However, as n becomes large, the least element in A_n becomes large; and the sum, which is dominated by $M\sum\{[ah(a)\log a]^{-1}\colon a\in A_n\}$, tends to zero. This contradiction gives the result. Professor Erdös has pointed out that it is possible to prove that $\delta(A(f))$ exists.

In conclusion, I wish to express my deep appreciation to my advisor, Professor Robert Zink. Also, I wish to thank Professor Paul Erdös for a number of helpful discussions.

References

[1] F. Behrend, *On sequences of numbers not divisible by one another*, J. London Math. Soc. 10 (1935), pp. 42-44.

[2] A. S. Besicovitch, *On the density of certain sequences of integers*, Math. Ann. 110 (1934), pp. 336-341.

[3] H. Davenport and P. Erdös, *On sequences of positive integers*, Acta Arith. 2 (1936), pp. 147-151.

[4] H. Davenport and P. Erdös, *On sequences of positive integers*, J. Indian Math. Soc. N. S. 15 (1951), pp. 19-24.

[5] P. Erdös, *Note on sequences of integers on one of which is divisible by any other*, J. London Math. Soc. 10 (1935), pp. 126-128.

[6] — *On the density of some sequences of integers*, Bull. Amer. Math. Soc. 54 (1948), pp. 685-692.

[7] — *Some remarks on prime factors of integers*, Canad. J. Math. 11 (1959), pp. 161-167.

[8] G. H. Hardy, *Divergent series*, London 1956.

[9] A. E. Ingham, *The distribution of prime numbers*, Cambridge 1932.

UNIVERSITY OF ILLINOIS

Reçu par la Rédaction le 10. 1. 1966

ACTA ARITHMETICA
XII (1967)

О рациональных точках некоторых кривых высшего рода

В. А. Демьяненко (Москва)

Способ нахождения точек алгебраической кривой рода $g>1$, рациональных над заданным полем K конечной степени, неизвестен. Существует лишь предположение, что такая кривая имеет в K только конечное число точек.

Значительно большие результаты получены при исследовании кривых первого рода. Морделл [1] доказал, что совокупность точек кривой первого рода из абсолютной области рациональности $R(1)$ образует коммутативную группу с конечным числом образующих. Таким образом, существует такое конечное число рациональных точек $P_1, P_2, \ldots, P_r$, что любая рациональная точка P представима в виде

$$P = n_1P_1+n_2P_2+\ldots+n_rP_r$$

с некоторыми целыми $n_1, n_2, \ldots, n_r$. Позднее доказательство Морделла было несколько упрощено и значительно обобщено Вейлем [2].

В настоящей работе мы будем рассматривать кривые

$$x^4+y^4 = A \tag{1}$$

и

$$x^6+y^6 = A \tag{2}$$

при определённых ограничениях, накладываемых на ранги кривых первого рода:

$$u^4-A = v^2 \tag{3}$$

и

$$u^3+1 = Av^2,\qquad v^2+1 = Au^3,\qquad u^3+v^2 = A. \tag{4}$$

В частности, мы установим, что если ранг одной из кривых (4) над полем $R(\sqrt{-3})$ не превышает 2, то кривая (2) не имеет в этом поле точек, за исключением случаев: $A=1$, $\{x, y\} = \{\varepsilon_1, 0\}, \{0, \varepsilon_2\}$; $A=2$, $\{x, y\} = \{\varepsilon_1, \varepsilon_2\}$, $\varepsilon_1^6 = \varepsilon_2^6 = 1$. Аналогичный результат будет также получен и для кривой (1), рассматриваемой над полем $R(\sqrt{-1})$.

§ 1. Точки кривой (1), рациональные над полем $R(1)$. Рассмотрим обладающие рациональными точками кривые

$$a_k x_k^4 + b_k y_k^4 = z_k^2, \quad a_k b_k = -A \tag{5}$$

и

$$c_j u_j^4 + d_j v_j^4 = w_j^2, \quad c_j d_j = 4A, \tag{6}$$

записанные в однородной форме. Легко проверить, что если точки $P_1 = \{x_1, y_1, z_1\}$, $P_2 = \{x_2, y_2, z_2\}$ принадлежат кривым

$$a_1 x_1^4 + b_1 y_1^4 = z_1^2, \quad a_2 x_2^4 + b_2 y_2^4 = z_2^2, \quad a_1 b_1 = a_2 b_2,$$

то точка $P_3 = \{x_3, y_3, z_3\}$ будет лежать на кривой

$$a_1 a_2 x_3^4 + \frac{b_1}{a_2} y_3^4 = z_3^2,$$

причем

$$x_3 = x_1 y_1 z_2 - x_2 y_2 z_1,$$
$$y_3 = a_1 x_1^2 y_2^2 - a_2 x_2^2 y_1^2,$$
$$z_3 = z_1 z_2 (a_1 x_1^2 y_2^2 + a_2 x_2^2 y_1^2) - 2 a_1 x_1 y_1 x_2 y_2 (a_2 x_1^2 x_2^2 + b_1 y_1^2 y_2^2).$$

Условимся, далее, не различать кривые

$$ax^4 + by^4 = cz^2, \quad a a_1^4 x_1^4 + b b_1^4 y_1^4 = c c_1^2 z_1^2,$$

так как они посредством простой подстановки

$$x \rightleftarrows a_1 x_1, \quad y \rightleftarrows b_1 y_1, \quad z \rightleftarrows c_1 z_1$$

переходят друг в друга. Отсюда нетрудно установить, что кривые (5) и (6) образуют конечные группы G и U, представимые в виде прямого произведения циклических групп второго порядка. Обозначим единицы этих групп через E_1 и E_2; тогда:

$$E_1:\ x^4 - Ay^4 = z^2, \quad E_2:\ u^4 + 4Av^4 = w^2.$$

Множества точек кривых групп G и U также образуют группы, которые обозначим через S и T. Обозначим ещё группы точек кривых E_1 и E_2 через S_1 и T_1. В этом случае фактор-группы S/S_1 и T/T_1 соответственно изоморфны группам G и U.

Пользуясь формулами сложения точек на кривой, можно доказать справедливость следующих утверждений:

1) *Если P — точка какой-либо из кривых* (5) *над полем K, то* $(1+i)P$ *есть точка кривой E_2 над тем же полем;*

2) *Если Q — точка какой-либо из кривых* (6) *над полем K, то* $(1-i)Q$ *есть точка кривой E_1 над тем же полем.*

Пусть базисы групп G и U состоят из кривых M_j $(j = 1, 2, \ldots, m)$ и N_s $(s = 1, 2, \ldots, n)$. Тогда базисы изоморфных им фактор-групп S/S_1 и T/T_1 будут состоять из смежных классов $S_1 + P_j$ $(j = 1, 2, \ldots, m)$ и $T_1 + Q_s$ $(s = 1, 2, \ldots, n)$.

Из работы Биллинга [3] следует, что если $A \neq \pm B^2$, $B \in R(1)$, то кривые групп G и U над полем $R(1)$ не имеют точек конечного порядка, за исключением $O = \{x, y, z\}$, где $y = 0$. Далее, способом, указанным Подсыпаниным [4], можно доказать следующие леммы:

Лемма 1. *Всякая рациональная точка кривой* $\prod_{j=1}^{m} M_j^{k_j}$ *при* $A \neq \pm B^2$, $B \in R(1)$ *имеет вид*

$$\sum_{j=1}^{m} a_j h_j + (1+i) \sum_{s=1}^{n} b_s g_s + O_1,$$

где $a_j \equiv k_j \pmod 2$, h_j, g_s $(j = 1, 2, \ldots, m;\ s = 1, 2, \ldots, n)$ — *базисы групп* S *и* T, O_1 — *одна из точек конечного порядка на кривой* E_1.

Лемма 2. *Всякая рациональная точка кривой* $\prod_{s=1}^{n} N_s^{l_s}$ *при* $A \neq \pm B^2$, $B \in R(1)$ *имеет вид*

$$(1-i) \sum_{j=1}^{m} a_j h_j + \sum_{s=1}^{n} b_s g_s + O_2,$$

где $b_s \equiv l_s \pmod 2$, h_j, g_s $(j = 1, 2, \ldots, m;\ s = 1, 2, \ldots, n)$ — *базисы групп* S *и* T, O_2 — *одна из точек конечного порядка на кривой* E_2.

Лемма 3. *Ранг каждой из кривых групп G и U равен сумме рангов этих групп.*

Теорема 1. *Если группа U — единичная, то кривая* (1), *за исключением случаев:* $A = 1$, $\{x, y\} = \{\pm 1, 0\}, \{0, \pm 1\}$; $A = 2$, $\{x, y\} = \{\pm 1, \pm 1\}$ *рациональными точками не обладает.*

Доказательство. Очевидно, A можно считать большим 0 и свободным от биквадратов. Далее, так как кривая (1) при $A = 2$, B^2 над полем $R(1)$ исследована полностью (Диксон [5]), то мы будем считать также, что $A \neq 2$, B^2. Возьмём какую-либо точку $P = \{x_0/z_0, y_0/z_0\}$ на кривой (1), она порождает две точки

$$P_1 = \{x_1, y_1, z_1\} = \{z_0, x_0, y_0^2\}, \quad P_2 = \{x_2, y_2, z_2\} = \{z_0, y_0, x_0^2\}$$

кривой $z^2 = Ax^4 - y^4$. Так как

$$P_1 + P_2 = \{x_{1,1}, y_{1,1}, z_{1,1}\} = \\ = \{x_0^2 + x_0 y_0 + y_0^2,\ z_0(x_0 + y_0),\ x_0 y_0 (2x_0^2 + 3x_0 y_0 + 2y_0^2)\},$$

$$P_1 - P_2 = \{x_{1,-1}, y_{1,-1}, z_{1,-1}\} = \\ = \{x_0^2 - x_0 y_0 + y_0^2,\ z_0(x_0 - y_0),\ x_0 y_0 (2x_0^2 - 3x_0 y_0 + 2y_0^2)\},$$

то из
$$\begin{cases} x_0y_0z_0(x_0+y_0)(x_0^2+x_0y_0+y_0^2)(2x_0^2+3x_0y_0+2y_0^2) = 0, \\ x_0^4+y_0^4 = Az_0^4 \end{cases}$$
и
$$\begin{cases} x_0y_0z_0(x_0-y_0)(x_0^2-x_0y_0+y_0^2)(2x_0^2-3x_0y_0+2y_0^2) = 0, \\ x_0^4+y_0^4 = Az_0^4 \end{cases}$$
при $A \neq 1, 2$ вытекает

(7) $$x_{1,1}\,y_{1,1}\,z_{1,1}, \quad x_{1,-1}\,y_{1,-1}\,z_{1,-1} \neq 0.$$

По условию группа U — единичная, поэтому на основании леммы 1
$$P_1 = \sum_{j=1}^{m} a_j h_j + O_1, \quad P_2 = \sum_{j=1}^{m} b_j h_j + O_1',$$
где $a_j \equiv b_j (\mathrm{mod}\, 2)$ $(j = 1, 2, \ldots, m)$. Так как $P_1 - O_1 \equiv P_2 - O_1' (\mathrm{mod}\, 2)$, то существуют рациональные точки $P_3 = \frac{1}{2}(P_1+P_2-O_1-O_1')$, $P_4 = \frac{1}{2}(P_1-P_2-O_1+O_1')$, принадлежащие соответственно кривым
$$\prod_{j=1}^{m} M_j^{(a_j+b_j)/2}, \quad \prod_{j=1}^{m} M_j^{(a_j-b_j)/2},$$
которые можно записать в виде
$$ax^4 - by^4 = z^2, \quad -ax^4+by^4 = z^2.$$
Легко заметить, что если $P_1 = \{x_1, y_1, z_1\}$, $P_2 = \{x_2, y_2, z_2\}$, то
$$P_1 - O_1 = \{d_1x_1, \pm d_1y_1, \pm d_1^2 z_1\}, \quad P_2 - O_1' = \{d_2x_2, \pm d_2y_2, \pm d_2^2 z_2\},$$
поэтому
$$P_1 - O_1 = P_3 + P_4, \quad P_2 - O_1' = P_3 - P_4,$$

(8) $$\begin{gathered} d_1x_1 = x_3^2y_4^2 + x_4^2y_3^2, \quad \pm d_1y_1 = x_3y_3z_4 - x_4y_4z_3, \\ \pm d_1^2z_1 = z_3z_4(x_3^2y_4^2 - x_4^2y_3^2) + 2x_3x_4y_3y_4(ax_3^2x_4^2 + by_3^2y_4^2), \\ d_2x_2 = x_3^2y_4^2 + x_4^2y_3^2, \quad \pm d_2y_2 = x_3y_3z_4 + x_4y_4z_3, \\ \pm d_2^2z_2 = z_3z_4(x_3^2y_4^2 - x_4^2y_3^2) - 2x_3x_4y_3y_4(ax_3^2x_4^2 + by_3^2y_4^2), \end{gathered}$$

где $P_3 = \{x_3, y_3, z_3\}$, $P_4 = \{x_4, y_4, z_4\}$.

Из условия (7) непосредственно вытекает: $x_3y_3z_3$, $x_4y_4z_4 \neq 0$. Далее, координаты точек P_1 и P_2 удовлетворяют следующим равенствам:
$$z_2 = x_0^2 = y_1^2, \quad z_1 = y_0^2 = y_2^2;$$
следовательно,

(9) $$\begin{gathered} \pm(x_3y_3z_4 + x_4y_4z_3)^2 = z_3z_4(x_3^2y_4^2 - x_4^2y_3^2) + 2x_3x_4y_3y_4(ax_3^2x_4^2 + by_3^2y_4^2), \\ \pm(x_3y_3z_4 - x_4y_4z_3)^2 = z_3z_4(x_3^2y_4^2 - x_4^2y_3^2) - 2x_3x_4y_3y_4(ax_3^2x_4^2 + by_3^2y_4^2). \end{gathered}$$

Поскольку равенства (9) оказываются зависимыми друг от друга, то из них вытекает лишь одно из следующих соотношений:
$$\pm 2x_3x_4y_3y_4 = x_3^2y_4^2 - x_4^2y_3^2$$
или
$$\pm z_3z_4 = ax_3^2x_4^2 + by_3^2y_4^2.$$

Очевидно, первое равенство невозможно; возводя обе части второго равенства в квадрат и решая его относительно a, получим:
$$4\frac{a}{b}x_3^4x_4^4 = (x_3^2y_4^2 - x_4^2y_3^2)^2 \pm \sqrt{(x_3^2y_4^2 - x_4^2y_3^2)^4 - (2x_3x_4y_3y_4)^4}.$$

Подкоренное выражение может представлять собою точный квадрат лишь при $\pm 2x_3x_4y_3y_4 = x_3^2y_4^2 - x_4^2y_3^2$ или $2x_3x_4y_3y_4 = 0$, что опять таки невозможно. Тем самым, теорема доказана.

Следствие. *Если ранг кривой E_1 над полем $R(1)$ не превышает 1, то кривая (1), за исключением случаев $A = 1$, $\{x, y\} = \{\pm 1, 0\}, \{0, \pm 1\}$; $A = 2$, $\{x, y\} = \{\pm 1, \pm 1\}$, рациональными точками не обладает.*

Действительно, если $A = \pm B^2$, то каковы бы ни были группы G и U, кривая (1) может обладать лишь следующими рациональными точками: $\{x, y\} = \{\pm 1, 0\}, \{0, \pm 1\}$ при $A = 1$. Поэтому достаточно рассмотреть только случай: $A \neq \pm B^2$. По лемме 3 ранг кривой E_1, не превышающий по условию 1, представляет собою сумму рангов групп G и U. В то же время если кривая (1) имеет некоторую рациональную точку, то кривая $Ax^4 - y^4 = z^2$, не совпадающая при $A \neq B^2$ с кривой E_1, принадлежит группе G. Следовательно, ранг группы G не ниже 1, а поэтому группа U — единичная.

§ 2. Точки кривых (1) и (2), рациональные над полями $R(\sqrt{-1})$ и $R(\sqrt{-3})$. Будем сначала заниматься задачей нахождения в поле $R(\sqrt{-1})$ точек кривой (1) при условии, что ранг кривой (3) над этим полем не превышает 2.

Прежде всего заметим, что геометрическим приёмом проведения секущих и касательных к кривой

(10) $$ax^4 + by^4 = cz^2$$

можно получить следующие результаты:

1) Если точка P кривой (10) имеет координаты $\{x, y, z\}$, то точка $2P = \{ax^4 - by^4, 2xyz, a^2x^8 + 6abx^4y^4 + b^2y^8\}$ принадлежит кривой

(11) $$x^4 + abc^2y^4 = z^2.$$

2) Если точки $P_1=\{x_1,y_1,z_1\}$, $P_2=\{x_2,y_2,z_2\}$ принадлежат соответственно кривым (10) и (11), то точка $P_1+P_2=\{x_+,y_+,z_+\}$ будет принадлежать кривой (10), причём

$$
\begin{aligned}
&x_+=x_1^2x_2^2-bcy_1^2y_2^2,\quad y_+=x_1y_1z_2+cx_2y_2z_1,\\
&z_+=z_1z_2(x_1^2x_2^2+bcy_1^2y_2^2)+2bx_1y_1x_2y_2(acx_1^2y_2^2+x_2^2y_1^2).
\end{aligned}
\tag{12}
$$

3) Если точки $P_1=\{x_1,y_1,z_1\}$, $P_2=\{x_2,y_2,z_2\}$ принадлежат кривой (10), то точка $P_1+P_2=\{x_+,y_+,z_+\}$ будет принадлежать кривой (11), причём

$$
\begin{aligned}
&x_+=ax_1^2x_2^2-by_1^2y_2^2,\quad y_+=x_1y_1z_2+x_2y_2z_1,\\
&z_+=cz_1z_2(ax_1^2x_2^2+by_1^2y_2^2)+2abx_1y_1x_2y_2(x_1^2y_2^2+x_2^2y_1^2).
\end{aligned}
\tag{13}
$$

Докажем теперь ряд лемм. Леммы 4-7 будем доказывать для произвольного алгебраического числового поля конечной степени, лишь при доказательстве лемм 8 и 9 будут использованы индивидуальные свойства поля $R(\sqrt{-1})$.

Лемма 4. *Если точка P кривой* (10) *имеет координаты* $\{x_1,y_1,z_1\}$, *то*

$$mP=\{x_m,y_m,z_m\},$$

$$x_m=x_1A_m,\quad y_m=y_1B_m,\quad z_m=z_1C_m,$$

$$A_m=\sum_{k=0}^{(m^2-1)/4}a_ku^{(m^2-1)/4-k}v^k,\quad B_m=\sum_{k=0}^{(m^2-1)/4}(-1)^ka_ku^{(m^2-1)/4-k}v^k,$$

$$C_m=\sum_{k=0}^{(m^2-1)/4}c_{2k}u^{(m^2-1)/2-2k}v^{2k},$$

$$a_0=\Big|\sum_{k=0}^{(m^2-1)/4}a_k\Big|=1,\quad |a_{(m^2-1)/4}|=2^{(m^2-1)/8},$$

при $m\equiv 1 \pmod 2$;

$$x_m=uA_m,\quad y_m=2x_1y_1z_1B_m,\quad z_m=C_m,$$

$$A_m=\sum_{k=0}^{(m^2-4)/8}a_{2k}u^{m^2/4-2k-1}v^{2k},\quad B_m=\sum_{k=0}^{(m^2-4)/8}b_{2k}u^{m^2/4-2k-1}v^{2k},$$

$$C_m=\sum_{k=0}^{m^2/4}c_{2k}u^{m^2/2-2k}v^{2k},$$

$$a_0=\Big|\sum_{k=0}^{(m^2-4)/8}a_{2k}\Big|=\Big|\sum_{k=0}^{(m^2-4)/8}(-1)^{2k}a_{2k}\Big|=1,\quad |a_{(m^2-4)/4}|=2^{(m^2-4)/8},$$

при $m\equiv 2 \pmod 4$ *и*

$$x_m=A_m,\quad y_m=4x_1y_1z_1uB_m,\quad z_m=C_m,$$

$$A_m=\sum_{k=0}^{m^2/8}a_{2k}u^{m^2/4-2k}v^{2k},\quad B_m=\sum_{k=0}^{(m^2-8)/8}b_{2k}u^{m^2/4-2-2k}v^{2k},$$

$$C_m=\sum_{k=0}^{m^2/4}c_{2k}u^{m^2/2-2k}v^{2k},$$

$$a_0=\Big|\sum_{k=0}^{m^2/8}a_{2k}\Big|=1,\quad |a_{m^2/4}|=2^{m^2/8},$$

при $m\equiv 0 \pmod 4$, *где* $u=ax_1^4-by_1^4$, $v=ax_1^4+by_1^4$, A_m, B_m, C_m — *взаимнопростые многочлены с целыми рациональными коэффициентами.*

Доказательство. Доказательство проведем методом математической индукции. По формулам (12) и (13) имеем:

$$O=\{1,0,1\},\quad P=\{x_1,y_1,z_1\},\quad 2P=\{u,2x_1y_1z_1,u^2-2v^2\},$$
$$3P=\{x_1(u^2+2uv-2v^2),\ y_1(u^2-2uv-2v^2),\ z_1(3u^4-4v^4)\}.$$

Следовательно, при $m=0,1,2,3$ лемма справедлива. Предположим теперь, что лемма справедлива для всех $m\leqslant 4n$ и докажем, что в этом случае она справедлива и при $m=4n+1, 4n+2, 4n+3, 4n+4$. Ввиду явной аналогии остановимся лишь на первом случае: $m=4n+1$. Воспользуемся для этого следующими формулами, легко вытекающими из формул сложения и вычитания точек на кривых (10) и (11):

$$
\begin{aligned}
x_{4n+1}x_{4n-1}&=x_1^2x_{4n}^2-bcy_1^2y_{4n}^2,\\
y_{4n+1}y_{4n-1}&=y_1^2x_{4n}^2-acx_1^2y_{4n}^2,\\
z_{4n+1}z_{4n-1}&=z_1^2z_{4n}^2+4abx_1^2y_1^2x_{4n}^2y_{4n}^2.
\end{aligned}
$$

Пусть

$$x_{4n-1}=x_1A_{4n-1},\quad y_{4n-1}=y_1B_{4n-1},\quad z_{4n-1}=z_1C_{4n-1},$$
$$x_{4n}=A_{4n},\quad y_{4n}=4x_1y_1z_1uB_{4n},\quad z_{4n}=C_{4n};$$

тогда

$$x_{4n+1}=x_1A_{4n+1},\quad y_{4n+1}=y_1B_{4n+1},\quad z_{4n+1}=z_1C_{4n+1},$$

где

$$
\begin{aligned}
&A_{4n+1}=\frac{A_{4n}^2+8u^2v(u-v)B_{4n}^2}{A_{4n-1}},\quad B_{4n+1}=\frac{A_{4n}^2-8u^2v(u+v)B_{4n}^2}{B_{4n-1}},\\
&C_{4n+1}=\frac{C_{4n}^2-16(u^2-v^2)u^2A_{4n}^2B_{4n}^2}{C_{4n-1}}.
\end{aligned}
\tag{14}
$$

Точка $(4n+1)P=\{x_{4n+1},y_{4n+1},z_{4n+1}\}$ принадлежит кривой (10), поэтому

$$(u+v)A_{4n+1}^4-(u-v)B_{4n+1}^4=2vC_{4n+1}^2. \tag{15}$$

Так как выражение (15) представляет собою тождество, а многочлены $A_{4n-1}, B_{4n-1}, C_{4n-1}$ взаимно-просты, то

$$A_{4n}^2+8u^2v(u-v)B_{4n}^2 \equiv 0 \pmod{A_{4n-1}},$$
$$A_{4n}^2-8u^2v(u+v)B_{4n}^2 \equiv 0 \pmod{B_{4n-1}},$$
$$C_{4n}^2-16(u^2-v^2)u^2A_{4n}^2B_{4n}^2 \equiv 0 \pmod{C_{4n-1}}.$$

Положим

$$A_{4n+1} = \sum_{j=0}^{4n^2+2n} a_j u^{4n^2+2n-j}v^j, \quad B_{4n+1} = \sum_{j=0}^{4n^2+2n} b_j u^{4n^2+2n-j}v^j,$$
$$C_{4n+1} = \sum_{j=0}^{8n^2+4n} c_j u^{8n^2+4n-j}v^j.$$

По условию многочлены $A_{4n-1}, B_{4n-1}, C_{4n-1}$; A_{4n}, B_{4n}, C_{4n} имеют целочисленные коэффициенты. Кроме того коэффициенты многочленов $A_{4n-1}, B_{4n-1}, C_{4n-1}$ при старших членах равны 1. Следовательно, многочлены $A_{4n+1}, B_{4n+1}, C_{4n+1}$ также имеют целочисленные коэффициенты. Нам остаётся показать, что

$$b_j = (-1)^j a_j, \quad c_{2j+1} = 0, \quad a_0 = \Big|\sum_{j=0}^{4n^2+2n} a_j\Big| = 1, \quad |a_{4n^2+2n}| = 2^{2n^2+n}.$$

Произведём подстановку: $u \to -u$, $v \to v$. По условию при этой подстановке $(A_{4n}, B_{4n}, C_{4n}) \to (A_{4n}, B_{4n}, C_{4n})$, $(A_{4n-1}, B_{4n-1}, C_{4n-1}) \to (B_{4n-1}, A_{4n-1}, C_{4n-1})$. Ввиду этого из формул (14) следует: $(A_{4n+1}, B_{4n+1}, C_{4n+1}) \to (B_{4n+1}, A_{4n+1}, C_{4n+1})$. Таким образом, $b_j = (-1)^j a_j$, $c_{2j+1} = 0$. Далее, из сравнений

$$A_{4n-1} \equiv u^{4n^2-2n} \pmod{v}, \qquad A_{4n-1} \equiv \pm(2v^2)^{2n^2-n} \pmod{u},$$
$$A_{4n-1} \equiv v^{4n^2-2n} \pmod{u-v}, \qquad A_{4n} \equiv u^{4n^2} \pmod{v},$$
$$A_{4n} \equiv \pm(2v^2)^{2n^2} \pmod{u}, \qquad A_{4n} \equiv v^{4n^2} \pmod{u-v}$$

и

$$A_{4n+1}A_{4n-1} \equiv A_{4n}^2 \big(\operatorname{mod} uv(u-v)\big)$$

вытекает:

$$a_0 = \Big|\sum_{j=0}^{4n^2+2n} a_j\Big| = 1, \quad |a_{4n^2+2n}| = 2^{2n^2+n},$$

что и требовалось доказать.

Лемма 5. *Координаты точек* $(2m+1)P = \{x_{2m+1}, y_{2m+1}, z_{2m+1}\}$, $2mP = \{x_{2m}, y_{2m}, z_{2m}\}$ *удовлетворяют следующим сравнениям:*

$$\frac{ax_{2m+1}^4}{(ax_{2m+1}^4, by_{2m+1}^4)} \equiv 0 \left(\operatorname{mod} \frac{ax_1^4}{(ax_1^4, by_1^4)}\right),$$
$$\frac{by_{2m+1}^4}{(ax_{2m+1}^4, by_{2m+1}^4)} \equiv 0 \left(\operatorname{mod} \frac{by_1^4}{(ax_1^4, by_1^4)}\right),$$
$$(16) \qquad \frac{2cz_{2m+1}^2}{(ax_{2m+1}^4, by_{2m+1}^4)} \equiv 0 \left(\operatorname{mod} \frac{cz_1^2}{(ax_1^4, by_1^4)}\right),$$
$$\frac{4abc^2y_{2m}^4}{(x_{2m}^4, abc^2y_{2m}^4)} \equiv 0 \left(\operatorname{mod} \frac{abc^2x_1^4y_1^4z_1^4}{(ax_1^4, by_1^4)^4}\right),$$

где $P = \{x_1, y_1, z_1\}$ — *точка на кривой* (10).

Доказательство. Согласно лемме 4

$$ax_{2m+1}^4 = ax_1^4\Big\{\sum_{j=0}^{m^2+m} a_{j,1}(ax_1^4)^{m^2+m-j}(by_1^4)^j\Big\}^4,$$
$$by_{2m+1}^4 = by_1^4\Big\{\sum_{j=0}^{m^2+m} b_{j,1}(ax_1^4)^{m^2+m-j}(by_1^4)^j\Big\}^4,$$
$$cz_{2m+1}^2 = cz_1^2\Big\{\sum_{j=0}^{2m^2+2m} c_{j,1}(ax_1^4)^{2m^2+2m-j}(by_1^4)^j\Big\}^2,$$
$$(17) \qquad x_{2m}^4 = \Big\{\sum_{j=0}^{m^2} a_{j,2}(ax_1^4)^{m^2-j}(by_1^4)^j\Big\}^4,$$
$$abc^2y_{2m}^4 = (ax_1^4)(by_1^4)(cz_1^2)^2\Big\{\sum_{j=0}^{m^2-1} b_{j,2}(ax_1^4)^{m^2-1-j}(by_1^4)^j\Big\}^4,$$
$$z_{2m}^2 = \Big\{\sum_{j=0}^{2m^2} c_{j,2}(ax_1^4)^{2m^2-j}(by_1^4)^j\Big\}^2,$$

где

$$(18) \qquad a_{0,1} = b_{m^2+m,1} = c_{0,1} = c_{m^2+m,1} = a_{0,2} = a_{m^2,2} = 1,$$
$$\Big|\sum_{j=0}^{m^2+m}(-1)^j a_{j,1}\Big| = \Big|\sum_{j=0}^{m^2+m}(-1)^j b_{j,1}\Big| = 2^{m^2+m}, \quad \Big|\sum_{j=0}^{m^2}(-1)^j a_{j,2}\Big| = 2^{m^2}.$$

Разложим двойку на простые идеалы $2 = \prod_{j=1}^{n} p_j^{m_j}$ и пусть $cz_1^2/(ax_1^4, by_1^4) = d\prod_{j=1}^{n} p_j^{k_j}$, где d — нечётный идеал. Из формул (17) видно, что идеалы

$$\frac{ax_{2m+1}^4}{(ax_1^4, by_1^4)^{(2m+1)^2}}, \quad \frac{by_{2m+1}^4}{(ax_1^4, by_1^4)^{(2m+1)^2}}, \quad \frac{cz_{2m+1}^2}{(ax_1^4, by_1^4)^{(2m+1)^2}}, \quad \frac{abc^2y_{2m}^4}{(ax_1^4, by_1^4)^{4m^2}}$$

целые и

$$\frac{ax_{2m+1}^4}{(ax_1^4,\, by_1^4)^{(2m+1)^2}} \equiv 0\left(\bmod \frac{ax_1^4}{(ax_1^4,\, by_1^4)}\right),$$
$$\frac{by_{2m+1}^4}{(ax_1^4,\, by_1^4)^{(2m+1)^2}} \equiv 0\left(\bmod \frac{by_1^4}{(ax_1^4,\, by_1^4)}\right),$$
$$\frac{cz_{2m+1}^2}{(ax_1^4,\, by_1^4)^{(2m+1)^2}} \equiv 0 (\bmod d),$$
$$\frac{abc^2y_{2m}^4}{(ax_1^4,\, by_1^4)^{4m^2}} \equiv 0\left(\bmod \frac{abd^2x_1^4y_1^4}{(ax_1^4,\, by_1^4)^2}\right).$$

Кроме того из условий (18) вытекает

$$\left(\frac{ax_{2m+1}^4}{(ax_1^4,\, by_1^4)^{(2m+1)^2}},\ \frac{bdy_1^4}{(ax_1^4,\, by_1^4)}\right) = \left(\frac{by_{2m+1}^4}{(ax_1^4,\, by_1^4)^{(2m+1)^2}},\ \frac{adx_1^4}{(ax_1^4,\, by_1^4)}\right) =$$
$$= \left(\frac{cz_{2m+1}^2}{(ax_1^4,\, by_1^4)^{(2m+1)^2}},\ \frac{abx_1^4y_1^4}{(ax_1^4,\, by_1^4)^2}\right) = \left(\frac{x_{2m}^4}{(ax_1^4,\, by_1^4)^{4m^2}},\ \frac{abdx_1^4y_1^4}{(ax_1^4,\, by_1^4)^2}\right) = 1.$$

Следовательно,

$$\frac{ax_{2m+1}^4}{(ax_{2m+1}^4,\, by_{2m+1}^4)} \equiv 0\left(\bmod \frac{ax_1^4}{(ax_1^4,\, by_1^4)}\right),$$
$$\frac{by_{2m+1}^4}{(ax_{2m+1}^4,\, by_{2m+1}^4)} \equiv 0\left(\bmod \frac{by_1^4}{(ax_1^4,\, by_1^4)}\right),$$
$$\frac{cz_{2m+1}^2}{(ax_{2m+1}^4,\, by_{2m+1}^4)} \equiv 0 (\bmod d), \tag{19}$$
$$\frac{abc^2y_{2m}^4}{(x_{2m}^4,\, abc^2y_{2m}^4)} \equiv 0\left(\bmod \frac{abdx_1^4y_1^4}{(ax_1^4,\, by_1^4)^2}\right).$$

Если для всех j $k_j \leqslant m_j$, то из сравнений (19) следуют сравнения (16) и лемма доказана. Предположим теперь, что при некотором $j = t$ $k_t > m_t$. В этом случае из формул

$$x_2^4 = (ax_1^4 - by_1^4)^4, \quad abc^2y_2^4 = 16abc^2x_1^4y_1^4z_1^4, \quad z_2^2 = (a^2x_1^8 + 6abx_1^4y_1^4 + b^2y_1^8)^2,$$
$$x_{m+2} = x_m^2x_2^2 - bcy_m^2y_2^2, \quad y_{m+2} = x_my_mz_2 + cx_2y_2z_m,$$
$$z_{m+2} = z_mz_2(x_m^2x_2^2 + bcy_m^2y_2^2) + 2bx_my_mx_2y_2(acx_m^2y_2^2 + x_2^2y_m^2)$$

при $\dfrac{cz_m^2}{(ax_m^4,\, by_m^4)} \equiv 0 (\bmod p_t^{k_t})$ вытекает

$$\frac{cz_{m+2}^2}{(ax_{m+2}^4,\, by_{m+2}^4)} \equiv 0 (\bmod p_t^{k_t}).$$

Так как при $m = 1$ $\dfrac{cz_1^2}{(ax_1^4,\, by_1^4)} \equiv 0 (\bmod p_t^{k_t})$, то

$$\frac{cz_{2m+1}^2}{(ax_{2m+1}^4,\, by_{2m+1}^4)} \equiv 0 (\bmod p_t^{k_t}), \quad k_t > m_t. \tag{20}$$

Аналогичным образом получаем

$$\frac{abc^2y_{2m}^4}{(x_{2m}^4,\, abc^2y_{2m}^4)} \equiv 0 (\bmod p_t^{2k_t}), \quad k_t > m_t. \tag{21}$$

Из сравнений (19)-(21) следуют (16), что и требовалось доказать.

Аналогичным образом доказываются

Лемма 6. *Если* $P = \{x_1, y_1, z_1\}$, $(m+ni)P = \{x_{m,n}, y_{m,n}, z_{m,n}\}$, *то*

$$\frac{ax_{m,n}^4}{(ax_{m,n}^4,\, by_{m,n}^4)} \equiv 0\left(\bmod \frac{ax_1^4}{(ax_1^4,\, by_1^4)}\right),$$
$$\frac{by_{m,n}^4}{(ax_{m,n}^4,\, by_{m,n}^4)} \equiv 0\left(\bmod \frac{by_1^4}{(ax_1^4,\, by_1^4)}\right),$$
$$\frac{2cz_{m,n}^2}{(ax_{m,n}^4,\, by_{m,n}^4)} \equiv 0\left(\bmod \frac{cz_1^2}{(ax_1^4,\, by_1^4)}\right)$$

при $m+ni \not\equiv 0 (\bmod 1+i)$;

$$\frac{4x_{m,n}^4}{(x_{m,n}^4,\, abc^2y_{m,n}^4)} \equiv 0\left(\bmod \frac{c^2z_1^4}{(ax_1^4,\, by_1^4)^2}\right),$$
$$\frac{abc^2y_{m,n}^4}{(x_{m,n}^4,\, abc^2y_{m,n}^4)} \equiv 0\left(\bmod \frac{abx_1^4y_1^4}{(ax_1^4,\, by_1^4)^2}\right)$$

при $m+ni \equiv 0 (\bmod 1+i)$, *но* $m+ni \not\equiv 0 (\bmod 2)$;

$$\frac{4abc^2y_{m,n}^4}{(x_{m,n}^4,\, abc^2y_{m,n}^4)} \equiv 0\left(\bmod \frac{abc^2x_1^4y_1^4z_1^4}{(ax_1^4,\, by_1^4)^4}\right)$$

при $m+ni \equiv 0 (\bmod 2)$.

Лемма 7. *Если* $Q_1 = \{a_0, b_0, c_0^2\}$, $Q_2 = \{c_0, b_0, a_0^2\}$, $mQ_1 + nQ_2 = \{a_{m,n}, b_{m,n}, c_{m,n}\}$, m, n — *целые числа из поля* $R(i)$, *то*

$$\frac{2aa_{m,n}^4}{(aa_{m,n}^4,\, bb_{m,n}^4)} \equiv 0\left(\bmod \frac{aa_0^4}{(aa_0^4,\, bb_0^4)}\right),$$
$$\frac{bb_{m,n}^4}{(aa_{m,n}^4,\, bb_{m,n}^4)} \equiv 0\left(\bmod \frac{bb_0^4}{(aa_0^4,\, bb_0^4)}\right),$$
$$\frac{2cc_{m,n}^2}{(aa_{m,n}^4,\, bb_{m,n}^4)} \equiv 0\left(\bmod \frac{cc_0^4}{(aa_0^4,\, bb_0^4)}\right)$$

при $m \not\equiv 0 (\bmod 1+i)$, $n \equiv 0 (\bmod 2)$;

$$\frac{2aa^4_{m,n}}{(aa^4_{m,n},\, bb^4_{m,n})} \equiv 0 \left(\mathrm{mod}\ \frac{ac_0^4}{(ac_0^4,\, bb_0^4)}\right),$$

$$\frac{bb^4_{m,n}}{(aa^4_{m,n},\, bb^4_{m,n})} \equiv 0 \left(\mathrm{mod}\ \frac{bb_0^4}{(ac_0^4,\, bb_0^4)}\right),$$

$$\frac{2cc^2_{m,n}}{(aa^4_{m,n},\, bb^4_{m,n})} \equiv 0 \left(\mathrm{mod}\ \frac{ca_0^4}{(ac_0^4,\, bb_0^4)}\right)$$

при $m \equiv 0 (\mathrm{mod}\, 2)$, $n \not\equiv 0 (\mathrm{mod}\, 1+i)$;

$$4 \equiv 0 \left(\mathrm{mod} \left(\frac{aca^4_{m,n} c^2_{m,n}}{(aa^4_{m,n},\, cc^2_{m,n})^2},\ \frac{aca_0^4 c_0^4}{(aa_0^4,\, cc_0^4)^2}\right)\right)$$

при $m, n \not\equiv 0 (\mathrm{mod}\, 1+i)$.

Лемма 8. *При* $ab \neq d^2, id^2, (1\pm i)d^2, (1\pm 2i)d^2, (2\pm i)d^2$ *кривая* (10) *не имеет в* $R(i)$ *точек конечного порядка, за исключением*: $O = \{x, y, z\}$, *где* $y = 0$.

Доказательство. Так как в поле $R(i)$ разложение на простые множители однозначно (конечно, с точностью до ассоциированности), то, не нарушая общности, можно считать, что $(ax^4, by^4, cz^2) = 1$ и $a, b, c, x, y, z \in R(i)$. Предположим, далее, что некоторая точка $P \neq 0$ кривой (10) имеет конечный порядок m, тогда справедливо следующее равенство

$$mP = 0. \tag{22}$$

Рассмотрим раздельно случаи: 1) $m \equiv 0 (\mathrm{mod}\, p)$, где $p = 2k+1$; 2) $m = 2^n$.

1) $m \equiv 0 (\mathrm{mod}\, p)$, $p = 2k+1$. На основании предыдущей леммы и (22)

$$y_m = y_{m/p} \sum_{j=0}^{(p^2-1)/4} (-1)^j a_j u^{(p^2-1)/4-j} v^j, \quad a_0 = 1, \quad |a_{(p^2-1)/4}| = 2^{(p^2-1)/8},$$

где $\frac{m}{p}P = \{x_{m/p}, y_{m/p}, z_{m/p}\}$, $mP = \{x_m, y_m, z_m\}$. Так как $\frac{m}{p}P \neq 0$ и p — нечётное, то $y_{m/p} \neq 0$, следовательно,

$$\sum (-1)^j a_j u^{(p^2-1)/4-j} v^j = 0,$$

откуда

$$\frac{u}{v} = \frac{ax^4_{m/p} - by^4_{m/p}}{ax^4_{m/p} + by^4_{m/p}} = \varepsilon (1+i)^t,$$

где ε — единица поля $R(i)$. С другой стороны

$$\sum_{j=0}^{(p^2-1)/4} (-1)^j a_j u^{(p^2-1)/4-j} v^j \equiv (by^4_{m/p})^{(p^2-1)/4} (\mathrm{mod}\, ax^4_{m/p}),$$

поэтому $ax^4_{m/p}$ также является единицей этого поля. Таким образом,

$$ax^4_{m/p} - by^4_{m/p} = \varepsilon_1 (1+i)^l, \qquad ax^4_{m/p} + by^4_{m/p} = \varepsilon_2 (1+i)^r,$$
$$2ax^4_{m/p} = 2\varepsilon_3 = \varepsilon_1 (1+i)^l + \varepsilon_2 (1+i)^r,$$

откуда и вытекает, что ab можно представить в одном из видов, указанных в формулировке леммы.

2) $m = 2^n$. Для этого случая имеем:

$$Q = \{x_{2^n}, y_{2^n}, z_{2^n}\}, \qquad y_{2^n} = 2^n y_1 \prod_{t=0}^{n-1} x_{2^t} z_{2^t}.$$

Если $\prod_{t=0}^{n-1} x_{2^t} z_{2^t} = 0$, то $ab = d^2$; если же $y_1 = 0$, то $P = \{x_1, y_1, z_1\}$, где $y_1 = 0$, что и требовалось доказать.

Лемма 9. *Кривая* (1) *при* $A = d^2, id^2, (1\pm i)d^2, (1\pm 2i)d^2, (2\pm i)d^2$ *не имеет точек в поле* $R(i)$, *за исключением случаев*: $A = 1$, $\{x, y\} = \{\varepsilon_1, 0\}, \{0, \varepsilon_2\}$; $A = 2$, $\{x, y\} = \{\varepsilon_1, \varepsilon_2\}$ *где* $\varepsilon_1, \varepsilon_2$ — *единицы этого поля*.

Доказательство. Прежде всего установим, что кривые

$$x_1^4 + y_1^4 = (1\pm i) z_1^2, \qquad x_2^4 + y_2^4 = (1\pm 2i) z_2^2, \qquad x_3^4 + y_3^4 = (2\pm i) z_3^2$$

в поле $R(i)$ вообще не имеют точек. Действительно, с одной стороны, не нарушая общности, можно считать $(x_1^4, y_1^4, (1\pm i)z_1^2) = (x_2^4, y_2^4, (1\pm 2i)z_2^2) = (x_3^4, y_3^4, (2\pm i)z_3^2) = 1$. С другой же стороны, при $(x_1 y_1, 1\pm i) = (x_2 y_2, 1\pm 2i) = (x_3 y_3, 2\pm i) = 1$ имеют место следующие сравнения:

$$x_1^4 + y_1^4 \equiv 2 (\mathrm{mod}\, 4), \qquad x_2^4 + y_2^4 \not\equiv 0 (\mathrm{mod}\, 1\pm 2i), \qquad x_3^4 + y_3^4 \not\equiv 0 (\mathrm{mod}\, 2\pm i),$$

поэтому

$$(1\pm i) z_1^2 \equiv 2 (\mathrm{mod}\, 4), \qquad (1\pm 2i) z_2^2 \not\equiv 0 (\mathrm{mod}\, 1\pm 2i), \qquad (2\pm i) z_3^2 \not\equiv 0 (\mathrm{mod}\, 2\pm i),$$

что невозможно.

Поскольку оставшиеся кривые $x^4 + y^4 = z^2$, $x^4 + y^4 = iz^2$ рассматриваются аналогично, то мы остановимся лишь на первой из них. Перепишем кривую $x^4 + y^4 = z^2$ в неоднородной форме: $x^4 + 1 = z^2$ и предположим, что ей принадлежит некоторая точка $P = \{a+bi, c+di\}$. В этом случае ей будет также принадлежать и сопряжённая точка

$P' = \{a-bi, c-di\}$. Сумма и разность этих точек дают нам следующие тождества:

$$(bc-ad)^4+(2ab)^4 = m^2, \quad (ac+bd)^4+(2ab)^4 = n^2,$$

где m и n — рациональные числа. Отсюда видно, что либо $2ab = 0$, либо $bc-ad = ac+bd = 0$. Из этих же равенств, соединенных с $(a+bi)^4+1 = (c+di)^2$ и вытекает утверждение леммы.

Теорема 2. *Если ранг кривой (3) над полем $R(i)$ не превышает 2, то кривая (1) не имеет точек в этом поле, за исключением случаев: $A=1$, $\{x,y\} = \{\varepsilon_1, 0\}, \{0, \varepsilon_2\}$; $A=2$, $\{x,y\} = \{\varepsilon_1, \varepsilon_2\}$, где $\varepsilon_1, \varepsilon_2$ — единицы этого поля.*

Доказательство. Согласно лемме 9 достаточно рассматривать кривую (1) при $A \neq d^2, id^2, (1\pm i)d^2, (1\pm 2i)d^2, (2\pm i)d^2$. Далее, если ранг этой кривой над полем $R(i)$ не превышает 2, то на основании работы [3] базис группы её точек может быть выбран следующим способом: $P_1 = P$, $P_2 = iP$. Как было отмечено в первом параграфе, каждая точка $Q = \{x_0, y_0, z_0\}$ кривой (1) порождает две точки $Q_1 = \{x_0, y_0, z_0^2\}$, $Q_2 = \{z_0, y_0, x_0^2\}$ кривой (3), причем, в силу однозначности разложения на простые множители в $R(i)$, можно считать, что $(x_0, y_0, z_0) = 1$.

Пусть $Q_1 = (m_1+n_1 i)P+O_1$, $Q_2 = (m_2+n_2 i)P+O_1'$; тогда найдутся такие взаимно-простые числа $c_1+d_1 i$, $c_2+d_2 i$, что

$$(c_1+d_1 i)Q_1' = (c_2+d_2 i)Q_2' = \{x,y,z\}, \quad Q_1' = Q_1-O_1, \quad Q_2' = Q_2-O_1'.$$

Очевидно, не нарушая общности, можно считать $c_1+d_1 i \not\equiv 0 \pmod{1+i}$.

Рассмотрим раздельно следующие два случая: 1) $c_2+d_2 i \not\equiv 0 \pmod{1+i}$, 2) $c_2+d_2 i \equiv 0 \pmod{1+i}$.

1) $c_2+d_2 i \not\equiv 0 \pmod{1+i}$. В поле $R(i)$ $(2) = (1+i)^2$, поэтому, на основании леммы 6, для этого случая выполняются сравнения:

$$\begin{aligned} x &\equiv 0 \pmod{x_0}, \quad (1+i)z \equiv 0 \pmod{z_0^2}, \\ x &\equiv 0 \pmod{z_0}, \quad (1+i)z \equiv 0 \pmod{x_0^2}. \end{aligned} \tag{23}$$

Так как $(x_0, z_0) = (x, z) = 1$, то из сравнений (23) следует:

$$1+i \equiv 0 \pmod{x_0^2 z_0^2},$$

то есть x_0, z_0 — единицы заданного поля $R(i)$.

2) $c_2+d_2 i \equiv 0 \pmod{1+i}$. Представим равенство $(c_1+d_1 i)Q_1' = (c_2+d_2 i)Q_2'$ в виде:

$$(p_1+q_1 i)Q_1'+(p_2+q_2 i)Q_2' = (r_1+s_1 i)Q_1'+(r_2+s_2 i)Q_2',$$

где $p_1+q_1 i, p_2+q_2 i, r_2+s_2 i \not\equiv 0 \pmod{1+i}$, $r_1+s_1 i \equiv 0 \pmod 2$. Очевидно, такое представление возможно. В этом случае, если положить

$(p_1+q_1 i)Q_1'+(p_2+q_2 i)Q_2' = \{x,y,z\}$, $(x,y,z) = 1$, то на основании леммы 7 x_0, y_0, z_0, x, y, z будут связаны следующими условиями:

$$1+i \equiv 0 \left(\mathrm{mod}\ (x_0 z_0, xz)\right),$$

$$(1+i)x \equiv 0 \pmod{z_0}, \quad (1+i)z \equiv 0 \pmod{x_0},$$

откуда

$$2 \equiv 0 \pmod{x_0 z_0}. \tag{24}$$

Таким образом, если ранг кривой (3) над полем $R(i)$ не превышает 2, то координаты точек кривой (1) удовлетворяют условию (24). Однако непосредственной проверкой убеждаемся, что кривая (3) имеет при указанных значениях x_0, y_0, z_0 ранг равный 2 лишь при $|x_0| = |y_0| = |z_0| = 1$, $A = 2$, что и требовалось доказать.

Аналогичным образом доказывается

Теорема 3. *Если ранг одной из кривых (4) над полем $R(\sqrt{-3})$ не превышает 2, то кривая (2) в этом поле точек не имеет, за исключением случаев: $A=1$, $\{x,y\} = \{\varepsilon_1, 0\}, \{0, \varepsilon_2\}$; $A=2$, $\{x,y\} = \{\varepsilon_1, \varepsilon_2\}$, $\varepsilon_1, \varepsilon_2$ — единицы поля $R(\sqrt{-3})$.*

§ 3. Точки кривых (1) и (2) во вполне вещественных алгебраических полях.

Лемма 10. *Если все сопряженные числа $A^{(p)}$ $(p = 1, 2, \ldots, n)$ положительны, то кривая (3) не имеет в K точек конечного порядка, за исключением случаев $A = 1$, $\{x,y,z\} = \{\pm 1, \pm 1, 0\}$ и $O = \{x,y,z\}$, где $y = 0$.*

Доказательство. Предположим, что некоторая точка P кривой (3) имеет конечный порядок m; тогда

$$mP = 0, \quad m = 2^{k_0}\prod_{j=1}^{t} p_j^{k_j}, \quad \left(\prod_{j=1}^{t} p_j^{k_j}, 2\right) = 1. \tag{25}$$

1) $k_j = 0$ $(j = 1, 2, \ldots, t)$. Действительно, если, например, $k_1 > 0$, то равенство (25) можно переписать в виде:

$$p_1 Q = 0, \quad Q = \left(2^{k_0} p_1^{k_1-1}\prod_{j=2}^{t} p_j^{k_j}\right)P \neq 0.$$

Обозначим координаты точек Q и $p_1 Q$ через $\{x_1, y_1, z_1\}$, $\{x_{p_1}, y_{p_1}, z_{p_1}\}$. На основании леммы 4

$$Ay_1^4 \equiv 0 \pmod{x_1^4}.$$

Так как по условию $A > 0$, то $x_1 \neq 0$ и (3) можно переписать в неоднородной форме:

$$1-\frac{Ay_1^4}{x_1^4} = \frac{z_1^2}{x_1^4}. \tag{26}$$

По доказанному левая часть (26) представляет собою целое число поля K, следовательно, правая часть также представляет собою целое число из этого поля. Очевидно, наряду с (26) можно записать следующую систему равенств:

$$1 = \left(\frac{Ay_1^4}{x_1^4} + \frac{z_1^2}{x_1^4}\right)^{(p)} \qquad (p = 1, 2, \ldots, n).$$

Из этих равенств вытекает:

$$N(1) = 1 = N\left(\frac{Ay_1^4}{x_1^4} + \frac{z_1^2}{x_1^4}\right) \geqslant 2^n \sqrt{N\left(\frac{Ay_1^4}{x_1^4}\right) N\left(\frac{z_1^2}{x_1^4}\right)}, \tag{27}$$

что возможно лишь при $z_1 = 0$. Однако при $z_1 = 0$

$$\Big|\sum_{k=0}^{(p_1^2-1)/4} (-1)^k a_k u^{(p_1^2-1)/4-k} v^k\Big| = 2^{(p_1^2-1)/8} v^{(p_1^2-1)/4} \neq 0,$$

что противоречит условию.

2) $k_0 \leqslant 1$. Предположим, что $k_0 \geqslant 2$. В этом случае в поле K должна существовать точка $Q = 2^{k_0-2}P$, порядок которой равен 4. Далее, из условий $Q = \{x_1, y_1, z_1\}$, $2Q = \{x_2, y_2, z_2\}$, $4Q = \{x_4, y_4, z_4\}$, $y_2 \neq 0$, $y_4 = 0$ вытекает: $x_2 z_2 = 0$. Как раннее было замечено, $x_2 \neq 0$, следовательно, $z_2 = z_1^4 + 4z_1^2 x_1^4 - 4x_1^8 = 0$, откуда $\pm z_1/x_1^2 = \sqrt{2\sqrt{2}-2}$. Однако при некотором p $(\pm z_1/x_1^2)^{(p)} = \sqrt{-2\sqrt{2}-2}$, то есть поле $K^{(p)}$ не вещественно, что противоречит условию. Случай $k_0 = 1$ легко проверяется непосредственным вычислением.

Следствие. *Если все сопряженные числа $A^{(p)}$ $(p = 1, 2, \ldots, n)$ положительны, то кривая*

$$Ax^4 - y^4 = z^2 \tag{28}$$

не имеет в K точек конечного порядка, за исключением случаев: $A = 1$, $\{x, y, z\} = \{\pm 1, \pm 1, 0\}$; $A = B^2$, $\{x, y, z\} = \{\pm 1, 0, B\}$.

Действительно, это утверждение непосредственно вытекает из предшествующей леммы если учесть, что каждая точка кривой (28) по формулам удвоения порождает точку кривой (3).

Теорема 4. *Если ранг кривой (3) над вполне вещественным полем K не превышает 1, то кривая (1) не имеет в этом поле точек, за исключением случаев: $A = 1$, $\{x, y\} = \{\pm 1, 0\}$, $\{0, \pm 1\}$; $A = 2$, $\{x, y\} = \{\pm 1, \pm 1\}$.*

Доказательство. При доказательстве этой теоремы целесообразно рассмотреть раздельно следующие 3 случая: a) $A \neq B^2$, b) $A = B^2$ но $\neq B^4$, c) $A = 1$.

Случай a). $A \neq B^2$. Предположим, что на кривой (1) лежит некоторая точка Q с координатами, принадлежащими полю K. В этом случае все сопряженные числа $A^{(p)}$ $(p = 1, 2, \ldots, n)$ положительны и кривая (28) также обладает точками из поля K. Нетрудно установить, что кривые (3) и (28) при $A \neq B^2$ различны. Действительно, если бы они совпадали, то для выполнения условий, указанных в первом параграфе, необходимо чтобы $A = B^2$ или $i \in K$, что невозможно. Далее, на основании леммы 10 и следствия из неё, эти кривые при $A \neq B^2$ не имеют точек конечного порядка, кроме $O = \{x, y, z\}$, где $y = 0$.

Обозначим базисную точку кривой (28) через $P = \{x_1, y_1, z_1\}$; тогда произвольно взятые точки P_1 и P_2 кривых (3) и (28) имеют соответственно вид: $mP + O_1$, $nP + O_1'$, где m — четное число, а n — нечетное. Возьмем какую-либо точку $Q = \{a, b, c\}$ кривой (1), как раннее было отмечено, она порождает две точки $Q_1 = \{a, b, c^2\}$, $Q_2 = \{c, b, a^2\}$ кривой (28), причем $Q_1 = (2m+1)P + O_1$, $Q_2 = (2n+1)P + O_1'$. На основании лемм 5 и 7 имеем:

$$\begin{aligned}
&\frac{x_{2m+1}^4}{(x_{2m+1}^4, Ay_{2m+1}^4)} \equiv 0\left(\bmod \frac{x_1^4}{(x_1^4, Ay_1^4)}\right),\\
&\frac{Ay_{2m+1}^4}{(x_{2m+1}^4, Ay_{2m+1}^4)} \equiv 0\left(\bmod \frac{Ay_1^4}{(x_1^4, Ay_1^4)}\right),\\
&\frac{2z_{2m+1}^2}{(x_{2m+1}^4, Ay_{2m+1}^4)} \equiv 0\left(\bmod \frac{z_1^2}{(x_1^4, Ay_1^4)}\right),\\
&\frac{4Ay_{2n}^4}{(x_{2n}^4, Ay_{2n}^4)} \equiv 0\left(\bmod \frac{Ax_1^4 y_1^4 z_1^4}{(x_1^4, Ay_1^4)^4}\right),\\
&\frac{2c_{2m+1,2n}^2}{(a_{2m+1,2n}^4, Ab_{2m+1,2n}^4)} \equiv 0\left(\bmod \frac{c^4}{(a^4, Ab^4)}\right),\\
&\frac{2a_{2m+1,2n}^4}{(a_{2m+1,2n}^4, Ab_{2m+1,2n}^4)} \equiv 0\left(\bmod \frac{a^4}{(a^4, Ab^4)}\right);
\end{aligned} \tag{29}$$

$$\begin{aligned}
&\frac{Ab_{2m+1,2n}^4}{(a_{2m+1,2n}^4, Ab_{2m+1,2n}^4)} \equiv 0\left(\bmod \frac{Ab^4}{(a^4, Ab^4)}\right),\\
&\frac{2a_{2n,2m+1}^4}{(a_{2n,2m+1}^4, Ab_{2n,2m+1}^4)} \equiv 0\left(\bmod \frac{c^4}{(a^4, Ab^4)}\right),\\
&\frac{Ab_{2n,2m+1}^4}{(a_{2n,2m+1}^4, Ab_{2n,2m+1}^4)} \equiv 0\left(\bmod \frac{Ab^4}{(a^4, Ab^4)}\right),\\
&\frac{2c_{2n,2m+1}^2}{(a_{2n,2m+1}^4, Ab_{2n,2m+1}^4)} \equiv 0\left(\bmod \frac{a^4}{(a^4, Ab^4)}\right),
\end{aligned} \tag{30}$$

где

$$(2m+1)\,P = \{x_{2m+1},\, y_{2m+1},\, z_{2m+1}\}, \qquad 2nP = \{x_{2n},\, y_{2n},\, z_{2n}\},$$
$$(2m+1)Q_1'+2nQ_2' = \{a_{2m+1,2n},\, b_{2m+1,2n},\, c_{2m+1,2n}\},$$
$$2nQ_1'+(2m+1)Q_2' = \{a_{2n,2m+1},\, b_{2n,2m+1},\, c_{2n,2m+1}\}.$$

По условию $Q_1' = (2m+1)P$, $Q_2' = (2n+1)P$, следовательно, можно подобрать такие две пары значений p и q, чтобы

$$p_1(2m+1)+q_1(2n+1) = p_2(2m+1)+q_2(2n+1),$$

где p_1, q_2 — четные, p_2, q_1 — нечетные. Тогда, на основании (30)

$$2\equiv 0\left(\mathrm{mod}\,\frac{a^4}{(a^4,\, Ab^4)}\right), \qquad 2\equiv 0\left(\mathrm{mod}\,\frac{c^4}{(a^4,\, Ab^4)}\right).$$

Поскольку $Q_1'\equiv Q_2' (\mathrm{mod}\, 2)$, то

$$\frac{a}{b} = \frac{x_{m+n+1}y_{m+n+1}z_{m-n}-x_{m-n}y_{m-n}z_{m+n+1}}{x^2_{m+n+1}y^2_{m-n}+x^2_{m-n}y^2_{m+n+1}},$$
$$\pm\frac{c^2}{b^2} = \frac{z_{m+n+1}z_{m-n}(x^2_{m+n+1}y^2_{m-n}-x^2_{m-n}y^2_{m+n+1})}{(x^2_{m+n+1}y^2_{m-n}+x^2_{m-n}y^2_{m+n+1})^2}+$$
$$+\frac{2x_{m+n+1}x_{m-n}y_{m+n+1}y_{m-n}(x^2_{m+n+1}x^2_{m-n}+Ay^2_{m+n+1}y^2_{m-n})}{(x^2_{m+n+1}y^2_{m-n}+x^2_{m-n}y^2_{m+n+1})^2},$$
(31)
$$\frac{c}{b} = \frac{x_{m+n+1}y_{m+n+1}z_{m-n}+x_{m-n}y_{m-n}z_{m+n+1}}{x^2_{m+n+1}y^2_{m-n}+x^2_{m-n}y^2_{m+n+1}},$$
$$\pm\frac{a^2}{b^2} = \frac{z_{m+n+1}z_{m-n}(x^2_{m+n+1}y^2_{m-n}-x^2_{m-n}y^2_{m+n+1})}{(x^2_{m+n+1}y^2_{m-n}+x^2_{m-n}y^2_{m+n+1})^2}-$$
$$-\frac{2x_{m+n+1}x_{m-n}y_{m+n+1}y_{m-n}(x^2_{m+n+1}x^2_{m-n}+Ay^2_{m+n+1}y^2_{m-n})}{(x^2_{m+n+1}y^2_{m-n}+x^2_{m-n}y^2_{m+n+1})^2}.$$

Разложим двойку на простые идеалы $2=\prod\limits_{j=1}^{t}p_j^{k_j}$. Нетрудно установить, что сравнения

(32) $$\frac{z^2_{m+n+1}}{(x^4_{m+n+1},\, Ay^4_{m+n+1})}\equiv 0, \qquad \frac{z^2_{m-n}}{(x^4_{m-n},\, Ay^4_{m-n})}\equiv 0\,(\mathrm{mod}\, p_j^{s_j})$$

могут одновременно выполняться лишь при $2\equiv 0(\mathrm{mod}\, p_j^{2s_j})$. Очевидно, $m+n+1,\, m-n\equiv 0\big(\mathrm{mod}\,(2m+1,\, 2n+1)\big)$. Поэтому, в силу (29)-(32)

(33) $$2(r,\, s)^2\equiv 0\,(\mathrm{mod}\, r^2+s^2),$$

где

$$r = x^2_{m+n+1}y^2_{m-n}-x^2_{m-n}y^2_{m+n+1}, \qquad s = 2x_{m+n+1}y_{m+n+1}x_{m-n}y_{m-n}$$

— целые числа.

Пусть число классов идеалов поля K равно h. Тогда идеал $(r,s)^h$ — главный и сравнение (33) можно переписать в виде

$$2^h(r,\, s)^{2h}\equiv 0\big(\mathrm{mod}\,(r^2+s^2)^h\big)$$

или

$$2^h(r^h,\, s^h)^2\equiv 0\big(\mathrm{mod}\,(r^2+s^2)^h\big),$$

откуда

$$2^{nh}N^2(r^h,\, s^h)\equiv 0\big(\mathrm{mod}\, N(r^2+s^2)^h\big).$$

Докажем, что числа r и s удовлетворяют одному из следующих соотношений:

(34) $$r=0, \qquad s=0, \qquad r=\pm s.$$

Доказательство проведем от противного. Предположим, что r и s не связаны ни одним из соотношений (34); тогда, учитывая, что K — вполне вещественное поле, имеем

$$(r^2+s^2)^{(p)} > 2\,|(r)^{(p)}(s)^{(p)}| \qquad (p=1, 2, \ldots, n),$$
$$2^{nh}N^2(r^h,\, s^h)\geqslant N(r^2+s^2)^h > 2^{nh}|N(r^h)|\,|N(s^h)|,$$

(35) $$1 > \left|\frac{N(r^h)}{N(r^h,\, s^h)}\right|\cdot\left|\frac{N(s^h)}{N(r^h,\, s^h)}\right|.$$

В силу (34), $\left|\frac{N(r^h)}{N(r^h,\, s^h)}\right|$, $\left|\frac{N(s^h)}{N(r^h,\, s^h)}\right|$ — натуральные числа, поэтому (35) невозможно, что и требовалось доказать.

Теперь рассмотрим раздельно следующие случаи: 1) $r=0$, 2) $s=0$, 3) $r=\pm s$.

1) $r=0$. Не нарушая общности, можно считать, что $m-n$ — четное, $m+n+1$ — нечетное. В этом случае система

$$x^4_{m-n}-Ay^4_{m-n}=z^2_{m-n}, \qquad Ay^4_{m+n+1}-x^4_{m+n+1}=z^2_{m+n+1},$$
$$x^2_{m+n+1}y^2_{m-n}-x^2_{m-n}y^2_{m+n+1}=0$$

дает

$$z^2_{m-n}y^4_{m+n+1}+z^2_{m+n+1}y^4_{m-n}=0,$$

что для вещественного поля возможно лишь при $z_{m-n}y_{m+n+1}= =z_{m+n+1}y_{m-n}=0$.

2) $s = 0$. Очевидно, этот случай возможен лишь при совпадении точек $Q_1 - O_1$ и $Q_2 - O_2$.

3) $r = \pm s$. Из

$$x_{m+n+1}^2 y_{m-n}^2 \pm 2x_{m+n+1}y_{m+n+1}x_{m-n}y_{m-n} - x_{m-n}^2 y_{m+n+1}^2 = 0$$

следует:

$$x_{m+n+1}y_{m-n} = (\pm 1 \pm \sqrt{2})x_{m-n}y_{m+n+1}.$$

Далее, система

$$x_{m-n}^4 - Ay_{m-n}^4 = z_{m-n}^2, \quad Ay_{m+n+1}^4 - x_{m+n+1}^4 = z_{m+n+1}^2,$$

даёт:

$$\pm 4\sqrt{2}(1 \pm \sqrt{2})^2 x_{m-n}^4 y_{m+n+1}^4 = z_{m-n}^2 y_{m+n+1}^4 + z_{m+n+1}^2 y_{m-n}^4.$$

На основании раннее доказанного, достаточно рассмотреть случай: $x_{m-n}y_{m+n+1} \neq 0$. Перепишем это равенство в виде:

$$\pm\sqrt{2} = \alpha^2 + \beta^2.$$

Так как K — вполне вещественное поле, то возможно лишь $\sqrt{2} = \alpha^2 + \beta^2$, но тогда для некоторого сопряженного поля $K^{(p)}$ выполнимо равенство $-\sqrt{2} = (\alpha^2+\beta^2)^{(p)}$, то есть $K^{(p)}$ не является вещественным, что противоречит условию.

Случай b). $A = B^2$, но $\neq B^4$. Отличие этого случая от раннее рассмотренного заключается в том, что нужно исследовать ещё и такие точки $Q_1 = mP + O_1$, $Q_2 = nP + O_1'$, при которых m и n будут различной чётности. Итак, пусть $m \equiv 0 \pmod 2$, а $n \not\equiv 0 \pmod 2$. Тогда

$$d_1(Ab^4) = Ax_m^4, \quad d_2(Ab^4) = Ay_n^4,$$
$$d_1a^4 = A^2y_m^4, \quad d_2c^4 = x_n^4,$$
$$d_1c^4 = Az_m^2, \quad d_2a^4 = z_n^2,$$

причём, на основании леммы 4,

$$\frac{Ay_m^4}{(x_m^4, Ay_m^4)}, \frac{Ay_n^4}{(x_n^4, Ay_n^4)} \equiv 0 \left(\operatorname{mod} \frac{Ay_1^4}{(x_1^4, Ay_1^4)}\right).$$

Следовательно,

$$\frac{a^4}{(a^4, Ab^4)}, \frac{Ab^4}{(a^4, Ab^4)} \equiv 0 \left(\operatorname{mod} \frac{Ay_1^4}{(x_1^4, Ay_1^4)}\right).$$

Таким образом, $x_1^4, z_1^2 \equiv 0 \pmod{Ay_1^4}$. Из равенства

$$Ay_1^4 - x_1^4 = z_1^2$$

видно, что все сопряженные числа $A^{(p)}$ $(p = 1, 2, \ldots, n)$ положительны. Далее, учитывая, что

$$1 = \left(\frac{x_1^4}{Ay_1^4} + \frac{z_1^2}{Ay_1^4}\right)^{(p)} \quad (p = 1, 2, \ldots, n),$$

имеем

$$1 \geqslant 2^n \sqrt{N\left(\frac{x_1^4}{Ay_1^4}\right) N\left(\frac{z_1^2}{Ay_1^4}\right)},$$

что при $x_1 z_1 \neq 0$ невозможно.

Случай c). $A = B^4$. Так как A можно считать свободным от биквадратов, то рассмотрению подлежит кривая (1) при условии $A = 1$. Заметим, что согласно случаям a) и b) и симметричности точек Q_1 и Q_2, достаточно рассмотреть лишь следующие два случая:

1) $Q_1 = mP + P_0 + O_1$, $Q_2 = nP + P_0 + O_1'$,

2) $Q_1 = mP + P_0 + O_1$, $Q_2 = nP + O_1'$,

где P_0 — точка второго порядка, указанная в лемме 10.

По формулам сложения для этих случаев имеем:

1)
$$d_1a^4 = (x_m^2 - y_m^2)^2, \qquad d_2c^4 = (x_n^2 - y_n^2)^2,$$
$$d_1b^4 = (x_m^2 + y_m^2)^2, \qquad d_2b^4 = (x_n^2 + y_n^2)^2,$$
$$d_1c^4 = 4x_m^2 y_m^2, \qquad d_2a^4 = 4x_n^2 y_n^2$$

и

2)
$$d_1a^4 = (x_m^2 - y_m^2)^2, \qquad d_2c^4 = y_n^4,$$
$$d_1b^4 = (x_m^2 + y_m^2)^2, \qquad d_2b^4 = x_n^4,$$
$$d_1c^4 = 4x_m^2 y_m^2, \qquad d_2a^4 = z_n^2,$$

откуда

$$\frac{a^4}{(a^4, c^4)}, \frac{c^4}{(a^4, c^4)} \equiv 0 \left(\operatorname{mod} \frac{x_1^2 y_1^2}{(x_1^4, y_1^4)}\right)$$

для первого случая и

$$\frac{a^4}{(a^4, b^4)} \equiv 0 \left(\operatorname{mod} \frac{x_1^2 y_1^2}{(x_1^4, y_1^4)}\right), \qquad \frac{b^4}{(a^4, b^4)} \equiv 0 \left(\operatorname{mod} \frac{y_1^4}{(x_1^4, y_1^4)}\right)$$

для второго. Следовательно, $x_1^4, z_1^2 \equiv 0 \pmod{y_1^4}$, что по раннее доказанному невозможно. Теорема доказана.

Аналогичным образом доказывается

Теорема 5. *Если ранг одной из кривых*

$$x^3 + y^2 = A, \quad x^3 + 1 = Ay^2, \quad y^2 + 1 = Ax^3$$

над вполне вещественным полем K не превышает 1, то кривая

$$x^6+y^6 = A$$

за исключением случаев: $A=1, \{x,y\} = \{\pm 1, 0\}, \{0, \pm 1\}$; $A = 2, \{x,y\} = \{\pm 1, \pm 1\}$ *в этом поле точек не имеет.*

В заключение, выражаю глубокую благодарность И. Р. Шафаревичу за ряд ценных замечаний, касающихся этой работы.

Цитированная литература

[1] L. J. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees*, Proc. Cambridge Philos. Soc. (1922), стр. 179-192.

[2] A. Weil, *Sur un théorème de Mordell*, Bull. Sci. Math. (2) 54 (1930), стр. 182-191.

[3] G. Billing, *Beiträge zur arithmetischen Theorie ebenen kubischen Kurven vom Geschlecht eins*, Nove acta regiae Societatis Scientiarum Upsaliensis, Ser. 4, 11 (1938), стр. 1-165.

[4] В. Д. Подсыпанин, *О неопределенном уравнении $x^3 = y^2+Az^6$*, Мат. сб. 24. 3 (1949), стр. 391-405.

[5] L. E. Dickson, *History of the theory of numbers*, vol. II, Washington 1920.

Reçu par la Rédaction le 20. 5. 1966

ACTA ARITHMETICA
XII (1967)

Некоторые критерии простоты чисел, связанные с малой теоремой Ферма

М. М. Артюхов (Орджоникидзе)

Основные результаты в задачах, относящихся к обращению теоремы Ферма, были сообщены ранее Крайчиком [1] и Лемером [2], [3]. В 1957 году Робинсон [4] опубликовал доказательство довольно своеобразной теоремы, формулировку которой я здесь приведу в следующей редакции:

Пусть даны: натуральное число $a>1$, нечетное натуральное число $m<3\cdot 2^{a+1}$, $n=2^am+1$, и пусть ω — какое нибудь целое число, для которого символ Якоби $\left(\frac{\omega}{n}\right) = -1$. Для того, чтобы n было простым числом, необходимо и достаточно, чтобы $n|\omega^{(n-1)/2}+1$.

Применимость теоремы Робинсона весьма ограничена условием $m<3\cdot 2^{a+1}$, поскольку при каждом данном a имеется не более, чем $3\cdot 2^a$ чисел n, допускающих испытание на простоту с помощью этого критерия. В связи с этим я предлагаю здесь несколько теорем, одни из которых приложимы при каждом фиксированном a к сколь угодно большим числам $n=2^am+1$ некоторых специальных видов, другие — имеют более универсальный характер.

Основные обозначения. a, h и ω будем считать заданными натуральными числами, причем h — нечетным, а $\omega>1$. Полагаем $n=2^ahk+1$, где k до наложения на него специальных условий будет любым нечетным натуральным числом, при котором $(n,\omega)=1$. Для краткости еще положим $\omega^{h2^{a-1}} = a$ и $a^{k-1}-a^{k-2}+\ldots+a^2-a+1 = N$. Символ $\left(\frac{\omega}{n}\right)$ всюду будет употребляться как символ Якоби.

Лемма 1 (Эйлера). 1-ая формулировка: *Если p простое число и ω — квадратичный невычет модуля p, то $p|\omega^{(p-1)/2}+1$.*

2-ая формулировка: *Если $\left(\frac{\omega}{n}\right) = -1$, то при n простом $n|\omega^{(n-1)/2}+1$.*