Известия Гомельского государственного университета
имени Ф. Скорины, № 6 (87), 2014

УДК 512. 542

О произведении обратимых элементов кольца классов вычетов

В.С. Монахов[1], И.К. Чирик[2]

Доказывается, что в кольце классов вычетов по модулю m произведение всех обратимых элементов равно $\bar{1}$ или $\overline{m-1}$.
Ключевые слова: вычет, кольца классов вычетов, конечная абелева группа, функция Эйлера.

We prove that the product of all inverse elements of residue classes modulo m is equal to $\bar{1}$ or $\overline{m-1}$.
Keywords: residue, residue class rings, finite Abelian group, Euler phi function.

Согласно теореме Вильсона натуральное число p является простым тогда и только тогда, когда $(p-1)!\equiv -1 \pmod p$. Карл Фридрих Гаусс заметил [1, с. 77–78]: «В более общем виде теорему Вильсона можно высказать так. Произведение всех чисел, которые меньше некоторого заданного числа A и одновременно взаимно просты с ним, сравнимы по модулю A с единицей, взятой с положительным или с отрицательным знаком. С отрицательным знаком единица получается когда A имеет вид p^m или $2\cdot p^m$, где p означает отличное от 2 простое число, и, кроме того, при $A=4$, во всех остальных случаях получается положительная единица». Далее Гаусс отмечает: «Теорема, высказанная Вильсоном, содержится в первом случае. Доказательство мы ради краткости не приводим, заметим только, что оно может быть проведено подобным же образом, как в предыдущем пункте, ... Можно было бы также вывести доказательство из рассмотрения индексов, ...».

В 1903 г. Миллер [2] привел новое доказательство, использующее теорию групп.

В настоящей заметке мы приводим более современное доказательство теоремы Миллера, которое затем применяем для получения обобщенной теоремы Вильсона. Все используемые понятия и обозначения соответствуют [3]–[4]. Через $|X|$ обозначается порядок конечной группы X, $p(G)$ – произведение всех элементов группы G.

Пусть m – натуральное число и $Z_m=\{\bar{0},\bar{1},\ldots,\overline{m-1}\}$ – кольцо классов вычетов по модулю m, где $0,1,\ldots,m-1$ – наименьшие неотрицательные вычеты. Мультипликативная группа Z_m^* обратимых элементов абелева порядка $\varphi(m)$ и состоит из тех классов, наименьшие неотрицательные вычеты которых взаимно просты с модулем m, [3, теорема 4.1, с. 86]. Здесь $\varphi(m)$ – функция Эйлера. Заметим, что класс $\overline{m-1}$ принадлежит группе Z_m^* при любом $m>1$ и является элементом порядка 2 при любом $m>2$. Группа Z_m^* циклическая [3, теорема 7.4, с. 168] тогда и только тогда, когда $m\in \mathrm{A}$, где $\mathrm{A}=\{2,\ 4,\ p^t,\ 2\cdot p^t \mid p\in \mathrm{P}\setminus\{2\},\ t\in \mathrm{N}\}$.

Здесь N – множество всех натуральных чисел, а P – множество всех простых чисел.

Лемма 1. *Если $G=A\times B$ – конечная абелева группа, A и B – ее подгруппы, то $p(G)=p(A)^{|B|}p(B)^{|A|}$.*

Доказательство. Пусть $A=\{1=a_1,\ a_2,\ ...,\ a_n\}$, $n=|A|$, $B=\{1=b_1,\ b_2,\ ...,\ b_m\}$, $m=|A|$. Все элементы группы G запишем в виде следующей таблицы умножения элементов подгрупп A и B. В последней строке (последнем столбце) указано произведение элементов столбца (строки) (таблица 1).

Таблица 1 – Умножение элементов подгрупп A и B

1	2	3	4	5	6	7
1	b_2	…	b_j	…	b_m	$p(B)$
a_2	a_2b_2	…	a_2b_j	…	a_2b_m	$a_2^m\,p(B)$
			…			
a_i	a_ib_2	…	a_ib_j	…	a_ib_m	$a_i^m\,p(B)$
			…			
a_n	a_nb_2	…	a_nb_j	…	a_nb_m	$a_n^m\,p(B)$
$p(A)$	$p(A)b_2^n$	…	$p(A)b_j^n$	…	$p(A)b_m^n$	$p(A)^m\,p(B)^n$

Ясно, что $p(G) = p(A)\cdot p(A)b_2^n\cdot\ldots\cdot p(A)b_j^n\cdot\ldots\cdot p(A)b_m^n = p(A)^m\,p(B)^n$.

Лемма 2. *Если G – абелева группа нечетного порядка, то $p(G)=1$.*

Доказательство. В группе G нечетного порядка нет элементов порядка 2 по теореме Лагранжа, поэтому $a\neq a^{-1}$ для любого $a\in G\setminus\{1\}$. Действительно, если существует элемент $a\in G\setminus\{1\}$ такой, что $a=a^{-1}$, то $a^2=a\cdot a=a\cdot a^{-1}=1$, противоречие. Поэтому все элементы группы G можно выписать, чередуя их с обратными: $a, a^{-1}, b, b^{-1}, c, c^{-1}, \ldots$. Теперь $p(G)=aa^{-1}bb^{-1}cc^{-1}\ldots=1$.

Лемма 3. *Если P – силовская 2-подгруппа абелевой группы G, то $p(G)=p(G)^{|G:P|}$.*

Доказательство. Так как G – абелева группа, то $G=P\times H$, где H – $2'$-холлова подгруппа группы G. По лемме 1 $p(G)=p(P)^{|H|}\,p(H)^{|P|}$. Так как $p(H)=1$ по лемме 2 и $|H|=|G:P|$, то $p(G)=p(G)^{|G:P|}$.

Заметим, что если в абелевой группе G четного порядка силовская 2-подгруппа циклическая, то элемент порядка 2 в группе G единственный.

Лемма 4. *Если $G=\langle a\rangle$ – циклическая группа порядка $2^k>1$, то $p(G)=a^{2^{k-1}}$.*

Доказательство. Пусть $G=\{1, a, a^2, \ldots, a^{2^k-1}\}$. Тогда

$$p(G)=a\cdot a^2\cdot\ldots\cdot a^{2^k-1}=a\cdot a^{2^k-1}a^2\cdot a^{2^k-2}\ldots a^{2^{k-1}}=a^{2^{k-1}}.$$

Заметим, что $a^{2^{k-1}}$ – элемент порядка 2.

Лемма 5. *Если абелева 2-группа G нециклическая, то $p(G)=1$.*

Доказательство. Пусть A – циклическая подгруппа наибольшего порядка в группе G. Согласно [4, лемма 3.3] существует подгруппа B такая, что $G=A\times B$. По лемме 1 $p(G)=p(A)^{|B|}\,p(B)^{|A|}$.

По лемме 4 $p(A)=a$, $|a|=2$. Так как $|B|=2^k\geq 2$, то $p(A)^{|B|}=1$.

Если B нециклическая, то по индукции $p(B)=1$ и $p(G)=1$.

Если B циклическая, то по лемме 4 $p(B)=b$, $|b|=2$. Так как $|A|=2^l\geq 2$, то $p(A)^{|B|}=1$ и $p(G)=1$.

Теорема 1. (Теорема Миллера) *Пусть G – конечная абелева группа с единичным элементом 1 и P – ее силовская 2-подгруппа. Если P нециклическая, то $p(G)=1$. Если P циклическая и $P\neq\{1\}$, то $p(G)=i$, где i – элемент порядка 2.*

Доказательство. Пусть P – силовская 2-подгруппа группы G. По лемме 3 $p(G)=p(G)^{|G:P|}$. Если P нециклическая, то $p(P)=1$ по лемме 5 и $p(G)=1$. Если P циклическая, то $p(P)=i$ по лемме 4, где i – элемент порядка 2. Так как $|G:P|$ – нечетное число, то $i^{|G:P|}=i$ и $p(G)=i$.

Следствие 1. *Пусть* $m \in \mathrm{N}$, $m > 1$. *Произведение всех обратимых элементов кольца* Z_m *равно* $\overline{m-1}$ *при* $m \in \mathrm{A}$ *и* $\bar{1}$ *при* $m \notin \mathrm{A}$.

Доказательство. Можно считать $m > 1$. Обратимые элементы кольца Z_m составляют абелеву группу Z_m^* четного порядка $\varphi(m)$. Поэтому произведение обратимых элементов кольца Z_m совпадает с $p(Z_m^*)$.

Если $m \in \mathrm{A}$, то группа Z_m^* циклическая [3, теорема 7.4, с. 168] и $p(Z_m^*)$ – элемент порядка 2 по теореме 2. Поскольку в циклической группе четного порядка существует только один элемент порядка 2, то $p(Z_m^*) = \overline{m-1}$.

Пусть $m \notin \mathrm{A}$. Тогда либо $m = 2^t > 4$, либо $m = m_1 m_2$, $m_1 > m_2 > 2$, где числа m_1 и m_2 взаимно просты. При $m = 2^t > 4$ группа Z_m^* будет нециклической группой порядка 2^{t-1}. При $m = m_1 m_2$ группа $Z_m^* = Z_{m_1}^* \times Z_{m_2}^*$ [3, теорема 7.4, с. 168].Так как $Z_{m_1}^*$ и $Z_{m_2}^*$ – группы четных порядков, то силовская 2-подгруппа в Z_m^* нециклическая. Итак, в любом случае при $m \notin \mathrm{A}$ силовская 2-подгруппа в Z_m^* нециклическая и $p(Z_m^*) = \bar{1}$ по теореме 2.

Следствие 2. (Теорема Вильсона) *Натуральное число* p *является простым тогда и только тогда, когда* $(p-1)! \equiv -1 \pmod{p}$.

Доказательство. Если p – простое, то все ненулевые элементы кольца Z_p обратимы и $\bar{1} \cdot \bar{2} \cdot \ldots \cdot \overline{p-1} = \overline{p-1}$ по теореме 1. Поэтому $(p-1)! \equiv -1 \pmod{p}$.

Обратно, пусть $(p-1)! \equiv -1 \pmod{p}$. Предположим, что p не простое. Тогда $p = kl$, $1 < k \le l < p$ и $(p-1)! \equiv 0 \pmod{p}$, противоречие.

Для натурального числа k через $k!_\varphi$ будем обозначать произведение всех тех чисел от 1 до k, которые взаимно просты с k.

Следствие 3. (Теорема Гаусса) *Пусть* m *– натуральное число. Если* $m \in \mathrm{A}$, *то* $m!_\varphi \equiv -1 \pmod{m}$. *Если* $m \notin \mathrm{A}$, *то* $m!_\varphi \equiv 1 \pmod{m}$.

Доказательство. Достаточно заметить, что $\overline{m!_\varphi}$ совпадает с произведением обратимых элементов кольца Z_m, а затем применить теорему 1.

Литература

1. Гаусс, К.Ф. Труды по теории чисел / К.Ф. Гаусс. – Москва : Издательство Академии наук СССР, 1959. – 981 с.

2. Miller, G.A. A new proof of the generalized Wilson's theorem / G.A. Miller // Ann. of Math. – 1903. – V. 4(2). – P. 188–190.

3. Нестеренко, Ю.В. Теория чисел / Ю.В. Нестеренко. – Москва : Издательский центр «Академия», 2008. – 273 с.

4. Монахов, В.С. Введение в теорию конечных групп и их классов / В.С. Монахов. – Минск : Вышэйшая школа, 2006. – 207 с.

[1]Гомельский государственный
университет им. Ф. Скорины

[2]Гомельский инженерный институт
МЧС Республики Беларусь

Поступила в редакцию 08.10.2014