COLLOQUIUM MATHEMATICUM

VOL. 93 2002 NO. 1

ON mTH ORDER BERNOULLI POLYNOMIALS OF DEGREE m THAT ARE EISENSTEIN

BY

ARNOLD ADELBERG (Grinnell, IA) and MICHAEL FILASETA (Columbia, SC)

Abstract. This paper deals with the irreducibility of the mth order Bernoulli polynomials of degree m. As m tends to infinity, Eisenstein's criterion is shown to imply irreducibility for asymptotically $> 1/5$ of these polynomials.

1. Introduction. The higher order Bernoulli polynomials $B_m^l(x)$ are defined by

$$\left(\frac{t}{e^t-1}\right)^l e^{tx} = \sum_{m=0}^{\infty} B_m^{(l)}(x)\frac{t^m}{m!}.$$

The polynomial $B_m^{(l)}(x)$ is of degree m and l is its order. This paper is concerned with an estimate for the number of polynomials $B_m^{(m)}(x)$ (i.e. the case when $l = m$ above) that satisfy Eisenstein's criterion. More precisely, for t large, we seek to determine a lower bound for the number of positive integers $m \le t$ for which there is a prime p (depending on m) such that p divides neither the numerator nor the denominator of the leading coefficient of $B_m^{(m)}(x)$, p divides the numerator but not the denominator of each of the other coefficients, and p^2 does not divide the numerator of the constant term. (Here we are viewing the coefficients as reduced fractions.) Eisenstein's criterion would imply that all such polynomials are irreducible over the rationals. Even though irreducibility is not an uncommon phenomenon among all polynomials with rational coefficients, polynomials satisfying Eisenstein's criterion are rare. We show that nevertheless a positive proportion of the polynomials $B_m^{(m)}(x)$ satisfy Eisenstein's criterion. Specifically, we establish

THEOREM 1. *Asymptotically more than one-fifth of the polynomials $B_m^{(m)}(x)$ are irreducible* (*and in fact Eisenstein*). *More precisely*,

$$\liminf_{t\to\infty} \frac{|\{m \le t : B_m^{(m)}(x) \textit{ Eisenstein}\}|}{t} > \frac{1}{5}.$$

2000 *Mathematics Subject Classification*: Primary 11B68; Secondary 11R09, 12E05.

The second author gratefully acknowledges support from the National Security Agency.

One can show that $x - m/2$ is a factor of $B_m^{(m)}(x)$ when m is odd; in particular, the number $1/5$ cannot be replaced by $1/2$ above. The first author [2] has conjectured that $B_m^{(m)}(x)$ is irreducible if m is even and is $x - m/2$ times an irreducible polynomial if m is odd.

Our demonstration of the above result in the next section is fairly simple. We refer to $B_m = B_m^{(1)}(0)$ as the mth Bernoulli number. For p a prime and m a nonnegative integer, define $\sigma = \sigma(p, m)$ as the unique nonnegative integer $< p - 1$ satisfying $m \equiv \sigma \pmod{p-1}$. We make use of the following result by the first author [1].

THEOREM 2. *Let p be a prime, and let l and m be positive integers with $m < p^2$, $\sigma > 1$ and $p \,\|\, l$. Suppose further that the sum of the base p digits of m is equal to σ. If m is even and*

$$B_\sigma \not\equiv 0 \pmod{p}, \tag{1}$$

then $B_m^{(l)}(x)$ satisfies Eisenstein's criterion (with prime p).

For our purposes, we consider p large and take $l = m = 2kp$ for some positive integer k satisfying $2k < p - 1$. One checks that $\sigma = 2k$ and the conditions of Theorem 2 are each satisfied except possibly (1). We use the classical von Staudt–Clausen theorem and a formula for the Bernoulli numbers in terms of the Riemann zeta-function $\zeta(s)$ to obtain an upper bound on the number of pairs (k, p) with $2kp \le t$, $2k < p-1$, and condition (1) not holding. It is well known (and we demonstrate) that a positive proportion of numbers $m \le t$ can be written in the form $m = 2kp$ with $2k < p - 1$. Combining these estimates will be sufficient to give us Theorem 1 above.

2. Details of the proof. We make use of the following two classical results.

THEOREM 3. *The Bernoulli number B_n is given explicitly by the following:*

- $B_1 = -1/2$ *and* $B_0 = 1$.
- $B_n = 0$ *if* $n = 2m + 1$ *for* $m > 0$.
- $B_n = (-1)^{m-1} \dfrac{2(2m)!}{(2\pi)^{2m}} \zeta(2m)$ *if* $n = 2m > 0$.

THEOREM 4 (the von Staudt–Clausen theorem). *Let B_m be the mth Bernoulli number with m an even integer >0, and let $B_m = N_m/D_m$ where N_m and D_m are relatively prime integers with $D_m > 0$.*

(i) *If p is a prime such that $(p-1) \mid m$, then $p \,\|\, D_m$ and $pB_m \equiv -1 \pmod{p}$.*

(ii) *If p is a prime such that $(p-1) \nmid m$, then $p \nmid D_m$.*

These results can be found in, for example, [3] and [4].

We will make use of the notation $B_m = N_m/D_m$ above as well as the notation given at the end of the Introduction. Observe that $2k < p-1$ implies from (ii) that $p \nmid D_{2k}$. Since $\sigma = 2k$, we are assured that the expression on the left of (1) is defined modulo p. This condition, in our case, can therefore be replaced by $p \nmid N_{2k}$.

Now we will formulate some lemmas, in order to examine those p such that $p \nmid N_{2k}$ and obtain an estimate on how many $B_m^{(m)}(x)$ satisfy Eisenstein's criterion (using this same prime p).

Lemma 1. *The number* $2(2^{2k}-1)B_{2k}$ *is an integer.*

Proof. Let q denote a prime. By Theorem 4, we have $q|D_{2k}$ if and only if $(q-1) \mid (2k)$. Also, $q \mid D_{2k}$ implies $q \parallel D_{2k}$. We need only show that if $(q-1) \mid (2k)$, then $q \mid (2(2^{2k}-1))$. Let q be a prime with $q-1$ dividing $2k$. If $q = 2$, then clearly $q \mid (2(2^{2k}-1))$. If $q \neq 2$, then Fermat's Little Theorem implies that q divides $2^{2k}-1$ as $(q-1) \mid (2k)$. Thus, $q \mid (2(2^{2k}-1))$. ∎

Lemma 2. *For each positive integer* k, $|N_{2k}| < (2k)^{2k}$.

Proof. First, by Theorem 3, we have

$$|B_{2k}| = \frac{2(2k)!}{(2\pi)^{2k}}\,\zeta(2k).$$

Observe that

$$\zeta(2k) = \sum_{n=1}^{\infty} \frac{1}{n^{2k}} \le \zeta(2) = \frac{\pi^2}{6} < 2.$$

Thus,

$$\begin{aligned}|B_{2k}| &= \frac{2(2k)!}{(2\pi)^{2k}}\,\zeta(2k) < \frac{4(2k)!}{(2\pi)^{2k}} = \frac{4(2k)!}{2^{2k}\cdot\pi^{2k}} \\ &\le \frac{4(2k)!}{2^{2k}\cdot\pi^{2}} < \frac{4(2k)!}{8\cdot 2^{2k}} < \frac{(2k)!}{2\cdot 2^{2k}}.\end{aligned}$$

From Lemma 1, we obtain

$$|N_{2k}| \le 2(2^{2k}-1)|B_{2k}| < \frac{2(2^{2k}-1)}{2\cdot 2^{2k}}(2k)! < (2k)! < (2k)^{2k}. \ ∎$$

We now use Theorem 2 to find a lower bound on the number of $m \le t$ for which $B_m^{(m)}(x)$ is Eisenstein. We view t as being sufficiently large. Fix $\varepsilon \in (0, 1/3)$. Set $\theta = 2/3 + \varepsilon$. Consider a positive integer k for which $2k < t^{1-\theta}$. Let $\mathcal{P}_{2k}$ denote the set of primes p dividing N_{2k} such that

$$t^{\theta} < p \le \frac{t}{2k}. \tag{2}$$

From Lemma 2, we obtain

$$(t^\theta)^{|\mathcal{P}_{2k}|} \le \prod_{p\in\mathcal{P}_{2k}} p \le |N_{2k}| \le (2k)^{2k} \le t^{(1-\theta)t^{1-\theta}}.$$

Taking logarithms of both sides we get

$$(\theta|\mathcal{P}_{2k}|)\log t \le (1-\theta)t^{1-\theta}\log t,$$

and so

$$|\mathcal{P}_{2k}| \le \frac{1-\theta}{\theta}\,t^{1-\theta} < t^{1-\theta}.$$

Let

$$\mathcal{P} = \bigcup_{k\le t^{1-\theta}/2} \mathcal{P}_{2k}.$$

Then $\mathcal{P}$ has the following properties:

(A) If $p\notin\mathcal{P}$ and (2) holds, then $p \nmid N_{2k}$.
(B) $|\mathcal{P}| \le \sum_{k\le t^{1-\theta}/2}|\mathcal{P}_{2k}| \le t^{2-2\theta}$.

We consider the $m\le t$ of the form $2kp$ with $p>t^\theta$. Since $\theta>2/3$ and $p\,|\,m$, there is exactly one such p corresponding to a given m. Also, $2kp\le t$ and $p>t^\theta$ implies $p\le t/(2k)$ and $2k\le t^{1-\theta}<t^{1/3}-1<p-1$. In particular, (2) holds. Also, from (A) and Theorem 4, if $p\notin\mathcal{P}$, then $B_m^{(m)}(x)$ is Eisenstein. Again noting the uniqueness of p for a given m, we deduce that the number of $m\le t$ for which $B_m^{(m)}(x)$ is Eisenstein is at least

$$\sum_{\substack{m\le t\\ m\,\text{even}}}\ \sum_{\substack{p|m\\ p>t^\theta\\ p\notin\mathcal{P}}} 1 = \sum_{\substack{t^\theta<p\le t\\ p\notin\mathcal{P}}}\ \sum_{\substack{m\le t\\ (2p)|m}} 1.$$

Define $\mathcal{E}_p$ by

$$\left[\frac{t}{2p}\right] = \frac{t}{2p} + \mathcal{E}_p.$$

Hence, $-1<\mathcal{E}_p\le 0$. Making use of this notation, we obtain

$$\sum_{\substack{t^\theta<p\le t\\ p\notin\mathcal{P}}}\ \sum_{\substack{m\le t\\ (2p)|m}} 1 = \sum_{\substack{t^\theta<p\le t\\ p\notin\mathcal{P}}}\left[\frac{t}{2p}\right] = \sum_{\substack{t^\theta<p\le t\\ p\notin\mathcal{P}}}\left(\frac{t}{2p}+\mathcal{E}_p\right).$$

Observe that

$$\sum_{\substack{t^\theta<p\le t\\ p\notin\mathcal{P}}} |\mathcal{E}_p| \le \sum_{p\le t} 1 \ll \frac{t}{\log t}.$$

Also,

$$\sum_{\substack{t^\theta<p\le t\\ p\in\mathcal{P}}} \frac{t}{2p} \le \frac{1}{2}\,t^{1-\theta}|\mathcal{P}|,$$

the latter being an upper bound on the number of terms times an upper bound on the size of a term. From (B), we deduce

$$\sum_{\substack{t^\theta<p\le t\\ p\in\mathcal{P}}} \frac{t}{2p} < t^{3-3\theta} = t^{1-3\varepsilon}.$$

Using the asymptotic formula

$$\sum_{p\le z} \frac{1}{p} = \log\log z + C + O(1/\log z),$$

we obtain

$$\begin{aligned}\sum_{t^\theta<p\le t} \frac{t}{2p} &= \frac{t}{2}(\log\log t - \log\log t^\theta + O(1/\log t))\\ &= \frac{\log(1/\theta)}{2}t + O(t/\log t).\end{aligned}$$

Using the fact that

$$\sum_{\substack{t^\theta<p\le t\\ p\notin\mathcal{P}}} \left(\frac{t}{2p} + \mathcal{E}_p\right) = \sum_{t^\theta<p\le t} \frac{t}{2p} - \sum_{\substack{t^\theta<p\le t\\ p\in\mathcal{P}}} \frac{t}{2p} + \sum_{\substack{t^\theta<p\le t\\ p\notin\mathcal{P}}} \mathcal{E}_p,$$

we conclude that the number of $m \le t$ for which $B_m^{(m)}(x)$ is Eisenstein is at least

$$\frac{\log(1/\theta)}{2}\,t + O(t^{1-3\varepsilon}) + O(t/\log t).$$

The first term dominates the above for any $\varepsilon > 0$. By allowing ε to approach 0 and noting

$$\frac{\log(3/2)}{2} = 0.2027\ldots,$$

we deduce that, for t sufficiently large, more than one-fifth of the integers $m \le t$ are such that $B_m^{(m)}(x)$ is Eisenstein. Hence, Theorem 1 is established.

REFERENCES

[1] A. Adelberg, *Congruence of p-adic integer order Bernoulli numbers*, J. Number Theory 59 (1996), 374–388.

[2] —, *Higher order Bernoulli polynomials and Newton polygons*, in: Proc. 7th Internat. Research Conf. on Fibonacci Numbers and their Applications, held at the Technische

Universität Graz, G. E. Bergum, A. N. Philippou and A. F. Horadam (eds.), Kluwer, Dordrecht, 1998, 1–8.

[3] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, New York, 1966.

[4] H. M. Edwards, *Fermat's Last Theorem*: *A Genetic Introduction to Algebraic Number Theory*, Springer, New York, 1977.

Department of Mathematics
Grinnell College
Grinnell, IA 50112, U.S.A.
E-mail: adelbe@math.grinnell.edu

Mathematics Department
University of South Carolina
Columbia, SC 29208, U.S.A.
E-mail: filaseta@math.sc.edu

Received 3 August 2001 (4097)