Федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский университет ИТМО»

Факультет Программной Инженерии и Компьютерной Техники

Лабораторная работа №6
Работа с системой компьютерной вёрстки $\TeX$
Вариант 31

Выполнил:
Марьин Григорий Алексеевич
Группа P3112
Проверил:
Малышева Т. А.
Доцент ФПИиКТ

Санкт-Петербург 2024г.

Золотая теорема

С. Г. Гиндикин

«Свойства чисел, известные сегодня, по большей части были открыты путём наблюдения и открыты задолго до того, как их истинность была подтверждена строгими доказательствами.»

Л. Эйлер

Мы совершим экскурс к истокам современной теории чисел - отрасли математики, изучающей натуральные числа. В то время математики подмечали удивительно простые и красивые закономерности в мире натуральных чисел. Но часто интригующая простота формулировок оборачивалась неприступностью решения. Лобовые атаки не давали успеха, приходилось придумывать обходные пути, создавать совершенно новый аппарат.

Мы расскажем здесь об одной такой задаче *) , формулировка которой понятна школьнику, знающему, что такое простое число. Но решить эту задачу далеко не просто, и первый шаг на пути ее решения совсем не сразу удалось сделать великому Эйлеру. Гипотезу, сформулированную Эйлером (но не доказанную им), пытались доказать Лангранж и Лежандр; удалось это сделать девятнадцатилетнему Гауссу. Это была его вторая работа*)).

Гаусс назвал доказанную им теорему «золотой теоремой». В ней идет речь о том, какими могут быть остатки от деления квадратов целых чисел на простые числа. Мы не будем сейчас приводить полной формули- ровки утверждения, доказанного Гауссом, отложив это до стр. 5. Сейчас же мы поясним постановку зада- чи, введем некоторые термины и подробно рассмотрим частный случай «золотой теоремы», доказанный Эйлером.

Хорошо известны различные условия, необходимые для того, чтобы целое число было квадратом. Например, такое число может оканчиваться только на 0, 1, 4, 5, 6 или 9. Другое часто используемое свойство состоит в том, что квадрат целого числа или делится на 3 или при делении на 3 дает остаток 1 (докажите). Первое свойство можно сформулировать в тех же терминах, что и второе, заметив, что последняя цифра это остаток от деления на 10.

Всюду ниже мы будем предполагать, что p — простое число, причем $p \neq 2$. Делить целые числа можно «с недостатком» или «с избытком». Иными словами, остатки можно считать положительными или отрицательными. Условимся выбирать остаток наименьшим по абсолютной величине. Нетрудно доказать, что если р нечетно, то всякое целое число п единственным образом представляется в виде

$$n = pq + r, |r| \leq \frac{p-1}{2}, \qquad (1)$$

где q и r - целые

*)О других задачах теории чисел можно прочитать в журнале «Квант»: Башмаков М.И. *Нравится ли вам возиться с целыми числами?, 3, 15, 1971;* Башмаков М.И.*О постулате Бертрана, 5, 4, 1971;* Депман И.Я. *Совершенные числа, 8, 1, 1971;* Гиндикин С.Г. *Дебют Гауса, 1, 2, 1972*; Гиндикин С.Г. *Малая теорема Ферма, 10. 2, 1972.*

*)О первой рассказывалось в статье «Дебют Гаусса» («Квант» №1, 1972 г.)

p	$p = \frac{p-1}{2}$	Вычеты (остатки) по модулю p
3	1	-1 0 1
5	2	-2 -1 0 1 2
7	3	-3 -2 -1 0 1 2 3
11	5	-5 -4 -3 -2 -1 0 1 2 3 4 5
13	6	-6 -5 -4 -3 -2 -1 0 1 2 3 4 5 6
17	8	-8 -7 -6 -5 -4 -3 -2 -1 0 1 2 3 4 5 6 7 8

Будем называть r остатком от деления n на p, или *вычетом* числа n *по модулю* p. Это обозначается так: $n \equiv r \pmod{p}$ *).

Выпишем в таблице 1 вычеты для нескольких первых простых чисел $p>2$. Нас интересует, какие вычеты (остатки) могут иметь *квадраты* целых чисел. Эти остатки мы будем называть *квадратичными вычетами*, а остальные — *квадратичными невычетами*.

Числа n^2 и r^2, где r — остаток числа n по модулю p, имеют один и тот же остаток при делении на p **). Поэтому, если мы хотим найти квадратичные вычеты, то достаточно возводить в квадрат лишь вычеты, то есть целые числа r, $|r| \leqslant k$, $k = \frac{p-1}{2}$. При этом, разумеется, достаточно рассматривать $r \geqslant 0$.

Проведем вычисления для простых чисел из предыдущей таблицы. Составим новую таблицу, в которой красные числа отвечают квадратичным вычетам (таблица 2). Попытаемся подметить некоторые закономерности и оценить степень их общности. Во-первых, *в каждой строке есть в точности $k+1$ красное число*. Покажем, что так обстоит дело для всех простых $p>2$. Из сказанного выше следует, что для каждого нечетного p (даже не простого) квадратичных вычетов *не больше* $k+1$. Мы покажем, что их *точно* $k+1$, если убедимся, что все числа r^2 $(0 \leqslant r \leqslant k)$ дают при делении на p различные остатки. Если $r_1 > r_2$ и r_1^2, r_2^2 дают одинаковые остатки, то $r_1^2 - r_2^2$ делится на p. Поскольку p — простое число, то $r_1 + r_2$ или $r_1 - r_2$ должно делиться на p, чего не может быть, так как $0 < r_1 \pm r_2 < 2k < p$. Здесь мы впервые воспользовались простотой p (покажите, что для со-

*) То, что мы называем вычетом (остатком), обычно называют *абсолютно наименьшим вычетом* (остатком). Мы сократили название, так как других вычетов нам не встретится. Обозначение $n \equiv r \pmod{p}$ также используется обычно в более общей ситуации: оно означает, что $n-r$ делится на p. См. также статью «Малая теорема Ферма» («Квант» № 10, 1972 г.); в дальнейшем, ссылаясь на эту статью, мы будем писать кратко: «МТФ».

**) Подробнее об арифметике остатков см. в МТФ.

Таблица 2

p	k	Квадратичные вычеты и невычеты по модулю p
3	1	−1 0 1
5	2	−2 −1 0 1 2
7	3	−3 −2 −1 0 1 2 3
11	5	−5 −4 −3 −2 −1 0 1 2 3 4 5
13	6	−6 −5 −4 −3 −2 −1 0 1 2 3 4 5 6
17	8	−8 −7 −6 −5 −4 −3 −2 −1 0 1 2 3 4 5 6 7 8