Теория дивизоров и комбинаторика в свободной полугруппе

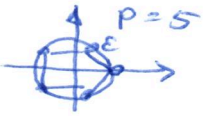
"Совр. математика"
Дубна, 23.07.19

1

Великая теорема Ферма (1637 г.) Ур-е $x^n+y^n=z^n$ при $n\geq 3$ не имеет решений в целых неотриц. числах.

Достаточно д-ть при $n=4$ (сделал ещё Ферма) и при $n=p$ – простое нечетное

Пусть ε – первообразный корень степени p из 1.



Тогда $x^p+y^p=\prod_{k=0}^{p-1}(x+\varepsilon^k y)=z^p$

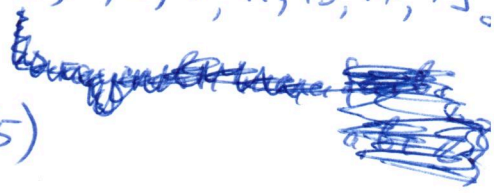
Идея: прийти в противоречие с однозначностью разложения на простые множители: если $x+y, x+\varepsilon y, \dots, x+\varepsilon^{p-1}y$ взаимно просты, то каждый из них является p-й степенью, а это вряд ли.

Аккуратное изложение: §1 главы III в Боревич–Шафаревич "Теория чисел"

Но **Проблема** Все происходит в кольце $\mathbb{Z}[\varepsilon]=\{a_0+a_1\varepsilon+\dots+a_{p-1}\varepsilon^{p-1}\}$, $a_i\in\mathbb{Z}$

Однозначно ли там разложение на простые множители?

Masley–Montgomery'1976: однозначно $\Leftrightarrow p=2,3,5,7,11,13,17,19$



Ближний пример: $\mathbb{Z}[\sqrt{-5}]$: $3\cdot 7=(1+2\sqrt{-5})(1-2\sqrt{-5})$

"неприводимы, друг на друга не делятся"

Идея Куммера: Вложить $\mathbb{Z}[\sqrt{-5}]$ в большее кольцо R с однозначным разложением на простые множители, где $3=\nu_1\nu_2$, $7=\nu_3\nu_4$, $1+2\sqrt{-5}=\nu_1\nu_3$, $1-2\sqrt{-5}=\nu_2\nu_4$; Элементы R – "идеальные числа"

"Мера нефакториальности" – группа классов дивизоров, измеряет отличие $\mathbb{Z}[\sqrt{-5}]$ от R.

Опр Простое число p **регулярно**, если порядок группы классов $\mathbb{Z}[\varepsilon]$ не делится на p.

В 1850 г. Куммер д-л Вел. теор. Ферма для всех регул. простых p.

Из простых чисел <100 иррегулярны только 37, 59 и 67.

Иенсен (1915): иррегулярных простых чисел бесконечно много.

Ок вопрос: бесконечно ли много регулярных простых?

(2) Теория дивизоров для полугрупп

Опр Мн-во S с заданной бинарной операцией $S \times S \to S, (a,b) \mapsto ab$, называется полугруппой, если операция ассоциативна, т.е. $(ab)c = a(bc)\ \forall a,b,c \in S$.

Полугруппа называется моноидом, если в ней есть единица, т.е. такой элемент $e \in S$, что $ea = ae = a\ \forall a \in S$.

Мы будем рассматривать только коммутативные полугруппы, т.е. считаем, что $ab = ba\ \forall a,b \in S$.

Как построить полугруппу?

Свободная полугруппа над произвольным алфавитом P:

$$\mathcal{F}(P) = \left\{ p_1^{k_1} \cdots p_r^{k_r},\ p_i \in P,\ k_i \in \mathbb{Z}_{\geq 0} \right\}$$

Замеч S - полугруппа с однозн. разлож. на простые множителя $\Leftrightarrow S \cong \mathcal{F}(P)$, где P - множество простых элементов в S.

Примеры свободных полугрупп (точнее, их реализаций):

Случай 1 P - конечно, $|P| = n \Rightarrow \mathcal{F}(P) \cong \mathbb{Z}^n_{\geq 0}$, $p_i = e_i = (0, \dots, \underset{i}{1}, \dots 0)$

$$p_1^{k_1} \cdots p_n^{k_n} \leftrightarrow (k_1, \dots, k_n)$$

Случай 2 P счетно $\Rightarrow \mathcal{F}(P) = (\mathbb{N}, \times)$, P - простые числа.

Опр Пусть S - произв. моноид. Гомоморфизм моноидов $\varphi: S \to \mathcal{F}(P)$ называется дивизориальным, если $\forall a,b \in S$ $a \mid b$ в $S \Leftrightarrow \varphi(a) \mid \varphi(b)$ в $\mathcal{F}(P)$.

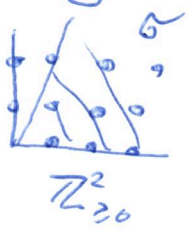
Напомин. $a \mid b$ в S, если $\exists c \in S : b = ac$

$\Rightarrow$ всегда, $\Leftarrow$ не всегда: $S = \langle 2,6 \rangle \subseteq (\mathbb{N}, \cdot)$

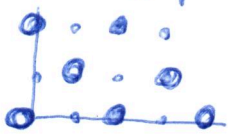
Опр Моноид Крулля - моноид, допускающий дивизориальное вложение в некоторый свободный моноид.

Цель: вложить моноид в $\mathcal{F}(P)$ с сохранением теории делимости.

Опр Теория дивизоров для моноида S это такое дивизориальное вложение $S \overset{\varphi}{\hookrightarrow} \mathcal{F}(\mathbb{P})$, что $\forall p \in \mathbb{P}$
$\exists$ конеч. подмн-во $A \subseteq S$: $p = HOД(\varphi(A))$.

Пример 

$S = \sigma \cap \mathbb{Z}^2_{\geq 0} = \langle (1,0), (1,1), (1,2) \rangle$
это не дивизор. вложение : $(1,2) = (1,0) + (0,2)$
$\in S$ $\in S$ $\notin S$

Дивизориальное вложение для S :

$S = \langle (2,0), (1,1), (0,2) \rangle = \{(i,j) \in \mathbb{Z}^2_{\geq 0} : i+j \in 2\mathbb{Z}\}$
это даже теория дивизоров: $(1,0) = HOД((2,0), (1,1))$
$(0,1) = HOД((0,2), (1,1))$

Теорема Любой моноид Крулля допускает теорию дивизоров и эта теория единственна с точностью до изоморфизма.

(3) Последовательности с нулевой суммой

Пусть $(G,+)$ - абелева группа, $A = \{g_1, \dots, g_\ell\}$, $g_i \in G$ - конечная неупоряд. последоват., возможно с повторениями.
Операция приписывания : $A = \{g_1, \dots, g_\ell\}$, $B = \{h_1, \dots, h_k\} \Rightarrow AB = \{g_1, \dots, g_\ell, h_1, \dots, h_k\}$
Мн-во последовательностей с этой операцией $\cong \mathcal{F}(G)$.
Определим $\sigma(A) = g_1 + \dots + g_\ell$, где $A = \{g_1, \dots, g_\ell\}$.
Пусть $\mathcal{B}(G) = \{A \mid \sigma(A) = 0\}$ - замкнуто от-но приписывания.
Теорема $\mathcal{B}(G) \hookrightarrow \mathcal{F}(G)$ - теория дивизоров для $\mathcal{B}(G)$.
Опр Послед. A элементов с нулевой суммой **неразложима** если $A \neq A_1 \cdot A_2$, где A_1, A_2 - собств. подпоследовательн. с нулев. суммой
Опр **Константа Дэвенпорта** $d(G)$ конечной группы G - это max длина неразлож. послед. с нулевой суммой.
Утв Конст. Дэвенпорта - это наименьшее d такое, что $\forall$ послед. длины d содержит подпослед. с нулевой суммой
□ $(g_1, \dots, g_d) \rightsquigarrow (g_1, \dots, g_d - \sum g_i)$ ■

Пример $G=(\mathbb{Z}_n,+) \Rightarrow d(G)=n$, $(1,1,\dots,1)$ — n раз

Если в послед. $\geq n+1$ эл-та, то две част. суммы совпадают $\Rightarrow$ их разность есть подпослед. с нулевой суммой.

Хорошо известно, что любая конеч. группа $G \cong \mathbb{Z}_{n_1} \oplus \dots \oplus \mathbb{Z}_{n_r}$, $n_1 | n_2 | \dots | n_r$

Гипотеза $d(G) = \sum_{i=1}^{r} (n_i - 1) + 1$

Опровергнута в 2012 г: $G = \mathbb{Z}_2 \oplus \mathbb{Z}_6^4$, "$\geq$" верно всегда.

(4) Группа классов

Пусть $S \hookrightarrow \mathcal{F}(P)$ - теория дивизоров для полугруппы S.

Опр Группа классов дивизоров полугруппы S это фактор группа $Cl(S) = \mathbb{Z}\mathcal{F}(P) / \mathbb{Z}S$, где $\mathbb{Z}H$ - группа разностей полугруппы H.

Утв S однозн. разл. на простые множ. $\Leftrightarrow Cl(S) = 0$

Теорема 1 Моноид Крулля S однозначно восстанавливается по группе $Cl(S)$ и распределению простых элементов из P по классам этой группы.

Теорема 2 Пусть S - моноид Крулля. Тогда сл. усл. эквив.

(1) $|Cl(S)| \leq 2$;

(2) для любого $a \in S$ любые два его разложения в произведение неразложимых элементов из S имеют одинаковую длину.