Об условиях, при которых число решений уравнения $X^n = 1$ в группе является наименьшим

А. Н. Прокофьев

Согласно известной теореме Г. Фробениуса, если число n делит порядок группы $\mathfrak{G}$, то число решений уравнения $X^n = 1$ в группе $\mathfrak{G}$ делится на n. Отсюда вытекает, что наименьшим возможным числом решений уравнения $X^n = 1$ будет n. Вопросом о том, при каких условиях число решений уравнения $X^n = 1$ в данной группе является наименьшим, также занимался еще Фробениус. Он получил следующий результат [1]:

Если $\mathfrak{G}$ есть группа порядка ab, число a не делится на квадрат простого числа, b взаимно просто с $a\varphi(a)$, то в группе $\mathfrak{G}$ имеется ровно b решений уравнения $X^b = 1$ [1].

Небольшое обобщение этой теоремы Фробениуса недавно найдено Ц. С. Фу [3]:

Если $\mathfrak{G}$ есть группа порядка ab, b взаимно просто с $a\varphi(a)$ и не существует двух различных циклических подгрупп, сопряженных в группе $\mathfrak{G}$ и заключенных в одной и той же силовской подгруппе порядка делящего a, то число решений уравнения $X^b = 1$ равно b.

В настоящей работе указанные результаты Фробениуса и Фу дополнены исследованием того случая, когда $b = p^k$, p — простое число (теорема 1), после чего выясняются еще некоторые достаточные условия равенства числа решений уравнения $X^b = 1$ числу b уже для b, делящегося на два различные простые числа (теорема 2).

Для дальнейшего изложения будут полезны следующие определения.

Определение 1. Силовская подгруппа порядка p^l группы $\mathfrak{G}$ называется особенной по числу q^k (q — простое число), если она удовлетворяет одному из следующих условий:

1°. $p = q$, $k = l$, силовская p-подгруппа инвариантна.

2°. $p = q$, $k < l$, силовские p-подгруппы циклические, а порядок их пересечения не меньше p^k.

---

[1] Ц. С. Фу в качестве окончательного результата Фробениуса по указанному вопросу рассматривает другую, менее общую, теорему (см. [3], стр. 253), а приведенный нами результат Фробениуса Фу формулирует в качестве следствия своей теоремы, не отмечая, что оно было получено еще Фробениусом.

3°. $p=q=2$, $k=1<l$, силовская p-подгруппа либо циклическая, либо определяется равенствами

$$A^{2^{l-1}}=1, \quad B^2=A^{2^{l-2}}, \quad B^{-1}AB=A^{-1} \qquad (l\geqslant 3). \tag{1}$$

4°. $p=q$, $k=0$.

5°. $p\neq q$.

Определение 2. Пусть $n=ab$, a взаимно просто с b; тогда силовская подгруппа группы $\mathfrak{G}$ называется особенной по числу n, если она является особенной по каждому из чисел a, b; в противном случае рассматриваемая силовская подгруппа называется неособенной по числу n.

Теорема 1. *Пусть простое число p не делит число a, порядок данной группы $\mathfrak{G}$ равен ap^l. Тогда число решений уравнения*

$$X^{p^k}=1, \quad k\leqslant l,$$

равно p^k в том, и только в том случае, когда силовская p-подгруппа группы $\mathfrak{G}$ является особенной по числу p^k.

Доказательство. Достаточно определить, в каких случаях число N решений уравнения $X^{p^k}=1$ в группе $\mathfrak{G}$ равно p^k и в каких оно больше p^k.

1. $k=l$, силовская p-подгруппа $\mathfrak{P}$ инвариантна.

Всякое решение уравнения $X^{p^k}=1$, будучи элементом порядка делящего p^k, входит в $\mathfrak{P}$, и любой элемент группы $\mathfrak{P}$ удовлетворяет уравнению $X^{p^k}=1$. Следовательно, в этом случае $N=p^k$.

2. $k=l$, силовская p-подгруппа не инвариантна. Так как число силовских p-подгрупп в этом случае более одной, то $N>p^k$.

3. $k<l$, $p\neq 1$ или $p\neq 2$, силовская p-подгруппа нециклическая. Тогда, в силу теоремы § 96(6), силовская p-подгруппа содержит более одной подгруппы порядка p^k, а потому $N>p^k$.

4. $k<l$, силовская p-подгруппа циклическая, порядок пересечения силовских p-подгрупп меньше p^k. Не трудно видеть, что если целое число n делит порядок циклической группы, то число решений уравнений $X^n=1$ в этой группе равно n. Поэтому произвольно выбранная силовская p-подгруппа $\mathfrak{P}$ группы $\mathfrak{G}$ содержит p^k решений уравнения $X^{p^k}=1$. Если допустить, что ни одна из остальных силовских p-подгрупп не содержит ни одного решения уравнения $X^{p^k}=1$, не входящего в $\mathfrak{P}$, то все p^k решений этого уравнения в группе $\mathfrak{G}$ входят в каждую силовскую p-подгруппу, а потому и в пересечение всех таких подгрупп, что противоречит исходной предпосылке. Следовательно, силовские p-подгруппы группы $\mathfrak{G}$ содержат по меньшей мере одно решение уравнения $X^{p^k}=1$ помимо тех его решений, которые входят в $\mathfrak{P}$, а потому $N>p^k$.

5. $k<l$, силовская p-подгруппа циклическая, порядок пересечения силовских p-подгрупп не меньше p^k. Это пересечение, будучи циклической группой, содержит ровно p^k решений уравнения $X^{p^k}=1$. Ни одна силовская p-подгруппа, поскольку она является циклической, не может содержать ни одного решения уравнения $X^{p^k}=1$ сверх p^k решений этого уравнения, принадлежащих указанному пересечению. Следовательно, в этом случае $N=p^k$.

6. $k = 1 < l$, $p = 2$, силовская p-подгруппа не является ни циклической, ни группой типа (I). Тогда в силу теоремы § 96(6) эта силовская подгруппа содержит более одной подгруппы второго порядка, а следовательно, $N > 2$, т. е. $N > p^k$.

7. $k = 1 < l$, $p = 2$, силовская p-подгруппа либо циклическая, либо типа (I). В этом случае согласно той же теореме § 96(6), $N = p^k$.

Случаи 1, 5, 7, а также случай $k = 0$ определяют силовскую p-подгруппу группы $\mathfrak{G}$ как особенную. Оказалось, что только в этих случаях $N = p^k$.

А. А. Кулаков в [2, § 2] указал достаточные условия, при которых число решений уравнения $X^{p^k} = 1$ в группе делится на p^{k+1}; эти достаточные условия дает, впрочем, и теорема V [5]. Теорема 1 дает по этому вопросу необходимые и достаточные условия, которая выражает очевидное

Следствие 1 теоремы 1. *Если p^k, p — простое число, делит порядок группы $\mathfrak{G}$, то для того, чтобы число решений уравнения $X^{p^k} = 1$ в группе $\mathfrak{G}$ делилось на p^{k+1}, необходимо и достаточно, чтобы силовская p-подгруппа группы $\mathfrak{G}$ была неособенной по числу p^k.*

Для применения теоремы V [5] Ф. Холла и тех из теорем и их следствий моей работы [5], в которых употребляется функция Холла $\varkappa(\mathfrak{G}, \mathfrak{H}, n)$ (определение этой функции см. в [4] или в [5]), иногда оказывается полезным

Следствие 2 теоремы 1. *Если h — порядок группы $\mathfrak{H}$, $(n, h) = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ — каноническое разложение числа (n, h), $p_1, p_2, \dots, p_\sigma$, где $\sigma \leqslant s$ — нечетные простые числа, которым соответствуют неособенные по (n, h) силовские подгруппы группы $\mathfrak{H}$, то функция Холла $\varkappa(\mathfrak{G}, \mathfrak{H}, n)$ делится на произведение*

$$p_1^{\alpha_1+1} p_2^{\alpha_2+1} \dots p_\sigma^{\alpha_\sigma+1} \dots p_s^{\alpha_s}.$$

В самом деле, сначала положим $n = p^k$. В определении функции Холла всегда $m_1 \geqslant m_3$, $m_2 \geqslant m_3$, а потому достаточно рассмотреть случай $m = m_3$. Но число ϱ_k для неособенной группы всегда больше k, а при $p > 2$, кроме того, и $k(p-1) > k$. Поэтому для $n = p^k$ теорема верна. Применив этот результат к каждому из чисел $p_1^{\alpha_1}, p_2^{\alpha_2}, \dots, p_s^{\alpha_s}$ и воспользовавшись равенством

$$\varkappa(\mathfrak{G}, \mathfrak{H}, p_1^{\alpha_1}) \varkappa(\mathfrak{G}, \mathfrak{H}, p_2^{\alpha_2}) \dots \varkappa(\mathfrak{G}, \mathfrak{H}, p_s^{\alpha_s}) = \varkappa(\mathfrak{G}, \mathfrak{H}, n),$$

получаем доказываемое следствие.

Теорема 2. *Если все силовские подгруппы группы $\mathfrak{G}$ являются особенными по числу n, делящему порядок группы $\mathfrak{G}$, то число решений уравнения $X^n = 1$ в группе $\mathfrak{G}$ равно n.*

Доказательство. Пусть каноническое разложение числа n есть $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$. По условию доказываемой теоремы все силовские подгруппы группы $\mathfrak{G}$ являются особенными по каждому из чисел $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$. Поэтому, в силу теоремы 1, уравнения

$$X^{p_1^{\alpha_1}} = 1, \quad X^{p_2^{\alpha_2}} = 1, \dots \quad X^{p_s^{\alpha_s}} = 1$$

имеют в группе $\mathfrak{G}$ соответственно ровно $p_1^{\alpha_1}, p_2^{\alpha_2}, \dots, p_s^{\alpha_s}$ решений. Принимая во внимание теорему § 69 [6], отсюда заключаем, что число решений уравнения $X^n = 1$ в группе $\mathfrak{G}$ равно n.

По поводу работы Ц. С. Фу [3] заметим еще, что ее теорему 2 очень легко усилить. Действительно, не трудно проверить, что условия теоремы 2 [3] означают выполнение теоремы 1 [3] для любых

$$a = cq_1^{r_1} \dots q_{\mu-1}^{r_{\mu-1}}, \quad b = b_\mu = q_\mu^{r_\mu} \dots q_m^{r_m}, \qquad \mu = 1, 2, \dots, m.$$

Поэтому согласно теореме 1 [3] при выполнении условий теоремы 2 [3] группа $\mathfrak{G}$ содержит ровно v_μ элементов, порядки которых делят b_μ.

Теперь воспользуемся следующей известной теоремой Фробениуса (см., например, в § 68 [6]).

Если порядок группы $\mathfrak{G}$ делится на число n, то элементы ее, порядки которых делят n, порождают характеристическую подгруппу группы $\mathfrak{G}$, порядок которой делится на n.

Положив в этой теореме $n = b_\mu$, приходим к следующему усилению теоремы 2 [3] Ц. С. Фу:

Пусть $q_1, \dots, q_m$ — *различные простые числа, не делящие* $c\varphi(c)$, *каждое* $q_\mu (1 < \mu \leqslant m)$ *не делит произведение* $(q_1 - 1) \dots (q_\mu - 1)$, $\mathfrak{G}$ — *группа порядка* $cq_1^{r_1} \dots q_m^{r_m}$, *в которой никакие две сопряженные циклические подгруппы не содержатся в одной и той же силовской подгруппе порядка, делящего* $cq_1^{r_1} \dots q_{m-1}^{r_{m-1}}$. *Тогда элементы группы* $\mathfrak{G}$, *порядки которых делят число*

$$b_\lambda = q_\lambda^{r_\lambda} \dots q_m^{r_m}, \quad \lambda = 1, 2, \dots, m,$$

составляют характеристическую подгруппу порядка b_λ, *группы* $\mathfrak{G}$.

Способом, которым мы получили это следствие теоремы 1 [3], можно, разумеется, получить подобное же следствие теоремы 2 настоящей работы.

ЛИТЕРАТУРА

1. G. Frobenius, Über auflösbare Gruppen, Sitzungsberichte Berl. Akad., 1893, стр. 337—345.

2. А. Л. Кулаков, Некоторые замечания на работу „О теореме Фробениуса" П. Холла. Матем. сборник, т. 3 (45), 1938, стр. 403—405.

3. C. S. Fu, On Frobenius'theorem, Quart. Journ. of math., Oxford series, Vol. 17, 1946, No 68, стр. 253—256.

4. А. Н. Прокофьев, О фундаментальной теореме Фробениуса, ДАН СССР, т. 65, № 6, 1949, стр. 801—804.

5. А. Н. Прокофьев, О фундаментальной теореме Г. Фробениуса, Ученые записки Калужского гос. педагогического и учительского института, вып. 1, 1950, стр. 61—116.

6. О. Ю. Шмидт, Абстрактная теория групп, изд. 2, 1933.

Получена 17.IV 1951 г.

Калуга.