The Congruences of Clausen- von Staudt and Kummer for Bernoulli-Hurwitz Numbers.

Katz, Nicholas M.

in: Mathematische Annalen | Mathematische Annalen | Periodical Issue | Article

1 - 4

Math. Ann. 216, 1—4 (1975)

The Congruences of Clausen – von Staudt and Kummer for Bernoulli-Hurwitz Numbers

Nicholas M. Katz

Let (E, ω) be a pair consisting of an elliptic curve E over a $\mathbb{Q}$-algebra B_0 together with a nowhere-vanishing invariant differential. We may define its Weierstrass $\mathscr{P}$-function as follows. There are unique meromorphic functions x and y on E having poles only along the identity section of orders two and three respectively, and elements $g_2, g_3 \in B_0$ such that (E, ω) is given by the Weierstrass equation

$$\begin{cases} E\colon\ y^2 = 4x^3 - g_2 x - g_3 \\ \omega\colon\ dx/y\,. \end{cases} \tag{1}$$

Because B_0 is a $\mathbb{Q}$-algebra, there is a unique formal parameter z along the zero section in terms of which $\omega = dz$. The Weierstrass $\mathscr{P}$-function is defined as the formal Laurent series expansion of the function x in terms of the parameter z.

$$\mathscr{P}(z, (E/B_0, \omega)) = \frac{1}{z^2} + 2\sum_{n \geqq 1} G_{2n+2}(E/B_0, \omega) \cdot \frac{z^{2n}}{(2n)!} \in B_0[[z]]\,. \tag{2}$$

In case $B_0 = \mathbb{C}$, the field of complex numbers, this is the usual $\mathscr{P}$-function associated to the lattice $L \subset \mathbb{C}$ of all the periods of ω over all elements of the topological fundamental group of E viewed as complex torus, and the coefficients are the classical Eisenstein series:

$$G_k = \frac{(-1)^k (k-1)!}{2} \sum_{l \in L - \{0\}} 1/l^k \quad \text{for} \quad k \geqq 4; \text{ it's 0 for } k \text{ odd} \tag{3}$$

whose q-expansions (= values on the lattice $2\pi i\mathbb{Z} + 2\pi i\mathbb{Z}\tau$, $\mathrm{Im}(\tau) > 0$, expressed as functions of $q = e^{2\pi i \tau}$) are given by the formulas

$$\begin{cases} G_{2k}(q) = -\dfrac{b_{2k}}{4k} + \displaystyle\sum_{n \geqq 1} q^n \sum_{d|n} d^{2k-1}, & k \geqq 2 \\ G_{\text{odd}} = 0 \end{cases} \tag{4}$$

where the b_{2k} are the Bernoulli numbers

$$\frac{x}{e^x - 1} = \sum b_k \frac{x^k}{k!}\,. \tag{5}$$

We propose to name the numbers $2kG_k(E, \omega) \in B_0$ the "Bernoulli-Hurwitz numbers" associated to (E, ω), and note them $BH_k(E, \omega)$:

$$BH_k(E, \omega) = 2kG_k(E, \omega), \quad k \geqq 4; \ = 0 \text{ if } k \text{ odd}\,. \tag{6}$$

In the case of the degenerate "curve at ∞" obtained by evaluating the q-series expansions at $q = 0$, we obtain the *negatives* of the Bernoulli numbers. In the case

of the lemniscatic curve ($y^2 = 4x^3 - 4x, dx/y$), we obtain the "Hurwitz numbers" E_n up to a power of two:

$$BH_k = \begin{cases} 0 & \text{unless } k \equiv 0(4) \\ 2^k E_{k/4} & \text{if } k \equiv 0(4). \end{cases} \tag{7}$$

These remarkable numbers were seen by Hurwitz as being analogues (for the Gaussian field) of the Bernoulli numbers (for the rational field $\mathbb{Q}$). Mindful of the Clausen-von Staudt and Kummer congruences for Bernoulli numbers according to which

$$b_k \equiv \sum_{p-1|k} \frac{-1}{p} \bmod \mathbb{Z} \tag{8}$$

and if $p-1 \nmid k$, then b_k/k is p-integral, and (8 bis)

$$b_{k+p-1}/k + p - 1 \equiv b_k/k \bmod p\mathbb{Z}_p .$$

Hurwitz proved that

$$E_k \equiv \frac{1}{2} + \sum_{\substack{p-1|4k \\ p \equiv 1(4)}} \frac{(\mathrm{trace}(\pi))^{4k/p-1}}{p} \bmod \mathbb{Z} \tag{9}$$

where $\pi = a + bi$ is either of the gaussian primes lying over p, normalized to be $\equiv 1\,(2+2i)$ in $\mathbb{Z}[i]$ [e.g. write $p = a^2 + b^2$ with a odd, b even, $a \equiv b + 1\,(4)$; then $\pi = a + bi$ and $\bar{\pi} = a - bi$ are the normalized gaussian primes over p, and $\mathrm{trace}(\pi) = \mathrm{trace}(\bar{\pi}) = 2a$].

We may *restate* Hurwitz's result as:

$$\begin{aligned} &2E_k \equiv 1 \bmod 2\mathbb{Z}_2 \\ &pE_k \equiv \begin{cases} 0 & \text{if } p-1 \nmid 4k \\ A(p)^{4k/p-1} & \text{if } p-1 | 4k \end{cases} \bmod p\mathbb{Z}_p \text{ for } p \text{ odd} \end{aligned} \tag{10}$$

where $A(p) \in \mathbb{F}_p$ is the *Hasse invariant* of the reduction modulo p of the lemniscate curve. The prime *two* plays a special role here *not* because it is the *even* prime, but because it is the unique prime at which the lemniscatic curve has bad reduction.

If we remark with Ribet that for primes p such that $p-1$ divides $4k$, we have $2^{4k} \equiv 1 \bmod p$, then Hurwitz's theorem for the primes p where there is *good* reduction is a special case of the following theorem, applied to the lemniscate curve over each $\mathbb{Z}_p$ where it has good reduction.

Theorem. Let $\mathcal{O}$ be a valuation ring of residue characteristic p, whose fraction field $\mathcal{O}\left[\frac{1}{p}\right]$ has characteristic zero. Let (E, ω) be an elliptic curve plus nowhere vanishing invariant differential over $\mathcal{O}$ (i.e. having *good* reduction). Let

$$BH_k = BH_k(E, \omega) \in \mathcal{O}\left[\frac{1}{p}\right]$$

be its Bernoulli-Hurwitz numbers, and let $A \in \mathcal{O}/p\mathcal{O}$ be the *Hasse invariant* of $(E, \omega) \bmod p$. Then

1) if $p-1$ divides k, then $p \cdot BH_k \in \mathcal{O}$, and

$$p \cdot BH_k \equiv A^{k/p-1} \text{ modulo } p\mathcal{O};$$

2) if $p-1$ does *not* divide k, then $BH_k/k \in \mathcal{O}$, and

$$BH_{k+p-1}/k + p - 1 \equiv A \cdot BH_k/k \text{ modulo } p\mathcal{O}.$$

Proof. Let us define modular forms F_k, $k \geqq 4$, by the formulas

$$F_k = \begin{cases} 2G_k & \text{if} \quad p-1 \nmid k \\ 2pkG_k & \text{if} \quad p-1 \mid k. \end{cases} \tag{11}$$

By the Clausen-von Staudt theorem and the q-expansion principle, the forms F_k are defined over $\mathbb{Q} \cap \mathbb{Z}_p$. Hence they take integral values on (E, ω):

$$F_k(E, \omega) \in \mathcal{O}. \tag{12}$$

Recall that the Hasse invariant $\mathbb{A}$ is the (unique) modular form over $\mathbb{F}_p$ of weight $p-1$, whose q-expansion is $\mathbb{A}(q) = 1 \in \mathbb{F}_p[[q]]$. By the Kummer and Clausen-von Staudt congruences, we therefore have congruences of q-expansions

$$F_{k+p-1}(q) \equiv \mathbb{A}(q) \cdot F_k(q) \bmod p\mathbb{Z}_p[[q]] \quad \text{if} \quad p-1 \nmid k, \quad k \geqq 4, \tag{13}$$

$$F_k(q) \equiv (\mathbb{A}(q))^{k/p-1} \bmod p\mathbb{Z}_p[[q]] \quad \text{if} \quad p-1 \mid k, \quad k \geqq 4. \tag{14}$$

By the q-expansion principle, we therefore have congruences of modular forms

$$\left.\begin{aligned} F_{k+p-1} &\equiv \mathbb{A} \cdot F_k \bmod p \quad \text{if} \quad p-1 \nmid k \\ F_k &\equiv \mathbb{A}^{k/p-1} \bmod p \quad \text{if} \quad p-1 \mid k \end{aligned}\right\} \text{equalities of modular forms over } \mathbb{F}_p \tag{15, 16}$$

and in particular we have congruences of their *values* at (E, ω):

$$F_{k+p-1}(E, \omega) \equiv A \cdot F_k(E, \omega) \bmod p\mathcal{O} \quad \text{if} \quad p-1 \nmid k, \tag{17}$$

$$F_k(E, \omega) \equiv A^{k/p-1} \bmod p\mathcal{O} \quad \text{if} \quad p-1 \mid k. \tag{18}$$

Recalling the relation of the F_k to the BH_k, namely

$$F_k(E, \omega) = \begin{cases} p \cdot BH_k(E, \omega) & \text{if} \quad p-1 \mid k \\ BH_k(E, \omega)/k & \text{if} \quad p-1 \nmid k \end{cases} \tag{19}$$

and substituting into the congruences (17–18) above, we get the desired congruences on the BH_k.

Remark. It would be extremely interesting to have an a priori proof of the Clausen-von Staudt congruences based on the moduli of elliptic curves.

References

1. Borevich, Z. I., Shafarevich, I. R.: Number Theory, New York: Academic Press 1966
2. Deligne, P., Rapoport, M: Les schémas de modules de courbes elliptiques, Proc. 1972 Antwerp Int'l Summer School on Modular Functions, Lecture Notes in Mathematics **349**, 143—317 (1973)
3. Hurwitz, A.: Über die Entwicklungskoeffitizienten der lemniscatischen Functionen, Math. Ann. **51**, 196—226 (1899)

4. Katz, N. M.: The Eisenstein measure and p-adic interpolation, to appear
5. Serre, J.-P.: Congruences et formes modularies, Seminaire N. Bourbaki 1971/72, Exposé 416, Lecture Notes in Mathematics **317**, 319—336, Berlin-Heidelberg-New York: Springer 1972

N.-M. Katz
I. H. E. S.
35, Route de Chartres
F-91440 Bures-sur Yvette, France

(Received May 28, 1974)