ՀԱՂՈՐԴՈՒՄՆԵՐ СООБЩЕНИЯ

УДК 511.212

В.С. АТАБЕКЯН

АЛГОРИТМ ЕВКЛИДА ДЛЯ ЦЕЛЫХ КВАТЕРНИОНОВ И ТЕОРЕМА ЛАГРАНЖА

В работе для некоммутативного кольца кватернионов с целыми коэффициентами доказываются теоремы, обобщающие алгоритм Евклида и понятие наибольшего общего делителя. В качестве приложения результатов приводится короткое доказательство теоремы Лагранжа о представимости натуральных чисел в виде суммы четырех квадратов.

Настоящая статья посвящена исследованию понятия делимости в специальном подкольце тела кватернионов. В качестве приложения из полученных результатов выводится теорема Лагранжа о том, что произвольное натуральное число является суммой квадратов четырех целых чисел. Существуют разные доказательства этой теоремы. В [1] доказательство основывается на теореме Минковского о выпуклых телах, в [2] применяются p-адические поля и квадратичные формы, в [3,4] теорема выводится из определенных утверждений о сравнениях. Следует отметить совсем недавно [5] предложенное элегантное доказательство теоремы Эйлера о представимости простых чисел вида $4k+1$ в виде суммы двух квадратов (см. также [1,3,4,6]. Отправным пунктом для нас является теорема, из которой в частности следует евклидовость кольца целых гауссовых чисел (см. [6]).

Пусть H — тело кватернионов, а $\overline{Z}=\{a+bi+cj+dk \mid a,b,c,d\in Z\}$ — множество кватернионов с целыми коэффициентами. Очевидно, $\overline{Z}$ — ассоциативное, но некоммутативное кольцо с единицей. Если $q=a+bi+cj+dk\in H$, то $\overline{q}=a-bi-cj-dk$ — сопряженный ему кватернион, $q\cdot\overline{q}=|q|^2=a^2+b^2+c^2+d^2$.

Лемма. Если a,b,c,d — нечетные числа, то $(a^2+b^2+c^2+d^2)\vdots 4$.

Теорема 1. Для любых $A,B\in\overline{Z}, B\neq 0$ справедливо одно из следующих условий: а) $\exists q\in\overline{Z}$, что $2\cdot A=B\cdot q$ и $|q|^2=4$; б) $\exists q,r\in\overline{Z}$, что $A=Bq+r$, где $|r|<|B|$.

Доказательство. Рассмотрим $B^{-1}\cdot A\in H$. Очевидно существуют $C,D\in H$ такие, что $B^{-1}\cdot A=C+D$, где $C\in\overline{Z}$, а $D=x+y\cdot i+z\cdot j+t\cdot k$, причем $x,y,z,t\in R$ и $|x|, |y|, |z|, |t|\leqslant\frac{1}{2}$.

а) Если $|x|=|y|=|z|=|t|=\frac{1}{2}$, то $2\cdot D\in\overline{Z}$ и $2\cdot A=B(2\cdot C+2\cdot D)$. Обозначив $q=2\cdot C+2\cdot D$ замечаем, что $q=a+bi+cj+dk$, где a,b,c,d — нечетные числа. По предыдущей лемме заключаем, что $|q|^2=(a^2+b^2+c^2+d^2)\vdots 4$.

б) Если же $|x|^2+|y|^2+|z^2|+|t|^2<1$, то $|D|<1$: Тогда $|B\cdot D|<|B|$. Одновременно $A=BC+BD$, где $BD=A-BC\in\overline{Z}$. Для завершения теоремы остается обозначить $C=q$ и $B\cdot D=r$.

Теорема 2. Пусть $d=A\cdot x_0+B\cdot y_0\neq 0$, где A,B,x_0,y_0 — фиксированные целые кватернионы и

$$\forall x,y\in\overline{Z}\ (|d|\leqslant|Ax+By|). \tag{1}$$

Тогда существует $q\in\overline{Z}$ такое, что $2\cdot A=d\cdot q$, причем $|q|^2\vdots 4$. (Аналогичное утверждение справедливо и для B).

Доказательство. В силу теоремы 1 или а) $2A=dq$, где $|q|^2\vdots 4$, или б) существуют $q,r\in\overline{Z}$ такие, что $A=dq+r$, где $0\leqslant|r|<|d|$. В случае б) получаем равенство

$$r=A(1-x_0\cdot q)+B\cdot(-y_0\cdot q). \tag{2}$$

Теперь, сопоставляя (1) и (2) с неравенством $|r|<|d|$, выводим $|r|=0$. Тогда $A=d\cdot q$. Поскольку $2A=d\cdot(2q)$, то теорема доказана.

Замечание. Предлагаем сравнивать теорему 2 с теоремой о наибольшем общем делителе для колец с главными идеалами.

Прежде чем перейти к теореме Лагранжа, приведем следующую лемму, которую можно найти в [1-4].

Лемма. В поле Z_p уравнение с двумя неизвестными $x^2+\hat{y}^2+1=0$ имеет решение.

Доказательство. Непосредственная проверка показывает, что множества $E=Z_p^2=\{x^2\,|\,x\in Z_p\}$, $F=\{-x^2-1\,|\,x\in Z_p\}$ — оба содержат ровно $\frac{p+1}{2}$ различных элементов поля Z_p. Следовательно, $E\cap F\neq\varnothing$, ибо $\frac{p+1}{2}+\frac{p+1}{2}>p$. Таким образом можно утверждать, что некоторый элемент $x_0^2\in E$ равняется некоторому элементу $(-y_0^2-1)\in F$, т.е. $x_0^2=-y_0^2-1$.

Теорема (Лагранж). Любое простое число p — сумма квадратов четырех целых чисел.

Доказательство. Согласно предыдущей лемме можно найти целые числа x,y,z такие, что $x^2+y^2+1=p\cdot z$. Обозначим $A=1+x\cdot i+y\cdot j$, тогда $\overline{A}=1-x\cdot i-y\cdot j$ и $A\cdot\overline{A}=p\cdot z$. Пусть $G=\{A\cdot u+P\cdot v\,|\,u,v\in Z\}$ и d — произвольный кватернион из множества G такой, что для всякого $g\neq 0$ из G выполняется условие $|d|\leqslant|g|$. Если $|d|=|p|$, то в силу теоремы 2 $2\cdot A=p\cdot q$, т.е. $2(1+x\cdot i+y\cdot j)=p\cdot q$, $q\in\overline{Z}$, тем самым $p=2=1^2+1^2+0^2+0^2$. Если же

$|d|<|p|$, то опять, по теореме 2 $2p=dq$, где $|q|^2 \vdots 4$. Таким образом $4p^2=|d|^2\cdot|q|^2$, поэтому или $|d|^2=p$ и теорема доказана, или $|d|^2=1$. В последнем случае можно считать, что $d=1$ и $Au_0+pv_0=d=1$, откуда следует, что $\overline{A}=p\cdot(z\cdot u_0+\overline{A}\cdot v_0)$, т.е. $1 \vdots p$ — противоречие.

Общий случай теоремы Лагранжа получается при совмещении предыдущей теоремы, основной теоремы арифметики и тождества $|q_1\cdot q_2|^2=|q_1|^2\cdot|q_2|^2$.

Кафедра алгебры и геометрии *Поступило 10.05.1991*

ЛИТЕРАТУРА

1. **Милнор Дж., Хьюзмоллер Д.** Симметрические билинейные формы. М.: Наука, 1986, 176с.
2. **Серр Ж.—П.** Курс арифметики. М.: Мир, 1972, 184 с.
3. **Чандрасекхаран К.** Введение в аналитическую теорию чисел. М.: Мир, 1974, 188 с.
4. **Бухштаб А.А.** Теория чисел. М.: Просвещение, 1966, 396 с.
5. **Zagier D.** A one-sentence proof that every prime $P\equiv1(\mathrm{mod}\ 4)$ is a sum of two squares. — Amer. Math. Mon., 1990, v.97, №2, p.144.
6. **Кострикин А.И.** Введение в алгебру. М.: Наука, 1977, 496 с.

Վ.Ս. ԱԹԱԲԵԿՅԱՆ

ԷՎԿԼԻԴԵՍԻ ԱԼԳՈՐԻԹՄԸ ԱՄԲՈՂՋ ՔՎԱՏԵՐՆԻՈՆՆԵՐԻ ՀԱՄԱՐ ԵՎ ԼԱԳՐԱՆԺԻ ԹԵՈՐԵՄԸ

Ամփոփում

Աշխատանքում ամբողջ գործակիցներով քվատերնիոնների ոչ տեղափոխելի օղակի համար ապացուցվում են էվկլիդեսի ալգորիթմը և ամենամեծ ընդհանուր բաժանարարի գաղափարը ընդհանրացնող թեորեմներ: Որպես ստացված արդյունքների կիրառություն տրվում է կարճ ապացույց Լագրանժի այն թեորեմի, ըստ որի յուրաքանչյուր բնական թիվ չորս ամբողջ թվերի քառակուսիների գումար է:

V.S. ATABEKIAN

THE EUCLIDEAN ALGORYTHM FOR WHOLE QUATERNIONS AND THE LAGRANGE THEOREM

Summary

In the paper the Euclidean algorythms and the generalizing theorems of the idea of the biggest common divident are proved. As an application of the received results a brief proof of Lagrange theorem is given, according to which every natural number is the sum of the squares of four whole numbers.