Canad. Math. Bull. Vol. **27** (2), 1984

A NOTE ON BERNOULLI–GOSS POLYNOMIALS

BY
K. IRELAND AND D. SMALL

ABSTRACT. In an important series of papers ([3], [4], [5]), (see also Rosen and Galovich [1], [2]), D. Goss has developed the arithmetic of cyclotomic function fields. In particular, he has introduced Bernoulli polynomials and proved a non-existence theorem for an analogue to Fermat's equation for regular "exponent". For each odd prime p and integer n, $1 \leq n \leq p^2-2$ we derive a closed form for the nth Bernoulli polynomial. Using this result a computer search for regular quadratic polynomials of the form x^2-a was made. For primes less than or equal to 269 regular quadratics exist for $p = 3, 5, 7, 13, 31$.

1. **Preliminary definitions and results (see Goss [5]).** Let p be a prime number and consider the polynomial ring $\mathbb{F}_P[T]$ with coefficients in the finite field $\mathbb{F}_p$ of p elements. If we denote by M_j the set of monic polynomials in $\mathbb{F}_P[T]$ of degree j define polynomials $s_j(n)$ by

$$s_j(n) = \sum_{\alpha \in M_j} \alpha^n. \tag{1}$$

For completeness we have included the proofs of several elementary lemmas. (See Goss [3], [5], [6].)

LEMMA 1. *$s_j(n) = 0$ if $(p-1)j > n$.*

Proof. We may write

$$s_j(n) = \sum (a_0 + a_1 T + \cdots + a_{j-1} T^{j-1} + T^j)^n$$

where $a_0, a_1, \ldots, a_{j-1}$ range independently over $\mathbb{F}_p$. A typical term of the product is of the form

$$\binom{n}{i_0}\binom{n}{i_1} \cdots \binom{n}{i_j} a_0^{i_0} a_1^{i_1} \cdots a_{j-1}^{i_{j-1}} T^{i_0 + i_1 + \cdots + i_j}$$

with $i_0 + i_1 + \cdots + i_j = n$. If $(p-1)(j+1) > n$ then there exists an s, $0 \leq s \leq j$ such that $p-1$ does not divide i_s. But then the cyclicity of the multiplicative group of $\mathbb{F}_p$ shows that $\sum_{a_s} a_s^{i_s} = 0$ and the results follows.

According to the above lemma one may then consider the sum of the nth

Received by the editors February 1, 1983 and in revised form March 29, 1983.
The 1980 Mathematical Subject Classification Number is 12C15.

powers of the monics in $\mathbb{F}_p[T]$. More generally we make the following definition.

DEFINITION. Let $n \in \mathbb{Z}$, $n \geq 0$. Put $\beta(0) = 0$ and for $n \in \mathbb{N}^+$ put

$$\beta(n) = \begin{cases} \sum_{j=0}^{\infty} s_j(n), & p-1 \nmid n \\ -\sum_{j=1}^{\infty} j s_j(n), & p-1 \mid n \end{cases}$$

We will refer to the $\beta(n)$ as Bernoulli–Goss polynomials. Note also that $s_0(n) = 1$ for all $n \geq 0$ since there is only one monic polynomial of degree 0, namely 1. Thus, if p is odd $\beta(1) = s_0(1) + s_1(1) + \cdots = 1 + 0 + 0 + \cdots = 1$.

The following lemma shows that the Bernoulli–Goss polynomials may be defined recursively (see Goss [5]).

LEMMA 2. *If* $n \geq 1$

$$\beta(n) = 1 - \sum_{\substack{p-1 \mid n-j \\ j=1}}^{n-1} \binom{n}{j} T^j \beta(j)$$

Proof. Consider first the quantities $s_j(n)$. If $j \geq 1$ we have

$$\begin{aligned} s_j(n) &= \sum_{f \in M_j} F^n \\ &= \sum_{\substack{g \in M_{j-1} \\ \alpha \in \mathbb{F}_p}} (\alpha + Tg)^n \\ &= \sum_{\substack{s=0 \\ \alpha \in \mathbb{F}_p \\ g \in M_{j-1}}}^{n} \alpha^{n-s} \binom{n}{s} T^s g^s \end{aligned}$$

For $s = n$ summing on α gives 0. If $p-1$ divides $n-s$ summing on α gives -1 while if $p-1$ does not divide $n-s$ the sum is 0. Thus

$$s_j(n) = -\sum_{\substack{p-1 \mid n-s \\ s=0}}^{n-1} \binom{n}{s} T^s s_{j-1}(s), \qquad j \geq 1 \tag{2}$$

Consider now the formal power series in $1/x$ with coefficients in $\mathbb{F}_P[T]$

$$\begin{aligned} F_n(T, x) &= \sum_{j=0}^{\infty} s_j(n) x^{-j} \\ &= 1 + \sum_{j=1}^{\infty} s_j(n) x^{-j} \\ &= 1 - \sum_{\substack{j=1 \\ p-1 \mid n-s \\ 0 \leq s \leq n-1}}^{\infty} \binom{n}{s} T^s s_{j-1}(s) x^{-j+1} x^{-1} \end{aligned}$$

https://doi.org/10.4153/CMB-1984-027-1 Published online by Cambridge University Press

the last inequality resulting from Lemma 2. However, this gives, by definition of $F_n(T, x)$

$$F_n(T, x) = 1 - \sum_{\substack{p-1 \mid n-s \\ 0 \le s \le n-1}} \binom{n}{s} T^s F_s(T, x) x^{-1} \tag{3}$$

If $p-1 \mid n$ put $x = 1$ to obtain the result. Suppose then that $p-1 \mid n$. If $n = 0$ then $F_n(T, 1) = 1$. Since $p-1 \mid s$ it follows by induction, using (3), that $F_n(T, 1) = 0$ if $p-1 \mid n$, $n > 0$. Now formally differentiate (3) with respect to x to obtain

$$F_n'(T, x) = \sum_{\substack{p-1 \mid n-s \\ 0 \le s \le n}} \binom{n}{s} T^s F_s(T, x) x^{-2} - x^{-1} \sum_{\substack{p-1 \mid n-s \\ s \le n-1}} \binom{n}{s} T^s F_s'(T, x) \tag{4}$$

Putting $x = 1$ the above comments show that the first term on the right hand side of (4) is 1 and the result follows by noting that $F_s'(T, 1) = \beta(s)$, if $p-1 \mid s$.

If n is a positive integer write the p-adic expansion of n as $n = a_0 + a_1 p + \cdots + a_l p^l$, $0 \le a_i < p$. The following important result is due to *E.* Thomas (Thomas [7]).

LEMMA 3. *$\beta(n) = 1$ if and only if $a_0 + a_1 + \cdots + a_l \le p-1$.*

2. **A closed expression for two digit Bernoulli Goss polynomials.** The Bernoulli–Goss polynomials are related to the arithmetic of cyclotomic function fields in a manner analogous to the relation between classical Bernoulli numbers and class numbers of cyclotomic number fields. For this reason, it is important to obtain closed expressions for these polynomials.

First we prove the following useful lemma due to Lucas.

LEMMA 4. *If $n = \sum_{i=0}^{s} a_i p^i$, $m = \sum_{i=0}^{t} b_i p^i$ then*

$$\binom{n}{m} \equiv \prod_{i=0}^{\infty} \binom{a_i}{b_i} \bmod p$$

where we make the conventions

$$\binom{a}{b} = 0$$

if $a < b$ $b > 0$,

$$\binom{a}{0} = 1.$$

Proof. Consider the congruence $(1+x)^n \equiv \prod_i (1+x^{p^i})^{a_i} \bmod p$ and equate coefficients of x^m. The result follows by uniqueness of the p-adic expansion of m.

https://doi.org/10.4153/CMB-1984-027-1 Published online by Cambridge University Press

LEMMA 5.

$$\binom{p-a}{p-b} \equiv \binom{b-1}{a-1}(-1)^{b-a} \bmod p$$

for positive integers a, b.

Proof. Using

$$\binom{n}{m} = \frac{n!}{m!\,(n-m)!}$$

one sees that the result is equivalent to

$$(-1)^a (p-a)!\,(a-1)! \equiv (-1)^b (p-b)!\,(b-1)! \bmod p.$$

However, each side is easily seen to be congruent to $-(p-1)!$ This completes the proof.

Consider now $\beta(N)$ and write $N = q + n(p-1)$ where $n \geq 0$ and $1 \leq q \leq p-1$. By Lemma 2 we may write

$$\beta(q+n(p-1)) = 1 - \sum_{m=1}^{n} \binom{n(p-1)+q}{m(p-1)} T^{(n-m)(p-1)+q} \beta((n-m)(p-1)+q) \tag{5}$$

Assume now that N has a two digit p-adic expansion $N = s + rp$. If $s + r < p$ then Lemma 3 shows that $\beta(N) = 1$. We assume then that $s + r \geq p$ so that $n = r+1$ and $q = 1 + \rho$ with $\rho = s + r - p$. Write

$$m(p-1) = (m-1)p + p - m, \qquad 1 \leq m \leq r+1.$$

Substituting this into (5) and using Lemma 4 and Lemma 3 we obtain

$$\begin{aligned} \beta(s+rp) &= 1 - \sum_{m=1}^{r+1} \binom{r}{m-1}\binom{p-r+\rho}{p-m} T^{(r-m+1)p+m-r+\rho} \\ &= 1 - \sum_{m=p-s}^{r+1} \binom{r}{m-1}\binom{p-r+\rho}{p-m} T^{(r-m+1)p+m-r+\rho} \end{aligned}$$

Substituting $j = m - r + \rho$ and eliminating m gives, using Lemma 5,

$$\beta(s+rp) = 1 - \sum_{j=0}^{\rho+1} \binom{r}{r+j-\rho-1}\binom{r+j-\rho-1}{r-\rho-1} T^{(\rho-j+1)p}(-)^j T^j$$

Using the binomial theorem this is easily seen to reduce to

$$\beta(s+rp) = 1 - \binom{r}{\rho+1}(T^p - T)^{\rho+1}$$

https://doi.org/10.4153/CMB-1984-027-1 Published online by Cambridge University Press

Thus we have proven the following result:

THEOREM. *Let* $N = s + rp$, $s + r \geq p$, $0 \leq s$, $r < p$. *Define* $\rho = r + s - p$. *Then*

$$\beta(s + rp) = 1 - \binom{r}{\rho + 1}(T^p - T)^{\rho+1}.$$

Special cases of this result have also been obtained by E. Thomas [7]. Also note that

$$\binom{r}{\rho + 1} = \binom{n-1}{q}$$

3. **Computer search for regular quadratic polynomials.** Let p be an odd prime. A monic irreducible polynomial of degree d is said to be regular if $P(T)$ does not divide $\beta(n)$ for $1 \leq n \leq p^d - 2$. In [3] Goss has introduced an analogue to the Fermat equation for cyclotomic function fields and established a Kummer criterion. Namely, if $P(T)$ is regular then the Fermat–Goss equation has no nontrivial solutions in $\mathbb{F}_p[T]$. In the case $d = 2$, the theorem of section 2 allows one to reduce the question of regularity to a set of numerical congruences modulo p. Namely, if $P(T) = T^2 - a$ is irreducible then $P(T)$ divides $\beta(s + rp)$ if and only if

$$1 \equiv \binom{r}{\rho + 1}(T^p - T)^{\rho+1} \bmod T^2 - a.$$

Writing $T^{p-1} = (T^2)^{(p-1)/2}$ and noting that $a^{(p-1)/2} \equiv -1 \bmod p$ the condition is immediately seen to be equivalent to

$$-2a(\rho + 1)/2\binom{r}{\rho + 1} \equiv 1 \bmod p$$

where $\rho + 1$ is even. If $\rho + 1$ is odd, then $T^2 - a$ does not divide $\beta(s + rp)$. A computer search was developed for regular quadratic irreducibles. The results show that for $3 \leq p \leq 269$ regular quadratic irreducibles exist only for $p = 3, 5, 7, 13, 31$. More precisely the regular quadratic polynomials are as follows:

$$\begin{aligned} p &= 3, T^2 + 1 \\ p &= 5, T^2 + 3 \\ p &= 7, T^2 + 1 \\ p &= 13, T^2 + 5 \\ p &= 31, T^2 + 5, T^2 + 25 \end{aligned}$$

This research was supported by the Natural Sciences and Engineering Council of Canada, Grant A8785 and by the University of New Brunswick Research Fund.

Bibliography

1. S. Galovich and M. Rosen, *The Class Number of Cyclotomic Function Fields*, Journal of Number Theory, Vol. 13, No. 3, August 1981, 363–375.

2. S. Galovich and M. Rosen, *Unit and Class Groups in Cyclotomic Function Fields*, Journal of Number Theory, Vol. 14, No. 2, 1982.

3. D. Goss, *On a Fermat Equation Arising in the Arithmetic Theory of Function Fields*, Math. Ann. **261,** 269–286 (1982).

4. D. Goss, *v-adic Zeta Functions, L-series and Measures for Function Fields*, Inven. Math. **55,** 107–116 (1979), pp. 107–119.

5. D. Goss, *The Arithmetic of Function Fields* 2: *The Cyclotomic Theory*, Journal of Algebra, **81,** (1), 1983, 107–149.

6. D. Goss, *On a New Type of L-function for Algebraic Curves Over Finite Fields*, Pacific Journal of Math.

7. E. Thomas, *On the Zeta Function for Function Fields Over* $\mathbb{F}_p$, Pacific Journal of Math., **107,** (1), 1983, 251–256.

Department of Mathematics and Statistics
University of New Brunswick
P. O. Box 4400
Fredericton, New Brunswick E3B 5A3