mathbf{Z}/p\mathbf{Z}$ .*

We now move on to the more interesting (and difficult)

**Theorem 2.** *Suppose that prime  $p$  and integers  $m$  and  $q$  are given, where  $1 \leq m \leq p-1$  and  $q$  is a primitive root  $\pmod{p}$ . For any function  $F: \mathbf{Z}/p\mathbf{Z} \rightarrow \mathbf{Z}/p\mathbf{Z}$  we have that (2) is satisfied for every  $x \in \mathbf{Z}/p\mathbf{Z}$  if and only if*

- (a)  $F(x) = (F(2) - F(1))B_m(x)/m$  for  $m \leq p-2$ ;  
 (b)  $F(x) = (F(2) - F(1))C_{p-1}(x) + F(0)$  for  $m = p-1$ ,

where

$$(F(2) - F(1)) \frac{q^{p-1} - 1}{p} = 0.$$

*Proof.* Let  $G(x) = F(x+1) - F(x)$  so that, by taking the difference of the equations for  $qx+1$  and  $qx$  in (2) we get

$$(3) \quad G(qx) = q^{m-1}G(x) \quad \text{for each } x \in \mathbf{Z}/p\mathbf{Z}.$$

Therefore  $G(x) = vx^{m-1}$  by (3), where  $v = G(1)$ , as  $q$  is a primitive root  $\pmod{p}$ . By Lemma 1 this gives  $F(x) = vC_m(x) + F(0)$ . When we substitute this back into (2) we find that

$$(4) \quad (q^m - 1) \left( F(0) - \frac{v}{m} B_m \right) = 0.$$

(a) If  $1 \leq m \leq p-2$  then  $p-1$  does not divide  $m$  and so, as  $q$  is a primitive root,  $(q^m - 1) \neq 0$ . Therefore  $F(0) = (v/m)B_m$  and so we get  $F(x) = vB_m(x)/m$ .

(b) If  $m = p-1$  then, as  $F(0) \in \mathbf{Z}/p\mathbf{Z}$ , we have  $(q^m - 1)F(0) = 0$ ; thus, as  $pB_{p-1} \equiv p-1 \pmod{p}$  (by the Von Staudt–Clausen theorem), we get from (4) that  $v(q^{p-1} - 1)/p = 0$ .

A number of corollaries follow.

**Corollary 1.** *Suppose that prime  $p$  and integers  $m$  and  $q$  are given, where  $1 \leq m \leq p - 1$  and  $q$  is a primitive root (mod  $p$ ). Then the equation (2), together with the value of  $F(0)$ , completely (and uniquely) characterize the function  $F: \mathbf{Z}/p\mathbf{Z} \rightarrow \mathbf{Z}/p\mathbf{Z}$  if and only if  $(q^m - 1)B_m \not\equiv 0 \pmod{p}$ .*

*Proof.* In order for  $F(x)$  to be completely characterized we see, from Theorem 2, that we must be able to compute the value of  $F(2) - F(1)$  from the given information.

In (a) this occurs only when  $B_m(0)/m \not\equiv 0 \pmod{p}$  (in which case  $F(x) = F(0)B_m(x)/B_m$ ), which is equivalent to  $(q^m - 1)B_m \not\equiv 0 \pmod{p}$ , as  $(q^m - 1) \not\equiv 0 \pmod{p}$  and  $B_m = B_m(0)$ .

In (b), as  $C_{p-1}(0) = 0$ , the value of  $F(2) - F(1)$  can be computed only if  $(q^{p-1} - 1)/p \not\equiv 0 \pmod{p}$  (in which case  $F(x) = F(0)$ ) which is equivalent to  $(q^{p-1} - 1)B_{p-1} \not\equiv 0 \pmod{p}$  by the Von Staudt–Clausen theorem.

A prime  $p$  is defined to be *regular* if  $p$  does not divide the class number of the cyclotomic field  $K = \mathbf{Q}(\xi_p)$ , which means that for any ideal class  $\mathfrak{J}$  of  $K$ , there exists an ideal class  $\mathfrak{D}$ , for which  $\mathfrak{D}^p = \mathfrak{J}$ . Kummer showed, as a consequence of this, that Fermat's last theorem is true for any regular prime exponent  $p$ . He also proved that  $p$  is regular if and only if  $p$  does not divide any of the Bernoulli numbers  $B_m$  for  $m$  even with  $1 \leq m \leq p - 3$ . We give here an equivalent set of criteria to regularity:

**Corollary 2.** *A given prime  $p$  is regular if and only if for a given primitive root  $q \pmod{p}$ , equation (2) (for each  $x \in \mathbf{Z}/p\mathbf{Z}$ ) together with the value of  $F(0)$  completely and uniquely characterize the function  $F: \mathbf{Z}/p\mathbf{Z} \rightarrow \mathbf{Z}/p\mathbf{Z}$  for each even positive integer  $m$ , less than  $p - 2$ .*

It should be noted that  $B_m = 0$  for any odd integer  $m > 1$ , and so one can deduce from Corollary 1:

**Corollary 3.** *Suppose that prime  $p$  and integers  $m$  and  $q$  are given, where  $3 \leq m \leq p - 2$ ,  $m$  is odd and  $q$  is a primitive root (mod  $p$ ). Then the equation (2), together with the value of  $F(0)$ , is satisfied by more than one function  $F: \mathbf{Z}/p\mathbf{Z} \rightarrow \mathbf{Z}/p\mathbf{Z}$ .*

It is also important in number theory to study those values of  $q$  for which  $p$  divides the "Fermat quotient"  $(q^{p-1} - 1)/p$ . Theorem 2 gives a new insight into that question:

**Corollary 4.** *Suppose that prime  $p$  and integer  $q$  are given, where  $q$  is a primitive root (mod  $p$ ). There exists a nonconstant function  $F: \mathbf{Z}/p\mathbf{Z} \rightarrow \mathbf{Z}/p\mathbf{Z}$  that satisfies*

$$F(x) = \frac{1}{q} \left[ F\left(\frac{x}{q}\right) + F\left(\frac{x+1}{q}\right) + \cdots + F\left(\frac{x+q-1}{q}\right) \right]$$

*if and only if  $p^2$  divides  $q^{p-1} - 1$ .*

Another interesting question is to consider (2) in the case that  $q$  is not a primitive root (mod  $p$ ).

**Theorem 3.** Suppose that prime  $p$ , and integers  $m$ ,  $q$ , and  $k$  are given, where  $1 \leq m \leq p-1$ ,  $k$  divides  $p-1$  and  $q$  is of order  $(p-1)/k$  (mod  $p$ ). Suppose that the multiplicative subgroup of  $\mathbf{Z}/p\mathbf{Z} \setminus \{0\}$ , generated by  $q$ , has cosets  $A_1, A_2, \dots, A_k$ . For any function  $F: \mathbf{Z}/p\mathbf{Z} \rightarrow \mathbf{Z}/p\mathbf{Z}$  we have that (2) is satisfied for every  $x \in \mathbf{Z}/p\mathbf{Z}$  if and only if there exist  $v_1, v_2, \dots, v_k \in \mathbf{Z}/p\mathbf{Z}$  such that

$$(5) \quad F(x) = F(1) + \sum_{i=1}^k v_i \sum_{\substack{1 \leq y \leq x-1 \\ y \in A_i}} y^{m-1} \quad \text{for } 1 \leq x \leq p$$

and

$$(6) \quad q(q^{-m} - 1)F(1) = \sum_{i=1}^k v_i \sum_{\substack{1 \leq y \leq p-1 \\ y \in A_i}} y^{m-1} \left[ \frac{qy}{p} \right].$$

*Remark.* These formulae are, of course, natural generalizations of the famous formulae of Voronoi [4]: i.e. Take each  $v_i = m$  to get

$$q(q^{-m} - 1)B_m \equiv m \sum_{1 \leq y \leq p-1} y^{m-1} \left[ \frac{qy}{p} \right] \pmod{p}.$$

*Proof.* As in the proof of Theorem 2, we see that (3) holds where  $G(x) = F(x+1) - F(x)$ . Therefore, if  $x \in A_i$  then  $G(x) = x^{m-1}v_i$ , for some fixed  $v_i \in \mathbf{Z}/p\mathbf{Z}$ , giving (5). Substituting (5) into (2) for  $x = 0$  gives (6), and it is easily verified that if (5) and (6) are satisfied then so is (2).

#### REFERENCES

1. T. Clausen, *Lehrsatz aus einer Abhandlung über die Bernoullischen Zahlen*, *Astronom. Nachr.* **17** (1840), 351–352.
2. L. J. Dickey, H.-H. Kairies and H. S. Shank, *Analogs of Bernoulli polynomials in fields  $\mathbf{Z}_p$* , *Aequationes Math.* **14** (1976), 401–404.
3. K. G. C. Von Staudt, *Beweis eines Lehrsatzes, die Bernoullischen Zahlen betreffend*, *J. Reine Angew. Math.* **21** (1840), 372–376.
4. G. F. Voronoi, *On Bernoulli numbers*, *Collected works I*, 1952, pp. 7–23.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF TORONTO, TORONTO, ONTARIO M5S 1A1  
CANADA

DEPARTMENT OF MATHEMATICS AND STATISTICS, QUEENS UNIVERSITY, KINGSTON, ONTARIO  
K7L 3N6 CANADA