

Оглавление

Предисловие	4
Раздел 1. Введение	5
Раздел 2. Вычеты, невычеты и арифметические операции над ними	9
Раздел 3. Критерий Эйлера и вычеты по простым модулям вида $4k \pm 1$	17
Раздел 4. Квадратичный закон взаимности	31
Раздел 5. Символ Якоби и обобщение КЗВ	50
Раздел 6. Комбинаторное доказательство КЗВ	56
Раздел 7. Решения задач	63
Литература	79

Предисловие

Данная брошюра написана по итогам летних сборов для кандидатов в сборную Москвы на Всероссийскую олимпиаду школьников по математике, проводившихся с 19 по 29 июня 2022 г. Основной темой по теории чисел на этих сборах была такая классическая вещь, как *квадратичные вычеты*. В ходе подготовки к занятиям, а также в процессе обсуждения задач со школьниками удалось обнаружить много новых, красивых и малоизвестных фактов, связанных с этим сюжетом. Особенно обращают на себя внимание шесть (!) различных доказательств квадратичного закона взаимности, предложенных школьниками, являющимися соавторами данного текста. (Нельзя не отметить, что столько же доказательств придумал и сам Карл Фридрих Гаусс, впервые доказавший квадратичный закон взаимности.)

Впечатлившись таким энтузиазмом со стороны ребят, П. В. Бибииков захотел сохранить эти результаты, в результате чего и родился данный текст. Его основу составляют два листка, составленных П. В. Бибииковым и А. Ю. Кушниром, однако в текст добавлены и многие другие задачи, прежде всего из зарубежных олимпиад. Текст книги основан на развитии идей, представленных в этих листках, и построен в формате рассказа о наиболее известных и важных фактах из теории квадратичных вычетов, которые сопровождаются большим количеством задач, методических комментариев, экскурсов в историю математики и замечаний о связи обсуждаемых вопросов с проблемами из современной теории чисел.

Брошюра рассчитана на школьников, знакомых со следующими фактами из теории чисел:

- сравнения по модулю и их свойства;
- деление остатков по простому модулю;
- малая теорема Ферма: $a^{p-1} \equiv_p 1$ при $a \not\equiv_p 0$;
- теорема Вильсона: $(p-1)! \equiv_p -1$.

В отдельных задачах также полезно знать о порядках чисел по простому модулю, но эти знания необязательны. Мы стремились сделать данную книгу самодостаточной и кратко изложили эти результаты в тексте. Для более детального изучения основ теории чисел можно обратиться к книге [6].