Generalization of the Von Staudt–Clausen Theorem

I. DIBAG

Faculty of Engineering and Sciences, Bilkent University,
P.O.B. 8, Maltepe, Ankara, Turkey

Communicated by Walter Feit

Received May 2, 1988

The localization $L_S(x)$ of $\log(1 + x)$ at a set of primes $S$ is defined by taking those powers of $x$ in the logarithmic series for $\log(1 + x)$ which lie in the span of $S$. The functional inverse $L_S^{-1}(x)$ of $L_S(x)$ also localizes the functional inverse $e^x - 1$ of $\log(1 + x)$ and a generalization of the Von Staudt–Clausen theorem is proved for the even coefficients in the power series expansion for $x/L_S^{-1}(x)$. This reduces to the Von Staudt–Clausen theorem when $S$ is the set of all primes and to a weaker version of Theorem 3.9 of I. Dibag (J. Algebra 87 (1984), 332–341) when $S$ consists of a single prime.

INTRODUCTION

The Bernoulli numbers $B_n$ are defined by the power series expansion $x/e^x - 1 = 1 - \frac{1}{2}x + \sum_{n=1}^{\infty} \frac{B_n}{(2n)!} x^{2n}$. The Von Staudt–Clausen theorem asserts that $B_n = - \sum_{p \mid n} (1/p)$ (mod $Z$). Let $p$ be a prime and define $L_p(x) = \sum_{k=0}^{\infty} \left( \frac{x^p}{p!} \right)^k = x + x^2/p + x^3/p^2 + x^4/p^3 + \cdots$ and $x/L_p^{-1}(x) = \sum_{n=0}^{\infty} \left( \frac{a_n}{(n(p - 1))!} \right) x^n(p-1)$. Then [2, Theorem 3.9] states that $a_n = - (1/p)$ (mod $Z$). In this note we aim to establish a unified theorem which can accommodate both results. For this purpose we define the localization $L_S(x)$ of $\log(1 + x)$ at a set of primes $S$ by taking those powers of $x$ in the logarithmic series for $\log(1 + x)$ which lie in the span of $S$. The functional inverse $L_S^{-1}(x)$ of $L_S(x)$ also localizes the functional inverse $e^x - 1$ of $\log(1 + x)$. If $x/L_S^{-1}(x) = \sum_{n=0}^{\infty} b_n(x^n/n!)$ then the main result of this note, Theorem 1.4, states that

$$b_{2n} = - \sum_{p \mid n \atop p - 1/2n \in S} \frac{1}{p} \quad \text{(mod $Z$)}.$$ 

This reduces to the Von Staudt–Clausen theorem itself when $S$ is the set of all primes and to a slightly weaker version of [2, Theorem 3.9] when $S$ consists of a single prime.
1. GENERALIZATION OF THE VON STAUDT-CLAUSEN THEOREM

DEFINITION 1.1. For a set $S$ of primes define the span $\mathbb{Q}_S$ of $S$ by
$$\mathbb{Q}_S = \{ n \in \mathbb{Z}/n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} : p_i \in S, 1 \leq i \leq k \}.$$ 

DEFINITION 1.2. Define the localization $L_S(x)$ of $\log(1 + x)$ by $L_S(x) = \sum_{n \in \mathbb{Q}_S} ((-1)^{n-1}/n) x^n$. Note that $L_S(x)$ is just $L_p(x)$ when $S$ consists of $p$ alone.

DEFINITION 1.3. Let $f(x) = \sum_{i=0}^{\infty} a_i x^i$, $g(x) = \sum_{j=0}^{\infty} b_j x^j$ be two power series. The star-product $f(x) \ast g(x)$ of $f(x)$ and $g(x)$ is defined by $f(x) \ast g(x) = \sum_{k=0}^{\infty} c_k x^k$, where $c_k = \sum_{\substack{a+b=k \ \text{in } \mathbb{Z} \times \mathbb{Z} \ \text{such that}}} a_i b_j$.

Observation 1.4. $L_S(x) = \ast_{p \in S} L_p(x)$.

Let $\mathbb{Z}_p$ denote the subring of rationals which are $p$-integral.

Observation 1.5. If $f(x) \in \mathbb{Z}_p[[x]]$ and $a \in \mathbb{Z}_p$ then $f(x)^a \in \mathbb{Z}_p[[x]]$.

Lemma 1.6. If $f(x) \in x \mathbb{Z}_p[[x]]$ then $e^{L_p(x) \ast f(x)} \in \mathbb{Z}_p[[x]]$.

Proof. Let $f(x) = \sum_{i=1}^{\infty} a_i x^i$, $a_i \in \mathbb{Z}_p$.

$$e^{L_p(x) \ast f(x)} = \exp \left( \sum_{k=1}^{\infty} x^k \left( \sum_{i=0}^{\infty} a_i \frac{1}{i!} \right) \right)$$

$$= \exp \left( \sum_{i=1}^{\infty} a_i \left( \sum_{j=0}^{\infty} \frac{x^j}{j!} \right) \right)$$

$$= \exp \left( \sum_{i=1}^{\infty} a_i L_p(x^i) \right)$$

$$= \prod_{i=1}^{\infty} (e^{L_p(x^i)})^{a_i} \in \mathbb{Z}_p[[x]]$$

since $e^{L_p(x^i)} \in \mathbb{Z}_p[[x]]$ by [3, Proposition 1] and $(e^{L_p(x^i)})^{a_i} \in \mathbb{Z}_p[[x]]$ by Observation 1.5 above.

Corollary 1.7. $e^{L_S(x)} \in \mathbb{Z}_p[[x]]$ for $p \in S$.

Proof. Let $p \in S$ and take

$$f(x) = \ast_{\substack{p' \in S \ \text{with} \ p' \neq p}} L_p(x)$$

in Lemma 1.6.
**Definition 1.8.** Define integers $A_{q,k}$ by $(e^x - 1)^k = \sum_{q \geq k} A_{q,k}(x^q/q!)$.

**Definition 1.9.** Define integers $B_{q,k}$ by $(L_S^{-1}(x))^k = \sum_{q \geq k} B_{q,k}(x^q/q!)$.

**Definition 1.10.** Define rational numbers $b_n$ by $x/L_S^{-1}(x) = \sum_{n=0}^{\infty} b_n(x^n/n!)$.

**Lemma 1.11.**

$$b_n = \sum_{k \leq n+1, k \in \mathbb{Q}_S} \frac{(-1)^{k-1}}{k} B_{n,k-1}.$$  

**Proof.**

$$\sum_{n=1}^{\infty} b_n \frac{x^n}{n!} = \frac{x}{L_S^{-1}(x)} = \frac{L_S(L_S^{-1}(x))}{L_S^{-1}(x)} = \sum_{k \in \mathbb{Q}_S} \frac{(-1)^{k-1}}{k} (L_S^{-1}(x))^{k-1}$$

$$= \sum_{n=1}^{\infty} \left( \sum_{k \geq n+1} \frac{(-1)^{k-1}}{k} B_{n,k-1} \frac{x^n}{n!} \right) = \sum_{n=1}^{\infty} \left( \sum_{k \leq n+1, k \in \mathbb{Q}_S} \frac{(-1)^{k-1}}{k} B_{n,k-1} \right) \frac{x^n}{n!}.$$  

Equating coefficients of $x^n$ yields the lemma.

Let $E(x) = e^x - 1$ and $L(x) = \log(1 + x)$. $L \circ E(x) = E \circ L(x) = x$.

**Lemma 1.12.** Let $p \in S$. Then there exist $c_r \in Z_p$ such that, $B_{n,r} = \sum_{m_1 + \ldots + m_r = r} (r!/m_1 \ldots m_r !) e_2^{m_2} \ldots e_s^{m_s} A_{n,m_1+2m_2+\ldots+sm_r}$.

**Proof.** Let $f = L_S^{-1} \circ L$ and expand $f(x) = \sum_{i=1}^{\infty} e_i x^i$, $e_1 = 1$. $f^{-1}(x) = (L_S^{-1} \circ L)^{-1}(x) = L^{-1} \circ L_S(x) = E \circ L_S(x) = e^{L_S(x)} - 1 \in Z_p[[x]]$ by Corollary 1.7. Then $f(x) \in Z_p[[x]]$ by [2, Corollary 2.7]. Hence $e_i \in Z_p$. $L_S^{-1}(x) = L_S^{-1} \circ L \circ E(x) = f(E(x)) = f(e^x - 1) = \sum_{i=1}^{\infty} e_i(x^i - 1)$. We raise both sides to the $r$th-power, i.e.,

$$\sum_{n=1}^{\infty} B_{n,r} \frac{x^n}{n!} = (L_S^{-1}(x))^r = \left( \sum_{i=1}^{\infty} e_i(e^x - 1)^i \right)^r.$$
Equating coefficients of $x^n$ yields the lemma.

**Observation 1.13.** If $k \in \mathbb{Z}$ is not a prime then $k$ divides $(k-1)!$

**Theorem 1.14.**

$$b_{2n} = \sum_{p \mid 0} \frac{1}{p^{1/2n}} \quad \text{(mod Z)}.$$  

**Proof.** (1) $b_{2n} - \sum_{k \leq 2n+1, k \in \mathbb{Q}_S} \left( \frac{(-1)^{k-1}/k}{A_{2n,k-1} - 1} \right) B_{2n,k-1}$ by Lemma 1.11.

(2) $B_{2n,k-1} = \sum_{m_1 + \ldots + m_s = k-1} \frac{(k-1)!}{m_1! \ldots m_s!} e_2^{m_1} \ldots e_s^{m_s} A_{2n,m_1+2m_2+\ldots+sm_s}$ by Lemma 1.12. Suppose $k \in \mathbb{Q}_S$ is not a prime. Then $k-1 = m_1 + m_2 + \ldots + m_s$ and thus $(k-1)!(m_1+2m_2+\ldots+sm_s)/k!(k-1)!$ by Observation 1.13 and $(m_1+2m_2+\ldots+sm_s)!/A_{2n,m_1+2m_2+\ldots+sm_s}$ by [5, Sect. 1.5, Lemma 2]. Thus $A_{2n,m_1+2m_2+\ldots+sm_s} = 0 \pmod{k}$, $e_2^{m_1} \ldots e_s^{m_s} \in \mathbb{Z}_p$ for all $p \in S$ and $k \in \mathbb{Q}_S$ and thus the denominator of $e_2^{m_1} \ldots e_s^{m_s}$ is prime to $k$.

Hence $B_{2n,k-1} = 0 \pmod{k}$ and $((-1)^{k-1}/k) B_{2n,k-1} \in \mathbb{Z}$. Suppose $k = p$ is a prime in $S$. Let $m_i \geq 1$ for some $i \geq 2$. Then $m_1 + 2m_2 + \ldots + sm_s \geq m_1 + m_2 + \ldots + m_s + (i-1) m_i \geq (p-1) + 1 = p$. Thus $p/p!(m_1+2m_2+\ldots+sm_s)!/A_{2n,m_1+2m_2+\ldots+sm_s} e_2^{m_1} \ldots e_s^{m_s} \in \mathbb{Z}_p$ and hence $((-1)!/m_1! \ldots m_s!) e_2^{m_1} \ldots e_s^{m_s} = 0 \pmod{k}$. Hence the only term in Eq. (2) that is possibly not zero mod $p$ is the one corresponding to the sequence $m_1 = p-1$ and $m_j = 0$ for $j \geq 2$ and we thus deduce from Eq. (2) that $B_{2n,p-1} = A_{2n,p-1} \pmod{p}$. If $p-1$ does not divide $2n$ then $A_{2n,p-1} = 0 \pmod{p}$ by [5, Sect. 1.5, Lemma 2]. Hence $B_{2n,p-1} = 0 \pmod{p}$ and $((-1)^{p-1}/p) B_{2n,p-1} \in \mathbb{Z}$. If $p$ is an odd prime and $(p-1)$ divides $2n$ then $A_{2n,p-1} = -1 \pmod{p}$ by [5, Sect. 1.5, Lemma 2]. Hence $B_{2n,p-1} = -1 \pmod{p}$ and $((-1)^{p-1}/p) B_{2n,p-1} = -1/p \pmod{Z}$ in Eq. (1). If $p = 2$ then $A_{2n,p-1} = A_{2n,1} = 1 = 1 \pmod{p}$ and $B_{2n,p-1} = 1 \pmod{p}$ and $((-1)^{p-1}/p) B_{2n,p-1} = -1/p \pmod{Z}$. We thus obtain from Eq. (1) that

$$b_{2n} = - \sum_{p \mid 0} \frac{1}{p^{1/2n}} \quad \text{(mod Z)}.$$
Corollary 1.15. The Von Staudt–Clausen theorem.

Proof. Take $S$ to be the set of all primes.

Corollary 1.16. Let $x/L_p^{-1}(x) = \sum_{n=0}^{\infty} b_n(x^n/n!)$. Then

\[ b_{2n} = \begin{cases} 
-1/p \pmod{Z} & \text{if } 2n = 0 \pmod{(p-1)} \\
0 \pmod{Z} & \text{if } 2n \neq 0 \pmod{(p-1)}. 
\end{cases} \]

Proof. Take $S = (p)$.

Note that Corollary 1.16 is a somewhat weaker version of [2, Theorem 3.9] which includes (i) and also states that $b_n = 0$ if $n \neq 0 \pmod{(p-1)}$.

References