ESSENTIAL KUMMER'S VECTORS

Zbyněk Uher

Abstract. In this paper Kummer's elements in the Stickelberger ideal of the group ring of the Galois group of the extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ over the ring of rational integers are studied. A special linear operator is constructed for better understanding to these elements, and Kummer's elements are mapped to Kummer's vectors. Then one computational method is presented and the coherence between its results and the property of being essential for Kummer's vectors is shown.

1. Notation and motivation

Through this paper we denote by:

l — the odd prime, $N = \frac{l-1}{2}$,

$i(l)$ — index of irregularity of the prime l,
i.e. $i(l) = \text{card } 1 \leqslant i \leqslant \frac{l-3}{2}, i \in \mathbb{Z} : l | B_{2i}\}$, where B_{2i} mean the Bernoulli numbers,

r — a primitive root modulo l,

r_i — the integer $(i \in \mathbb{Z})$, $1 \leqslant r_i \leqslant l-1$, $r_i \equiv r^i \pmod{l}$,

ind x — index of x relative to the primitive root r $(x \in \mathbb{Z}, l \nmid x)$,

$\zeta = e^{\frac{2\pi i}{l}}$ — l-th root of unity,

h^- — the first factor of the class number of $\mathbb{Q}(\zeta)$,

$G = \{1, s, s^2, \dots, s^{l-2}\}$ — the Galois group of the extension $\mathbb{Q}(\zeta)/\mathbb{Q}$, where $s(\zeta) = \zeta^r$,

Received: 8.10.2002.

The author was financially supported by the Grant Agency of the Czech Republic, grant 201/01/0471.

$R = \mathbb{Z}[G] = \{\sum_i a_i s^i \mid a_i \in \mathbb{Z}\}$ — the group ring of G over the ring $\mathbb{Z}$,

$I = \{\alpha \in R \mid \exists \varrho \in R : \varrho \cdot \sum_i r_{-i} s^i = l \cdot \alpha\}$ — the Stickelberger ideal of the ring R,

$R^\star = \{\alpha \in R \mid (1 + s^N)\alpha \in \mathbb{Z} \cdot \sum_i s^i\}$,

$$R^- = \{\alpha = \sum_i a_i s^i \in R \mid \forall k \in \mathbb{Z} : a_k + a_{k+N} = 0\} = \{\alpha \in R \mid \alpha(1 + s^N) = 0\},$$

$I^- = I \cap R^-$ — the Stickelberger ideal of the ring R^-.

The study of the quotient-rings of the type R/I was begun by K. Iwasawa [1], who proved the following class number formula:

$$[R^- : I^-] = h^-$$

(original results deal with the l^{n+1}-th cyclotomic field (n is a non-negative integer) but applications in this paper concern only the case of the l-th cyclotomic field).

W. Sinnott [3] extended this formula to a general cyclotomic field and transfered it for the case of the Stickelberger ideal:

$$[R^\star : I] = h^-$$

(originally more general case — l^{n+1}-th cyclotomic field).

L. Skula [4] investigated the Stickelberger ideal $I(l)$ (mod l) in the group ring $R(l) = (\mathbb{Z}/l\mathbb{Z})[G]$ and proved that

$$[R^-(l) : I^-(l)] = l^{i(l)},$$
$$\dim I^-(l) = N - i(l).$$

The property of annihilation of elements of the Stickelberger ideal in the class group of the field $\mathbb{Q}(\zeta)$ really originates from E. E. Kummer [2]: for $i, \varrho \in \mathbb{Z}$ put

$$\kappa_{i,\varrho} = \begin{cases} 1 & \text{if } r_i + r_{i+\varrho} \geqslant l, \\ 0 & \text{if } r_i + r_{i+\varrho} < l, \end{cases}$$

and denote

$$\kappa_\varrho = \sum_{i=0}^{l-2} \kappa_{-i,\varrho} s^i \in R, \qquad \kappa_N = \delta = \sum_{i=0}^{l-2} s^i \in R.$$

These elements will be referred to as *Kummer's elements.* Kummer proved that they act trivially in the class group of l–th cyclotomic field.

Kummer's elements κ_ϱ are contained in the Stickelberger ideal I and L. Skula [5] proved the following statement:

THEOREM 1.1 (Skula). *Kummer's elements*

$$\kappa_{\mathrm{ind}(j+1)} \quad (0 \leqslant j \leqslant N-1), \quad \kappa_N = \delta$$

form a basis of the $\mathbb{Z}$*-module* I.

The goal of this work is to describe those of Kummer's elements which must be contained in every basis of I (considered as a module over the ring of rational integers $\mathbb{Z}$). A linear operator $\mathcal{F}$ is used for better understanding to Kummer's elements κ_ϱ. Therefore we will denote:

NOTATION 1.2.

$\mathbb{V} = \{(v_1, \dots, v_N) \mid v_i \in \mathbb{Z}/l\mathbb{Z}\}$ — the vector space over the field $\mathbb{Z}/l\mathbb{Z}$ with operations componentwise,

$$p(y,x) = \begin{cases} 1 & \text{if } \exists k \in \mathbb{N} \cup \{0\} : \frac{k}{y} l < x < \frac{k+1}{y+1} l \\ 0 & \text{if } \exists k \in \mathbb{N} \cup \{0\} : \frac{k+1}{y+1} l < x < \frac{k+1}{y} l \end{cases} \quad \text{for integers } 1 \leqslant y, x \leqslant N,$$

$\boldsymbol{p}(y) = (p(y,1), p(y,2), \dots, p(y,N)) \in \mathbb{V}$ — *Kummer's vector,*

$\mathcal{P} = [\,p(y,x)]_{1 \leqslant y,x \leqslant N}$ — the matrix of Kummer's vectors,

$r(l)$ — rank of $\mathcal{P}$ over the field $\mathbb{Z}/l\mathbb{Z}$.

REMARK 1.3. It is easy to see that for $1 \leqslant y, x \leqslant N$, $k \in \mathbb{N} \cup \{0\}$ hold $\frac{k}{y} < \frac{k+1}{y+1}$, $\frac{k+1}{y+1} < \frac{k+1}{y}$, and $\frac{k}{y} l \neq x \neq \frac{k+1}{y+1} l$ (it means that the definition of $p(y,x)$ is correct). Further we can show that $p(y,x) = 1 + \left[\frac{yx}{l}\right] - \left[\frac{(y+1)x}{l}\right]$, where $[q]$ denotes the integral part of the rational number q. This expression will be useful in proofs at the end of this paper.

Vectors $\boldsymbol{p}(1), \boldsymbol{p}(2), \dots, \boldsymbol{p}(N)$ generate the subspace $\mathbb{S}$ (*the Stickelberger subspace*) in $\mathbb{V}$.

Let $\alpha = \sum_i a_i s^i \in \overline{R}^-$, where $\overline{R}^-$ is the minus part of the group ring $\overline{R}$ of the group G over the ring of l-adic integers $\overline{\mathbb{Z}}$. According to [4] let us put

$$\mathcal{F}(\alpha) = (v_1, \dots, v_N) \in \mathbb{V}, \; \textit{where } a_i \in v_t \in \mathbb{Z}/l\mathbb{Z}, \; 1 \leqslant t \leqslant N, \; t = r_{-i}.$$

Then $\mathcal{F}$ is the linear operator from $\overline{\mathbf{Z}}$-module $\overline{R}^-$ to the vector space $\mathbb{V}$, and $\mathbb{S} = \mathcal{F}(\overline{I}^-)$, where $\overline{I}^-$ is the Stickelberger ideal of the ring $\overline{R}^-$. We have

$$\mathcal{F}(\delta - 2\kappa_{\operatorname{ind} y}) = 2\,\boldsymbol{p}(y) - \varepsilon,$$

where $\varepsilon = (1, \ldots, 1) \in \mathbb{V}$. Therefore [4]:

$$r(l) + i(l) = N,$$

resp.

$$(*) \qquad \dim \mathbb{S} = N - i(l) = r(l),$$

and our goal is now reduced to the description of those Kummer's vectors which cannot be skipped in the generation of $\mathbb{S}$.

DEFINITION 1.4. Kummer's vector $\boldsymbol{p}(y_0)$ $(1 \leqslant y_0 \leqslant N)$ is said to be *essential* if $\mathbb{S} \neq \mathbb{S}(y_0)$, where $\mathbb{S}(y_0)$ is the subspace in $\mathbb{V}$ generated by vectors $\boldsymbol{p}(y)$, $1 \leqslant y \leqslant N$ and $y \neq y_0$.

REMARK 1.5. The regular prime l and $(*)$ implies the essentiality of all Kummer's vectors.

2. Computational method

One method of computation of essential Kummer's vectors for irregular primes smaller than 5000 will be shown here. Thanks to these results some hypothesis could be formulated and proved. The visualization of the matrix consisting of Kummer's vectors was useful specially for finding right ways in proofs.

NOTATION 2.1. In this Section we will denote by:

m, n — fixed positive integers,

V — a vector space,

$\boldsymbol{p}_i = (p_{i1}, \ldots, p_{im})$, $\mathbf{0} = (0, \ldots, 0)$ — vectors from V,

$\sum_{i=1}^{n} x_i \boldsymbol{p}_i = \mathbf{0}$ — system (A) of linear homogeneous equations with $\boldsymbol{X} = (x_1, \ldots, x_n)^T$ as a vector of variables.

k — rank of (A),

$\{\varphi_i = (x_1^{(i)}, \ldots, x_n^{(i)})^T \mid i = 1, \ldots, k\}$ — fundamental system of (A).

The vector $\boldsymbol{p}_j$ ($j \in \{1, \dots, n\}$) is said to be *necessary* if scalars x_i ($i \in \{1, \dots, j-1, j+1, \dots, n\}$) holding $\boldsymbol{p}_j = \sum_{j \neq i=1}^{n} x_i \boldsymbol{p}_i$ do not exist.

PROPOSITION 2.2. *The vector $\boldsymbol{p}_j$ is necessary if and only if $x_j^{(1)} = \cdots = x_j^{(k)} = 0$.*

PROOF. I. Suppose $1 \leqslant k' \leqslant k$, $x_j^{(k')} \neq 0$. Since $\boldsymbol{X} = \varphi_{k'}$ is the solution of (A), we have $\sum_{i=1}^{n} x_i^{(k')} \boldsymbol{p}_i = \boldsymbol{0}$, hence $\boldsymbol{p}_j = \sum_{j \neq i=1}^{n} \left(-\frac{x_i^{(k')}}{x_j^{(k')}}\right) \boldsymbol{p}_i$, and therefore $\boldsymbol{p}_j$ is not necessary.

II. Suppose $\boldsymbol{p}_j = \sum_{j \neq i=1}^{n} x_i \boldsymbol{p}_i$. Then $\boldsymbol{X} = (x_1, \dots, x_{j-1}, -1, x_{j+1}, \dots, x_n)^T$ is the solution of (A), which completes the proof.

Put $V = \mathbb{V}$. The essentiality of Kummer's vector is exactly the same property as the necessity of the vector $\boldsymbol{p}_j$. Proposition 2.2 leads us to the method of computation of essential Kummer's vectors — we must find the fundamental system of $\mathcal{P}^T \boldsymbol{X} = \boldsymbol{0}^T$, where $\mathcal{P}$ is the matrix of Kummer's vectors. We could use `matker`($\mathcal{P}^T$), resp. more effective `ker_mod_p`($\mathcal{P}^T$, *prime* l) due to $\mathbb{V}$ (is over field $\mathbb{Z}/l\mathbb{Z}$) for solving this system in GP/PARI [1)].

A table of essential Kummer's vectors gained in this way is added as an appendix. One visualization of matrix $\mathcal{P}$ is included as well.

3. Essential Kummer's Vectors

We will describe some requirements for Kummer's vectors in order to be essential. It will give us the condition under which the vector has to be contained in every set of generators of the Stickelberger subspace $\mathbb{S}$ in $\mathbb{V}$. But still there are vectors (e.g. $\boldsymbol{p}(84)$ for prime $l = 263$) for which we have no general rule for describing their essentiality.

THEOREM 3.1. *Vectors $\boldsymbol{p}(\frac{l-1}{2})$, $\boldsymbol{p}(\frac{l-1}{3})$, $\boldsymbol{p}(\frac{l-2}{3})$, $\boldsymbol{p}(\frac{l-1}{4})$, $\boldsymbol{p}(\frac{l-3}{4})$, $\boldsymbol{p}(\frac{l-1}{6})$, and $\boldsymbol{p}(\frac{l-5}{6})$ are essential if $\frac{l-1}{3}$, $\frac{l-2}{3}$, $\frac{l-1}{4}$, $\frac{l-3}{4}$, $\frac{l-1}{6}$, resp. $\frac{l-5}{6}$ are integers.*

PROOF. It is not hard to show that $p(\frac{l-1}{2}, 1) = 1$, $p(\frac{l-1}{2}, 2) = 0$, and $p(y, 1) = p(y, 2) = 1$ for $1 \leqslant y < \frac{l-1}{2}$. This is the reason for $\boldsymbol{p}(\frac{l-1}{2})$ to be essential. Arguments for other Kummer's vectors from Theorem are similar — consider $p(\frac{l-1}{3}, 1)$ and $p(\frac{l-1}{3}, 3)$, $p(\frac{l-2}{3}, 1)$ and $p(\frac{l-2}{3}, 3)$, $p(\frac{l-1}{4}, 1)$ and

1) HW: AMD Duron 1.2 GHz, 256 MB RAM; computing time: $l \sim 100$ — seconds, $l \sim 5000$ — hours

$p(\frac{l-1}{4}, 4)$, $p(\frac{l-3}{4}, 1)$ and $p(\frac{l-3}{4}, 4)$, $p(\frac{l-1}{6}, 1)$ and $p(\frac{l-1}{6}, 6)$, resp. $p(\frac{l-5}{6}, 1)$ and $p(\frac{l-5}{6}, 6)$.

COROLLARY 3.2. *There are at least four essential Kummer's vectors for every irregular prime.*

PROOF. Prime l is the odd integer. Thus number $\frac{l-1}{2}$ together with just one from each of pairs $\frac{l-1}{3}$ and $\frac{l-2}{3}$, $\frac{l-1}{4}$ and $\frac{l-3}{4}$, $\frac{l-1}{6}$ and $\frac{l-5}{6}$ are integers.

References

[1] K. Iwasawa, *A class number formula for cyclotomic fields*, Ann. of Math. **76** (1962), 171–179.

[2] E. E. Kummer, *Über die Zerlegung der aus Wurzeln der Einheit gebildeten complexen Zahlen in ihre Primfactoren*, J. Reine Angew. Math. **35** (1847), 327–367 (Coll. Papers I, 211–251).

[3] W. Sinnott, *On the Stickelberger ideal and the circular units of an abelian field*, In: Invent. Math. **62** (1980), Springer, Berlin–New York, 181–234.

[4] L. Skula, *A note on the index of irregularity*, J. Number Theory **22** (1986), 125–138.

[5] L. Skula, *Some bases of the Stickelberger ideal*, Math. Slovaca **43** (1993), 541–571.

Appendix

A1. Essential Kummer's vectors, index of irregularity 1

Prime l	$p(\frac{l-1}{2})$	$p(\frac{l-1}{3})$	$p(\frac{l-1}{4})$	$p(\frac{l-1}{6})$	$p(\frac{l-2}{3})$	$p(\frac{l-3}{4})$	$p(\frac{l-5}{6})$	"Others"
37	$p(18)$	$p(12)$	$p(9)$	$p(6)$				
59	$p(29)$				$p(19)$	$p(14)$	$p(9)$	
67	$p(33)$	$p(22)$		$p(11)$		$p(16)$		
101	$p(50)$		$p(25)$		$p(33)$		$p(16)$	
103	$p(51)$	$p(34)$		$p(17)$		$p(25)$		
131	$p(65)$				$p(43)$	$p(32)$	$p(21)$	
149	$p(74)$		$p(37)$		$p(49)$		$p(24)$	
233	$p(116)$		$p(58)$		$p(77)$		$p(38)$	
257	$p(128)$		$p(64)$		$p(85)$		$p(42)$	
263	$p(131)$				$p(87)$	$p(65)$	$p(43)$	$p(84)$
271	$p(135)$	$p(90)$		$p(45)$		$p(67)$		$p(118)$
283	$p(141)$	$p(94)$		$p(47)$		$p(70)$		
293	$p(146)$		$p(73)$		$p(97)$		$p(48)$	
311	$p(155)$				$p(103)$	$p(77)$	$p(51)$	
347	$p(173)$				$p(115)$	$p(86)$	$p(57)$	

Prime l	$p\left(\frac{l-1}{2}\right)$	$p\left(\frac{l-1}{3}\right)$	$p\left(\frac{l-1}{4}\right)$	$p\left(\frac{l-1}{6}\right)$	$p\left(\frac{l-2}{3}\right)$	$p\left(\frac{l-3}{4}\right)$	$p\left(\frac{l-5}{6}\right)$	"Others"
389	$p(194)$		$p(97)$		$p(129)$		$p(64)$	
401	$p(200)$		$p(100)$		$p(133)$		$p(66)$	
409	$p(204)$	$p(136)$	$p(102)$	$p(68)$				
421	$p(210)$	$p(140)$	$p(105)$	$p(70)$				$p(183)$, $p(205)$
433	$p(216)$	$p(144)$	$p(108)$	$p(72)$				
461	$p(230)$		$p(115)$		$p(153)$		$p(76)$	
463	$p(231)$	$p(154)$		$p(77)$		$p(115)$		$p(136)$, $p(201)$
523	$p(261)$	$p(174)$		$p(87)$		$p(130)$		
541	$p(270)$	$p(180)$	$p(135)$	$p(90)$				$p(208)$
557	$p(278)$		$p(139)$		$p(185)$		$p(92)$	
577	$p(288)$	$p(192)$	$p(144)$	$p(96)$				
593	$p(296)$		$p(148)$		$p(197)$		$p(98)$	
607	$p(303)$	$p(202)$		$p(101)$		$p(151)$		
613	$p(306)$	$p(204)$	$p(153)$	$p(102)$				
619	$p(309)$	$p(206)$		$p(103)$		$p(154)$		
653	$p(326)$		$p(163)$		$p(217)$		$p(108)$	
659	$p(329)$				$p(219)$	$p(164)$	$p(109)$	$p(100)$
677	$p(338)$		$p(169)$		$p(225)$		$p(112)$	
683	$p(341)$				$p(227)$	$p(170)$	$p(113)$	$p(49)$
727	$p(363)$	$p(242)$		$p(121)$		$p(181)$		$p(81)$, $p(258)$
751	$p(375)$	$p(250)$		$p(125)$		$p(187)$		
757	$p(378)$	$p(252)$	$p(189)$	$p(126)$				
761	$p(380)$		$p(190)$		$p(253)$		$p(126)$	
773	$p(386)$		$p(193)$		$p(257)$		$p(128)$	
797	$p(398)$		$p(199)$		$p(265)$		$p(132)$	
811	$p(405)$	$p(270)$		$p(135)$		$p(202)$		
821	$p(410)$		$p(205)$		$p(273)$		$p(136)$	
827	$p(413)$				$p(275)$	$p(206)$	$p(137)$	
839	$p(419)$				$p(279)$	$p(209)$	$p(139)$	$p(408)$
877	$p(438)$	$p(292)$	$p(219)$	$p(146)$				
881	$p(440)$		$p(220)$		$p(293)$		$p(146)$	
887	$p(443)$				$p(295)$	$p(221)$	$p(147)$	
953	$p(476)$		$p(238)$		$p(317)$		$p(158)$	
971	$p(485)$				$p(323)$	$p(242)$	$p(161)$	$p(345)$, $p(365)$
1061	$p(530)$		$p(265)$		$p(353)$		$p(176)$	

Prime l	$p\left(\frac{l-1}{2}\right)$	$p\left(\frac{l-1}{3}\right)$	$p\left(\frac{l-1}{4}\right)$	$p\left(\frac{l-1}{6}\right)$	$p\left(\frac{l-2}{3}\right)$	$p\left(\frac{l-3}{4}\right)$	$p\left(\frac{l-5}{6}\right)$	"Others"
1091	$p(545)$				$p(363)$	$p(272)$	$p(181)$	
1117	$p(558)$	$p(372)$	$p(279)$	$p(186)$				
1129	$p(564)$	$p(376)$	$p(282)$	$p(188)$				
1153	$p(576)$	$p(384)$	$p(288)$	$p(192)$				$p(6)$, $p(196)$
1193	$p(596)$		$p(298)$		$p(397)$		$p(198)$	
1201	$p(600)$	$p(400)$	$p(300)$	$p(200)$				$p(4)$, $p(393)$, $p(398)$, $p(457)$
1229	$p(614)$		$p(307)$		$p(409)$		$p(204)$	
1237	$p(618)$	$p(412)$	$p(309)$	$p(206)$				
1279	$p(639)$	$p(426)$		$p(213)$		$p(319)$		
1283	$p(641)$				$p(427)$	$p(320)$	$p(213)$	$p(82)$
1301	$p(650)$		$p(325)$		$p(433)$		$p(216)$	
1319	$p(659)$				$p(439)$	$p(329)$	$p(219)$	
1327	$p(663)$	$p(442)$		$p(221)$		$p(331)$		$p(85)$
1367	$p(683)$				$p(455)$	$p(341)$	$p(227)$	
1409	$p(704)$		$p(352)$		$p(469)$		$p(234)$	$p(299)$, $p(685)$
1429	$p(714)$	$p(476)$	$p(357)$	$p(238)$				$p(228)$
1439	$p(719)$				$p(479)$	$p(359)$	$p(239)$	$p(152)$, $p(578)$
1483	$p(741)$	$p(494)$		$p(247)$		$p(370)$		
1499	$p(749)$				$p(499)$	$p(374)$	$p(249)$	
1523	$p(761)$				$p(507)$	$p(380)$	$p(253)$	$p(610)$
1559	$p(779)$				$p(519)$	$p(389)$	$p(259)$	$p(640)$
1609	$p(804)$	$p(536)$	$p(402)$	$p(268)$				
1613	$p(806)$		$p(403)$		$p(537)$		$p(268)$	
1619	$p(809)$				$p(539)$	$p(404)$	$p(269)$	
1621	$p(810)$	$p(540)$	$p(405)$	$p(270)$				
1637	$p(818)$		$p(409)$		$p(545)$		$p(272)$	
1663	$p(831)$	$p(554)$		$p(277)$		$p(415)$		$p(19)$, $p(525)$, $p(815)$, $p(830)$
1721	$p(860)$		$p(430)$		$p(573)$		$p(286)$	
1753	$p(876)$	$p(584)$	$p(438)$	$p(292)$				
1759	$p(879)$	$p(586)$		$p(293)$		$p(439)$		
1777	$p(888)$	$p(592)$	$p(444)$	$p(296)$				$p(271)$
1787	$p(893)$				$p(595)$	$p(446)$	$p(297)$	
1831	$p(915)$	$p(610)$		$p(305)$		$p(457)$		$p(712)$
1871	$p(935)$				$p(623)$	$p(467)$	$p(311)$	
1879	$p(939)$	$p(626)$		$p(313)$		$p(469)$		

Prime l	$p\left(\frac{l-1}{2}\right)$	$p\left(\frac{l-1}{3}\right)$	$p\left(\frac{l-1}{4}\right)$	$p\left(\frac{l-1}{6}\right)$	$p\left(\frac{l-2}{3}\right)$	$p\left(\frac{l-3}{4}\right)$	$p\left(\frac{l-5}{6}\right)$	"Others"
1889	$p(944)$		$p(472)$		$p(629)$		$p(314)$	
1901	$p(950)$		$p(475)$		$p(633)$		$p(316)$	
1951	$p(975)$	$p(650)$		$p(325)$		$p(487)$		$p(737)$
1979	$p(989)$				$p(659)$	$p(494)$	$p(329)$	$p(372)$
1987	$p(993)$	$p(662)$		$p(331)$		$p(496)$		$p(565)$
1993	$p(996)$	$p(664)$	$p(498)$	$p(332)$				
2017	$p(1008)$	$p(672)$	$p(504)$	$p(336)$				
2039	$p(1019)$				$p(679)$	$p(509)$	$p(339)$	$p(749)$
2053	$p(1026)$	$p(684)$	$p(513)$	$p(342)$				$p(571)$, $p(842)$
2099	$p(1049)$				$p(699)$	$p(524)$	$p(349)$	
2111	$p(1055)$				$p(703)$	$p(527)$	$p(351)$	$p(610)$
2137	$p(1068)$	$p(712)$	$p(534)$	$p(356)$				
2143	$p(1071)$	$p(714)$		$p(357)$		$p(535)$		
2153	$p(1076)$		$p(538)$		$p(717)$		$p(358)$	$p(348)$
2213	$p(1106)$		$p(553)$		$p(737)$		$p(368)$	
2239	$p(1119)$	$p(746)$		$p(373)$		$p(559)$		
2267	$p(1133)$				$p(755)$	$p(566)$	$p(377)$	
2293	$p(1146)$	$p(764)$	$p(573)$	$p(382)$				
2357	$p(1178)$		$p(589)$		$p(785)$		$p(392)$	$p(906)$
2377	$p(1188)$	$p(792)$	$p(594)$	$p(396)$				$p(50)$, $p(343)$, $p(759)$
2381	$p(1190)$		$p(595)$		$p(793)$		$p(396)$	
2389	$p(1194)$	$p(796)$	$p(597)$	$p(398)$				
2411	$p(1205)$				$p(803)$	$p(602)$	$p(401)$	
2503	$p(1251)$	$p(834)$		$p(417)$		$p(625)$		
2543	$p(1271)$				$p(847)$	$p(635)$	$p(423)$	
2557	$p(1278)$	$p(852)$	$p(639)$	$p(426)$				$p(628)$
2579	$p(1289)$				$p(859)$	$p(644)$	$p(429)$	
2621	$p(1310)$		$p(655)$		$p(873)$		$p(436)$	
2633	$p(1316)$		$p(658)$		$p(877)$		$p(438)$	$p(480)$
2647	$p(1323)$	$p(882)$		$p(441)$		$p(661)$		
2657	$p(1328)$		$p(664)$		$p(885)$		$p(442)$	
2663	$p(1331)$				$p(887)$	$p(665)$	$p(443)$	
2689	$p(1344)$	$p(896)$	$p(672)$	$p(448)$				
2753	$p(1376)$		$p(688)$		$p(917)$		$p(458)$	$p(1327)$
2767	$p(1383)$	$p(922)$		$p(461)$		$p(691)$		$p(292)$

Prime l	$p\left(\frac{l-1}{2}\right)$	$p\left(\frac{l-1}{3}\right)$	$p\left(\frac{l-1}{4}\right)$	$p\left(\frac{l-1}{6}\right)$	$p\left(\frac{l-2}{3}\right)$	$p\left(\frac{l-3}{4}\right)$	$p\left(\frac{l-5}{6}\right)$	"Others"
2777	$p(1388)$		$p(694)$		$p(925)$		$p(462)$	
2791	$p(1395)$	$p(930)$		$p(465)$		$p(697)$		
2833	$p(1416)$	$p(944)$	$p(708)$	$p(472)$				
2857	$p(1428)$	$p(952)$	$p(714)$	$p(476)$				
2861	$p(1430)$		$p(715)$		$p(953)$		$p(476)$	$p(345)$, $p(675)$, $p(1233)$
2927	$p(1463)$				$p(975)$	$p(731)$	$p(487)$	
2999	$p(1499)$				$p(999)$	$p(749)$	$p(499)$	
3011	$p(1505)$				$p(1003)$	$p(752)$	$p(501)$	
3023	$p(1511)$				$p(1007)$	$p(755)$	$p(503)$	
3049	$p(1524)$	$p(1016)$	$p(762)$	$p(508)$				
3061	$p(1530)$	$p(1020)$	$p(765)$	$p(510)$				
3083	$p(1541)$				$p(1027)$	$p(770)$	$p(513)$	
3089	$p(1544)$		$p(772)$		$p(1029)$		$p(514)$	
3119	$p(1559)$				$p(1039)$	$p(779)$	$p(519)$	$p(51)$
3181	$p(1590)$	$p(1060)$	$p(795)$	$p(530)$				$p(34)$, $p(396)$
3203	$p(1601)$				$p(1067)$	$p(800)$	$p(533)$	
3221	$p(1610)$		$p(805)$		$p(1073)$		$p(536)$	
3229	$p(1614)$	$p(1076)$	$p(807)$	$p(538)$				
3257	$p(1628)$		$p(814)$		$p(1085)$		$p(542)$	$p(136)$, $p(360)$
3313	$p(1656)$	$p(1104)$	$p(828)$	$p(552)$				
3323	$p(1661)$				$p(1107)$	$p(830)$	$p(553)$	
3329	$p(1664)$		$p(832)$		$p(1109)$		$p(554)$	
3433	$p(1716)$	$p(1144)$	$p(858)$	$p(572)$				
3469	$p(1734)$	$p(1156)$	$p(867)$	$p(578)$				
3491	$p(1745)$				$p(1163)$	$p(872)$	$p(581)$	$p(185)$
3529	$p(1764)$	$p(1176)$	$p(882)$	$p(588)$				$p(267)$, $p(460)$
3581	$p(1790)$		$p(895)$		$p(1193)$		$p(596)$	$p(1170)$
3583	$p(1791)$	$p(1194)$		$p(597)$		$p(895)$		$p(1017)$
3607	$p(1803)$	$p(1202)$		$p(601)$		$p(901)$		$p(92)$
3613	$p(1806)$	$p(1204)$	$p(903)$	$p(602)$				$p(1011)$
3631	$p(1815)$	$p(1210)$		$p(605)$		$p(907)$		$p(1434)$
3671	$p(1835)$				$p(1223)$	$p(917)$	$p(611)$	$p(804)$
3677	$p(1838)$		$p(919)$		$p(1225)$		$p(612)$	$p(548)$
3697	$p(1848)$	$p(1232)$	$p(924)$	$p(616)$				
3779	$p(1889)$				$p(1259)$	$p(944)$	$p(629)$	

Prime l	$p\left(\frac{l-1}{2}\right)$	$p\left(\frac{l-1}{3}\right)$	$p\left(\frac{l-1}{4}\right)$	$p\left(\frac{l-1}{6}\right)$	$p\left(\frac{l-2}{3}\right)$	$p\left(\frac{l-3}{4}\right)$	$p\left(\frac{l-5}{6}\right)$	"Others"
3797	$p(1898)$		$p(949)$		$p(1265)$		$p(632)$	$p(1656)$, $p(1659)$
3821	$p(1910)$		$p(955)$		$p(1273)$		$p(636)$	
3853	$p(1926)$	$p(1284)$	$p(963)$	$p(642)$				
3917	$p(1958)$		$p(979)$		$p(1305)$		$p(652)$	
3967	$p(1983)$	$p(1322)$		$p(661)$		$p(991)$		$p(288)$, $p(768)$
3989	$p(1994)$		$p(997)$		$p(1329)$		$p(664)$	$p(110)$
4001	$p(2000)$		$p(1000)$		$p(1333)$		$p(666)$	$p(290)$, $p(1215)$
4021	$p(2010)$	$p(1340)$	$p(1005)$	$p(670)$				$p(1702)$
4027	$p(2013)$	$p(1342)$		$p(671)$		$p(1006)$		$p(1481)$
4049	$p(2024)$		$p(1012)$		$p(1349)$		$p(674)$	$p(820)$
4051	$p(2025)$	$p(1350)$		$p(675)$		$p(1012)$		$p(938)$
4073	$p(2036)$		$p(1018)$		$p(1357)$		$p(678)$	
4129	$p(2064)$	$p(1376)$	$p(1032)$	$p(688)$				
4219	$p(2109)$	$p(1406)$		$p(703)$		$p(1054)$		$p(494)$
4261	$p(2130)$	$p(1420)$	$p(1065)$	$p(710)$				$p(1484)$
4339	$p(2169)$	$p(1446)$		$p(723)$		$p(1084)$		
4349	$p(2174)$		$p(1087)$		$p(1449)$		$p(724)$	
4421	$p(2210)$		$p(1105)$		$p(1473)$		$p(736)$	$p(614)$
4457	$p(2228)$		$p(1114)$		$p(1485)$		$p(742)$	
4493	$p(2246)$		$p(1123)$		$p(1497)$		$p(748)$	$p(383)$, $p(2208)$
4519	$p(2259)$	$p(1506)$		$p(753)$		$p(1129)$		
4523	$p(2261)$				$p(1507)$	$p(1130)$	$p(753)$	$p(1587)$
4561	$p(2280)$	$p(1520)$	$p(1140)$	$p(760)$				$p(1307)$, $p(1618)$
4637	$p(2318)$		$p(1159)$		$p(1545)$		$p(772)$	
4639	$p(2319)$	$p(1546)$		$p(773)$		$p(1159)$		$p(1242)$, $p(2016)$
4679	$p(2339)$				$p(1559)$	$p(1169)$	$p(779)$	$p(1741)$
4691	$p(2345)$				$p(1563)$	$p(1172)$	$p(781)$	
4751	$p(2375)$				$p(1583)$	$p(1187)$	$p(791)$	$p(2275)$
4783	$p(2391)$	$p(1594)$		$p(797)$		$p(1195)$		$p(279)$, $p(764)$, $p(1708)$, $p(2270)$
4793	$p(2396)$		$p(1198)$		$p(1597)$		$p(798)$	$p(720)$, $p(1663)$, $p(1703)$
4813	$p(2406)$	$p(1604)$	$p(1203)$	$p(802)$				
4861	$p(2430)$	$p(1620)$	$p(1215)$	$p(810)$				
4889	$p(2444)$		$p(1222)$		$p(1629)$		$p(814)$	$p(1447)$
4903	$p(2451)$	$p(1634)$		$p(817)$		$p(1225)$		
4909	$p(2454)$	$p(1636)$	$p(1227)$	$p(818)$				$p(1807)$

Prime l	$p\left(\frac{l-1}{2}\right)$	$p\left(\frac{l-1}{3}\right)$	$p\left(\frac{l-1}{4}\right)$	$p\left(\frac{l-1}{6}\right)$	$p\left(\frac{l-2}{3}\right)$	$p\left(\frac{l-3}{4}\right)$	$p\left(\frac{l-5}{6}\right)$	"Others"
3797	$p(1898)$		$p(949)$		$p(1265)$		$p(632)$	$p(1656)$, $p(1659)$
3821	$p(1910)$		$p(955)$		$p(1273)$		$p(636)$	
4943	$p(2471)$				$p(1647)$	$p(1235)$	$p(823)$	
4957	$p(2478)$	$p(1652)$	$p(1239)$	$p(826)$				
4969	$p(2484)$	$p(1656)$	$p(1242)$	$p(828)$				
4973	$p(2486)$		$p(1243)$		$p(1657)$		$p(828)$	

A2. Essential Kummer's vectors, index of irregularity 2

Prime l	$p\left(\frac{l-1}{2}\right)$	$p\left(\frac{l-1}{3}\right)$	$p\left(\frac{l-1}{4}\right)$	$p\left(\frac{l-1}{6}\right)$	$p\left(\frac{l-2}{3}\right)$	$p\left(\frac{l-3}{4}\right)$	$p\left(\frac{l-5}{6}\right)$	"Others"
3797	$p(1898)$		$p(949)$		$p(1265)$		$p(632)$	$p(1656)$, $p(1659)$
3821	$p(1910)$		$p(955)$		$p(1273)$		$p(636)$	
157	$p(78)$	$p(52)$	$p(39)$	$p(26)$				
353	$p(176)$		$p(88)$		$p(117)$		$p(58)$	
379	$p(189)$	$p(126)$		$p(63)$		$p(94)$		
467	$p(233)$				$p(155)$	$p(116)$	$p(77)$	
547	$p(273)$	$p(182)$		$p(91)$		$p(136)$		
587	$p(293)$				$p(195)$	$p(146)$	$p(97)$	
631	$p(315)$	$p(210)$		$p(105)$		$p(157)$		
673	$p(336)$	$p(224)$	$p(168)$	$p(112)$				
691	$p(345)$	$p(230)$		$p(115)$		$p(172)$		
809	$p(404)$		$p(202)$		$p(269)$		$p(134)$	
929	$p(464)$		$p(232)$		$p(309)$		$p(154)$	
1291	$p(645)$	$p(430)$		$p(215)$		$p(322)$		
1297	$p(648)$	$p(432)$	$p(324)$	$p(216)$				
1307	$p(653)$				$p(435)$	$p(326)$	$p(217)$	
1669	$p(834)$	$p(556)$	$p(417)$	$p(278)$				
1733	$p(866)$		$p(433)$		$p(577)$		$p(288)$	
1789	$p(894)$	$p(596)$	$p(447)$	$p(298)$				
1933	$p(966)$	$p(644)$	$p(483)$	$p(322)$				
1997	$p(998)$		$p(499)$		$p(665)$		$p(332)$	
2003	$p(1001)$				$p(667)$	$p(500)$	$p(333)$	
2087	$p(1043)$				$p(695)$	$p(521)$	$p(347)$	
2273	$p(1136)$		$p(568)$		$p(757)$		$p(378)$	
2309	$p(1154)$		$p(577)$		$p(769)$		$p(384)$	
2371	$p(1185)$	$p(790)$		$p(395)$		$p(592)$		
2383	$p(1191)$	$p(794)$		$p(397)$		$p(595)$		

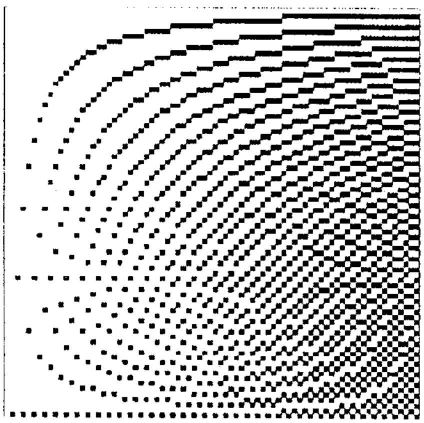
Prime l	$p\left(\frac{l-1}{2}\right)$	$p\left(\frac{l-1}{3}\right)$	$p\left(\frac{l-1}{4}\right)$	$p\left(\frac{l-1}{6}\right)$	$p\left(\frac{l-2}{3}\right)$	$p\left(\frac{l-3}{4}\right)$	$p\left(\frac{l-5}{6}\right)$	"Others"
2423	$p(1211)$				$p(807)$	$p(605)$	$p(403)$	
2441	$p(1220)$		$p(610)$		$p(813)$		$p(406)$	
2591	$p(1295)$				$p(863)$	$p(647)$	$p(431)$	
2671	$p(1335)$	$p(890)$		$p(445)$		$p(667)$		
2789	$p(1394)$		$p(697)$		$p(929)$		$p(464)$	
2909	$p(1454)$		$p(727)$		$p(969)$		$p(484)$	
2957	$p(1478)$		$p(739)$		$p(985)$		$p(492)$	
3391	$p(1695)$	$p(1130)$		$p(565)$		$p(847)$		
3407	$p(1703)$				$p(1135)$	$p(851)$	$p(567)$	
3511	$p(1755)$	$p(1170)$		$p(585)$		$p(877)$		
3517	$p(1758)$	$p(1172)$	$p(879)$	$p(586)$				
3533	$p(1766)$		$p(883)$		$p(1177)$		$p(588)$	
3539	$p(1769)$				$p(1179)$	$p(884)$	$p(589)$	
3559	$p(1779)$	$p(1186)$		$p(593)$		$p(889)$		
3593	$p(1796)$		$p(898)$		$p(1197)$		$p(598)$	
3617	$p(1808)$		$p(904)$		$p(1205)$		$p(602)$	
3637	$p(1818)$	$p(1212)$	$p(909)$	$p(606)$				
3851	$p(1925)$				$p(1283)$	$p(962)$	$p(641)$	
3881	$p(1940)$		$p(970)$		$p(1293)$		$p(646)$	
4157	$p(2078)$		$p(1039)$		$p(1385)$		$p(692)$	
4243	$p(2121)$	$p(1414)$		$p(707)$		$p(1060)$		
4259	$p(2129)$				$p(1419)$	$p(1064)$	$p(709)$	
4409	$p(2204)$		$p(1102)$		$p(1469)$		$p(734)$	
4451	$p(2225)$				$p(1483)$	$p(1112)$	$p(741)$	
4591	$p(2295)$	$p(1530)$		$p(765)$		$p(1147)$		
4663	$p(2331)$	$p(1554)$		$p(777)$		$p(1165)$		

A3. Essential Kummer's vectors, index of irregularity 3

Prime l	$p\left(\frac{l-1}{2}\right)$	$p\left(\frac{l-1}{3}\right)$	$p\left(\frac{l-1}{4}\right)$	$p\left(\frac{l-1}{6}\right)$	$p\left(\frac{l-2}{3}\right)$	$p\left(\frac{l-3}{4}\right)$	$p\left(\frac{l-5}{6}\right)$	"Others"
491	$p(245)$				$p(163)$	$p(122)$	$p(81)$	
617	$p(308)$		$p(154)$		$p(205)$		$p(102)$	
647	$p(323)$				$p(215)$	$p(161)$	$p(107)$	
1151	$p(575)$				$p(383)$	$p(287)$	$p(191)$	
1217	$p(608)$		$p(304)$		$p(405)$		$p(202)$	

Prime l	$p\left(\frac{l-1}{2}\right)$	$p\left(\frac{l-1}{3}\right)$	$p\left(\frac{l-1}{4}\right)$	$p\left(\frac{l-1}{6}\right)$	$p\left(\frac{l-2}{3}\right)$	$p\left(\frac{l-3}{4}\right)$	$p\left(\frac{l-5}{6}\right)$	"Others"
1811	$p(905)$				$p(603)$	$p(452)$	$p(301)$	
1847	$p(923)$				$p(615)$	$p(461)$	$p(307)$	
2939	$p(1469)$				$p(979)$	$p(734)$	$p(489)$	
3833	$p(1916)$		$p(958)$		$p(1277)$		$p(638)$	
4003	$p(2001)$	$p(1334)$		$p(667)$		$p(1000)$		
4657	$p(2328)$	$p(1552)$	$p(1164)$	$p(776)$				
4951	$p(2475)$	$p(1650)$		$p(825)$		$p(1237)$		

A4. Visualization of the matrix $\mathcal{P}$, prime $l = 157$



black points = zeroes
white points = ones

(Visualizations of the matrix $\mathcal{P}$ for all irregular primes smaller than 5000 are available on URL http://www.math.muni.cz/~xuher/KummerViz/KummerViz.html.)

Mathematics Section
Faculty of Science
Masaryk University
Janáčkovo nám. 2a
662-95 Brno
Czech Republic