Acta Mathematica et Informatica Universitatis Ostraviensis

David Jedelský; Ladislav Skula

Some results from the tables of irregularity index of a prime

Acta Mathematica et Informatica Universitatis Ostraviensis, Vol. 8 (2000), No. 1, 45--50

Persistent URL: http://dml.cz/dmlcz/120558

Acta Mathematica et Informatica Universitatis Ostraviensis 8 (2000) 45–50

Some Results from the Tables of Irregularity Index of a Prime

David Jedelský
Ladislav Skula

Abstract: This paper is an announcement on the form of certain matrices related to the Stickelberger ideal over the Galois field $\mathbf{Z}/l\mathbf{Z}$. This result was obtained from the tables of the irregularity index for primes to eight million ([BCEMS], 1998) and from that of J. P. Buhler (personal communication) extended for primes to twelve million. The article extends the results of Cikánek ([C], 1991) for primes up to 125,000. Except two "exceptional" primes discovered by Cikánek all primes up to 12.10^6 have the investigated matrices in the "natural" form.

In the conclusion all primes to 12.10^6 are presented for which the dimension of the ideal $\mathcal{B}^-(l)$ generated by the Kummer element κ_0 is nontrivial.

Key Words: Stickelberger Ideal, Bernoulli numbers, irregularity index of a prime, Kummer element

Mathematics Subject Classification: 11R54, 11B68, 11R29, 11Y40

1. Notation

In the whole paper we will use the following notation:

l an odd prime,

$N = \frac{1}{2}(l-1)$,

$\mathbf{Z}$ the ring of rational integers,

r a primitive root modulo l,

r_i the integer $(i \in \mathbf{Z})$, $0 < r_i < l$, $r_i \equiv r^i (\mathrm{mod}\ l)$,

ind x index of x relative to the primitive root r mod l,

Supported by the grant no. 201/97/0433 of the Czech Grant Agency

B_n the nth Bernoulli number ($B_0 = 1,\ B_1 = -\frac{1}{2},\ B_2 = \frac{1}{6},\ B_3 = 0,\ \ldots$),

$A = \{a \in \mathbf{Z} : 1 \leq a \leq \frac{l-3}{2},\ l/B_{2a}\}$,

$\bar{A} = A \cup \{N\}$,

$i(l) = \#A = \operatorname{card} A$ the index of irregularity (the irregularity index) of l,

f the order of 2 mod l,

$$e = \frac{l-1}{f},$$

$$g(l) = \begin{cases} e-1 & \text{if } f \text{ is even} \\ \frac{e}{2}-1 & \text{if } f \text{ is odd,} \end{cases}$$

$j(l) = \#\{1 \leq \nu \leq e-1,\ \nu \in \mathbf{Z} : f\nu \text{ even},\ l/B_{f\nu}\}$,

$$\varepsilon(l) = \begin{cases} 1 & \text{if } l \text{ is a Wieferich prime, i.e. } 2^{l-1} \equiv 1 (\mathrm{mod}\ l^2), \\ 0 & \text{otherwise,} \end{cases}$$

$\beta(l) = i(l) - j(l) + g(l) + \varepsilon(l)$,

$\mathcal{R}(l)$ the group ring of the cyclic group $G = \{1, s, s^2, \ldots, s^{l-2}\}$ of order $l-1$ over the residue class field $\mathbf{Z}/l\mathbf{Z}$, thus $\alpha \in \mathcal{R}(l)$ has the form

$$\alpha = \sum_{i=0}^{l-2} a_i s^i,\ a_i \in \mathbf{Z}/l\mathbf{Z},$$

$$\mathcal{R}^-(l) = \left\{ \alpha = \sum_{i=0}^{l-2} a_i s^i \in \mathcal{R}(l) : a_i + a_{i+N} = 0 \text{ for each } 0 \leq i \leq N-1 \right\},$$

$\mathcal{I}(l)$ the Stickelberger ideal of the ring $\mathcal{R}(l)$ (for an exact definition of the Stickelberger ideal $\mathcal{I}$ of the group ring $\mathbf{Z}[G]$, see e.g. [Ws] § 6.2,

$$\mathcal{I}^-(l) = \mathcal{I}(l) \cap \mathcal{R}^-(l) = \mathcal{R}^-(l) \prod_{a \in A} (s - r_{-2a+1}) \quad ([S2], 4.3.3),$$

$$\mathcal{I}^-{}_0(l) = \mathcal{R}^-(l) \prod_{a \in \bar{A}} (s - r_{-2a+1}) = \mathcal{I}^-(l)\ (s - r),$$

$\mathcal{B}(l)$ the ideal of the ring $\mathcal{R}(l)$ generated by the Kummer element

$$\kappa_0 = \sum_{i=0}^{l-2} k_i s_i,$$

where

$$k_i = \begin{cases} 1 & \text{if } r_{-i} > \frac{l}{2} \\ 0 & \text{if } r_{-i} < \frac{l}{2} \end{cases}$$

hence $\mathcal{B}(l) \subseteq \mathcal{I}(l)$ (cf. [S3]),

$$\mathcal{B}^-(l) = \mathcal{B}(l) \cap \mathcal{R}^-(l) \subseteq \mathcal{I}^-(l).$$

The algebraic structures $\mathcal{R}^-(l)$, $\mathcal{I}^-(l)$, $\mathcal{I}_0^-(l)$, and $\mathcal{B}^-(l)$ are considered to be vector spaces over the Galois field $\mathbf{Z}/l\mathbf{Z}$. Using Consequence 2.2 in [S1], 4.3.2. in [S2], and Theorem 4.5 in [S3] we have

$$\dim \mathcal{R}^-(l) = N, \quad \dim \mathcal{I}^-(l) = N - i(l), \quad \dim \mathcal{I}_0^-(l) = N - 1 - i(l),$$
$$\dim \mathcal{B}^-(l) = N - \beta(l).$$

Furthermore we will denote by

$\mathbf{V} = \{(v(1), \ldots, v(N)) : v(i) \in \mathbf{Z}/l\mathbf{Z}, 1 \leq i \leq N\}$ the vector space over the Galois field $\mathbf{Z}/l\mathbf{Z}$ ($\dim \mathbf{V} = N$),

$F : \mathcal{R}^-(l) \longrightarrow \mathbf{V}$ the isomorphism of the vector space $\mathcal{R}^-(l)$ onto $\mathbf{V}$ defined by $F(\alpha) = \mathbf{u} = (u(1), \ldots, u(N)) \in \mathbf{V}$,

where

$$\alpha = \sum_{i=0}^{l-2} a_i s^i \in \mathcal{R}^-(l)$$

and

$$u(x) = a_{l-1-\mathrm{ind}\ x} \quad (a_{l-1} := a_0)\,(1 \leq x \leq N).$$

Definition 1.1. Let $\mathbf{U}$ be a subspace of the vector space $\mathbf{V}$ and let $d = \dim \mathbf{U} \geq \geq 1$. Consider an $l^d \times N$ matrix $\mathcal{M}$ whose each row consists of the coordinates of an element of $\mathbf{U}$. Let the matrix $\mathcal{M}$ be brought to reduced row-echelon form by the use of elementary row operations and zero rows be omitted. This new matrix will be denoted by $M(\mathbf{U})$ and is uniquely determined by the subspace $\mathbf{U}$. The matrix $M(\mathbf{U})$ is of size $d \times N$ and there exist integers $1 \leq j_1 < j_2 < \ldots < j_d \leq N$ such that for the entries of the matrix $M(\mathbf{U}) = [m_{ij}]_{1 \leq i \leq d, 1 \leq j \leq N}$ we have

$$m_{ij} = \begin{cases} 1 & \text{if } j = j_i \\ 0 & \text{if } j < j_i \\ 0 & \text{if } j = j_k,\ 1 \leq k \leq d,\ k \neq i. \end{cases}$$

2. Normal Primes

Definition 2.1. Denote by $\mathbf{U}_1$ and $\mathbf{U}_2$ the subspaces $F(\mathcal{I}^-(l))$ and $F(\mathcal{I}_0^-(l))$ of $\mathbf{V}$, respectively. Then $d_1 = \dim \mathbf{U}_1 = \dim \mathcal{I}^-(l) = N - i(l)$ and $d_2 = \dim \mathbf{U}_2 = = \dim \mathcal{I}_0^-(l) = N - i(l) - 1$. The matrices $M(\mathbf{U}_1)$ and $M(\mathbf{U}_2)$ are of sizes $d_1 \times N$ and $d_2 \times N$, respectively. If l is regular or if, in the case $d_1 < N$, the matrix $M(\mathbf{U}_1)$ has the form

$$M(\mathbf{U}_1) = [I_{d_1} | X]$$

(I_n is the identity matrix of order n), where X is a $d_1 \times (N - d_1)$ matrix, then we call the prime l *normal*. If the matrix $M(\mathbf{U}_2)$ has the form

$$M(\mathbf{U}_2) = [I_{d_2}|Y],$$

we call the prime l 0-*normal*.

Using Proposition 5.6 of [S2] we can characterize the normal and 0-normal primes by means of a special determinant as follows:

Theorem 2.1.
(1) *The following statements together are equivalent for l being irregular:*
  (1a) *l is normal,*
  (1b) $\det[x^{2a}]$ $(a \in A,\ d_1 + 1 \leq x \leq N) \not\equiv 0 \pmod{l}$.
(2) *The following statements are equivalent:*
  (2a) *l is 0-normal,*
  (2b) $\det[x^{2a}]$ $(a \in \bar{A},\ d_2 + 1 \leq x \leq N) \not\equiv 0 \pmod{l}$.

An easy consequence is the following.

Corollary 2.2.
(a) *If l is regular, then l is both normal and 0-normal.*
(b) *Let $i(l) = 1$. Then*
  ($b1$) *l is normal.*
  ($b2$) *l is 0-normal if and only if $3^{2a} \not\equiv 1 (mod\ l)$, where $A = \{a\}$.*

3. Computations on Normality of a Prime

Using the familiar tables of the irregular pairs $[l,\ 2a]$ (l/B_{2a}) and Theorem 2.1 it was shown in [S2], Proposition 5.9.1 that

3.1. *Each prime l, $3 \leq l < 1{,}000$ is both normal and 0-normal.*

P. Cikánek ([C], 1991) made use of the tables of the irregular primes to 125,000 by S. S. Wagstaff, Jr. ([Wg], 1978) and extended the result of 3.1:

3.2.
(a) *Each prime l, $3 \leq l < 125{,}000$ is normal.*
(b) *Each prime l, $3 \leq l < 125{,}000$ is 0-normal with exception of two primes $l_1 = 19{,}927$ and $l_2 = 68{,}737$ which are not 0-normal.*

Note that the both primes l_1 and l_2 discovered by Cikánek satisfy the condition ($b2$) of Corollary 2.2.

J. W. Tanner and S. S. Wagstaff, Jr. ([TW], 1987) extended the tables of Wagstaff for irregular primes up to 150,000. Using Newton method for polynomial (power series) inversion (with use of FFT and multisectioning of power series) Buhler, Crandall, and Sompolski ([BCS], 1992) were successful in extending the tables of irregular primes to one million and subsequently Buhler, Crandall, Ernvall, and Metsänkylä ([BCEM], 1993) extended these tables to four million.

Using the tables ([BCEMS], 1998) provided us kindly by T. Metsänkylä and with his allowance, for irregular primes up to 8.10^6, the extended tables for irregular primes up to 12.10^6, which we obtained by J. P. Buhler (personal communication), and using Theorem 2.1 we have got the following result:

Theorem 3.3.
(a) Each prime l, $3 \leq l < 12.10^6$ *is normal.*
(b) Each prime l, $3 \leq l < 12.10^6$ *is* 0*-normal with exception of primes* $l_1 = 19,927$ *and* $l_2 = 68,737$ (discovered by Cikánek).

Note to the computation. All computations were established using the Mathematica system on the standard PC and were ready within an hour.

At the conclusion we have got from the mentioned tables the values of the function $j(l)$ for $l < 12.10^6$ relative to the dimension of $\mathcal{B}^-(l)$. With exception only of three cases, $j(l) = 0$. The first two cases were found out by K. Dilcher (cf.[S1], p.189) from the tables [BCS]. All the three cases are presented in the following table:

l	f	l/B_{2a}: $(1 \leq a \leq \frac{l-3}{2})$ $2a$	$l/B_n, n = f\nu$ even $(1 \leq \nu \leq e-1)$ n	$i(l)$	$j(l)$
130811	26162	52324, 88910	52324	2	1
599479	33	359568,471754	359568	2	1
2010401	1795	1234960	1234960	1	1

The irregular primes $l < 12.10^6$ *with* $j(l) > 0$

Acknowledgment

The authors wish to thank T. Metsänkylä and J. P. Buhler for their willingness to provide the elaborated tables of irregular primes.

References

[BCEM] J. Buhler, R. Crandall, R. Ernvall, and T. Metsänkylä, Irregular primes and cyclotomic invariants to four million, Math.Comp.61 (1993), 151-153.

[BCEMS] J. Buhler, R. Crandall, R. Ernvall, T. Metsänkylä, and M. A. Shokrollahi, Irregular primes and cyclotomic invariants to eight million, to appear.

[BCS] J. P. Buhler, R. E. Crandall, and R. W. Sompolski, Irregular primes to one million, Math.Comp.59 (1992), 717-722.

[C] P. Cikánek, Matrices of the Stickelberger ideals mod l for all primes up to 125,000,
Archivum Mathematicum (Brno) 27 a (1991), 3-6.

[S1] L. Skula, A note on the index of irregularity, Journal of Number Theory 22 (1986), 125-138.

[S2] L. Skula, Special invariant subspaces of a vector space over $\mathbf{Z}/l\mathbf{Z}$, Archivum Mathematicum (Brno) 25 (1989), 35-46.

[S3] L. Skula, On a special ideal contained in the Stickelberger ideal, Journal of Number Theory 58 (1996), 173-195.

[TW] J. W. Tanner and S.S.Wagstaff, Jr., New congruences for the Bernoulli numbers, Math.Comp. 48 (1987), 341-350.

[Wg] S. S. Wagstaff, Jr., The irregular primes to 125,000, Math. Comp. 32 (1978), 583-591.

[Ws] L. C. Washington, Introduction to Cyclotomic Fields, Second Edition, Springer, 1997.

Author's address: David Jedelský, Department of Mathematics, University of Ostrava, Bráfova 7, 701 03 Ostrava 1, Czech Republic

E-mail: jedelsky@vsb.cz

Ladislav Skula, Department of Applied Mathematics, Masaryk University, Janáčkovo nám. 2a, 662 95 Brno, Czech Republic

E-mail: skula@math.muni.cz,

Received: September 10, 1999