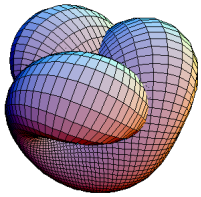
VII Санкт-Петербургский Турнир юных математиков
Санкт-Петербург 25 - 31 марта 2019 года

Зодача^{TM} 2
Нет Монет

Артем Семидетнов, ЛНМО



Аннотация
Решены все пункты кроме 4го

1 Дефиниции

Определение 1.1. *Соотношение Безу (Bézout's Identity) - утверждение из теории чисел заключающееся в том, что для любого набора целых чисел существует их линейная комбинация равная их наибольшему общему делителю. То есть для любых* $x_1, x_2, \ldots, x_n \in \mathbb{Z}$

$$\exists\{c_i\}_{i=1}^{n} \subset \mathbb{Z} \quad \sum_{i=1}^{n} c_i \cdot x_i = \gcd(x_1, x_2, \ldots, x_n)$$

Определение 1.2. *Если множество* S *является порождающим в плане полугруппы для* G*, будем писать* $\langle S \rangle_{sem} = G$*. Понятно, что* $S^+ = \langle S \rangle_{sem}$*. Мы будем придерживаться обоих обозначений.*

Определение 1.3. *Для группы* $G = \langle S \mid R \rangle$ *введем метрику на графе Кэли :* $d_S(\cdot, \cdot)$ *– кратчайший путь от одного элемента к другому(иначе - от класса эквивалентности одного слова к другому).*

Определение 1.4. *Длиной элемента* $g \in G$ *будем называть* $l(g) = d_S(e_G, g)$

Замечание 1.5. *Понятно, что введенная в задаче функция* $M_S(g)$ *является тем же самым, что и общепринятая длина слова. Далее в работе мы будем придерживаться терминалогии* $l(g)$*.*

Определение 1.6. *Элемент* g *называется тупиком, если* $l(gs) \leqslant l(g), \quad \forall s \in S \cup S^{-1}$

2 Пункт 1

Теорема 2.1. *Пусть* $\langle S\rangle_{sem} = X$, *причем* $S = \{a, b\} \subset \mathbb{N} \quad (\gcd(a, b) = 1)$, *тогда*

$$\forall n \geqslant a \cdot b - a - b + 1 \quad n \in X$$

Доказательство. Докажем по индукции:

1. Порождается $a \cdot b - a - b + 1$. Это проверяется по ссылке — [2]. Можно заметить, что конкретно проверять разрешимость данного диофантова уравнения не обязательно, поскольку существует теорема, утверждающая, что любое диофантово уравнение вида $ax + by = c$, где $\gcd(a, b) = 1$ имеет решения - [3].
2. Пусть порождается $\tilde{n} \geqslant a \cdot b - a - b + 1$. Докажем, что породится $\tilde{n} + 1$. Понятно, что существуют такие x_1, x_2, что $x_1 \cdot a + x_2 \cdot b = \tilde{n}$. Нам необходимо найти такие y_1, y_2, что $y_1 \cdot a + y_2 \cdot b = \tilde{n} + 1$. Приравняем некоторые части уравнений, а именно:

   $$x_1 \cdot a + x_2 \cdot b = y_1 \cdot a + y_2 \cdot b - 1$$

   Получим:

   $$(y_1 - x_1) \cdot a + (y_2 - x_2) \cdot b = 1$$

   Поскольку a и b взаимно просты такие коэффициенты будут существовать по соотношению Безу.

□

Следствие 2.2. *Для подполугруппы* $\langle 3, 5\rangle_{sem}$ *все будет порождаться с номера* $3 \cdot 5 - 3 - 5 + 1 = 8$. *А это пункт* $1(a)$

$$S^+ = \{3\} \cup \{5\} \cup \mathbb{N}_8$$

Замечание 2.3. *Подробнее про данное явление написано в* **Пункте 2**.

Теорема 2.4. *При любом множестве состоящим из взаимно простых чисел* S

$$\langle S\rangle = \mathbb{Z}$$

Доказательство. Этот факт - прямое следствие соотношения Безу. Поскольку нод всех чисел из S равен 1, можно линейной комбинацией получить ее. Далее понятно, что $\langle 1\rangle = \mathbb{Z}$ □

3 Пункт 2

Весь раздел задачи, представленный в этом пункте является проблемой Фробениуса(Frobenius Problem), также известной как "Coin problem". Это довольно известная задача на оценку числа обозначаемого $g(a_1, a_2, \ldots, a_n)$ для неотрицательных a_i, коий наибольший общий делитель равен 1, являющегося максимальным не имеющим решений в диофантовом уравнении(с неотрицательными коэффициентами) числом. То есть это максимальное число $\omega \in \mathbb{N}$, что диофантово уравнение

$$x_1a_1 + x_2a_2 + \cdots + x_na_n = \omega$$

от неотрицательных переменных и коэффициентах не имеет решений. Можно дать еще одну формулировку:

$$g(a_1, a_2, \ldots, a_n) \stackrel{\text{def}}{=} \max\{n \in \mathbb{N} \mid \nexists\{x_i\}_{i=1}^n \subset \mathbb{N} \quad \sum_{i=1}^{n} a_i \cdot x_i = n\}$$

Заметим, что $g(a_1, a_2)$ - двух чисел вычислен и известен(см. [6]). Оно имеет вид

$$g(a_1, a_2) = a_1 \cdot a_2 - a_1 - a_2$$

Легко видеть, что это еще один способ доказательства пункта $1(a)$ - все числа начиная с $a_1 \cdot a_2 - a_1 - a_2 + 1$ будут входить в $\langle a_1, a_2\rangle_{sem}$(в частном случае для $\langle 3, 5\rangle_{sem}$ это будет 8).
Строго говоря, еще можно дать оценку на $g(a_1, a_2, a_3)$ (см. [7]):

$$g(a_1, a_2, a_3) \geqslant \sqrt{3a_1a_2a_3} - a_1 - a_2 - a_3$$

Заметим, что существует алгоритм, вычислющий за полиномиальное время $g(a_1, a_2, \ldots, a_n)$ при заданных $a_i, \quad i = \overline{1, n}$. Он представлен в [5].

4 Пункт 3

Замечание 4.1. *Понятно, что относительно абелевой группы* $\mathbb{Z} = \langle S \,|\, S \rangle$ *поиск неудачных слов (таких, что* $l(g+s) < l(g)+1$*) эквивалентен поиску тупиков.*

Теорема 4.2. *Пусть* $S = \{a, b\}$ $(\gcd(a, b) = 1)$*. Не умаляя общности считаем, что* $a > b \geqslant 1$*. Тогда справедливо одно из двух:*

1. $a + b$ *четно — тогда существует ровно* $b - 1$ *тупиков в* $\langle S \rangle$*. И каждый из них имеет вид*

$$\frac{(a+b)\cdot(2\alpha - b)}{2}$$

Для $\alpha = \overline{1, b-1}$

2. $a + b$ *нечетно — тогда существует ровно* $2 \cdot (b-1)$ *тупиков в* $\langle S \rangle$*. И каждый из них имеет вид*

$$\frac{(a+b)\cdot(2\alpha - b) \pm b}{2}$$

Для $\alpha = \overline{1, b-1}$

Доказательство. Доказательство данного факта можно найти в [4]. □

Следствие 4.3. *В пункте 3 можно дать ответ на частный случай -* $7 + 9$ *четно. Тогда множество тупиков следующее*

$$F(S) = F(\{7, 9\}) = \left\{ \frac{16 \cdot (2\alpha - 7)}{2} \mid \alpha = \overline{1, 6} \right\} = \{8 \cdot (2\alpha - 7) \mid \alpha = \overline{1, 6}\}$$

Следствие 4.4. *Можно описать множество* $\{n/16 \,|\, n \in F(S)\}$*. Это будет множество вида*

$$\left\{ \frac{2\alpha - 7}{2} \mid \alpha = \overline{1, 6} \right\}$$

Лемма 4.5. $S^+ \cap F(S) = \varnothing$

Доказательство. Для этого опять обратимся к статье [4]. В ней для фиксированного порождающего множества вводилось понятие фробениусова числа — в нашем случае для $S = \{a, b\}$. Итого, число $\omega \in \mathbb{N}$ назовем фробениусовым, если

$$\nexists x, y \in \mathbb{N} \quad x \cdot a + y \cdot b = \omega$$

Было доказано(см. [4]), что число фробениусово для $\langle a, b \rangle_{sem}$ тогда и только тогда когда оно тупик в $\langle a, b \rangle$. Тогда понятно, что вское фробениусово число для $S = \{a, b\}$ не может быть порождено в $\langle a, b \rangle_{sem}$. Тоже верно в обратную сторону. □

Замечание 4.6. *На вопросы* $3(a)$*,* $3(b)$ *и* $3(c)$ *отвечают вышеизложенные теорема, два замечания и лемма.*

Список литературы

[1] THE UNBOUNDED DEAD-END DEPTH PROPERTY IS NOT A GROUP INVARIANT TIM R. RILEY and ANDREW D. WARSHALL

[2] `https://www.wolframalpha.com/input/?i=diophantine(x*a%2By*b+%3D+(a-1)*(b-1))`

[3] Линейные диофантовы уравнения. Г.И. Фалин

[4] Frobenius Problem and dead ends in integers. Zoran Šunić

[5] "Lattice translates of a polytope and the Frobenius problem". Combinatorica. Ravi Kannan (1992)

[6] `https://en.wikipedia.org/wiki/Coin_problem`

[7] The solution of Arnold's problem on the weak asymptotics of Frobenius numbers with three arguments. A. V. Ustinov