The main congruences on generalized Bernoulli-Hurwitz numbers for the curves of cyclotomic type

Yoshihiro Ônishi

1. We consider the curve

$$\mathscr{E} \ : \ y^2 = x^3 - 1.$$

Let $u \to x(u)$ and $u \to y(u)$ are the set of inverse functions of

$$u = \int_{\infty}^{(x,y)} \frac{dx}{2y}.$$

Then

$$x'(u)^2 = 4(x(u)^3 - 1).$$

We define a series of rational numbers $\{F_n\}$ by

$$x(u) = \frac{1}{u^2} + \sum_{n=1}^{\infty} \frac{F_{6n}}{6n} \frac{u^{6n-2}}{(6n-2)!},$$

and by $F_n = 0$ if $6 \not| n$. We call F_n the *n-th Bernoulli-Hurwitz number* for $\mathscr{E}$. Let $p \equiv 1 \bmod 3$ be a rational prime, $\zeta = e^{2\pi \boldsymbol{i}/3}$, and let

$$p = P\overline{P}, \quad P \equiv 1 \mod 3 \quad \text{in } \mathbb{Z}[\zeta];$$

$$A_p = (-1)^{(p-1)/6} \begin{pmatrix} \frac{p-1}{2} \\ \frac{p-1}{6} \end{pmatrix}.$$

Suppose $m \equiv n \mod p^{a-1}(p-1)$ and $m \not\equiv 0 \mod (p-1)$. Then, it is know that

(1)
$$\begin{gathered} (1 - p^{m-1}\overline{P}^{-m}) \, \frac{F_m}{m} \, {A_p}^{(n-m)/(p-1)} \equiv (1 - p^{n-1}\overline{P}^{-n}) \, \frac{F_n}{n} \mod P^a \\ \left((1 - P^m p^{-1}) \, \frac{F_m}{m} \, {A_p}^{(n-m)/(p-1)} \equiv (1 - P^n p^{-1}) \, \frac{F_n}{n} \mod P^a \right). \end{gathered}$$

2. Now, we consider the curve

$$\mathscr{C} \;:\; y^2 = x^5 - 1$$

of genus two. Let $u \to x(u) = \frac{1}{u^2} + \cdots$ be the *formal* inverse series of u given by

$$u = \int_{\infty}^{(x,y)} \frac{xdx}{2y} = \int_{\infty}^{x} \frac{xdx}{2\sqrt{x^5-1}}.$$

We define a series of rational numbers $\{C_n\}$ by

$$x(u) = \frac{1}{u^2} + \sum_{n=1}^{\infty} \frac{C_{10n}}{10n} \frac{u^{10n-2}}{(10n-2)!},$$

and by $C_n = 0$ if $10 \not| n$. We call C_n the *n-th generalized Bernoulli-Hurwitz number* for $\mathscr{C}$. Let $p \equiv 1 \bmod 5$ be a rational prime, and

$$A_p = (-1)^{(p-1)/10} \binom{\frac{p-1}{2}}{\frac{p-1}{10}}.$$

Let $\zeta = e^{2\pi \boldsymbol{i}/5}$ and τ be the element of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ such that

$$\tau \;:\; \zeta \mapsto \zeta^2.$$

Choose a $P \in \mathbb{Z}[\zeta]$ such that

$$p = P^{1+\tau+\tau^2+\tau^3}, \quad P \equiv 1 \mod (1-\zeta)^2 \quad \text{in } \mathbb{Z}[\zeta].$$

Then I shall present the following problem. Does the following congruence hold?

If $m \equiv n \mod p^{a-1}(p-1)$ and $m \not\equiv 0 \mod (p-1)$, then

$$(2) \quad \begin{gathered} \left(1 - p^{m-1}\overline{P}^{-m(1+\tau)}\right) \frac{C_m}{m} A_p{}^{(n-m)/(p-1)} \equiv \left(1 - p^{n-1}\overline{P}^{-n(1+\tau)}\right) \frac{C_n}{n} \mod P^a \\ \left((1 - P^{m(1+\tau)}p^{-1}) \frac{C_m}{m} A_p{}^{(n-m)/(p-1)} \equiv (1 - P^{n(1+\tau)}p^{-1}) \frac{C_n}{n} \mod P^a \right), \end{gathered}$$

where "over-line" stands for the complex conjugation. While we have ambiguity on choosing P, namely, a multiplication by some real unit ε such that $\varepsilon \equiv 1 \bmod (1-\zeta)^2$, $P^{1+\tau}$ is uniquely determined by canceling out such multiplication.

Because of the conditions in Remark 2.18 of the other attached file, the set of numbers in the smallest non-trivial example is

$$\begin{aligned} p &= 31, \\ a &= 9, \\ m &= 10, \\ n &= m + p^{9-1}(p-1) = 10 + 31^8 \times 30 = 25586731123240. \end{aligned}$$

This seems to be too large to check.

Aug. 26, 2011