Оглавление

Глава 1

Алгебраическое введение

1.1 Кольцо целых алгебраических

Чтобы понять что тут вообще происходит, нужно немного алгебры.
Основное поле - $\mathbb{Q}$. Корни полиномов с коэффициентами из $\mathbb{Q}$ называют алгебраическими над $\mathbb{Q}$. Алгебраическое число называется целым алгебраическим, если его минимальный многочлен $g(x) \in \mathbb{Z}[x]$. Введем множество целых алгебраических поля $\mathbb{Q}(\alpha)$

$$\mathfrak{O}_{\mathbb{Q}(\alpha)} = \{x \mid x \in \mathbb{Q}(\alpha) \,\&\, x \text{ - целое алгебраическое}\}$$

T(?). *$\mathfrak{O}_{\mathbb{Q}(\alpha)}$ - кольцо. Кроме того $\mathbb{Z}[\alpha] \subseteq \mathfrak{O}_{\mathbb{Q}(\alpha)}$ - подкольцо.*

T(?). *K - поле, $R \subset K$ - подкольцо с однозначным разложением на множители. Тогда R содержит корни всех неприводимых унитарных многочленов из $R[x]$*

Нас будет интересовать подкольцо $\mathbb{Z}[\alpha]$ с однозначным разложением на множители. Но в каких случаях будет получаться это однозначное разложение? Теорема гарантирует однозначное разложение в $\mathbb{Z}[\alpha]$, если $\mathbb{Z}[\alpha] = \mathfrak{O}_{\mathbb{Q}(\alpha)}$. Но это не всегда так. Что делать когда это не так?

Пример. *Рассмотрим $\gamma = -\frac{1}{2} + \frac{\sqrt{5}}{2} \notin \mathbb{Z}[\sqrt{5}]$. Но γ корень $x^2 + x - 1 \in \mathbb{Z}[x]$, значит $\gamma \in \mathfrak{O}_{\mathbb{Q}(\sqrt{5})}$*

T(?). *$\forall \beta \in \mathfrak{O}_{\mathbb{Q}(\alpha)} \to \beta \cdot f'(\alpha) \in \mathbb{Z}[\alpha]$, где $f'(x)$ - минимальный многочлен α*

1.2 Норма

Вспомним, что $\mathbb{Q}(\alpha)$ - в.п. над $\mathbb{Q}$. Введем в этом пространстве линейный оператор, соответствующий некоторому элементу $\beta \in \mathbb{Q}(\alpha)$

$$\mathcal{H}_\beta : \ \mathbb{Q}(\alpha) \xrightarrow[x \mapsto \beta x]{} \mathbb{Q}(\alpha)$$

Опр. *Норма $\beta \in \mathbb{Q}(\alpha)$ определяется следующим равенством*

$$\mathcal{N}(\beta) = det(\mathcal{H}_\beta)$$

Как вычислять эту норму для произвольного элемента? Пока не ясно. В алгоритме говорится, что норму элемента вида $\beta = a + b\alpha$ можно вычислить по формуле

$$\mathcal{N}(\beta) = F(a, b) = b^{degf} f(\frac{a}{b}), \text{ где } f \text{ - полином степени порождающий поле.}$$

Откуда эта формула? Как ее получить из определения? Нужно разбираться. Но пока будем считать, что все норм.

Пример. *Попробуем вычислить норму $\beta = a + b\sqrt{5}$ в $\mathbb{Q}(\sqrt{5})$.*
Найдем $\mathcal{H}_\beta = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}$. По определению эта матрица соответствует оператору, который x отправляет в βx. Подействуем этой матрицей на элементы 1 и $\sqrt{5}$. Им соответствуют векторы $(1, 0)$ и $(0, 1)$.

$$\beta \cdot 1 = \beta = a + b\sqrt{5} \;\Rightarrow \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_3 \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}$$

$$\beta \cdot \sqrt{5} = 5b + a\sqrt{5} \;\Rightarrow \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} x_2 \\ x_4 \end{pmatrix} = \begin{pmatrix} 5b \\ a \end{pmatrix}$$

Получили матрицу $\begin{pmatrix} a & 5b \\ b & a \end{pmatrix}$. Делаем вывод, что $\mathcal{N}(\beta) = det(\mathcal{H}_\beta) = a^2 - 5b^2$. Попробуем вычислить по формуле. Поле $\mathbb{Q}(\sqrt{5})$ построено с помощью полинома $f(x) = x^2 - 5$.

$$\mathcal{N}(\beta) = F(a, b) = b^2 f(\frac{a}{b}) = b^2((\frac{a}{b})^2 - 5) = a^2 - 5b^2$$

Магия...

Глава 2

Разность квадратов

Есть несколько подходов к факторизации целых чисел. Один из них основан на соотношении

$$x^2 \equiv y^2 \; mod \; n$$

Если мы каким-либо образом получим такое соотношение, то в случае $x \not\equiv \pm y$ мы получим нетривиальный делитель d

$$d = GCD(x \pm y, \; n)$$

Как строить такие соотношения? Один из вариантов сейчас будет описан. Пусть R - евклидово кольцо и в нашем распоряжении есть гомоморфизм колец

$$\phi : \; R \to \mathbb{Z}/n\mathbb{Z}$$

Найдем(построим) в R элемент α, который является квадратом. Кроме того образ α должен быть квадратом в $\mathbb{Z}/n\mathbb{Z}$, т.е.

$$\phi(\alpha) = x^2, \; x \in \mathbb{Z}/n\mathbb{Z}$$

Тогда получим следующее соотношение

$$x^2 = \phi(\alpha) = \phi(\beta^2) = \phi^2(\beta) = y^2$$

Таким образом

$$x^2 \equiv y^2 \; mod \; n$$

Как строить квадраты в R?

2.1 Построение квадрата в евклидовом кольце

Для построения квадратов нам потребуется конечное множество неразложимых элементов F_R кольца R

$$F_R = \{p_1, p_2, ..., p_s\}$$

Назовем его алгебраической факторной базой. Элемент $x \in R$ назовем гладким относительно F_R, если он полностью раскладывается по элементам F_R, т.е.

$$x = p_1^{\alpha_1} ...\ p_s^{\alpha_s},\ p_i \in F_R$$

Пример. $R = \mathbb{Z}$, $F_R = \{2, 3, 5, 7\}$. *Тогда* $60 = 2^2 \cdot 3 \cdot 5$ *будет гладким, а* $22 = 2 \cdot 11$ *не является гладким*

Очевидно, что x квадрат в $R \Leftrightarrow \forall i\ \alpha_i \equiv 0\ mod\ 2$. Построим множество гладких элементов мощности t

$$S = \{x \mid x \text{ - гладкий относительно } F_R\}$$

Каждому элементу x из S можно поставить в соответствие двоичный s-мерный вектор

$$(\alpha_1\ mod\ 2, ..., \alpha_s\ mod\ 2)$$

Тогда умножению элементов соответствует сумма векторов. Наша цель получить нулевой вектор, комбинируя данные векторы. Очевидно, что нулевому вектору соответствует некоторый квадрат. Как получить нулевой вектор? Построим матрицу M из всех векторов. Размер этой матрицы $s \times t$. Эта матрица соответствует СЛАУ. Если $t > s$, то СЛАУ будет иметь ненулевое решение (мы получаем условие на размер S, т.е. чтобы получить квадрат, нам нужно собрать гладких чисел по крайней мере на единицу больше, чем размер факторной базы). Таким образом задача построения квадрата сведена к задаче поиска решения уравнения

$$Mx = 0$$

Ну вообще в идеале нам нужно найти базис $kerM$, чтобы по этому базису строить другое решение, т.к. будут возникать ситуации когда найденное решение не подходит нам и мы хотим сразу попробовать другое решение, а не проделывать всю работу заново. (Такая задача у нас на 1 курсе называлась поиском фундаментальной системы решений. В принципе алгоритм Гаусса можно легко модифицировать для решения этой задачи. Но вот на счет "крутых"методов я не уверен, т.к. они дают просто решение. В любом случае для начала сгодится простой алгоритм Гаусса)

2.2 Получение гладких чисел

Наше кольцо R евклидово, следовательно определена норма $\mathcal{N}$. Чтобы построить факторную базу, нужно перебирать элементы кольца и брать те, норма которых - простое число. (пусть $x = p_1 p_2$ не является неразложимым и его норма проста, тогда $\mathcal{N}(x) = \mathcal{N}(p_1)\mathcal{N}(p_2) = p$. Противоречие. Вроде все ок.)

Для построения множества гладких пар нужно проверять делимость на элементы алгебраической факторной базы. Это проверяется с помощью нормы. Берем элемент $x = p_1^{\alpha_1} ... \ p_s^{\alpha_s}$ и вычисляем $\mathcal{N}(x) = \mathcal{N}^{\alpha_1}(p_1) ... \ \mathcal{N}^{\alpha_s}(p_s) = a$. Далее перебираем все элементы факторной базы. Пусть p_i - очередной элемент факторной базы и $\mathcal{N}(p_i) = q_i$. Проверяем делимость a на q_i. Если делится, то делим a на q_i, пока q_i не перестанет делить a. Повторяем процедуру для слудующего элемента факторной базы. В конце мы получим $a = 1$, если a разлагается по данной факторной базе. Иначе a не раскладывается. Вроде все ок, но есть одна проблемка. А вдруг существует неразложимый элемент, который не принадлежит факторной базе, но его норма совпадает с некоторым элементом из факторной базы. Тогда a может не раскладываться по нашей базе, хотя мы сделаем вывод, что раскладывается. Короче нужно подробней разобраться в этом моменте.

Глава 3

Специальный метод решета числового поля

Пусть нужно факторизовать число

$$n = r^t - s$$

Нам нужно построить поле по некоторому полиному $f(x)$. Выберем d - степень полинома.

$$r^t - s \equiv 0 \; mod \; n$$

$$r^t \equiv s \; mod \; n$$

Положим $k = \lceil \frac{t}{d} \rceil$ и домножим обе части на r^{kd}

$$r^{t+kd} \equiv sr^{kd} \; mod \; n$$

$$r^{kd} \equiv sr^{kd-t} \; mod \; n$$

Положим $m = r^k$ и $c = sr^{kd-t}$

$$m^d \equiv c \; mod \; n$$

В качестве полинома возьмем

$$f(x) = x^d - c$$

Построим поле

$$\mathbb{Q}[x]/(f) \cong \mathbb{Q}(\alpha), \text{ где } \alpha \text{ - корень } f(x)$$

Что же делать дальше?

Литература

[1] Text

Приложение A

Приложение