Построение базы неразложимых многочленов

Терентьев М. Ю.

Гр. 6302

Постановка задачи

- Необходимо построить базу данных, в которой будут храниться многочлены степени не выше **n**, неприводимые в поле вычетов $\mathbf{Z_p}$, где **p** может быть любым простым числом.

- Созданную базу многочленов в дальнейшем можно будет применять для проверки неприводимости многочлена с целыми коэффициентами над полем рациональных чисел **Q**.

- В силу слабых вычислительных мощностей мы ограничимся многочленами степени не выше десятой, а поля вычетов будем брать только по модулю простых чисел, меньших десяти.

Подзадачи

- Для создания базы данных с помощью переборного алгоритма будем проверять каждый многочлен степени меньше 10 на неприводимость в полях вычетов $\mathbf{Z}_2$, $\mathbf{Z}_3$, $\mathbf{Z}_5$, $\mathbf{Z}_7$. Если многочлен неприводим в каком-либо из полей, он будет записан в соответствующий блок в файле.

- При проверке многочлена по базе, сначала мы берем исходный полином в поле вычетов $\mathbf{Z}_2$ и сравниваем с каждым в блоке $\mathbf{Z}_2$, потом исходный полином переводим в поле вычетов $\mathbf{Z}_3$ и проверяем, и так пока не встретим в одном из полей такой же полином или не дойдем до конца списка.

Теория

- Определение:
  Многочлен **P(x)** называется неприводимым(примитивным) над полем **K**, если его нельзя представить в виде произведения двух многочленов $\mathbf{P(x) = P_1(x) * P_2(x)}$ с коэффициентами из того же поля, не являющихся константами.

- Теорема:
  Если многочлен с целыми коэффициентами неприводим над полем $\mathbf{Z_p}$, где **p** – простое число, и старший коэффициент данного многочлена не делится на **p**, то многочлен неприводим над полем рациональных чисел.

- Данная теорема и является основой для создания базы многочленов для проверки их приводимости.

Проверка приводимости многочлена

- Пользуясь теоремой о том, что неприводимый над $\mathbf{Z}_p$ многочлен с целыми коэффициентами неприводим и над полем рациональных чисел **Q**, мы получаем возможность относительно просто проверять, приводимость многочлена.

- Для этого достаточно последовательно проверять приводимость многочлена над $\mathbf{Z}_p$, что для небольших **p** довольно просто, особенно, если степень многочлена не слишком велика.

Проверка приводимости над Z_p

- Для проверки приводимости многочлена над полем $\mathbf{Z_p}$ достаточно составить базу неразложимых многочленов степени меньше, чем проверяемый, после чего разделить исходный многочлен на каждый многочлен из составленной базы, тогда, если во всех случаях получился ненулевой остаток, многочлен неприводим.

- Так как многочлен(моном) ***x*** будет являться неприводимым над любым полем, построение базы всегда можно начинать с него. Далее, например, многочлен ***x + 1*** будет также неприводимым, так как ***(x + 1)*** даст в остатке **1** при делении на ***x***.

Пример

- Рассмотрим пример: $\boldsymbol{x^3 + 5x^2 + 4x + 3}$ – рассмотрим этот многочлен над полем Z_2.
  В Z_2 коэффициенты исходного многочлена заменяются на остаток от деления на 2: $\boldsymbol{x^3 + x^2 + 1}$.
- Так как степень многочлена равна 3, нам достаточно рассмотреть неприводимые многочлены над Z_2 не выше второй степени:
  1) x
  2) $x + 1$
  Многочлены x^2 и $x^2 + 1$ будут приводимы над Z_2 (очевидно, $x^2 = x \cdot x$,
  $(x^2 + 1) = (x^2 + 2x + 1) = (x + 1)(x + 1)$)
- А теперь разделим $\boldsymbol{(x^3 + x^2 + 1)}$ на $\boldsymbol{(x + 1)}$ – остаток равен **1**, как в случае и с делением на $\boldsymbol{x}$. Значит, многочлен неприводим над Z_2, а следовательно и над полем рациональных чисел.

Количество неразложимых многочленов

- Количество неразложимых многочленов довольно высоко. Ниже указано поле и количество в нём неразложимых многочленов степени не выше 8-й.

- Z_2 – 70 многочленов
- Z_3 – 1318 многочленов
- Z_5 – 63319 многочленов
- Z_7 – 861580 многочленов
- Итого: 70 + 1318 + 63319 + 861580 = 926287

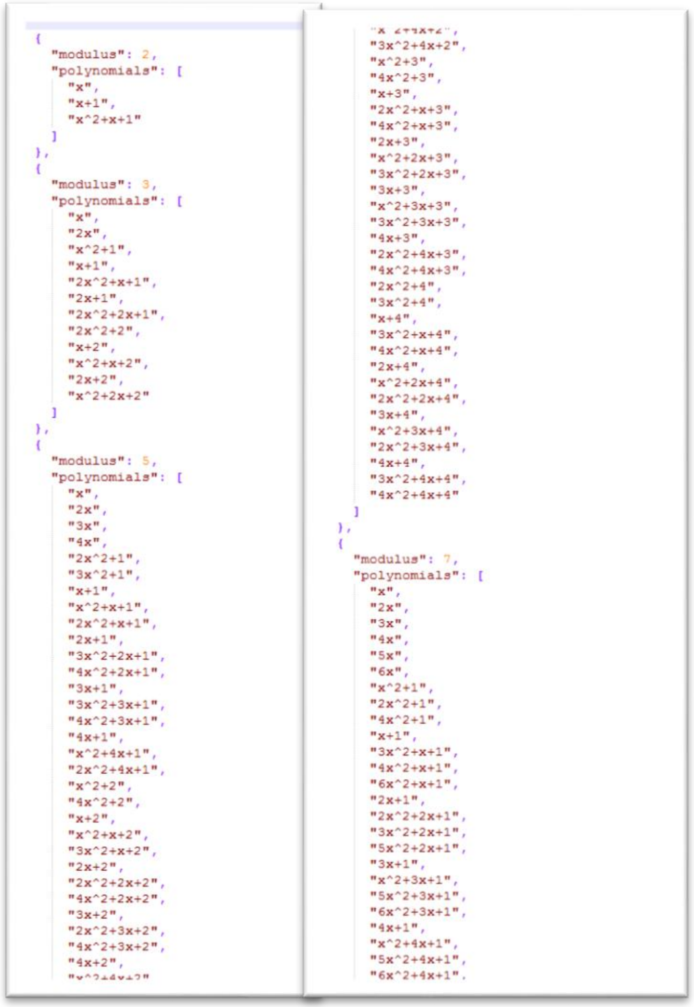
- Данные расчеты были предоставлены студенткой гр. 6371 Симбирцевой Мариной

Реализация в программе

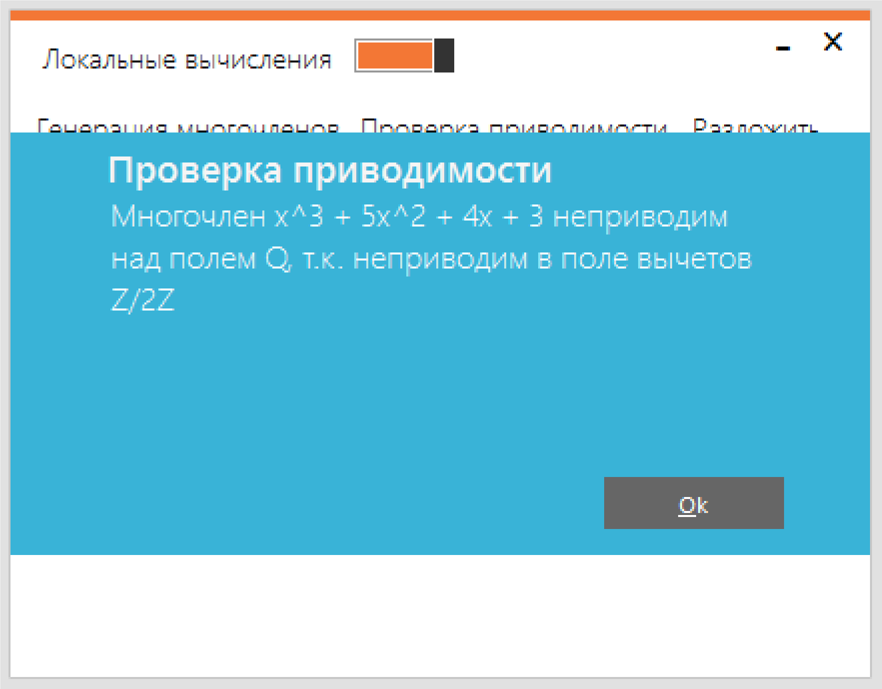
- При генерации базы данных для проверки неприводимости многочлена мы генерируем многочлен в поле $\boldsymbol{Z_p}$ и пытаемся его поделить на многочлен меньшей степени, который уже есть в нашей базе. Если хоть в одном случае остаток равен нулю – многочлен приводим
- При проверке многочлена по базе данных, сначала коэффициенты переводятся в поле $\boldsymbol{Z_p}$, после чего программа ищет многочлен в данном блоке файла. Если такой многочлен найден, значит, исходный многочлен неприводим, в противном случае, идет поиск в следующем поле вычетов $\boldsymbol{Z_p}$.
- Если по базе многочлен не был найден ни в одном из полей $\boldsymbol{Z_p}$, то неизвестно, приводим он или нет, так как в программе рассматриваются только $p < 10$.

Пример работы программы

Файл, сгенерированный программой, содержащий полиномы неприводимые над полем рациональных чисел, степени не выше 2



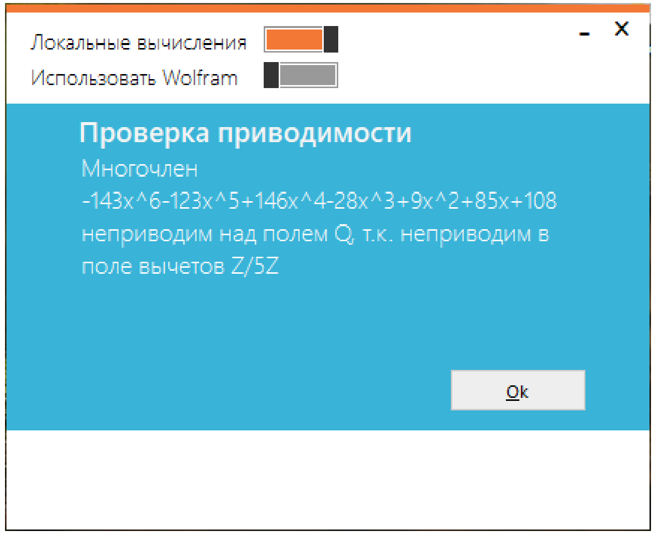
Проверка разложимости
$x^3 + 5x^2 + 4x + 3$ по базе данных



Неразложим в Z_2

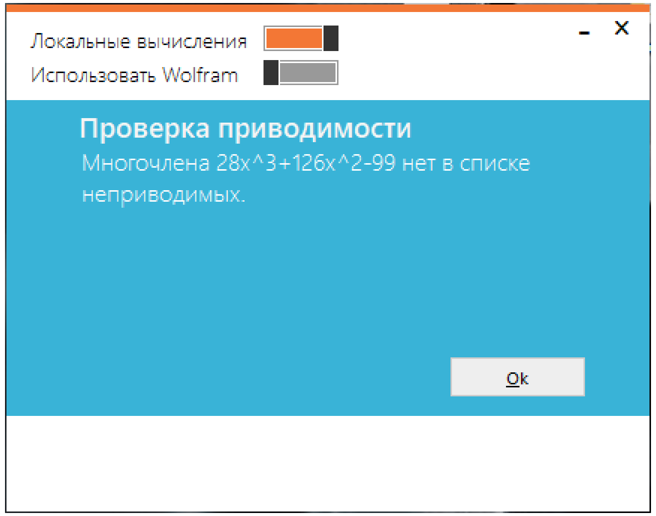
Пример работы программы

$-143x^6 - 123x^5 + 146x^4 – 28x^3 + 9x^2 + 85x + 108$



Неразложим в Z_5

$28x^3 + 126x^2 - 99$



Неразложим в $\mathbf{Z_{13}}$, однако отсутствует в базе. Т.к. мы использовали $p < 10$

Заключение

- Неприводимые многочлены являются довольно актуальной и востребованной темой, например, в криптографии при генерировании открытых и закрытых ключей, в теории кодирования и т.д., поэтому и методы определения неприводимости многочлена так же необходимы.