Доклады Академии Наук СССР
1947. Том LVIII, № 6

МАТЕМАТИКА

А. В. ДОРОДНОВ

О КРУГОВЫХ ЛУНОЧКАХ, КВАДРИРУЕМЫХ ПРИ ПОМОЩИ ЦИРКУЛЯ И ЛИНЕЙКИ

(Представлено академиком С. Н. Бернштейном 19 V 1947)

Постановка задачи. В уравнении

$$P(x) = n\left(\frac{x^m-1}{x-1}\right)^2 - mx^{m-n}\left(\frac{x^n-1}{x-1}\right)^2 = 0 \qquad (*)$$

определить целые, положительные и взаимно простые числа $m > n$ так, чтобы группа Галуа какого-либо его неприводимого множителя имела порядок, равный степени числа 2.

Гиппократ (440 г. до н. э.) нашел следующие решения:

$$m=2,\quad n=1;\qquad m=3,\quad n=1;\qquad m=3,\quad n=2.$$

Clausen (1840 г.) добавил еще два случая:

$$m=5,\quad n=1;\qquad m=5,\quad n=3.$$

и высказал предположение, что этими пятью случаями исчерпываются все квадрируемые луночки.

E. Landau в 1903 г. и Л. Чакалов в 1927 и 1929 гг. ([1-3]) показали, что во многих случаях уравнение (*) не решается в квадратных радикалах.

Н. Г. Чеботарев в 1934 г. ([4,5]) методами теории p-адических чисел доказал справедливость утверждения Clausen'а для случая, когда оба числа m, n нечетные.

Настоящая работа служит продолжением исследований Н. Г. Чеботарева для случая, когда одно из чисел m, n четное, а другое нечетное. В ней задача решена до конца.

Положим в уравнении (*) $x=y^2$ и рассмотрим в поле $K\left(\sqrt{\frac{m}{n}}\right)$ один из его множителей, умноженный на $(x-1)^2$:

$$y^{2m} - 1 - \sqrt{\frac{m}{n}}\, y^{m-n}(y^{2n}-1) = 0. \qquad (1)$$

Разложим его корни в ряды по возрастающим степеням простого числа, входящего в m, n и $m-n$, и определим вид показателей ρ при p:

$$x_i = a + a_1 p^{\rho_1} p + a_2 p^{\rho_2} + \ldots$$

1. $m = p^k \cdot m_1$, $(m_1, p) = 1$. Тогда ρ имеют вид:

1) a — иррационально. $\rho = \dfrac{1}{p^i(p-1)}$, $\rho = \dfrac{2i-k}{2p^i}$, $\dfrac{k}{2} < i \leqslant k$. (1,0)

Число корней, соответствующих этим ρ, равно $(m_1-1)\cdot p^k$, если m_1 — нечетное, и $(m_1-2)\cdot p^k$, если m_1 — четное число.

2) $a = \pm 1$. $\rho = \dfrac{1}{p^i(p-1)}$, $\rho = \dfrac{2i-k}{2(p^i-1)}$, $\dfrac{k}{2} < i \leqslant k$. (1,1)

Число корней, соответствующих $a=+1$, равно p^k и для $a=-1$ тоже p^k.

2. $n=q^{k_1}\cdot n_1$, $(n_1, q)=1$. $\rho=0$, $\rho=\pm\frac{k_1}{2(m-n)}$. (1,2)

Для $\rho=0$ дальнейшие члены разложения дадут:

1) $a\neq\pm 1$. $\rho=\frac{1}{q^i(q-1)}$, $\rho=\frac{2i-k_1}{2q^i}$, $\frac{k_1}{2}<i\leqslant k_1$. (1,3)

2) $a=\pm 1$. $\rho=\frac{1}{q^i(q-1)}$, $\rho=\frac{2i-k_1}{2(q^i-1)}$, $\frac{k_1}{2}<i\leqslant k_1$. (1,4)

Число корней с $\rho=0$ будет n, а с $\rho=\pm\frac{k_1}{2(m-n)}$ их будет $2(m-n)$.

3. $m-n=r^{k_2}\cdot r_1$, $(r, r_1)=1$.

1) $a^n\neq 1$. $\rho=\frac{i}{r^{i-1}(r-1)}$, $\rho=\frac{1}{r}$, $i\leqslant k_2$. (1,5)

2) $a^n=1$. $\rho=\frac{1}{r^{i-1}(r-1)}$, $\rho=\frac{1}{r-1}$, $i=2, 3, \ldots, k_2$. (1,6)

Число корней с $\rho=\frac{1}{r-1}$ равно r^{k_2}.

4. $m=2^\lambda m_1$, $(m_1, 2)=1$.

1) $a^{2n}\neq 1$. $\rho=\frac{1}{2^{i-1}}$, $\rho=\frac{2i-\lambda}{2^{i+1}}$, $\frac{\lambda}{2}<i\leqslant\lambda$. (1,7)

2) $a^{2n}=1$. $\rho=\frac{1}{2^i}$, $\rho=\frac{2i-\lambda}{2(2^i-1)}$, $\frac{\lambda}{2}<i\leqslant\lambda$. (1,8)

Рассмотрим отдельно случаи, когда m — четное, а n — нечетное число, и наоборот.

1. $m=2^\lambda\cdot p^k\ldots$, $n=q^s\ldots$

Разлагая корни уравнения (1) в ряды по степеням простых чисел $2, p, q, \ldots$, мы найдем для m, n следующие возможные значения:

1)	$m=2^\lambda$,	$n=9$,	$\lambda=4, 5, 6, 7, 8, 9$.
2)	$m=2^\lambda$,	$n=27$,	$\lambda=5, 6, 7, 8, 9$.
3)	$m=2^\lambda\cdot 17$,	$n=9$,	$\lambda=1, 2, 3, \ldots, 9$.
4)	$m=2^\lambda\cdot 17$,	$n=27$,	$\lambda=1, 2, 3, \ldots, 9$.
5)	$m=2^\lambda\cdot 5$,	$n=9$,	$\lambda=2, 3, \ldots, 7$.
6)	$m=2^\lambda\cdot 5$,	$n=27$,	$\lambda=3, 4, \ldots, 7$.
7)	$m=2^\lambda$,	$n=45$,	$\lambda=6, 7$.
8)	$m=2^\lambda$,	$n=153$,	$\lambda=8, 9$.
9)	$m=2^9$,	$n=27\cdot 17$,	
10)	$m=2^\lambda\cdot 3$,	$n=5$,	$\lambda=2, 3, 4, 5$,
11)	$m=2^\lambda\cdot 9$,	$n=5$,	$\lambda=1, 2, \ldots, 7$.
12)	$m=2^\lambda\cdot 27$,	$n=5$,	$\lambda=1, 2, \ldots, 7$.
13)	$m=2^\lambda\cdot 9$,	$n=17$,	$\lambda=2, 3, \ldots, 9$.
14)	$m=2^\lambda\cdot 27$,	$n=17$,	$\lambda=1, 2, \ldots, 9$.

(2)

(3)

Кроме того, $m=2^\lambda$, $n=2^{2^s}+1$ — простое гауссово число.

Случаи (2), (3) не дают уравнений, решаемых в квадратных радикалах. В этом проще всего убедиться, рассматривая уравнение (1) как сравнение по простому модулю, делящему разность $m-n$. Тогда левая часть сравнения будет содержать неприводимые по этому модулю множители, из которых нельзя составить полинома, степень ко-

торого есть степень числа 2. Этот способ проверки не охватывает лишь следующих четырех случаев:

$$m=16,\ n=9;\quad m=72,\ n=5;\quad m=144,\ n=5;\quad m=864,\ n=5.$$

Однако полное построение многоугольника Ньютона показывает, что все они неблагоприятны.

Особого исследования требует случай, когда $m=2^\lambda$, $n=2^{2^\sigma}+1$ (простое число). Рассмотрим уравнение (*). Л. Чакалов ([1,3]) доказал, что оно или неприводимо, или разлагается в произведение двух неприводимых полиномов степеней $2(n-1)$ и $2(m-n)$. Покажем, что здесь оно всегда неприводимо. Разлагая корни уравнения (*) по степеням числа 2, получим для λ ограничение

$$2^\sigma<\lambda\leqslant 2\cdot 2^\sigma-2. \qquad (**)$$

Обозначим через $g(x)$ тот неприводимый множитель левой части уравнения (*), который имеет степень $2(n-1)$ и старший коэффициент единицу. $g(x)$ — возвратный полином первого рода. Рассмотрим уравнение (*) как сравнение по модулю n. Тогда

$$g(x)\equiv\left(\frac{x^n-1}{x-1}\right)^2 \pmod n.$$

Лемма. $g(-1)=1$.

Доказательство. Из $P(-1)=g(-1)\cdot h(-1)=2^\lambda$ следует, что $g(-1)=2^\alpha$, $h(-1)=2^\beta$, где $\alpha+\beta=\lambda\leqslant 2\cdot 2^\sigma-2$. Полагая в сравнении

$$g(x)\equiv\left(\frac{x^n-1}{x-1}\right)^2 \pmod n$$

$x=-1$, получим $g(-1)\equiv 1 \pmod n$, т. е. $2^\alpha-1=n\cdot Q$. Следовательно, должно быть $\alpha=2\cdot\alpha_1$, где α_1 кратно 2^σ. Но в силу (**) может быть только $\alpha=0$.

Теорема. *Уравнение* (*) *неприводимо.*

Доказательство. Пусть оно приводимо: $P(x)=g(x)\cdot h(x)=0$. Рассмотрим его как сравнение по модулю 2; получим $g(x)\cdot h(x)\equiv n(x-1)^{2m-2} \pmod 2$. Отсюда $g(x)\equiv(x-1)^{2n-2} \pmod 2$. Положим $x=-1$. Получается

$$g(-1)=1\equiv 2^{2n-2} \pmod 2,$$

т. е. противоречие. Итак, рассматриваемый случай неблагоприятен, так как уравнение (*) неприводимо, а следовательно, его степень $2\cdot 2^\lambda-2$ делится на нечетное число.

Случай $m=2^\lambda$, $n=1$. Уравнение (*) имеет все комплексные корни, среди которых два с модулем, равным единице. Но так как в возвратное уравнение первого рода корни с отличным от единицы модулем входят по четыре, то после понижения степени при помощи подстановки $z=x+\frac{1}{x}$ в уравнении окажется один вещественный корень, а все остальные комплексные. Таким образом, степень неприводимого множителя, который имеет этот вещественный корень, нечетная, и случай неблагоприятен. Благоприятный случай может наступить только тогда, когда степень уравнения (*) равна 2, откуда $\lambda=1$, так что тогда

$$m=2,\ n=1.$$

2. $m=p^k\ldots$, $n=2^\lambda\cdot q^s\ldots$

Разлагая корни уравнения (1) в ряды по степеням простых чисел, входящих в m и n, найдем следующие возможные значения:

1) $m=p=2^{2^\sigma}+1$, $n=2^\lambda$, 4) $m=27$, $n=2^\lambda\cdot 5$,
2) $m=15$, $n=2^\lambda$, 5) $m=9$, $n=2^\lambda$.
3) $m=27$, $n=2^\lambda$,

Исследуем их.

1) $m=p=2^{2^\sigma}+1$, $n=2^\lambda$, причем p простое число. В этом случае степень неприводимого множителя $g(x)$ равна или $2(p-1)$, или $p-1$. В первом случае уравнение (1) после удаления тривиальных корней $x=\pm 1$ станет неприводимым, а это означает, что все значения ρ должны быть благоприятны, т. е. что их знаменатель должен быть равен степени 2. Но среди них находятся значения

$$\rho=\frac{2i-\lambda}{2^2(2^i-1)},\quad \rho=\pm\frac{1}{2(m-n)}.$$

Первое говорит о том, что должно быть $i=\lambda=1$, а второе требует, чтобы $m-n=1$. Окончательно имеем

$$m=3,\qquad n=2.$$

Если же степень $g(x)$ равна $p-1$, то примем во внимание, что значению $\rho=0$ соответствует $2n$ корней, среди которых находятся и тривиальные $x=\pm 1$; следовательно, на долю $g(x)$ приходятся корни из числа $2(n-1)$. Но $p>n$, и между n и $2n$ нет числа, равного степени двойки, а потому должно быть $p-1=2(n-1)$, т. е. опять $m=3$, $n=2$.

2) $m=15$, $n=2^\lambda$. Степень неприводимого множителя $g(x)$ должна быть равна 4, следовательно $\lambda=2, 3$. Рассматривая уравнение (1) как сравнение по модулям 11 и 7, получим:

$$(x^{11}-1)(x^{19}+1)\equiv 0 \pmod{11},\quad (x^7-1)(x^{23}+1)\equiv 0 \pmod 7.$$

Из $11^f\equiv 1 \pmod{19}$ и $7^f\equiv 1 \pmod{23}$ следует соответственно $f=3$ и $f=22$. Оба случая неблагоприятны.

3) $m=27$, $n=2^\lambda$. Степень $g(x)$ или равна 16, или равна 8. Оба случая неблагоприятны.

4) $m=27$, $n=2^\lambda\cdot 5$. Степень $g(x)$ равна 8, следовательно, $\lambda=1, 2$. Тогда уравнение (1), как сравнение, запишется так:

$$(x^{17}-1)(x^{37}+1)\equiv 0 \pmod{17},\quad (x^7-1)(x^{47}+1)\equiv 0 \pmod 7.$$

Из $17^f\equiv 1 \pmod{37}$ следует $f=36$, а из $7^f\equiv 1 \pmod{47}$ следует $f=23$, т. е. оба случая неблагоприятны.

5) $m=9$, $n=2^\lambda$. Степень $g(x)$ равна или 8, или 16. В обоих случаях $\lambda=3$. Тогда, если степень $g(x)$ равна 16, уравнение (1) неприводимо после удаления тривиальных корней $x=\pm 1$, и все циклы должны быть благоприятны. Но мы имеем

$$\rho=\pm\frac{\lambda}{2(m-n)}=\pm\frac{3}{2},\qquad \rho=\frac{2i-\lambda}{2^2(2^i-1)},$$

где $\lambda/2<i\leqslant\lambda$, т. е. $i=2, 3$. Оба значения i дают знаменатель, отличный от чистой степени 2. Для исследования случая, когда степень $g(x)$ равна 8, построим многоугольник Ньютона для уравнения (*), разлагая его корни в ряды по степеням 3 и предварительно сделав замену $x=y+1$. Мы увидим, что оно неприводимо. Случай неблагоприятный. Итак, утверждение Clausen'a полностью доказано.

Институт математики и
механики при Казанском
государственном университете

Поступило
19 V 1947

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] L. Tschakaloff, Math. Z., **30**, 552 (1929). [2] Л. Чакалов, 23. Годишникъ на Соф. унив., физ.-мат. фак., кн. 1, 201 (1927). [3] Л. Чакалов, Спис. на Бѣлг. акад. на наукитѣ, **41**, 1 (1929). [4] N. Tschebotarëw, Math. Z., **39**, 161 (1934). [5] Н. Чеботарев, Основы теории Галуа, **1**, 1934.