ON FERMAT'S LAST THEOREM AND THE ARITHMETIC OF $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$

Francisco Thaine

RELATÓRIO TÉCNICO Nº 22/87

ABSTRACT. Let $p \geq 5$ be a prime and a, b, c relatively prime integers such that $a^p + b^p + c^p = 0$. A theorem, similar to Stickelberger's, is used to obtain certain relations involving a, b and c. If $p \nmid abc$, for example, these relations give a complement of Kummer-Mirimanoff congruences when we have a knowledge of which of the numbers $\prod_{k=1}^{p-1} (1 - \zeta_p^k)^{k^r}$, r even, $2 \leq r \leq p - 3$, are p-th power in $\mathbb{Z}[\zeta_p]$.

Universidade Estadual de Campinas
Instituto de Matemática, Estatística e Ciência da Computação
IMECC – UNICAMP
Caixa Postal 6065
13.081 - Campinas, SP
BRASIL

Junho – 1987

ON FERMAT'S LAST THEOREM AND THE ARITHMETIC OF $\mathbb{Z}[\zeta_p + \zeta_p^{-1}]$ (*)

Francisco Thaine
Departamento de Matemática
Universidade Estadual de Campinas
13.100 - Campinas , SP, Brazil

ABSTRACT. Let $p \geq 5$ be a prime and a, b, c relatively prime integers such that $a^p + b^p + c^p = 0$. A theorem, similar to Stickelberger's, is used to obtain certain relations involving a, b and c. If $p \nmid abc$, for example, these relations give a complement of Kummer-Mirimanoff congruences when we have a knowledge of which of the numbers $\prod_{k=1}^{p-1} (1 - \zeta_p^k) k^r$, r even, $2 \leq r \leq p-3$, are p-th powers in $\mathbb{Z}[\zeta_p]$.

Let $p \geq 5$ be a prime number, $\zeta = \zeta_p$ a primitive p-th root of unity, Δ the Galois group of $\mathbb{Q}(\zeta+\zeta^{-1})/\mathbb{Q}$, A the ideal class group and E the group of units of $\mathbb{Z}[\zeta + \zeta^{-1}]$. Let

$$C = \{ \prod_{k=1}^{\frac{p-1}{2}} [(1 - \zeta^k)(1 - \zeta^{-k})]^{a_k} : a_k \in \mathbb{Z} \} \cap E ,$$

it is a subgroup of finite index of E. Denote by W the quotient group E/C, and by $(A)_p$ and $(W)_p$ the p-Sylow subgroups of A and W. The following result has been proven in [6] (Corollary of Theorem 2) and can also be deduced from a Theorem of Mazur and

---

(*) This research was partially supported by a fellowship of the Brazilian CNPq.

Wiles (see [2] page 146).

THEOREM 1. Every annihilator, in $\mathbb{Z}[\Delta]$, of $(W)_p$ also annihilates $(A)_p$.

In this note we give an application of Theorem 1 to the study of Fermat's last theorem. Let $a,b,c \in \mathbb{Z}\setminus\{0\}$ relatively prime, suppose that $a^p + b^p + c^p = 0$. Denote by τ the number $(a+b\zeta)(a+b\zeta^{-1})$ if $p \nmid c$, and the number $(\frac{a+b\zeta}{1-\zeta})(\frac{a+b\zeta^{-1}}{1-\zeta^{-1}})$ if $p \mid c$. Then $\tau \in \mathbb{Z}[\zeta+\zeta^{-1}]$ and, as is known since Kummer, there exists an ideal $\mathfrak{R}$ of $\mathbb{Z}[\zeta+\zeta^{-1}]$ such that

$$(\tau) = \mathfrak{R}^p . \tag{1}$$

Our results are summarized in the following theorem. We denote by B_n the n-th Bernoulli number defined by $\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} t^n$.

THEOREM 2. For all r even, $2 \le r \le p-3$, we have either $\prod_{k=1}^{p-1} (1-\zeta^k)^{k^r} = \alpha^p$, for some $\alpha \in \mathbb{Z}[\zeta]$, and hence $B_{p-1-r} \equiv 0 \bmod p$, or

$$\Big[\prod_{k=1}^{p-1} (1-\zeta^k)^{k^r}\Big]^s \prod_{j=1}^{p-1} (a+b\zeta^j)^{j^r} = \beta^p, \tag{2}$$

for some $s \in \mathbb{Z}$ and $\beta \in \mathbb{Z}[\zeta]$, which implies that: $sB_{p-1-r} \equiv 0 \bmod p$, if $p \mid ab$; $(s+1)B_{p-1-r} \equiv 0 \bmod p$, if $p \mid c$; and

$$(3)\qquad s\,\frac{B_{p-1-r}}{p-1-r} \equiv \frac{1}{1-u}\sum_{j=1}^{p-1} j^{p-2-r}\,u^j \bmod p\ ,$$

where $u = -\frac{a}{b}$, if $p \nmid abc$.

OBSERVATIONS. Theorem 2 and its Corollary (iii) extend, to arbitrary p, results of [5] Part II, as was promised in that article. We can think in this theorem as a complement of the following consequence of Stickelberger's Theorem, that implies Kummer-Mirimanoff congruences (references [1], [3] and [4]): Let r be odd, $1 \le r \le p-4$, then either $p \mid B_{r+1}$, or there exists $\gamma \in \mathbb{Z}[\zeta]$ such that

$$\prod_{k=1}^{p-1} (a+b\zeta^k)^{k^r} = \gamma^p\ .$$

If $p \nmid abc$, this equality implies that $\sum_{j=1}^{p-1} j^{p-2-r}\,u^j \equiv 0 \bmod p$, where $u = -\frac{a}{b}$.

PROOF. For $1 \le k \le p-1$ denote by σ_k the element of Δ such that $\sigma_k(\zeta+\zeta^{-1}) = \zeta^k+\zeta^{-k}$. Let r be even, $2 \le r \le p-3$, $\chi : \Delta \longrightarrow \mathbb{Z}_p^\times$ the p-adic Dirichlet character such that $\chi(\sigma_k) \equiv k^{p-1-r} \bmod p$, and $e_\chi = \frac{1}{|\Delta|}\sum_{\sigma\in\Delta} \chi(\sigma)\sigma^{-1}$ the corresponding idempotent. We know that $|e_\chi(W)_p| \neq 1$ if and only if $\prod_{k=1}^{p-1} (1-\zeta^k)^{k^r} = \alpha^p$ for some $\alpha \in \mathbb{Z}[\zeta]$ and that in such case we have $p \mid B_{p-1-r}$ ([2], §8.3 or [4]).

Suppose that $|e_\chi(W)_p| \neq 1$, then e_χ annihilates $(W)_p$. By Theorem 1 we conclude that e_χ annihilates $(A)_p$. Let $\lambda = (p-2)\sum_{k=1}^{\frac{p-1}{2}} k^r\sigma_k$,

then $\lambda \equiv e_\chi \bmod p$. By (1) we have $(\tau)^\lambda = (\beta_1)^p$ for some $\beta_1 \in \mathbf{Z}[\zeta + \zeta^{-1}]$, hence $\varepsilon_1 \tau^\lambda = \beta_1^p$ for some $\varepsilon_1 \in E$. Since e_χ annihilates $(W)_p$ we have that $\varepsilon_1^\lambda = \delta \varepsilon_2^p$ for some $\delta \in C$ and $\varepsilon_2 \in E$. We have also $\lambda^2 \equiv \lambda \bmod p$, therefore $\delta \tau^\lambda = \beta_2^p$ for some $\beta_2 \in \mathbf{Z}[\zeta + \zeta^{-1}]$. Now, $\delta^\lambda = [(1-\zeta)(1-\zeta^{-1})]^{s_o \lambda} \beta_3^p$ for some positive integer s_o and $\beta_3 \in \mathbf{Z}[\zeta + \zeta^{-1}]$, so $[(1-\zeta)(1-\zeta^{-1})]^{s_o \lambda} \tau^\lambda = \beta_4^p$ for some $\beta_4 \in \mathbf{Z}[\zeta + \zeta^{-1}]$. Since r is even, this equality is equivalent to (2), that we can also write (since $\sum_{k=1}^{p-1} k^r \equiv 0 \bmod p$) in the form

$$(4) \qquad \left[\prod_{k=1}^{p-1} \left(\frac{1-\zeta^k}{1-\zeta}\right) k^r\right]^s \prod_{j=1}^{p-1} (a + b\zeta^j) j^r = \gamma^p \text{ , if } p \nmid c \text{ , and}$$

$$(5) \qquad \left[\prod_{k=1}^{p-1} \left(\frac{1-\zeta^k}{1-\zeta}\right) k^r\right]^{s+1} \prod_{j=1}^{p-1} \left(\frac{a+b\zeta^j}{1-\zeta^j}\right) j^r = \gamma^p \text{ , if } p \mid c \text{ ,}$$

for some $\gamma \in \mathbf{Z}[\zeta]$.

Since $\gamma^p \equiv d \bmod p$, for some $d \in \mathbf{Z}$, we have that (4) implies (2) if $p \nmid abc$, as has been proven in [5] Proposition 2 of Part II. If $p \mid abc$, then (4) or (5) imply that

$$\left[\prod_{k=1}^{p-1} \left(\frac{1-\zeta^k}{1-\zeta}\right) k^r\right]^{s+\nu} \equiv e \bmod p \text{ ,}$$

for some $e \in \mathbf{Z}$, where $\nu = 0$ if $p \mid ab$ and $\nu = 1$ if $p \mid c$, (note that $p^2 \mid a+b$ if $p \mid c$), and this congruence in his turn implies that $(s+\nu) B_{p-1-r} \equiv 0 \bmod p$ (references [4] and [5]). This

ends the proof of Theorem 2.

COROLLARY. Let r be even, $2 \leq r \leq p-3$.

i) If $p \mid ab$ and $p \nmid B_{p-1-r}$, then $\prod_{j=1}^{p-1} (a+b\zeta^j)^{j^r} = \gamma^p$ for some $\gamma \in \mathbb{Z}[\zeta]$.

ii) If $p \mid c$ and $p \nmid B_{p-1-r}$, then $\prod_{j=1}^{p-1} \left(\frac{a+b\zeta^j}{1-\zeta^j}\right)^{j^r} = \gamma^p$ for some $\gamma \in \mathbb{Z}[\zeta]$.

iii) If $p \nmid abc$ and $p \mid B_{p-1-r}$ but $\prod_{k=1}^{p-1} (1-\zeta^k)^{k^r}$ is not a p-th power in $\mathbb{Z}[\zeta]$, then $\prod_{j=1}^{p-1} j^{p-2-r} v^j \equiv 0 \bmod p$, for all $v \in \{-\frac{a}{b}, -\frac{b}{a}, -\frac{a}{c}, -\frac{c}{a}, -\frac{b}{c}, -\frac{c}{b}\}$.

PROOF. (i) and (ii) are immediate consequences of the theorem, (iii) follows from (3) and from the symmetry in the hypothesis on a, b and c, when $p \nmid abc$.

REFERENCES

[1] P. RIBENBOIM, "13 Lectures on Fermat's Last Theorem", Springer-Verlag, Berlin/New York, 1979.

[2] L.C. WASHINGTON, "Introduction to Cyclotomic Fields", Graduate Texts in Mathematics, Springer-Verlag, New York, 1982.

[3] D. MIRIMANOFF, L'equation indéterminée $x^l + y^l + z^l = 0$ et le critérium de Kummer, J. Reine Angew. Math. 128(1905), 45-68.

[4] F. THAINE, Polynomials generalizing binomial coefficients and their application to the study of Fermat's last theorem, J. Number Theory 15 (1982), 304-317.

[5] F. THAINE, On the First Case of Fermat's Last Theorem, J. Number Theory 20, No. 2 (1985), 128-142.

[6] F. THAINE, On the Ideal Class Groups of Real Abelian Number Fields, to appear in Annals of Mathematics.