A VON STAUDT-CLAUSEN THEOREM FOR CERTAIN BERNOULLIANLIKE NUMBERS AND REGULAR PRIMES OF THE FIRST AND SECOND KIND

Esayas George Kundert
University of Massachusetts, Amherst, MA 01003

(Submitted January 1988)

In a previous paper [6] we have shown that certain operators in a certain completion $\hat{A}$ of the s-d-ring A over the rational numbers determine a well-defined basis. One of the operators which we considered there was $H' = E - Q_1D$ and we called its corresponding basis $\{u_n'\}$. It was shown in that paper that

$$(u_1')^2 = \sum_{n=0}^{\infty} b_n u_n',$$

where the coefficients b_n are the Bernoulli numbers. The partial fraction decomposition of these numbers is given by the von Staudt-Clausen Theorem (see, for example, [1]):

$$b_0 = 1,\ b_1 = 1/2,\ b_{2m+1} = 0,\ b_{2m} = (-1)^m \left(\text{integer} + \sum_i 1/p_i\right),\ m \geq 1,$$

where p_i is a prime number so that $(p_i - 1) | 2m$. (Note that p_i occurs in the first power only.)

Now, let

$$(u_1')^3 = \sum_{n=0}^{\infty} c_n u_n'.$$

In this paper we will give the partial fraction decomposition for the coefficients c_n. It will turn out for certain c_n that higher powers of primes in the partial fraction denominators will occur, namely, second and third powers of 2 and at most second powers of the other primes.

Definition: We will call a prime $p > 3$ regular of the first kind if a partial fraction belonging to p^1 does occur for all $n \equiv 2m \bmod p - 1$, $n \not\equiv 2m \bmod p$, $m = 1, 2, \ldots, (p - 3)/2$.

We will call a prime $p > 3$ regular of the second kind if a partial fraction belonging to p^1 does occur for all $n \equiv 0 \bmod p - 1$, $n \not\equiv 0 \bmod p$.

It will be seen that our definition of a regular prime of the first kind is equivalent to Kummer's definition of a regular prime [5]. It is not known whether there exist an infinite number of such primes. On the other hand, it is well known that there exist infinitely many irregular primes of the first kind. Robert Gonter from the Computer Center at the University of Massachusetts was kind enough to test all primes up to about 12×10^6 for regularity of the second kind and found that 5, 13, and 563 are the only irregular ones under those primes (see [8]).

Theorem: The partial fraction decomposition of the coefficients c_n with respect to the rest system $\{0, \pm 1, \pm 2, \ldots, (p - 1)/2\}$ is as follows for $n \geq 1$:

I. Partial fractions with 2, 2^2, 2^3 in the denominator. Let

$$r_{n1} = \begin{cases} 0 & \text{for } n = 2, 6, 7, 9, 10 \\ 1 & \text{for } n = 1, 3, 4, 5, 8 \end{cases}$$

$$r_{n2} = \begin{cases} 0 & \text{for } n = 4, 6, 7, 8, 9, 10 \\ 1 & \text{for } n = 1, 2, 3, 5 \end{cases}$$

$$r_{n3} = \begin{cases} 0 & \text{for } n = 1, 2, 4, 6, 8, 10 \\ 1 & \text{for } n = 3, 5, 7, 9 \end{cases}$$

then

$$s_n = \frac{r_{n1}}{2} + \frac{r_{n2}}{2^2} + \frac{r_{n3}}{2^3}$$

occur as partial fractions of c_n for $n = 1$ through 10 and when $n' \equiv n \bmod 8$ for $n, n' \geq 3$, then $s_{n'} = s_n$ occurs in $c_{n'}$.

II. Partial fractions with 3, 3^2 in the denominator. Let

$$\rho_{n1} = \begin{cases} -1 & \text{for } n = 4, 5, 11, 12, 17 \\ 0 & \text{for } n = 1, 6, 7, 8, 10, 13, 14, 19, 20 \\ 1 & \text{for } n = 2, 3, 9, 15, 16, 18 \end{cases}$$

$$\rho_{n2} = \begin{cases} -1 & \text{for } n = 2, 4, 6, 10, 12, 16, 18 \\ 0 & \text{for } n = 1, 3, 5, 7, 8, 9, 11, 13, 14, 15, 17, 19, 20 \end{cases}$$

then

$$\sigma_n = \frac{\rho_{n1}}{3} + \frac{\rho_{n2}}{3^2}$$

occur as partial fractions of c_n for $n = 1$ through 20 and when $n' \equiv n \bmod 18$ for $n, n' \geq 3$, then $\sigma_{n'} = \sigma_n$ occurs in $c_{n'}$.

III. Partial fractions with p or p^2 ($p \geq 5$) in the denominator.

(a) If $n \equiv 1 \bmod p - 1$ and $n \not\equiv p - 2 \bmod p$, $n > 1$, let

$$\rho \equiv -1 + (n - 1)[(p - 1)/2] + n[(p - 1)/2]^2 \bmod p \text{ in } R,$$

then ρ/p occurs as a partial fraction.

(b) Let b_{2m} be the $2m^{\text{th}}$ Bernoulli number, N_{2m} the numerator, and D_{2m} the denominator of b_{2m}, $n \equiv 2m \bmod p - 1$, $m = 1, 2, \ldots, (p - 3)/2$, and $p \nmid N_{2m}$ and $n \not\equiv 2m \bmod p$, $\rho \equiv (2m)^{-1}D_{2m}^{-1}N_{2m}(n - 2m) \bmod p$ in R, then ρ/p occurs as a partial fraction.

(c) By Wilson's theorem, we may write $1 + (p - 1)! = \alpha p$. If $n \equiv 0 \bmod p - 1$, $n \not\equiv 0 \bmod p$, $\alpha \not\equiv 0 \bmod p$, let $\rho \equiv -n\alpha \bmod p$ in R, then $-1/p^2 + \rho/p$ occurs in the decomposition.

Remark 1: Let

$$2m = \prod p_i^{s_i} \prod q_j^{r_j} \quad \text{(prime factorization!)}$$

so that $(p_i - 1) \mid 2m$. Let

$$\tau = N_{2m} / \prod q_j^{r_j}$$

which is an integer, then we may also use

$$\rho \equiv \tau \prod p_i^{-(s_i+1)} (n - 2m) \bmod p \text{ in } R \text{ in III(b)}.$$

Remark 2: It can be shown that

$$1 + (p - 1)! \equiv pb_{p-1} - p + 1 \bmod p^2.$$

See [2] where this has been used to show that $1 + (p - 1)! \not\equiv 0 \bmod p^2$ for all $p < 114$ except for $p = 5$ and 13, but, as mentioned above, R. Gonter has shown, using the computer, that 563 is the only other irregular prime $< 12 \times 10^6$. See [8]. Other interpretations of α are given in [3] and [7].

Corollary 1: Let $m = 1, 2, \ldots, (p - 3)/2$, then

p is regular of the 1st kind $\Longleftrightarrow p \nmid N_{2m} \Longleftrightarrow p$ is Kummer regular.

Corollary 2: If $\alpha = [1 + (p - 1)!]/p$, then

$1 + (p - 1)! \not\equiv 0 \bmod p^2 \Longleftrightarrow \alpha \not\equiv 0 \bmod p \Longleftrightarrow p$ is regular of the 2nd kind.

Proofs: From [6], we know that

$$u_1' = \sum_{k=1}^{\infty} (1/k) x_k',$$

where $\{x_k'\}$ is the basis belonging to the operator $D' = E - D$. For this basis, the multiplication in $\hat{A}$ is especially simple, namely component-wise, so that

$$(u_1')^3 = \sum_{k=1}^{\infty} (1/k^3) x_k'.$$

Also

$$x_k' = \sum_{n=0}^{\infty} B_n^k u_n',$$

where the B_n^k are defined as follows:

$B_n^k = (-1)^{k+1} k! S_{n+1}^k$ where S_{n+1}^k is determined by the iteration

$S_{n+1}^k = S_n^{k-1} + kS_n^k$, $S_n^1 = 1$, and $S_1^k = 0$ for $k > 1$.

The reader should be warned that our definition of the B_n^k differs from the one in [6] by a factor of $(-1)^n$. If we now put

$$(u_1')^3 = \sum_{n=0}^{\infty} c_n u_n',$$

it follows that $c_0 = 1$ and

$$c_n = \sum_{k=1}^{n+1} B_n^k / k^3.$$

After this we do not have to refer to [6] anymore. In the following proofs, "~" always means "equal up to an added integer."

I. To prove the statements of the theorem in part I, we note first that powers of 2 in the prime factorization of k^3 divide into $k!$ unless $k = 2$, 4, or 8. For $k = 2$, $2!/2^3 = 1/4$; for $k = 4$, $4!/4^3 = 3/8$; for $k = 8$, $8!/8^3 \sim -1/4$. Using this and the iteration from above to calculate the reduced numerators of

B_n^k/k^3 for $k = 2, 4, 8 \bmod 4, 8, 4$, respectively, we see that they repeat periodically with increasing n with periods of length 1, 2, and 8, respectively. Computing next the partial fractions of the so reduced sums $B_n^2/2^3 + B_n^4/4^3 + B_n^8/8^3$ for $n = 1, 2, \ldots, 10$, we get the statements in part I of the theorem.

II. Similarly, one proves the the statements in part II of the theorem.

III. To prove the statements of part III, one uses the following formulas:

(1) $S_n^k = (-1)^k 1/k! \sum_{j=1}^{k} (-1)^j \binom{k}{j} j^n$ (see, for example, [4]);

(2) $S_n^k = 0$ for $n < k$ and $S_n^n = 1$ [this follows readily from (1)];

(3) $B_n^k = \sum_{j=1}^{k} (-1)^{j+1} \binom{k}{j} j^{n+1}$ [follows from (1)];

(4) Let ${}_B\Delta_{(r,s)}^k = B_{s+(r+1)(p-1)}^k - B_{s+r(p-1)}^k$, then

$$ {}_B\Delta_{(r+1,s)}^k - {}_B\Delta_{(r,s)}^k = \sum_{j=1}^{k} (-1)^{j+1} j^{s+r(p-1)} (j^{p-1} - 1)^2 \equiv 0 \bmod p^2 $$

(since, by Fermat's theorem, $j^{p-1} - 1 \equiv 0 \bmod p$). It follows that ${}_B\Delta_{(r,s)}^k$ is independent with respect to $r \bmod p^2$.

(5) Wilson's theorem: $(p + 1)! + 1 \equiv 0 \bmod p$.

Now let $p \geq 5$. First we realize that $k!/k^3$ contains a power of p in the denominator (after cancellation) only if $k = p$ or $k = 2p$. For $k = p$ we have

$$ p!/p^3 = (p - 1)!/p^2 $$

and for $k = 2p$ we have

$$ (2p)!/(2p)^3 \sim [(p-1)/2]^2/p. $$

To compute $B_n^{2r}/(2p)^3$ that is $\sim -[(p - 1)/2]^2 S_{n+1}^{2p}/p$, one uses $S_{n+1}^{2p} \equiv S_n^{2p-1} \bmod p$ and

$$ S_{s+t(p-1)}^{2p-1} \equiv t\,{}_S\Delta_{(0,s)}^{2p-1} \equiv \begin{cases} 0 & \text{if } s < p \\ t & \text{if } s = p \end{cases} \bmod p $$

where ${}_S\Delta_{(r,s)}^k$ is defined as $S_{s+(r+1)(p-1)}^k - S_{s+r(p-1)}^k$ and shows independence with respect to $r \bmod p$ by using formula (4) from above. It follows that

$$ B_{s+t(p-1)}^{2p}/(2p)^3 \sim \begin{cases} 0 & \text{if } s < p \\ \rho_1/p & \text{if } s = p \end{cases} \quad \text{where } \rho_1 \equiv -t[(p - 1)/2]^2 \bmod p. $$

To compute B_n^p/p^3 which is $\sim (p - 1)!S_{n+1}^p/p^2 \sim (p - 1)!S_{s+r(p-1)}^{p-1}/p^2$ if $s < p$ and $\sim (p - 1)!S_{s+r(p-1)}^{p-1}/p^2 - 1/p$ if $s = p$ where n has been replaced by $s + r(p - 1)$ but

$$ S_{s+r(p-1)}^{p-1} \equiv \begin{cases} r\,{}_S\Delta_{(0,s)}^{p-1} & \text{for } s < p - 1 \\ 1 + r\,{}_S\Delta_{(0,s)}^{p-1} & \text{for } s = p - 1 \end{cases} \bmod p^2. $$

The statements in III(a) can now be proved. Let $s = 1$ so that

$$ \Delta_{(0,1)}^{p-1} \equiv -p/2 \bmod p^2 $$

and, therefore,

$$B^p_{1+r(p-1)}/p^3 \sim \rho_2/p$$

where $\rho_2 \equiv -[r(p-1)/2 + 1] \bmod p$ and $B_1/p^3 \sim 0$. Putting

$$n = 1 + r(p-1) = p + t(p-1)$$

and

$$\rho = \rho_1 + \rho_2 \equiv -1 + (n-1)(p-1)/2 + n[(p-1)/2]^2 \bmod p,$$

then ρ/p occurs as a partial fraction of c_n if $n \neq 1$ and $n \not\equiv p - 2 \bmod p$. It is clear that, if $n = 1$ and $n \equiv p - 2 \bmod p$, then $\rho \equiv 0 \bmod p$ and p does not occur in a partial fraction.

III(b). Let $n = s + r(p-1)$ where $s = 2, 3, \ldots, p-2$.

$$B^p_n/p^3 \sim B^{p-1}_{n-1}/p^2 \sim -rS^{p-1}_{s+p-1}/p/p.$$

To compute S^{p-1}_{s+p-1}/p, we utilize the following Bernoulli numbers:

$$b_s = \sum_{k=1}^{s+1} B^k_s/k^2 = \sum_{k=1}^{s+1} (-1)^{k+1}[(k-1)!/k]S^k_{s+1}, \quad s = 2, 3, \ldots, p-2,$$

and

$$b_{s+p-1} \equiv \sum_{k=1}^{s+1} (-1)^{k+1}[(k-1)!/k]S^k_{s+1} + \sum_{k=s+2}^{p-1} (-1)^{k+1}[(k-1)!/p]S^k_{s+1}$$
$$-\frac{1}{p} S^p_{s+p} + \sum_{k=p+1}^{s+p} (-1)^{k+1}[(k-1)!/p]S^k_{s+p} \bmod p.$$

The first sum is equal to b_s, the second and third sums $\equiv 0 \bmod p$. Therefore, we have

$$-S^{p-1}_{s+p-1}/p \sim -S^p_{s+p}/p \equiv b_{s+p-1} - b_s \equiv -(1/s)b_s \bmod p.$$

The last congruence follows from a theorem of Kummer. (See, for example, Nr. 14 in [1].). Finally, we have

$$B^p_n/p^3 \sim \begin{cases} 0 & \text{for } s \text{ odd, since } b_s = 0 \\ \rho/p & \text{for } s = 2m,\ m = 1, \ldots, \dfrac{p-3}{2} \end{cases}$$

where

$$\rho \equiv -(r/s)b_s \equiv -(2m)^{-1}D^{-1}_{2m}N_{2m}r \bmod p$$

where D_{2m} and N_{2m} are the denominator and numerator of b_{2m}. Note that $(2m)^{-1}$ exists for our m's and that

$$D^{-1}_{2m} = \prod p^{-1}_i \text{ for } (p_i - 1)\,|\,2m \text{ (by the von Staudt-Clausen theorem)}$$

exists also for our m's. Furthermore, $n = 2m + r(p-1)$, so $-r \equiv n - 2m \bmod p$ and therefore

$$\rho \equiv (2m)^{-1}D^{-1}_{2m}N_{2m}(n - 2m) \bmod p \text{ if } p \nmid N_{2m} \text{ and } p \nmid n - 2m$$

which proves III(b).

III(c). Here $n = p - 1 + r(p-1) \equiv 0 \bmod p - 1$,

$$B^p_{p-1+r(p-1)}/p^3 \sim -B^{p-1}_{p-2+r(p-1)}/p^3$$

and

$$-B^{p-1}_{p-2+r(p-1)} \equiv -B^{p-1}_{p-2} - r \cdot {}_B\Delta^{p-1}_{(r,p-2)} \cdot$$
$$(p-1)! - r \cdot {}_B\Delta^{p-1}_{(p-1,p-2)} \bmod p^2,$$

but

$$-{}_B\Delta^{p-1}_{(p-1,p-2)} \equiv B^{p-1}_{p^2-p-1} - B^{p-1}_{p-2} \equiv 1 + (p+1)! \equiv \alpha \cdot p \bmod p^2$$

for some integer $\alpha = 0, 1, 2, \ldots, p - 1$. Therefore,

$$-B^{p-1}_{p-2+r(p-1)} \equiv -1 + (r + 1)\alpha p \bmod p^2.$$

Put $\rho - (r + 1)\alpha \equiv -n\alpha \bmod p$, then $\rho/p - 1/p^2$ occurs in the decomposition of c_n provided that $n \not\equiv 0 \bmod p$ and $\alpha \not\equiv 0 \bmod p$, which proves III(c).

Proof of Remark 1: We use a theorem of von Staudt (see, for example, [1], vol. 2, p. 55) which says that τ is an integer, then

$$(2m)^{-1}D_{2m}^{-1}N_{2m} = \tau \prod p_i^{-1-s_i}.$$

Proof of Remark 2:

$$b_{p-1} = \sum_{k=1}^{p-1} (-1)^{k+1}[(k - 1)!/k]S_p^k + (p - 1)!/p,$$

so

$$pb_{p-1} \equiv p + (p - 1)! \bmod p^2 \text{ (since } pS_p^k \equiv 0 \bmod p^2 \text{ for } 1 \le k \le p - 1),$$

so

$$1 + (p - 1)! \equiv pb_{p-1} - p + 1 \bmod p^2.$$

Proof of Corollary 1: The first equivalence follows at once from our definition of a regular prime of the first kind and from III(b). The second equivalence was proved by Kummer himself [5].

Proof of Corollary 2: The first equivalence follows from the proof of III(c) and the second equivalence from the definition of primes of the second kind.

References

1. P. Bachmann. *Niedere Zahlentheorie*, 2-ter Teil Nr. 14 and 15. New York: Chelsea, 1968.
2. N. G. W. H. Beeger. "Quelques remarques sur les congruences $r^{p-1} \equiv 1 \pmod{p^2}$ et $(p - 1)! \equiv -1 \pmod{p^2}$." *Messenger Math.* *43* (1913):72-84.
3. Ch. Y. Chao. "Generalizations of Theorems of Wilson, Fermat and Euler." *J. Number Theory* *15* (1982):95-114.
4. Ch. Jordan. "On Stirling Numbers." *Tohoku Math. J.* *37* (1933):254-278.
5. E. E. Kummer. "Allgemeiner Beweis des Fermat's schen Satzes etc." *J. fuer Math.* (Crelle) *40* (1850):130-138.
6. E. G. Kundert. "Basis in a Certain Completion of the *s-d*-Ring over the Rational Numbers." Nota II, *Rendiconti della Academia dei Lincei*, Serie VIII, vol. LXIV, fasc. 6 (1979):543-547.
7. E. Lehmer. "On Congruences Involving Bernoulli Numbers and the Quotients of Fermat and Wilson." *Annals of Math.* *39* (1938):350-359.
8. R. Gonter & E. G. Kundert. "Wilson's Theorem $(p - 1)! + 1 \equiv 0 \bmod p^2$." *SIAM Conference on Discrete Mathematics in San Francisco, June 13-16, 1988.* Report pages 1-8.

*****