Petr Cikánek

Matrices of the Stickelberger ideals mod L for all primes up to 125,000

Archivum Mathematicum, Vol. 27 (1991), No. 1-2, 3--6

Persistent URL: http://dml.cz/dmlcz/107397

MATRICES OF THE STICKELBERGER IDEALS MOD L FOR ALL PRIMES UP TO 125,000

PETR CIKÁNEK

(Received April 21, 1988)

Abstract. By using Wagstaff's tables for the irregular primes and computer is shown that the "normal" matrices $M(A_l)$ (l an odd prime) corresponding the Stickelberger ideal $A_l = \left\{1 \leqq a \leqq \frac{l-3}{2} : l/B_{2a}\right\}$ have very "convenient" form for primes up to 125,000. The same applies for the matrices $M(\bar{A}_l)$ $\left(\bar{A}_l = A_l \cup \left\{\frac{l-1}{2}\right\}\right)$ except two primes $l = 19{,}927$ and $l = 68{,}737$.

Key words. Stickelberger ideal, Bernoulli numbers, index of irregularity of a prime, normal matrix.

MS Classification. 10 M 20.

0. INTRODUCTION

In the algebraic number theory particularly in the theory of cyclotomic field the Stickelberger ideal plays the great role (s.e.g. [3]). In the paper of Skula [1] the image of the Stickelberger ideal $\mathfrak{J}^-(l) \bmod l$ (l an odd prime) in a special isomorphism F is considered, the matrix $M(A_l)$ in s. c. normal form of this image is introduced $A_l = \left\{1 \leqq a \leqq \frac{l-3}{2} : l/B_{2a}\right\}$ and it is shown that for $3 \leqq l < 1{,}000$ these matrices $M(A_l)$ have a very "convenient" form. Similarly, it is done for $\bar{A}_l = A_l \cup \left\{\frac{l-1}{2}\right\}$. By using Wagstaff's tables for the irregular primes to 125,000 [2], one Proposition from Skula's paper [1] and the computer I found that for $3 \leqq l < 125{,}000$ the matrices $M(A_l)$ had also this "convenient" form. For the matrices $M(\bar{A}_l)$ this result also applies except two primes: $l = 19{,}927$ and $l = 68{,}737$.

1. BASIC NOTIONS

Recall the basic facts from Skula's paper [1].

1.1. A matrix $M = (m_{ij})$ of size $m \times n (m \leqq n)$ over $\mathbf{Z}/l\,\mathbf{Z}$ is in *normal form* if there exist integers $1 \leqq j_1 < j_2 < \dots < j_m \leqq n$ with following property:

$$m_{ij} = \begin{cases} 1 & \text{for } j = j_i, \\ 0 & \text{for } j < j_i, \\ 0 & \text{for } j = j_k,\ 1 \leqq k \leqq m,\ k \neq i, \end{cases}$$

$1 \leqq i \leqq m$.

1.2. Let $\mathbf{V}$ be the vector space over the Galois field $\mathbf{Z}/l\mathbf{Z}$, l an odd prime, $\mathbf{V} = (\mathbf{Z}/l\mathbf{Z})^{(N)} = \{(v_1, \dots, v_N) : v_i \in \mathbf{Z}/l\mathbf{Z}\}$, $N = \frac{l-1}{2}$, with operations defined componentwisely. For a subset $A \subseteq \{1, 2, \dots, N\}$ put $\mathscr{S}(A) = \{\alpha = (a_1, \dots, a_N) \in \mathbf{V}: \sum_{x=1}^{N} a_x x^{2a-1} = 0$ for each $a \in A\}$.

Let U be the matrix of coordinates of vectors of a basis of $\mathscr{S}(A)$ $(A \neq \{1, 2, \dots, N\})$. The matrix U can be transformed in the uniquely determined matrix $M(A)$ in normal form by a sequence of elementary row operations and omitting rows containing only zeros. The matrix $M(A)$ is of size $(N - |A|) \times N$, $(|A| = \text{card } A)$.

1.3. The subset $A \subseteq \{1, 2, \dots, N\}$ is called *normal* (for the prime l) if $A = \emptyset$ or $A = \{1, 2, \dots, N\}$ or $\emptyset \neq A \neq \{1, 2, \dots, N\}$ and $M(A) = (E, X)$, where E is the unit matrix of order $N - |A|$ and X is a matrix of size $(N - |A|) \times |A|$.

1.4. For the practical computation the following criterion of the normality of A has the great meaning: Let suppose $A \subseteq \{1, 2, \dots, N\}$, $\emptyset \neq A \neq \{1, 2, \dots, N\}$ and denote by B the set $B = \{a - a^* : a \in A\}$, where a^* is the least integer in A. Then it holds ([1], 5.6):

1.4.1. Proposition. *The set A is normal for the prime l if and only if*

$$\det ((2x - 1)^{2b}) \, (b \in B,\ 1 \leqq x \leqq |A|) \not\equiv 0 \pmod{l}.$$

2. SPECIAL SUBSETS A

In this Section we put $A_l = \left\{1 \leqq a \leqq \frac{l-3}{2} : l/B_{2a}\right\}$, where B_{2a} means the Bernoulli numbers, and $\bar{A}_l = A_l \cup \left\{\frac{l-1}{2}\right\}$. Then $\mathscr{S}(A_l)$ is the image of the Stickelberger ideal $\mathfrak{J}^-(l)$ mod l in a special isomorphism F from the group ring $\mathbf{R}^-(l)$ (considered as a vector space over $\mathbf{Z}/l\mathbf{Z}$) on to $\mathbf{V}$ (s. [1], Section 4). It was proved in [1] (5.9.1):

2.1. Proposition. *For each l, $3 \leqq l < 1{,}000$ the sets A_l and $\bar{A}_l$ are normal (for the prime l).*

I used Wagstaff's tables [2], proposition 1.4.1 (Skula [1], 5.6) and minicomputer SM 4–20 for extending this results. I made a program for computing of the determinant from 1.4.1. Using computer I got after four hours of computer work the next theorems:

2.2. Theorem. *For each prime l, $3 \leqq l < 125{,}000$ the set*

$$A_l = \left\{1 \leqq a \leqq \frac{l-3}{2} : l/B_{2a}\right\}$$

is normal (for the prime l).

I suppose that in spite of this fact there are still a few casses for general validity of 2.2 because there exist 4,605 irregular primes and only 2,046 of these primes have index of irregularity greater than 1.

On the other hand for the set $\bar{A}_l$ I have obtained:

2.3. Theorem. *For each prime l, $3 \leqq l < 125{,}000$, $l \neq 19{,}927$, $l \neq 68{,}737$, the set $\bar{A}_l = \left\{1 \leqq a \leqq \frac{l-3}{2} : l/B_{2a}\right\} \cup \left\{\frac{l-1}{2}\right\}$ is normal for the prime l. For $l = 19{,}927$ and $l = 68{,}737$ the matrix $M(\bar{A}_l)$ of size $(N-2)\times N$ has the following form:*

$$M(\bar{A}_l) = \begin{bmatrix} & & x_1 & 0 & y_1 \\ & E & \vdots & \vdots & \vdots \\ & & x_{N-3} & 0 & y_{N-3} \\ 0 & \dots\ 0 & 0 & 1 & y_{N-2} \end{bmatrix},$$

where E means the unit matrix of order $N-3$ and $x_1, \dots, x_{N-3}, y_1, \dots, y_{N-2} \in \mathbf{Z}/l\mathbf{Z}$. Note that the index irregularity $i(l) = \operatorname{card}\left\{1 \leqq a \leqq \frac{l-3}{2} : l/B_{2a}\right\}$ for these both primes l is equal to 1.

REFERENCES

[1] L. Skula, *Special invariant subspaces of a vector space over $\mathbf{Z}/l\mathbf{Z}$*, Archivum Math. BRNO, to appear.

[2] S. S. Wagstaff, Jr., *The irregular primes to 125,000*, Math. Comp. 32 (1978), 583–591; the more detailed results in personal communication to L. Skula.

[3] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, New York, Heidelberg, Berlin, 1982.

Petr Cikánek
The computer center of NÁŘADÍ HULÍN,
ul. 9. května,
768 24 Hulín,
Czechoslovakia