Approaches to Fermat's Last Theorem and Belyi pairs

Nikolaj Glazunov
(Glushkov Institute of Cybernetics of NASU, Kyiv, Ukraine.)
E-mail: glanm@yahoo.com

To the memory of G.V. Belyi

Plan

We survey results by G.V. Belyi from papers [1, 2, 3]. For papers [2, 3] we discuss their possible extensions. In the early 70s, before entering the postgraduate course to I.R. Shafarevich in 1975, G. Belyi was for some time in Lvov and Kiev, where he worked under the leadership of O.N. Vvedenskii and communicated with his students and colleagues [1]. In particular, G. Belyi met with the author of the abstract and discussed with him the mathematical questions. Along with the Lie algebras of l-adic representations according to J.-P. Serre, on the study of which G. Belyi with V. Korolevich worked on the instructions of O.N. Vvedenskii at that time, he was interested in the development of the methods of the monograph [4] in the direction of Fermat's Last Theorem proof, which was not yet proven at the time. Notes on the Theorem written by G. Belyi's hand will be presented. We present known results on Fermat curves and Belyi pairs and connections between Belyi pairs and p-divisible groups of Jacobians of the Fermat curves. If will sufficient time, I tell about discrete analogue of Belyi pairs, follow to W. Thurston, P. Bowers, K. Stephenson. In our case these analogs are related to the structures defined by the packing of the circles in the metrics $(|x|^p + |y|^p)^{\frac{1}{p}} \leq R > 0,\ p \geq 1$ [6, 7] on triangulated surfaces, within the framework of Grothendieck's theory of Dessins d'Enfants.

1. Belyi Results

Let $\overline{\mathbb{Q}}$ denote the algebraic closure of the field of rational numbers $\mathbb{Q}$.

Inverse problem of Galois theory:

Is every finite group the Galois group of some Galois extension of the field $\mathbb{Q}$?

“ Можно заметить, что во многих случаях существенные трудности при построении расширений K/L с заданной группой Галуа возникают в связи с тем, что в поле L не содержатся некоторые корни из единицы. Поэтому можно предположить, что задача построения таких расширений значительно упростится, если ограничиться случаем, когда L содержит все корни из 1, например, $L = \mathbb{Q}_{ab}$ максимальное абелево расширение поля $\mathbb{Q}$. “(Г. Белый. [2])

“It can be noted that in many cases essential difficulties in constructing extensions K/L with a given Galois group arise due to the fact that in the field L some roots of unity are missing. Therefore, we can assume that the task of constructing of such extensions will be greatly simplified if we restrict ourselves to the case when L contains all roots from 1, for example, $L = \mathbb{Q}_{ab}$ maximal abelian extension of the field $\mathbb{Q}$.”

Let $\mathbb{Q}^c$ be the maximal cyclotomic extension of the field of rational numbers.

G. Belyi's result on conjugacy classes of a finite group.

Let a finite group G be given, which contains three classes $K_1,\ K_2,\ K_3$ of its conjugate elements. such that there are $g_1 \in K_1, g_2 \in K_2, g_3 \in K_3,\ g_1g_2g_3 = 1$, which generate (spawn) the G group and conjugation by elements of $g \in G$ transforms this system into a system with the same properties (rigid system).

Let $\mathbb{F}_q$ be the finite fields with q elements

Example 2. Examples of Galois groups of Galois extensions of the field $\mathbb{Q}^c$.
$GL(n, \mathbb{F}_q) = GL(n, q)$;
$S0(2n+1, q), q \equiv 1 \pmod 2$;
$CSp(2n, q), q \equiv 1 \pmod 2$ and, if $n \equiv 0 \pmod 2$, then $q \neq 9$; (CSp - Finite conformal symplectic group);
$U(n, q), q \equiv 1 \pmod 2$.

Theorem. (Belyi [2, 3]). Let X be a complete non-singular algebraic curve defined over a field of characteristic zero. The following properties are equivalent.
1) There is a finite covering $f : X \to \mathbb{P}^1$ unramified outside $0, 1, \infty$.
2) X is defined over $\overline{\mathbb{Q}}$.
3) There is a subgroup $\Gamma < SL_2(\mathbb{Z})$ of finite index such that X is isomorphic to the quotient of the upper half-plane $\mathbb{H}$ compactified by addind the cusps.

Belyi's theorem has an easy and a hard (2) $\to$ 1)) parts.

But before discussing the Belyi's theorem I want to review some knowledge that G. Belyi has obtained from work with O.N. Vvedenskii, as well as some mathematical interests by G. Belyi before post graduate course at I.R. Shafarevich.

Some G. Belyi Biographic facts

Gennady Belyi was born on February 2, 1951, in Magnitogorsk. Died: January 29, 2001, Vladimir, G. Belyi parents studied in Dnepropetrovsk Institute of Railway Transport Engineers. His parents moved to the Dnepropetrovsk district. In 1968 Gennady Belyi left the Kiev Physics and Mathematics boarding school (at KSU) and entered the Department of Mechanics and Mathematics of Moscow State University. After graduation from 1973 to 1975 he worked in Lvov and in Kiev. At this time he work with O.N. Vvedenskii.

3. Serre Lie algebras of generalized Jacobians

The paper (O.N. Vvedenslii. On local “ class fields ” of elliptic curves,)[5] have presented by O.N. Vvedenslii in 1971 year.
One of main ingredients of the paper is the notion and investigation of the generalized Jacobian.

O.N. Vvedenskii have formulated for G. Belyi and for V. Korolevich next problem:
“ пусть $J_{\mathfrak{m}}$ - обобщенный якобиан эллиптической кривой , определенной над полем k, $\mathfrak{m} = c_1 + \cdots + c_s + \infty$ где ∞ - нуль A, $c_1, \ldots, c_s$ - различные ненулевые точки A, определенные над k, и $T_p(J_{\mathfrak{m}})$ - модуль Тэйта, соответствующий простому числу p;
будет ли алгебра Ли представления ρ группы $G = Gal(\overline{k}/k)$ в $T_p(J_{\mathfrak{m}})$ редуктивной?
Ответ оказывается отрицательным. [1]”

“let $J_{\mathfrak{m}}$ be the generalized Jacobian of the elliptic curve A defined over the field k, $\mathfrak{m} = c_1 + \cdots + c_s + \infty$ is zero A, $c_1, \ldots, c_s$ are different nonzero points of A defined over k, and $T_p(J_{\mathfrak{m}})$ - Tate module corresponding to the prime number p; is the Lie algebra of the representation ρ of the group $G = Gal(\overline{k}/k)$ in $T_p(J_{\mathfrak{m}})$ reductive?
The answer turns out to be negative’. [1]’

Vvedenskii O.N. was my algebra teacher. By the reason I have met with Gennady in these years in Lvov and in Kiev. My first contacts with G. Belyi concerned Lie algebras of elliptic curves.
In 1966-1968 by the leadership of O.N. Vvedenskii I repeated Serre's results on Lie algebras of elliptic curves.

For this I received 3 certificates (university, regional (Lvov) and republican (Kiev)), and also reported these results in 1968 at the seminar of academician A.V. Reuter.

But, of course, G. Belyi (at that date) received incomparably more knowledge and skills from O.N. Vvedenskii.

This knowledge and skills (obtained from O.N. Vvedensky) concerned Galois groups, their l-adic representations, generalized Jacobians of elliptic curves and Lie algebras.

4. Conversations with G. Belyi

It seems to me that G. Belyi (before entering graduate school at Shafarevich) was interested, along with calculating the Lie algebras of generalized Jacobians of elliptic curves, in problems related to the (not yet proven) Fermat theorem. And, perhaps, Fermat's theorem interested G. Belyi then even more.

There are two cases under investigation of Fermat's theorem [4]

$FE:\ x^l + y^l = z^l,\ l \geq 3$, l odd prime number

1) the equation FE has no solution in integers x, y, z not divisible by l.

2) it has no integer solutions in x, y, z, among which one (and only one) is divisible by l.

Belyi, it seems to me, was more interested in the second case, which is not presented in the monograph [4]

Please see the appendix (with Belyi notes to Fermat theorem) to this presentation

My communications to Belyi:

O. Vvedensky at one time (1965-1966) drew my attention to the following articles and results, which may have applications to Fermat's theorem:

Papers by Yves Hellegouarch: connection of Fermat curves and elliptic curves.

l-adic representations of elliptic curves by J.-P. Serre

I communicated about these works to G. Belyi.

Remark 5. Elliptic curves and l-adic representations are important ingredients in Wiles and Wiles&Taylor proof of Fermat's Last Theorem.
It seems that in school of I. Shafarevich have considered the possibility of this approach to Fermat's Last Theorem.

6. Jacobian Variety of Fermat Curves and Belyi pairs

6.1. **Fermat Curves.**

Let $m \geq 3$ be an rational integer.

6.1.1. *Projective models of Fermat Curves over $\mathbb{C}$.*

Example 7. (Demyanenko, Manin)
$PFC_n : X^n + Y^n - Z^n = 0,\ n \geq 3.$

$g = \frac{(n-1)(n-2)}{2}$

$F_4 = F(1, 1, -1) : X^4 + Y^4 - Z^4 = 0.$

The genus of F_4 is equal $g = \frac{3 \times 2}{2} = 3.$

The Jacobian $J(F_4)$ of F_4 is isojenous to the product of 3 elliptic curves

$v^2 = u^3 + 4u;\ u^2 = u^3 + 4u,\ u^2 = u^3 - 4u.$

The genus of $J(F_4)$ is equal 3.

7.0.1. *Affine models of Fermat curves.*

Remark 8. From theorem of Belyi follow that for non-singular algebraic curve C defined over a number field that there exists a morphism, defined over $\mathbb{Q}$:
$\beta : C \to \mathbb{P}^1$

Definition 9. A tuple (C, β) consisting of a non-singular algebraic curve C and a morphism $\beta : C \to \mathbb{P}^1$ that is ramified in at most three points is called a Belyi pair.

Example 10. (Belyi pairs of Fermat curves)
(F_n, β)

$F_n = x^n + y^n = 1, n \geq 3$

Belyi function of F_n is $\beta = x^n$

11. p-DIVICIBLE GROUPS OF FERMAT CURVES

Here we follpw to Dieudonne, Manin, Demazure, Yui.

Let k be a finite field of characteristic p.

Let $W(k)$ be the corresponding Witt ring,, F, V Frobenius and Verschiebung morphisms.

Let E_k be the noncommutative ring with elements

$a = w + \sum_{r=1}^{\infty} a_r F^r + \sum_{s=1}^{\infty} b_s V^s,\ w, a, b \in W(k)$

Let $G_{n,m}$ be the formal group whose Dieudonne module is isomorphic to

$E/E(F^m - V^n)$

For instance, over $\mathbb{F}_{29}$ for Fermat curve $F_{13} : x^{13} + y^{13} = 1$ the p-divisible group of the

Jacobian $J(F_{13})$ is

Example 12. $21G_{1,0} + 15(G_{1,2} + G_{2,1})$.

Problem 13. Is every prime finite group the Galois group of some Galois extension of a maximal Abelian extension of an imaginary quadratic field.

And

Problem 14. The similar problem for the Hilbert class field.

References

[1] Belyi G. V., Korolevich V. A., Serre Lie algebras of generalized Jacobians, Mat. Zamitki, vol. 19, no. 4, 571–576. 1976.

[2] Belyi, G. V., Galois extensions of a maximal cyclotomic field, Izv. Akad. Nauk SSSR, Ser. Mat., vol. 43(2), 267–276. 1979.

[3] Belyi V. A., Another proof of the three points theorem, Sb. Math., 193:3, 329–332. 2002.

[4] Borevich, Z., Shafarevich, I. *Number Theory*, Pure and Applied mathematics, Academic Press, New York. 1986.

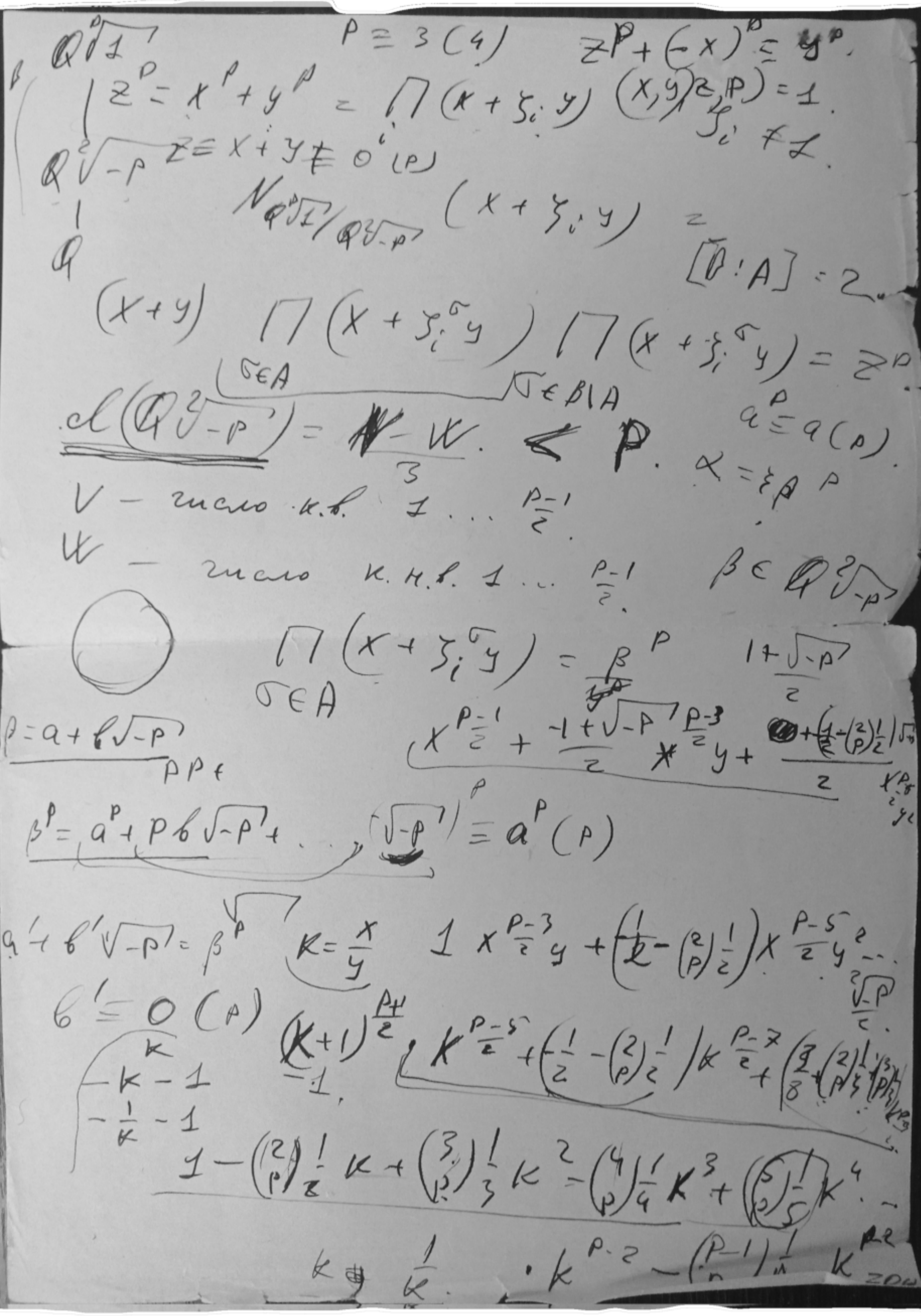
[5] Введенский О. Н. О локальных “полях классов” эллиптических кривых, Izv. Akad. Nauk SSSR, Ser. Mat., vol. 37(1), 20–88. 1973, Mathematics of the USSR-Izvestiya, 1973, 7:1, 19–84

[6] Glazunov N. M. On A.V. Malyshev's approach to Minkowski's conjecture concerning the critical determinant of the region $|x|^p + |y|^p < 1$ for $p > 1$, Chebyshevskii Sbornik, vol. 17, no. 4, 185–193. 2016.

[7] Glazunov N. M. Chebyshev metrics and their applications to the study of critical determinants and Diophantine approximations. Int. Conf. “P. Chebyshev Mathematical Ideas”, RAS, Obninsk. 66–67. 2021.

Thank you for your attention!

Back-up slides



$\mathbb{Q}\sqrt[p]{1}$ $p \equiv 3\,(4)$ $z^p + (-x)^p = y^p$.

$z^p = x^p + y^p = \prod (x + \zeta_i y)$ $(x, y, z, p) = 1$. $\zeta_i \neq 1$.

$\mathbb{Q}\sqrt[2]{-p}$ $z \equiv x + y \not\equiv 0\,(p)$

$\mathbb{Q}$

$N_{\mathbb{Q}\sqrt[p]{1}/\mathbb{Q}\sqrt[2]{-p}}(x + \zeta_i y) =$

$[B : A] = 2$.

$(x+y) \underbrace{\prod_{\sigma \in A} (x + \zeta_i^\sigma y) \prod_{\sigma \in B\setminus A} (x + \zeta_i^\sigma y)} = z^p$.

$a^p \equiv a\,(p)$.

$cl(\mathbb{Q}\sqrt[2]{-p}) = \frac{\cancel{V} - W}{3} < p$. $\alpha = \varepsilon \beta^p$.

V — число к.в. $1 \ldots \frac{p-1}{2}$.

W — число к.н.в. $1 \ldots \frac{p-1}{2}$. $\beta \in \mathbb{Q}\sqrt[2]{-p}$

○

$\prod_{\sigma \in A} (x + \zeta_i^\sigma y) = \beta^p$ $\frac{1+\sqrt{-p}}{2}$

$\beta = a + b\sqrt{-p}$

ppt

$x^{\frac{p-1}{2}} + \frac{-1+\sqrt{-p}}{2} x^{\frac{p-3}{2}} y + \frac{\ldots + (\frac{1}{2} - \binom{2}{p}\frac{1}{2})\sqrt{-p}}{2} x^{\frac{p-5}{2}} y^2$

$\beta^p = a^p + pb\sqrt{-p} + \ldots + (\sqrt{-p})^p \equiv a^p\,(p)$

$a' + b'\sqrt{-p} = \sqrt[p]{\beta^p}$ $k = \frac{x}{y}$ $1\, x^{\frac{p-3}{2}} y + (\frac{1}{2} - \binom{2}{p}\frac{1}{2}) x^{\frac{p-5}{2}} y^2 \ldots$ $\frac{\sqrt[2]{-p}}{2}$.

$b' \equiv 0\,(p)$ $(k+1)^{\frac{p+1}{2}}$ $k^{\frac{p-5}{2}} + (\frac{1}{2} - \binom{2}{p}\frac{1}{2}) k^{\frac{p-7}{2}} + (\frac{3}{8} + \binom{2}{p}\frac{1}{4} + \binom{3}{p}\frac{1}{3})$

-1.

k

$-k - 1$

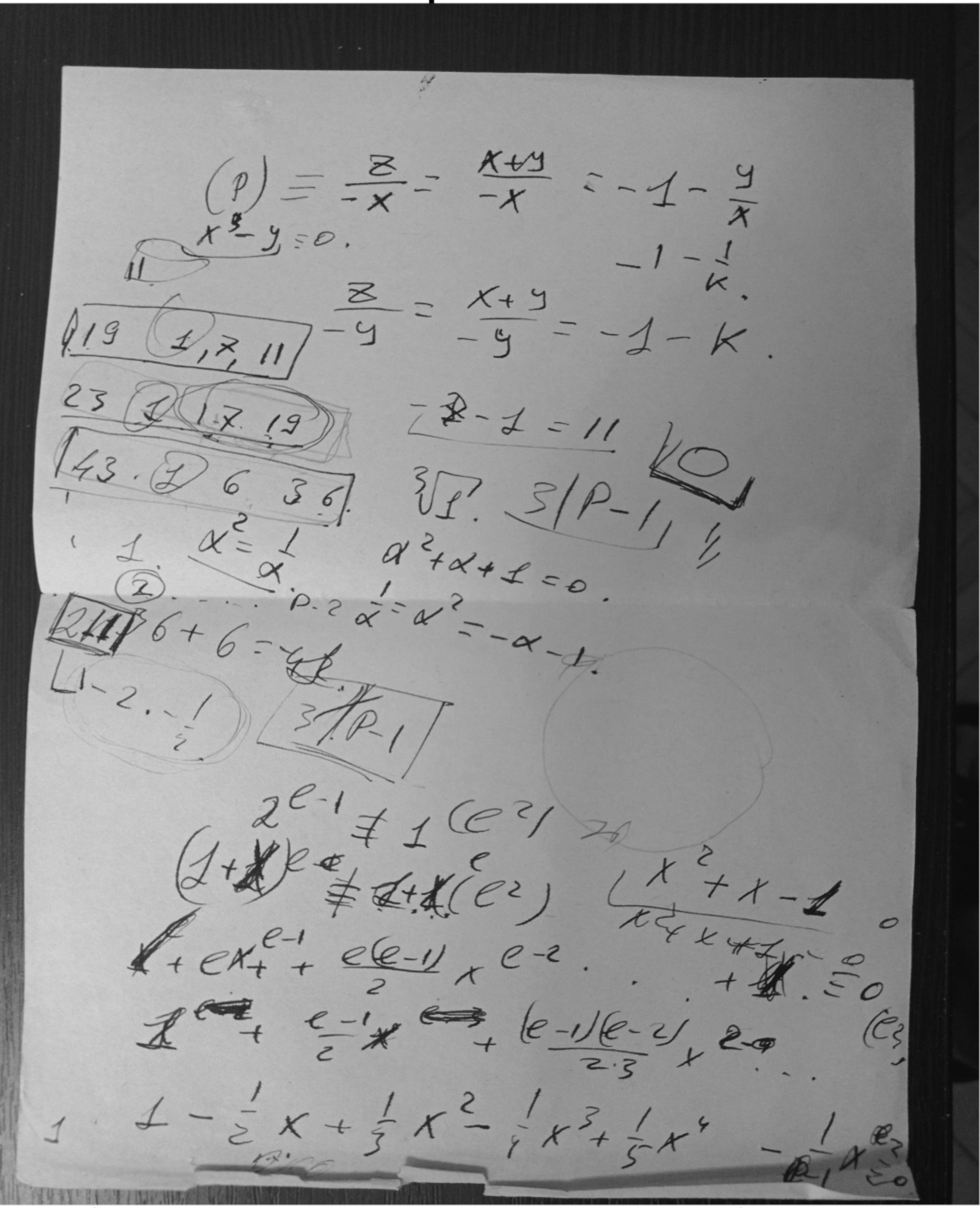
$-\frac{1}{k} - 1$

$1 - \binom{2}{p}\frac{1}{2} k + \binom{3}{p}\frac{1}{3} k^2 - \binom{4}{p}\frac{1}{4} k^3 + \binom{5}{p}\frac{1}{5} k^4 \ldots$

$k \Leftrightarrow \frac{1}{k}$ $\cdot k^{p-2} - \binom{p-1}{p}\frac{1}{p-1} k^{p-2}$

Заметки Геннадия Белого, стр. 1

Back-up slides



$(p) = \frac{z}{-x} = \frac{x+y}{-x} = -1 - \frac{y}{x}$

$x^3 - y = 0.$

11. $-1 - \frac{1}{k}.$

$\frac{z}{-y} = \frac{x+y}{-y} = -1 - k.$

19 1, 7, 11

23 1 1.7. 19 $-2 - 1 = 11$ 0

43. 1 6 3 6. $\sqrt[3]{1}.$ $3 | p-1$

1. $\alpha^2 = \frac{1}{\alpha}$ $\alpha^2 + \alpha + 1 = 0.$

2. $p\cdot 2$ $\frac{1}{\alpha} = \alpha^2 = -\alpha - 1.$

$2 \nmid 1$ $6 + 6 = 41$

$1 - 2 \ldots \frac{1}{2}$

$3 \nmid p-1$

$2^{e-1} \not\equiv 1 \ (e^2)$

$(1+1)^e \not\equiv 1+1 \ (e^2)$

$x^2 + x - 1$

$x^2 + x + 1 \ 0$

$1 + e x^{e-1} + \frac{e(e-1)}{2} x^{e-2} \ldots + 1 \equiv 0$

$1 + \frac{e-1}{2} x + \frac{(e-1)(e-2)}{2 \cdot 3} x^2 \ldots \ (e^3),$

$1 - \frac{1}{2} x + \frac{1}{3} x^2 - \frac{1}{4} x^3 + \frac{1}{5} x^4 - \frac{1}{e-1} x^{e-2} \equiv 0$

Заметки Геннадия Белого,страница 2