НИУ ИТМО

Факультет программной инженерии и компьютерной техники

Отчёт

По лабораторной работе №6

по дисциплине «Информатика»

«Работа с системой компьютерной вёрстки TEX»

Работу выполнил:
Рюмин Семён Андреевич,
группа P3111

Работу приняла:
Малышева Татьяна Алексеевна

Санкт-Петербург
2022 г.

Приложение

Перейдём теперь ко второй части нашего рассказа, из которой наиболее настойчивые читатели узнают доказательство гипотезы Эйлера.

30 марта 1796 года девятнадцатилетний Гаусс доказал возможность построения правильного семнадцатиугольника циркулем и линейкой. С этого дня начинается дневник Гаусса – летопись его удивительных открытий. Вторая запись в дневнике появилась уже 8 апреля. В ней сообщалось, что найдено строгое доказательство «золотой» теоремы – так назвал Гаусс гипотезу Эйлера. Он переоткрыл её, ещё учась в брауншвейгской гимназии, когда ему не были доступны произведения Эйлера, Лагранжа, Лежандра, с которыми он познакомился лишь после переезда в Геттинген в 1795 году. Вначале он, как и его предшественники, замечает утверждение для a=−1, затем, уже угадав результат для общего случая, последовательно разбирает случай за случаем, продвинувшись дальше других: им рассмотрены a=±2, ±3, ±5, ±7. Наконец, 8 апреля 1796 года он находит общее доказательство, которое Кронекер (1823 – 1891) очень метко назвал «пробой сил гауссова гения». Доказательство проводится двойной индукцией по a и p; Гауссу приходится придумывать существенно различные соображения для рассмотрения восьми (!) различных случаев. Нужно было иметь не только поразительную изобретательность, но и удивительное мужество, чтобы не остановиться на этом пути. Позднее Гаусс нашёл ещё шесть доказательств «золотой» теоремы (ныне их известно около пятидесяти). Как это часто бывает, после того как теорема доказана, удаётся найти доказательства много более простые, чем первоначальное. Мы приведём здесь доказательство, мало отличающееся от третьего доказательства Гаусса. В его основе лежит ключевая лемма, доказанная Гауссом не ранее 1808 года.

Л е м м а 2. *Пусть $p = 2k + 1$ — простое число, a — целое число, $0 < |a| \le 2k$; $r_1, r_2, \ldots, r_k$ — вычеты чисел $a, 2a, \ldots, ka$; ν — число отрицательных среди них.*

Тогда

$$a^k \equiv (-1)^\nu (mod\, p) \qquad (6)$$

Применяя критериий Эйлера, получаем такое следствие:

К р и т е р и й к в а д р а т и ч н о с т и в ы ч е т а. *Вычет является квадратичным тогда и только тогда, когда фигурирующее в лемме 2 число ν чётно.*

Д о к а з а т е л ь с т в о л е м м ы 2. Заметим, что все вычеты $r_1, \ldots, r_k$ различны по абсолютной величине. Это следует из того, что сумма и разность любых двух из них не делится на p: $r_i \pm r_j \approx (i \pm j)a, i \ne j; |i \pm j| < p$. Таким образом, набор модулей $|r_1|, \ldots, |r_k|$ — это числа 1, 2, ..., k, в некотором порядке. В результате произведение $a \cdot 2a \ldots ka = a^k k!$ при делении на p даёт тот же остаток, что $r_1, \ldots, r_k = (-1)^\nu k!$. Учитывая, что $k!$ не делитсчя на простое число p, получаем (6).

Д о к а з а т е л ь с т в о г и п о т е з ы Э й л е р а. Заметим, что в приводимом ниже рассуждении уже не используется простота p — она в полной мере использована в лемме Гаусса. Отметим на числовой оси точки (рис. 1, *а, б)* $m\frac{p}{2}$, если a<0; m = 0, 1, 2, ..., $|a|$ — синие точки (m — их номера). Занумеруем интервалы с концами в этих точках по номерам левых концов (на рисунках номера интервалов — красные). Отметим теперь a, $2a$, ..., ka — зелёные точки; так как a — целое, не делящееся на p, то синие точки не могут сопасть

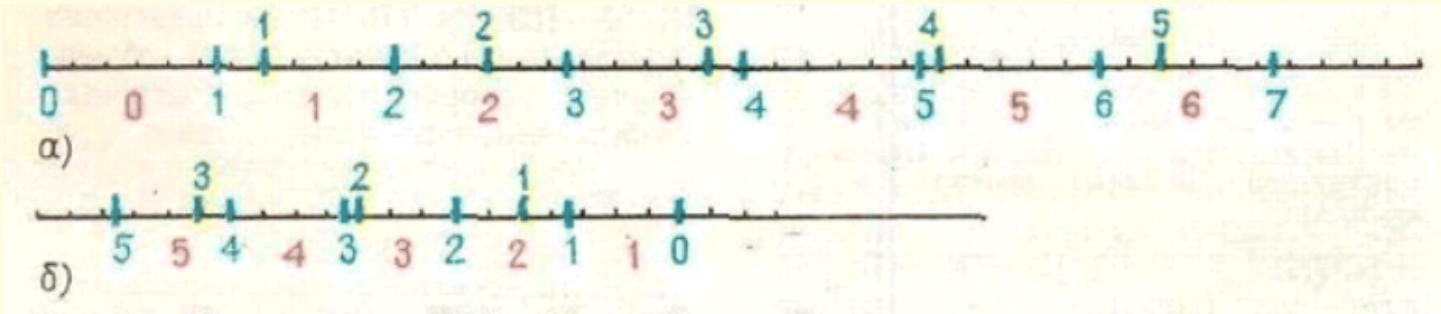

Рис.1, а. На рисунке $p = 11$ ($k = 5$), $a = 7$, $\nu = 3$.
Рис. 1, б. На рисунке $p = 7$ (k = 3), a = -5, $\nu = 2$.

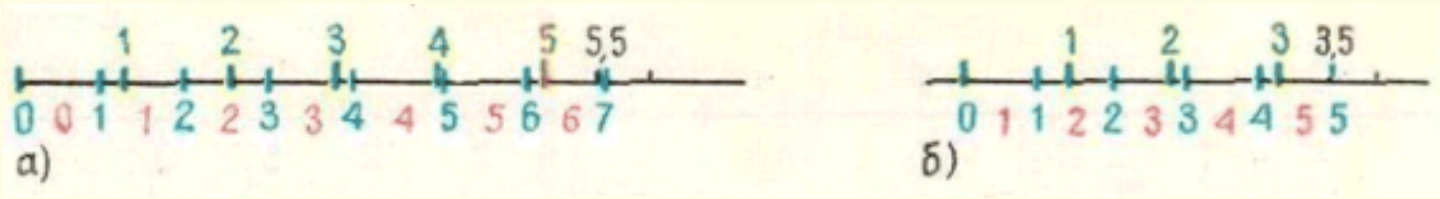

Рис. 2.

с зелёными, причём все зелёные точки попадут в какие-то из построенных интервалов $\left(|a\frac{p}{2} > |a|k\right)$. Легко заметить, что фигурирующее в лемме число ν — это число зелёных точек, попавших в интервалы с нечётными номерами (докажите!).

Подвергнем теперь нашу картинку преобразованию подобия с коэффициентом $\frac{1}{a}$ (рис. 1 перейдёт в рис. 2). При этом синие точки перейдут в точки, делящие отрезок $\left[0, \frac{p}{2}\right]$ на $|a|$ равных частей, а зелёные точки — в целочисленные точки 1, 2, ..., k.

Нумерация интервалов теперь будет зависеть от знака a: при $a > 0$ они нумеруются номерами левых концов, при $a < 0$ — номерами правых концов; ν — число целочисленных точек в интервалах с нечётными номерами. Если мы увеличим p на $4al$, то в каждый интервал добавится точно $2l$ целых точек. Это следует из того, что при сдвиге интервала на целое число количество целых точек в нём не меняется, а на любом отрезке целочисленной длины n с нецелочисленными концами имеется ровно n целых точек (докажите!). Итак, при изменении p на $p + 4al$ величина ν изменится на чётное число, а $(-1)^\nu$ не изменрится. Значит, для всех p в арифметической прогрессии $p = 4aq + r$ значение $(-1)^\nu$ — одно и то же, и гипотеза Эйлера доказана.

Одновременно указан некоторый способ выяснить, является ли a квадратичным вычетом для p. Нужно взят остаток r от деления p на $4a$ (для удобства положительный); разделить $\left(0, \frac{r}{2}\right)$ на $|a|$ частей, занумеровав их номерами левых (правых) концов, если — положительное (отрицательное); сосчитать число ν целых точек, попавших в интервалы с нечётными номерами; а — квадратичный вычет в том и только том случае, когда ν чётно.

Проделаем эти вычисления для $a = 2$, чтобы подтвердить наблюдения Эйлера, о которых говорилось на стр. 5. Пусть $a = 2$; Тогда достаточно рассмотреть $r = 1$, 3, 5, 7, поскольку в остальных случаях арифметическая прогрессия не будет содержать простых чисел. Как видно из рис. 3, число 2 является квадратичным вычетом для

$$p = 8q + 1, p = 8q + 7,$$

то есть $p = 8q \pm 1$.

Упражнение. Покажите, что -2 есть квадратичный вычет для $p = 8q + 1, p = 8q + 3$.

Аналогично рассматривается случай $a = \pm 3$. Приведём итоги вычислений (таблица для ν):

a \ r	1	5	7	11
3	0	1	1	2
-3	0	1	2	3

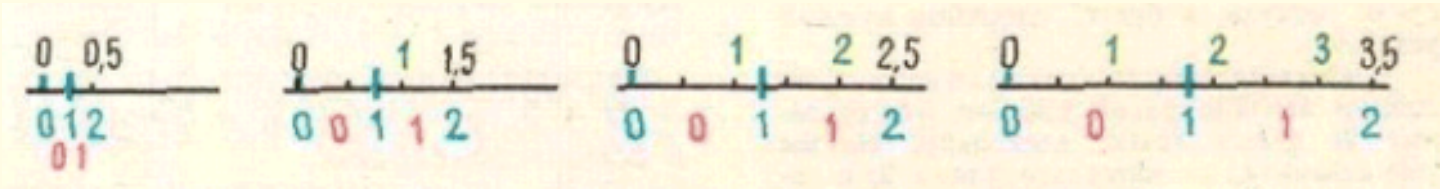

Рис. 3. $r = 1$, $a = 2$, $\nu = 0$; $r = 3$, $a = 2$, $\nu = 1$; $r = 5$, $a = 2$, $\nu = 1$; $r = 7$, $a = 2$, $\nu = 2$.