ԵՐԵՎԱՆԻ ՊԵՏԱԿԱՆ ՀԱՄԱԼՍԱՐԱՆԻ ԳԻՏԱԿԱՆ ՏԵՂԵԿԱԳԻՐ
УЧЕНЫЕ ЗАПИСКИ ЕРЕВАНСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА

Բնական գիտություններ 3, 2007 Естественные науки

Математика

УДК 511

Е. С. МКРТЧЯН

ОБ ОДНОМ ОБОБЩЕНИИ ФОРМУЛ АБЕЛЯ

Получено одно обобщение формул Абеля, относящихся к последней теореме Ферма. Для случая, когда ни одно из чисел не делится на p ($p=3$ и $p=5$), получено простое доказательство теоремы.

Введение. Рассмотрим следующее диофантовое уравнение:

$$z_1^p + z_2^p = z_3^p, \tag{1}$$

где $p \geq 3$ – произвольное натуральное число, а z_1, z_2 и z_3 – искомые целые числа уравнения (1). Как известно, последняя теорема Ферма утверждала, что уравнение (1) не имеет целых решений. В предположении, что диофантовое уравнение (1) имеет решение, в начале прошлого века Абель получил формулы для этих решений (см. [1], стр. 21). Не перечисляя все работы по этой задаче (см., напр., [2]), отметим, что полное решение этого уравнения получено А. Вилисом [3].

В этой статье доказана следующая основная теорема, которая обобщает формулы Абеля:

Теорема. Если $p \geq 3$ – простое число и z_1, z_2, z_3 – взаимно простые числа, удовлетворяющие уравнению (1), то необходимо выполнение следующих условий:

случай 1. Если ни одно из чисел z_1, z_2 и z_3 не делится на p, то существуют такие натуральные числа q, a, b и R, что

$$\begin{cases} z_1 = a^p + pqabR, \\ z_2 = b^p + pqabR, \\ z_3 = a^p + b^p + pqabR, \end{cases} \tag{2}$$

$$q^p = a^p + b^p + 2pqabR; \tag{3}$$

случай 2. Если одно из чисел z_1, z_2, z_3 делится на p, то существуют такие натуральные числа q, a, b, R, что либо при z_2 / p (или z_1 / p) имеем

$$\begin{cases} z_1 = a^p + pqabR, \\ z_2 = p^{p-1}b^p + pqabR, \\ z_3 = a^p + p^{p-1}b^p + pqabR, \end{cases} \quad (4)$$

$$q^p = a^p + p^{p-1}b^p + 2pqabR, \quad (5)$$

либо при z_3 / p имеем

$$\begin{cases} z_1 = a^p + pqabR, \\ z_2 = b^p + pqabR, \\ z_3 = a^p + b^p + 2pqabR, \end{cases} \quad (6)$$

$$p^{p-1}q^p = a^p + b^p + 2pqabR. \quad (7)$$

Формулы (2), (4), (6) являются обобщением формул Абеля [1]. В качестве применения этих формул для *случая 1* получено простое доказательство при $p = 3$ и $p = 5$.

Доказательство теоремы. Предположим, что уравнение (1) имеет нетривиальное решение, т.е. существуют натуральные числа w, z и c такие, что $z_1 = w$, $z_2 = z$, $z_3 = c$ и $(w,z) = (w,c) = (z,c) = 1$, т.е. все они взаимно простые числа. Тогда

$$w^p + z^p = c^p. \quad (8)$$

Обозначим $x = c - w$ и подставим в (8):

$$(c - x)^p + z^p = c^p. \quad (9)$$

Из (9) простыми преобразованиями получим, что

$$z^p = xQ, \quad (10)$$

где вид Q очевиден. Из (10) видно, что ее левая часть делится на x. Запишем x в следующем виде:

$$x = ra^p, \quad (11)$$

где a – некоторое натуральное число, r – натуральное число, не являющееся p-ой степенью некоторого натурального числа (случай $a = 1$, а также $(a,r) = r_1 \neq 1$ не исключаются). Сначала рассмотрим случай, когда $r \neq 1$ – простое число. Тогда из (10) получим, что

$$z = ram, \quad (12)$$

где m – некоторое натуральное число. Подставив (11) и (12) в (9), получим

$$(c - ra^p)^p + (ram)^p = c^p. \quad (13)$$

Раскрыв скобки и разделив обе части на $a^p r$, получим

$$-pc^{p-1} + \frac{p(p-1)}{2!}ra^p c^{p-2} - \ldots + r^{p-1}m^p = 0. \quad (14)$$

Из (14) следует, что pc^{p-1} делится на r. Так как $(c,z) = 1$, то $p = r$. Тогда из (14) будет следовать также, что c делится на p, что невозможно. Таким образом, мы получаем, что $x = a^p$ и $z = am$.

Теперь рассмотрим случай, когда r не является простым числом. Пусть $r=\lambda_1^{m_1}...\lambda_k^{m_k}$, где $m_1,m_2,...m_k$ – натуральные числа, а $\lambda_1,\lambda_2,...,\lambda_k$ – простые числа. По условию $(z,c)=1$, следовательно, $(c,\lambda_i)=1$, $i=1,2,...,k$. Если $m_i=pq_i+l_i$, где $0\le l_i\le p-1$, $i=1,2,...,k$, то вместо $\lambda_i^{m_i}$ мы можем рассмотреть $\lambda_i^{l_i}$, присоединяя $\lambda_i^{q_i}$ к a. Таким образом, мы можем написать

$$x=\lambda_1^{l_1}...\lambda_k^{l_k}(\tilde{a})^p, \qquad (15)$$

где $\tilde{a}=\lambda_1^{q_1}...\lambda_k^{q_k}a$. Значение x из (15) подставим в (10) и получим $z=\lambda_1...\lambda_k\tilde{a}\tilde{m}$, где $\tilde{m}\in N$. Значит, (9) можно записать следующим образом:

$$(c-\lambda_1^{l_1}...\lambda_k^{l_k}\tilde{a}^p)^p+(\lambda_1...\lambda_k\tilde{a}\tilde{m})^p=c^p.$$

Раскрыв скобки и сократив на $\lambda_1^{l_1}...\lambda_k^{l_k}\tilde{a}^p$, получим

$$-pc^{p-1}+\frac{p(p-1)}{2!}c^{p-2}(\lambda_1^{l_1}...\lambda_k^{l_k})\tilde{a}^p-...+\lambda_1^{p-l_1}...\lambda_k^{p-l_k}\tilde{m}^p=0.$$

Отсюда следует, что либо $\lambda_i=1$ для всех $i=1,2,...,k$, либо $\lambda_i=p$, $l_1=p-1$, а остальные $\lambda_i=1$, $i=2,...,k$. В этом случае $x=p^{p-1}a^p$, $z=pam$.

Таким образом, мы получили

Утверждение 1. Если w,z и c – взаимно простые числа и удовлетворяют (8), то либо 1) $w=c-a^p$ и $z=am$, либо 2) $w=c-p^{p-1}a^p$ и $z=pam$.

Повторяя эти рассуждения для $z=c-y$, получим

Утверждение 2. Если w,z и c – взаимно простые числа и удовлетворяют (8), то существуют такие натуральные числа b и n, что либо 1) $w=bn$ и $z=c-b^p$, либо 2) $w=pbn$ и $z=c-p^{p-1}b^p$.

Объединив эти два утверждения, мы можем сказать, что при $(c, p)=1$ возможны следующие два случая:

случай 1

$$\begin{cases} c-a^p=bn, \\ c-b^p=am. \end{cases}$$

случай 2

$$\begin{cases} c-a^p=pbn, \\ c-p^{p-1}b^p=am. \end{cases}$$

Рассмотрим их по отдельности.

Случай 1. Так как $x=a^p$, $w+x=c$ и $z=am$, мы можем написать $w^p+(am)^p=(w+x)^p$ или

$$w^p+(am)^p=w^p+pw^{p-1}x+...+pwx^{p-1}+x^p. \qquad (16)$$

После преобразования (16) получим, что

$$m^p+(a^{p-1})^p=pR_1. \qquad (17)$$

К левой части (17) добавим и отнимем $m-a^{p-1}$:

$$m^p-m+m-a^{p-1}+(a^{p-1}-(a^{p-1})^p)=pR_1. \qquad (18)$$

Используя малую теорему Ферма (см., напр., [4], стр. 97), из (18) получим, что $m-a^{p-1}=pR_2$ или $m=a^{p-1}+pR_2$. Из (17) следует, что $R_2>0$ – целое

число. Таким образом, мы получили, что

$$(c-a^p)^p+(a^p+paR_2)^p=c^p. \qquad (19)$$

Совершенно аналогично получим

$$(b^p+pb\tilde{R}_2)^p+(c-b^p)^p=c^p, \text{ где } n-b^{p-1}=p\tilde{R}_2>0.$$

Утверждение 3. Существует натуральное число q такое, что либо

$$c=q^p-pqaR_3, \qquad (20)$$

либо

$$c=p^{2(p+2)}q^p-p^{k+1}qR_4, \text{ где } R_3,R_4\in N. \qquad (21)$$

Доказательство. Из (19) получим, что

$$(c+paR_2)Q_1=c^p. \qquad (22)$$

Пусть $c+paR_2=q_1^{r_1}...q_l^{r_l}$, где все q_i, $i=1,2,...,l$, – взаимно простые числа, а $r_i\ge 0,\ i=1,2,...,l$, – целые числа. Подставляя эти значения в (22), получим, что $c=q_1...q_lQ_2$, а это возможно, если $R_2=q_1...q_2R_2^*$. Отсюда либо

$$(q_i,p)=1,\ i=1,2,...,n, \qquad (23)$$

либо $q_1=p$ и, следовательно, $R_2=q_2...q_lR_2^{**}$, так как $(c,a)=1$. Учитывая значения z и R_2, из (23) получим $z=a^p+paR_2=a^p+paq_1...q_lR_2^*$, значит, $c-a^p=c+paR_2-(a^p+paR_2)=q_1^{r_1}...q_l^{r_l}-z$.

Подставляя эти значения в (19), получим

$$(q_1^{r_1}...q_l^{r_l}-z)^p+z^p=(q_1^{r_1}...q_l^{r_l}-paq_1...q_lR_2^*)^p. \qquad (24)$$

Отсюда получим

$$\begin{aligned}&-(q_1^{r_1}...q_l^{r_l})^{p-1}z+\frac{p-1}{2}(q_1^{r_1}...q_l^{r_l})^{p-2}z^2+...+(q_1^{r_1}...q_l^{r_l})z^{p-1}=\\ &=-(q_1^{r_1}...q_l^{r_l})^{p-1}paq_1...q_lR_2^*+...+(q_1^{r_1}...q_l^{r_l})(paq_1...q_lR_2^*)^{p-1}-(aq_1...q_lR_2^*)^p p^{p-1}.\end{aligned} \qquad (25)$$

Покажем, что $r_i\ge p\ \ \forall i=1,2,...,l,$ если $(q_ip)=1,\ i=1,2,...,l$. Действительно, если $r_{i_0}<\rho$, то сокращая (25) на $q_{i_0}^{r_{i_0}+1}$, получим, что z делится на q_{i_0}, что невозможно из-за условия $(q_{i_0},a)=1$. В равенстве (25), разделив обе части на $q_{i_0}^{r_{i_0}}$, получим, что $q_{i_0}^{r_{i_0}}=q_{i_0}^{pk_{i_0}}$, т.е. $r_{i_0}=pk_{i_0}$. Таким образом, мы имеем, что $q_1^{r_1}...q_l^{r_l}=(q_1^{k_1}...q_l^{k_l})^p=q^p$, где $q_1^{k_1}...q_l^{k_l}$ обозначено через q, Тогда из (22) можем написать, что $Q_1=\left(\frac{c}{q}\right)^p$, т.е. $c=qQ_3$, и, следовательно, из $c+paR_3=q^p$ следует, что $R_2=qR_3$ или $c=q^p-paqR_3$, т.е. получаем (20).

Теперь рассмотрим случай, когда одно из q_i равно p. Повторяя предыдущие рассуждения для q_i, $i=2,3,...,l$, докажем, что $c=qQ_2$, $q=q_2^{k_2}...q_l^{k_l}$, $q^p=q_2^{r_2}...q_l^{r_l}$, $R_2=qR_3$.

В (25) подставим $q_1 = p$ и получим, что

$$-(p^{r_1}q^p)^{p-1} + \frac{(p-1)}{2}p^{r_1(p-2)}q^{p(p-2)}z^2 + \ldots + p^{r_1}q^p z^{p-1} =$$
$$= -p^{r_1(p-1)}q^{p-1}p^2 aq^{(q_2\ldots q_l)}R_3 + \ldots + p^{r_1}q^p p^{2p-2}(q_2\ldots q_l)^{p-1}q^{p-1}R_2^* - \qquad (26)$$
$$-(aq_2\ldots q_l q^p R_3)^p p^{2p-1}$$

Если $r_1 < 2p-1$, то из (26) будет следовать, что $(z,p) = p$, что невозможно, ибо $c = pq_2\ldots q_l Q_2$. Если же $2p-1 \le r_1$, то из (26) следует, что $r_1 = 2p-1+kp$, так как в этом случае $R_3 = p^k R_4$. Тогда получим $c = p^{2(k+2)-1}q^p - p^{k+1}qaR_4$.

Утверждение доказано.

Так как $R_2 = qR_3$, то из (19), (20) получим, что

$$w + z = (c - a^p) + (a^p + pqaR_3) = c + pqaR_3 = q^p. \qquad (27)$$

Из (21) следует, что

$$w + z = c + p^{k+1}qaR_4 = p^{p(k+2)-1}q^p. \qquad (28)$$

С другой стороны,

$$q^p = w + z = b^p + pqb\tilde{R}_2 + c - b^p = c + pqb\tilde{R}_2, \qquad (29)$$
$$p^{p(k+2)-1}q^p = w + z = c + p^{k+1}qb\tilde{R}_2. \qquad (30)$$

Сравнивая (27) и (29), получим, что $aR_3 = b\tilde{R}_2$, т.е. $R_3 = bR$ (R – натуральное число). Отсюда следует

$$c = q^p - pqabR. \qquad (31)$$

Аналогично из (28) и (30) получим, что

$$c = p^{p(k+2)-1}q^p - p^{k+1}qabR. \qquad (32)$$

В формулах (31) и (32) R – разные числа.

Для *случая 1*, обозначая $x = a^p$, $y = b^p$ и $t = pqabR$, получим $c - b^p = am = a^p + pqabR$, следовательно, $c = x + y + t$ и

$$q^p = c + pqabR = a^p + b^p + 2pqabR = x + y + 2t. \qquad (33)$$

Таким образом, когда ни одно из чисел w, z и c не делится на p, получаем

$$\begin{cases} (x+t)^p + (y+t)^p = (x+y+t)^p, \\ q^p = x + y + 2t, \end{cases} \qquad (34)$$

где $\begin{cases} x + t = w = a^p + pqabR, \\ y + t = z = b^p + pqabR, \\ x + y + t = c. \end{cases}$

Для *случая 2* имеем $c-a^p=bn=b^p+p^{k+1}qabR$. Обозначая $x=a^p$, $y=b^p$, $t=p^{k+1}qabR$, получим $c=x+y+t$, $p^{p(k+2)-1}q^p=x+y+2t$.

Когда c делится на p, имеем $\begin{cases}(x+t)^p+(y+t)^p=(x+y+t)^p,\\ p^{p(k+2)-1}q^p=x+y+2t.\end{cases}$

Когда w делится на p, то при $x=a^p$ $w=c-a^p=c-x$, и из (8) получим

$$w^p+(am)^p=(w+x)^p. \qquad (35)$$

Раскрывая скобки и сокращая на x, получим

$$m^p-x^{p-1}=p(w^{p-1}+...+wx^{p-1})=pR_1>0, \qquad (36)$$

где $R_1=w^{p-1}+...+wx^{p-1}$. Тогда из (36) и малой теоремы Ферма получим, что $m-a^{p-1}=pR_2$, $R_2>0$, так как $0<pR_2=m^p-x^{p-1}=m^p-m+m-a^{p-1}+$ $+a^{p-1}-(a^{p-1})^p$. Таким образом, можем написать, что

$$am=a^p+paR_2. \qquad (37)$$

Утверждение 4. Существуют натуральные числа q и R_3 такие, что

$$c=q^p-pqabR_3. \qquad (38)$$

Доказательство. Из (37) мы имеем, что

$$(c-a^p)^p+(a^p+paR_2)^p=c^p. \qquad (39)$$

Следовательно, $(c+paR_2)Q_1=c^p$.

Пусть

$$c+paR_2=q_1^{r_1}...q_l^{r_l}, \qquad (40)$$

где q_i, $i=1,2,...,l$, – простые числа, отличные от p, a, r_i, $i=1,2,...,l$. Значит,

$$c=q_1...q_lR_2^*. \qquad (41)$$

Подставляя c в (39), получим

$$(q_1^{r_1}...q_l^{r_l}-z)^p+z^p=(q_1^{r_1}...q_l^{r_l}-paq_1...q_lR_2^*).$$

Как и в утверждении 3, получим, что $c=qQ_3$ и $R_2^*=qR_3$, где $q=q_1^{k_1}...q_l^{k_l}$, $r_i=k_ip$, $i=1,2,...,l$, что равносильно (38).

Так как $z=c-p^{p-1}b^p=am=a^p+pqaR_3$, то

$$c=p^{p-1}b^p+a^p+pqaR_3. \qquad (42)$$

Но $w=c-a^p=pbn$, значит,

$$c=a^p+pbm. \qquad (43)$$

Сравнивая (42) и (43), получим, что $p^{p-1}b^p+pqaR_3=pbn$, т.е. $R_3=bR$, значит, (42) запишется: $c=p^{p-1}b^p+a^m+pqabR$ или $c=q^p-pqabR$. Используя обозначения $t=pqabR$, $x=p^{p-1}b^p$, $y=a^p$, получим

$$\begin{cases}(x+t)^p+(y+t)^p=(x+y+t)^p,\\ q^p=x+y+2t.\end{cases}$$

Примеры применения основной теоремы.

1^0**.** Рассмотрим *случай 1,* $p=3$. Тогда имеем, что

$$\begin{cases}(a^3+3qabR)^3+(b^3+3qabR)^3=(a^3+b^3+3qabR)^3,\\ q^3=a^3+b^3+6qabR.\end{cases}$$

Раскрывая скобки в первом уравнении и учитывая второе, получим

$$9R^3=1. \tag{44}$$

Но (44) невозможно, ибо по предположению $R\in N$. Мы получили, что в этом случае уравнение (1) не имеет целых решений.

2^0. Рассмотрим *случай 1,* $p=5$. Тогда

$$\begin{cases}(a^5+5qabR)^5+(b^5+5qabR)^5=(a^5+b^5+5qabR)^5,\\ q^5=a^5+b^5+10qabR.\end{cases} \tag{45}$$

Если обозначить $d=q^5$, то (34) примет вид

$$(x+t)^5+(d-(x+t))^5=(d-t)^5, \tag{46}$$

$$(y+t)^5+(d-(y+t))^5=(d-t)^5. \tag{47}$$

Раскрывая в (46) скобки и сокращая на $5dx$, получим

$$5^4R^5y=-d^3+2d^2(x+2t)-2d(x^2+sxt+3t)+x^3+4x^2t+6xt^2+4t^3. \tag{48}$$

Аналогично для (47) получим

$$5^4R^2x=-d^3+2d^2(y+2t)-2d(y^2+3yt+3t)+y^3+4y^2t+6yt^2+4t^3. \tag{49}$$

Из (48) и (49) имеем

$$5^4R^5=x^2+xy+y^2+2(x+y)t+2t^2. \tag{50}$$

Из (46) следует, что

$$x^2+xy+y^2\equiv 0(\mathrm{mod}\,5). \tag{51}$$

Очевидно, что любая комбинация чисел ±1, ±2 не удовлетворяет (51). Значит, (45) не имеет решения.

Кафедра численного анализа и математического моделирования

Поступила 22.02.2007

ЛИТЕРАТУРА

1. **Постников М.М.** Теорема Ферма. М.: Наука, 1978, с. 128.
2. **McMullen C.** – Bull. Amer. Math. Sos., 2000, v. 37, p. 119–140.
3. **Wiles A.** – Ann. of Math., 1995, v. 141, p. 443–551.
4. **Бухштаб А.А.** Теория чисел. М.: Просвещение, 1966, с. 384.

Ե. Ս. ՄԿՐՏՉՅԱՆ

ԱԲԵԼԻ ԲԱՆԱՁԵՎԵՐԻ ՄԻ ԸՆԴՀԱՆՐԱՑՄԱՆ ՄԱՍԻՆ

Ամփոփում

Ստացված է Ֆերմայի վերջին թեորեմին առնչվող Աբելի բանաձևերի մի ընդհանրացում: Ենթադրելով, որ թեորեմը ճիշտ չէ, ստանում ենք հավասարման լուծմանը բավարարող անհրաժեշտ պայմաններ: Եվ երբ լուծման թվերից ոչ մեկը չի բաժանվում p-ի վրա, ստացվում է թեորեմի պարզ ապացույց $p=3$ և $p=5$ դեպքերում:

Yer. S. MKRTCHYAN

ABOUT ONE GENERALIZATION OF ABEL'S FORMULAE

Summary

One generalization of formulae of Abel concerning to the Fermat's last theorem is received. Supposing that the theorem is not true, for the solution of the equation the necessary condition is obtained. In the case when none of the numbers is divided by p, we get a simple proof of the theorem for $p=3$ and $p=5$.