Разложение на множители

М.Д. Малых, РУДН

27 октября 2022 г.

Содержание

1. Разложение на множители в кольце $\mathbb{Z}$

Теорема 1. Всякое натуральное число, большее 1, можно представить как произведение простых чисел.

Доказательство. Если число a — простое, это и есть искомое представление. Если оно не является простым, то оно представимо в виде произведения двух меньших чисел. Если одно из них или оба не являются простыми, их можно представить в виде произведения еще меньших чисел. Действуя

так далее не более чем за a шагов мы придем к простым числам. Поэтому число a можно представить в виде произведения простых чисел. $\square$

Таким образом, всякое натуральное число $a > 1$ можно представить как произведение простых чисел

$$a = p_1^{m_1} \dots p_r^{m_r},$$

где $p_1, \dots, p_r$ — простые числа, а $m_1, \dots, m_r$ — натуральные числа. При этом m_i называют кратностью (multiplicity), с которой множитель p_i входит в представление.

Это представление единственно с точностью до порядка сомножителей, поскольку верна след. теорема.

Теорема 2. Пусть число a раскладывается на простые сомножители:

$$a = p_1^{m_1} \dots p_r^{m_r},$$

где $p_1, \dots, p_r$ — простые числа, а $m_1, \dots, m_r$ — натуральные числа. Если простое число q не совпадает с $p_1, \dots, p_r$, то a не делится на q.

Доказательство. Класс эквивалентности $[a]$ в факторкольце $\mathbb{Z}/q\mathbb{Z}$ равен нулю, а с другой стороны он равен

$$(p_1 + (q)) \dots (p_r + (q))$$

Поскольку $p_1, \dots, p_r$ не делятся на q, эти сомножители не являются нулями факторкольца. Но, поскольку факторкольцо — поле, их произведение не может равно нулю. $\square$

Задача 1. Дано натуральное число. Разложить его на простые множители.

Вообще говоря, задача решается перебором всех произведений всех простых чисел, которые меньше заданного числа. Хотя такое решение чрезвычайно расточительно, обсуждение эффективных алгоритмов решения этой задачи мы отнесем к компьютерной алгебре.

Разложение на множители реализовано в Sage в виде функции `factor`:

```
sage: ZZ(12421354).factor()
2 * 11 * 564607
```

Иногда бывает полезным получить ответ в виде списка:

```
sage: list(ZZ(12421354).factor())
[(2, 1), (11, 1), (564607, 1)]
```

При этом список состоит из элементов вида $[p, m]$, где p — простое число, а m — его кратность.

Определение 1. Натуральное число, на которое делятся натуральные числа $a_1, \ldots, a_n$ нацело, называется их общим делителем. Наибольший из делителей называется наибольшим общим делителем (gcd, greatest common divisor).

Чтобы найти gcd, нужно найти общие множители в разложении числа $a_1, \ldots, a_n$ на простые множители. В Sage для отыскания gcd имеется функция `gcd`, аргументами которой могут быть или два числа, или список чисел:

```
sage: gcd(3,9)
3
sage: gcd([3,9,12])
3
```

Всякий идеал кольца $\mathbb{Z}$ является главным.

Теорема 3. Если идеал $(a_1, \ldots, a_n)$ совпадает с идеалом (q), то q — наибольший общий делитель чисел $a_1, \ldots, a_n$.

Доказательство. По условию теоремы

$$(a_1, \ldots, a_n) = (q)$$

Из $a_i \in (q)$ следует, что q — общий делитель чисел $a_1, \ldots, a_n$. Из $q \in (a_1, \ldots, a_n)$ следует, что найдутся такие числа $u_1, \ldots u_n \in \mathbb{Z}$, что

$$q = u_1 a_1 + \cdots + u_n a_n,$$

то есть этот общий делитель является линейной комбинацией заданных чисел. Допустим, что q не является наибольшим. Тогда имеется простое число p, что все числа $a_1, \ldots, a_n$ делятся на qp. Но тогда q делится на qp нацело, что невозможно. □

Как следствие имеем:

Теорема 4. Наибольший общий делитель чисел $a_1, \ldots, a_n$ является линейной комбинацией этих чисел.

Напр.,

```
sage: gcd([121,11])
11
sage: gcd(121,9)
1
sage: xgcd(121,9)
(1, -2, 27)
sage: 1==-2*121+27*9
True
```

2. Разложение на множители в кольце $k[x]$

Пусть k — произвольное поле. Поскольку $k[x]$ — кольцо главных идеалов, все сказанное про целые числа можно перенести на него.

Теорема 5. Всякий многочлен кольца $k[x]$ степени 1 и выше, можно представить как произведение простых многочленов.

Доказательство. Если число f — простой многочлен, это и есть искомое представление. Если он не является простым, то он представим в виде произведения двух многочленов меньшей степени. Если один из них или оба не являются простыми, их можно представить в виде произведения многочленов еще меньшей степени. Действуя так далее мы придем к простым

многочленам. Поэтому многочлен f можно представить в виде произведения простых многочленов. $\square$

Таким образом, всякий многочлен f положительной, степень можно представить как произведение простых многочленов:

$$f = p_1^{m_1} \dots p_r^{m_r},$$

где $p_1, \dots, p_r$ — простые многочлены, а $m_1, \dots, m_r$ — натуральные числа. При этом m_i называют кратностью (multiplicity), с которой множитель p_i входит в представление.

Поскольку мы работаем над полем k, p_1 можно умножить на $a \in k$, а, скажем, p_2 поделить на a, сохранив равенство. Чтобы избавится от этой неоднозначности, можно принять, что

$$\mathrm{lc}(p_i) = 1, \quad i = 1, \dots, r$$

и тогда

$$f = a p_1^{m_1} \dots p_r^{m_r},$$

где $a = \mathrm{lc}(f)$. Это представление единственно с точностью до порядка сомножителей, поскольку верна след. теорема.

Теорема 6. Пусть многочлен f раскладывается на простые сомножители:

$$f = p_1^{m_1} \dots p_r^{m_r},$$

где $p_1, \dots, p_r$ — простые многочлены, а $m_1, \dots, m_r$ — натуральные числа. Если простой многочлен q не совпадает с $p_1, \dots, p_r$, то f не делится на q.

Доказательство. Класс эквивалентности $[a]$ в факторкольце $k[x]/(q)$ равен нулю, а с другой стороны он равен

$$(p_1 + q_i k[x]) \dots (p_r + q_i k[x])$$

Поскольку $p_1, \dots, p_r$ не делятся на q, эти сомножители не являются нулями факторкольца. Но, поскольку факторкольцо — поле, их произведение не может равно нулю. $\square$

Задача 2. Дан многочлен из $k[x]$. Разложить его на простые множители.

Алгоритмы решения этой задачи существенно зависят от выбор поля k. Многие их них реализованы в Sage в виде функции `factor`:

```
sage: var("x")
x
sage: QQ[x](x^3-1).factor()
(x - 1) * (x^2 + x + 1)
sage: GF(2)[x](x^3-1).factor()
(x + 1) * (x^2 + x + 1)
sage: GF(3)[x](x^3-1).factor()
(x + 2)^3
sage: RR[x](x^3-1).factor()
(x - 1.00000000000000) * (x^2 + x +
  1.00000000000000)
sage: CC[x](x^3-1).factor()
(x - 1.00000000000000) * (x + 0.500000000000000 -
  0.866025403784439*I) * (x + 0.500000000000000 +
  0.866025403784439*I)
```

Иногда бывает полезным получить ответ в виде списка:

```
sage: list(QQ[x](x^3-1).factor())
[(x - 1, 1), (x^2 + x + 1, 1)]
```

При этом список состоит из элементов вида $[p, m]$, где p — простое число, которое входит в представление заданного числа в степени m, кратности (multiplicity) множителя p.

Определение 2. Многочлен из $k[x]$, на который делятся многочлены $f_1, \ldots, f_n$ этого кольца нацело, называется их общим делителем. Делитель наибольшей степени называется наибольшим общим делителем (gcd, greatest common divisor).

Чтобы найти gcd, нужно найти общие множители в разложении числа $a_1, \ldots, a_n$ на простые множители. В Sage для отыскания gcd имеется функция `gcd`, аргументами которой могут быть или два числа, или список чисел:

```
sage: gcd([QQ[x](x^2-1),QQ[x](x^2-2*x+1)])
x - 1
```

В полях Галуа ответ может быть неожиданным:

```
sage: gcd([GF(3)[x](x^2-1),GF(3)[x](x^2-2*x+1)])
x + 2
sage: GF(3)[x](x^2-1).factor()
(x + 1) * (x + 2)
sage: GF(3)[x](x^2-2*x+1).factor()
(x + 2)^2
```

Всякий идеал кольца $k[x]$ является главным.

Теорема 7. Если идеал $(f_1, \ldots, f_n)$ совпадает с идеалом (q), то q — наибольший общий делитель чисел $f_1, \ldots, f_n$.

Доказательство. По условию теоремы

$$(f_1, \ldots, f_n) = (q)$$

Из $f_i \in (q)$ следует, что q — общий делитель $f_1, \ldots, f_n$. Из $q \in (q) = (f_1, \ldots, f_n)$ следует, что найдутся такие многочлены $u_1, \ldots u_n$, что

$$q = u_1 f_1 + \cdots + u_n f_n,$$

то есть этот общий делитель является линейной комбинацией заданных чисел. Допустим, что q не является наибольшим. Тогда имеется такой простой многочлен p, что все многочлены $f_1, \ldots, f_n$ делятся на qp. Но тогда q делится на qp нацело, что невозможно. □

Как следствие имеем:

Теорема 8. Наибольший общий делитель многочленов $f_1, \ldots, f_n$ является линейной комбинацией этих многочленов.

Напр.,

```
sage: xgcd(QQ[x](x^2-1),QQ[x](x^2-2*x+1))
(x - 1, 1/2, -1/2)
```

Линейные многочлены, входящие в разложение многочлена f, указывают на корни многочлена, лежащие в k. Верно и обратное.

Теорема 9. Если многочлен f из $k[x]$ имеет корень a в этом кольце, то он делится нацело на $x - a$.

Доказательство. Поскольку $x - a$ имеет степень 1, остаток r от деления f на $x - a$ принадлежит k, то есть найдется такой многочлен u, что

$$f = u \cdot (x - a) + r.$$

Полагая сюда $x = a$, имеем $f(a) = r$. По условию $x = a$ — корень многочлена, значит, $r = f(a) = 0$ и $f = u \cdot (x - a)$. □

Определение 3. Кратностью корня $x = a$ многочлена f называют кратность, с которой множитель $x - a$ входит в разложение f на простые множители.

Теорема 10. Если многочлен f из $k[x]$ степени n имеет не более чем n корней в этом поле.

Доказательство. Допустим, что многочлен f имеет более, чем n корней, скажем, $x_1, \ldots, x_{n+1}$. Тогда f делится на $x - x_1$, то есть

$$f = f_1(x - x_1) = f_2(x - x_1)(x - x_2) = \cdots = a(x - x_1) \ldots (x - x_n).$$

Но тогда он не может делится на $x - x_{n+1}$. □

3. Разложение в кольце $\mathbb{C}[x]$

Теорема 11. Всякий многочлен кольца $\mathbb{C}[x]$ раскладывается на линейные множители.

Доказательство. Пусть $f \in \mathbb{C}[x]$. В силу основной теоремы алгебры этот многочлен имеет комплексный корень, скажем, x_1. В силу теоремы 9 этот многочлен делится на $x - x_1$, то есть найдется такой многочлен f_1, что

$$f = f_1 \cdot (x - x_1).$$

Степень многочлена f_1 меньше степени f. По тем же причинам f_1 делится на $x - x_2$ и т.д.:

$$f = f_1(x - x_1) = f_2(x - x_1)(x - x_2) = \cdots = a(x - x_1)\dots(x - x_n),$$

где a — многочлен нулевой степени, то есть элемент поля k. □

В силу теоремы 9 решение задачи 2 над $\mathbb{C}$ сводится к отысканию корней.

Примеры:

```
sage: CC[x](x^3-1).factor()
(x - 1.00000000000000) * (x + 0.500000000000000 -
  0.866025403784439*I) * (x + 0.500000000000000 +
  0.866025403784439*I)
sage: CC[x](x^3-1).roots()
[(1.00000000000000, 1), (-0.500000000000000 -
  0.866025403784439*I, 1), (-0.500000000000000 +
  0.866025403784439*I, 1)]
sage: CC[x](x^5+5*x^3-1).factor()
(x - 0.572554529005009) * (x - 0.0199681344229776 -
  2.23669210964067*I) * (x - 0.0199681344229776 +
  2.23669210964067*I) * (x + 0.306245398925482 -
  0.505274897227857*I) * (x + 0.306245398925482 +
  0.505274897227857*I)
```

```
sage: CC[x](x^5+5*x^3-1).roots()
[(0.572554529005009, 1), (-0.306245398925482 -
  0.505274897227857*I, 1), (-0.306245398925482 +
  0.505274897227857*I, 1), (0.0199681344229776 -
  2.23669210964067*I, 1), (0.0199681344229776 +
  2.23669210964067*I, 1)]
sage: CC[x](x^3+3*x^2+3*x+1).factor()
(x + 1.00000000000000)^3
sage: CC[x](x^3+3*x^2+3*x+1).roots()
[(-1.00000000000000, 3)]
```

Нетрудно заметить, что сумма кратностей линейных множителей, на которые раскладывается многочлен, равна степени этого многочлена. Часто говорят короче, что в поле многочлен n-й степени имеет n корней (с учетом их кратности). Пример:

```
sage: CC[x](x^8 + 4*x^7 + 7*x^6 + 12*x^5 + 15*x^4 +
  12*x^3 + 13*x^2 + 4*x + 4).roots()
[(-2.00000000000000, 2), (-1.00000000000000*I, 3),
  (1.00000000000000*I, 3)]
sage: 2+3+3
8
sage: CC[x](x^8 + 4*x^7 + 7*x^6 + 12*x^5 + 15*x^4 +
  12*x^3 + 13*x^2 + 4*x + 4).degree()
8
```

4. Разложение в кольце $\mathbb{R}[x]$

Всякий многочлен f из $\mathbb{R}[x]$ можно рассматривать как многочлен из $\mathbb{C}[x]$ и разложить на комплексные множители:

$$f = a(x - x_1)^{m_1} \dots (x - x_r)^{m_r}.$$

Здесь $a = \mathrm{lc}(f)$ — вещественное число, а среди корней могут быть и комплексные числа.

Обозначим как l — произведение линейных множителей с вещественными коэффициентами. Тогда f как элемент $\mathbb{C}[x]$ делится на l нацело. При делении f на l потребуется решить линейную систему с коэффициентами из $\mathbb{R}$, поэтому получится многочлен $g \in \mathbb{R}[x]$

Рассмотрим отображение $F : \mathbb{C} \to \mathbb{C}$, при котором число $a + ib$ переходит в $a - ib$ (его называют комплексно сопряженным с $a + ib$). При этом вещественные числа соответствуют сами себе, а арифметические действия сохраняются. Напр.,

$$F((a + ib) \cdot (a' + ib')) = aa' - bb' - i(ab' + a'b)$$

и

$$F(a + ib) \cdot F(a' + ib') = (a - ib)(a' - ib') = aa' - bb' - i(ab' + a'b).$$

Пусть

$$g = a_n x^n + \dots a_0, \quad a_i \in \mathbb{R}$$

имеет комплексный корень $x = a + ib$. Тогда

$$a_n(a + ib)^n + \cdots + a_0 = 0$$

Отсюда

$$F(a_n(a + ib)^n + \cdots + a_0) = F(0)$$

или в силу сохранения арифметических действий

$$a_n(a - ib)^n + \cdots + a_0 = 0,$$

то есть $a - ib$ тоже корень.

Следовательно, $x - (a + ib)$ присутствует в разложении g вместе с $x - (a - ib)$, поэтому g делится на

$$(x - a - ib)(x - a + ib) = (x - a)^2 + b^2 \in \mathbb{R}[x].$$

Применяя аналогичные размышления к частному от деления, видим, что f есть произведение линейных и квадратичных функций с вещественными коэффициентами.

Теорема 12 (Даламбера)**.** Многочлен f кольца $\mathbb{R}[x]$ разлагается на линейные и квадратичные множители.

При этом, в силу теоремы 9, квадратичные множители не должны иметь корней в $\mathbb{R}$, ведь иначе они не будут простыми.

Примеры:

```
sage: RR[x](x^3-1).factor()
(x - 1.00000000000000) * (x^2 + x +
  1.00000000000000)
sage: RR[x](x^3-1).roots()
[(1.00000000000000, 1)]
sage: RR[x](x^5+5*x^3-1).factor()
(x - 0.572554529005009) * (x^2 - 0.0399362688459553*
  x + 5.00319031972115) * (x^2 + 0.612490797850964*x
   + 0.349088966131650)
sage: RR[x](x^5+5*x^3-1).roots()
[(0.572554529005009, 1)]
sage: RR[x](x^3+3*x^2+3*x+1).factor()
(x + 1.00000000000000)^3
sage: RR[x](x^3+3*x^2+3*x+1).roots()
[(-1.00000000000000, 3)]
```

5. Разложение в кольце $\mathrm{GF}(p)[x]$

В полях Галуа имеется конечное число элементов, поэтому многочленов, степень которых меньше степени заданного многочлена, тоже конечное число. Это позволяет решить задачу о разложении на множители над по-

лями Галуа простым перебором.

Пример 1. Пусть дан многочлен $x^3 + 2$ над GF(3). Если он не простой, то он может быть произведением или трех линейных многочленов, или одного линейного и одного квадратичного. В любом случае он делится на линейный многочлен. В GF(3) всего 3 элемента: 0, 1 и 2. Поэтому имеется ровно 3 линейных многочлена с единичным старшим коэффициентом:

$$x, \quad x + 1, \quad x + 2$$

Делим на них исходный многочлен:

```
sage: GF(3)[x](x^3+2).quo_rem(GF(3)[x](x))
(x^2, 2)
sage: GF(3)[x](x^3+2).quo_rem(GF(3)[x](x+1))
(x^2 + 2*x + 1, 1)
sage: GF(3)[x](x^3+2).quo_rem(GF(3)[x](x+2))
(x^2 + x + 1, 0)
```

В последнем случае остаток равен нулю, то есть

$$x^3 + 2 = (x + 2)(x^2 + x + 1)$$

Квадратичный множитель или прост, или делится на линейный множитель. Проверим это:

```
sage: GF(3)[x](x^2 + x + 1).quo_rem(GF(3)[x](x))
(x + 1, 1)
sage: GF(3)[x](x^2 + x + 1).quo_rem(GF(3)[x](x+1))
(x, 1)
sage: GF(3)[x](x^2 + x + 1).quo_rem(GF(3)[x](x+2))
(x + 2, 0)
```

Получается, что

$$x^3 + 2 = (x + 2)(x^2 + x + 1) = (x + 2)^3.$$

Разумеется, Sage выдается это сразу:

```
sage: GF(3)[x](x^3+2).factor()
(x + 2)^3
```

Поля Галуа удобны тем, что разложение на множители в $\mathrm{GF}(p)[x]$ происходит очень быстро.

6. Разложение в кольце $\mathbb{Q}[x]$

Первый алгоритм решения задачи о разложении на множители над полем $\mathbb{Q}$ был предложен Кронекером в конце XIX века. Мы ограничимся здесь обсуждением теорем, лежащих в его основе, и решением несложных примеров.

Ключом к разложению на множители в кольце $\mathbb{Q}[x]$ является лемма Гаусса, которая сводит разложение к разложению в кольце $\mathbb{Z}[x]$.

Теорема 13 (лемма Гаусса)**.** Пусть $f, g \in \mathbb{Z}[x]$ и простое число p делит все коэффициенты произведения fg, то все коэффициенты f или g делятся на p.

Доказательство. Пусть

$$f = a_n x^n + \ldots, \quad g = b_m x^m + \ldots,$$

Допустим, что p не делит в совокупности ни коэффициенты f, ни g. Тогда существуют наименьшие i, j, для которых a_i и b_j не делятся на p. Коэффициент при x^{i+j} в произведении fg равен

$$\sum_{k<i} a_k b_{i+j-k} + a_i b_j + \sum_{l<j} a_{i+j-l} b_l$$

Обе суммы на p делятся, а $a_i b_j$ — нет. Поэтому коэффициент при x^{i+j} в произведении fg не делится на p, что невозможно. □

Теорема 14. Если многочлен $f \in \mathbb{Z}[x]$ разлагается на множители в $\mathbb{Q}[x]$, то он разлагается на множители и в кольце $\mathbb{Z}[x]$.

Доказательство. Пусть имеются такие $g, h \in \mathbb{Q}[x]$, что $f = gh$. Приводя коэффициенты g и h к общему знаменателю можем написать

$$af = g'h', \quad f', g' \in \mathbb{Z}[x],\ a \in \mathbb{Z}.$$

Но тогда в силу леммы Гаусса или коэффициенты g', или коэффициенты h' можно сократить на простые множители числа a. Поэтому $f \in \mathbb{Z}[x]$ разлагается на множители и в $\mathbb{Z}[x]$. □

Теорема 15. Если $f \in \mathbb{Z}[x]$ не разлагается на множители в кольце $\mathrm{GF}(p)[x]$ при некотором простом p, то он не разлагается на множители и в кольце $\mathbb{Q}[x]$.

Доказательство. Допустим, что $f \in \mathbb{Z}[x]$ разлагается на множители в $\mathbb{Q}[x]$, тогда он разлагается на простые множители и в $\mathbb{Z}[x]$:

$$f = gh, \quad f, g \in \mathbb{Z}[x].$$

Переход к факторкольцам согласован с арифметическими действиями, поэтому $f = gh$ сохраняет силу в $\mathrm{GF}(p)[x]$, что противоречит условию теоремы. □

Пример 2. Рассмотрим многочлен

```
sage: f=2*x^4 + 3*x^3 + 2*x^2 + 5*x + 3
```

Над первыми $\mathrm{GF}(p)$ он разлагается на множители:

```
sage: GF(3)[x](f).factor()
(2) * x * (x + 2) * (x^2 + x + 2)
sage: GF(5)[x](f).factor()
(2) * (x + 4) * (x^3 + x + 1)
sage: GF(7)[x](f).factor()
(2) * (x + 5) * (x^3 + x + 1)
sage: GF(11)[x](f).factor()
(2) * (x + 7) * (x + 9) * (x^2 + 2*x + 5)
```

Это не гарантирует, что многочлен можно разложить на множители и над $\mathbb{Q}$, но заставляет исследовать задачу дальше.

```
sage: RR[x](f).factor()
(2.00000000000000) * (x + 0.682327803828019) * (x +
  1.50000000000000) * (x^2 - 0.682327803828019*x +
  1.46557123187677)
```

Корень $x = -\frac{3}{2}$ виден невооруженным взглядом. Проверим эту догадку

```
sage: QQ[x](f).quo_rem(QQ[x](x+3/2))
(2*x^3 + 2*x + 2, 0)
```

Таким образом,

$$2x^4 + 3x^3 + 2x^2 + 5x + 3 = (2x^3 + 2x + 2)\left(x + \frac{3}{2}\right) = (x^3 + x + 1)(2x + 3)$$

Над GF(5) первый множитель далее не разлагается:

```
sage: GF(5)[x](x^3+x+1).factor()
x^3 + x + 1
```

Поэтому он не разлагается на множители и над $\mathbb{Q}$. Таким образом, искомое представление дается формулой

$$2x^4 + 3x^3 + 2x^2 + 5x + 3 = (x^3 + x + 1)(2x + 3)$$

Проверка:

```
sage: QQ[x](f).factor()
(2) * (x + 3/2) * (x^3 + x + 1)
```

Теорема 16 (критерий Эйзенштейна)**.** Если

$$a_n x^n + \ldots a_0 \in \mathbb{Z}[x]$$

и a_n не делится на p, $a_{n-1}, \ldots, a_0$ делятся на p, а a_0 не делится на p^2, то многочлен простой.

Доказательство. Пусть, вопреки утверждению теоремы,

$$a_n x^n + \dots a_0 = (b_m x^m + \dots + b_0)(c_r x^2 + \dots + c_0).$$

В условиях теоремы в $\mathrm{GF}(p)[x]$ имеем

$$[a_n] x^n = ([b_m] x^m + \dots + [b_0])([c_r] x^2 + \dots + [c_0]).$$

Поскольку разложение в $\mathrm{GF}(p)[x]$ однозначно, оба множителя сводятся к мономам. Но тогда b_0 и c_0 делятся на p, а $a_0 = b_0 c_0$ — на p^2, что противоречит условиям теоремы. □

Напр., многочлен $x^5 + 3x + 6$ — простой.

```
sage: QQ[x](x^5+3*x+6).is_prime()
True
```

7. Задания

Теоретические вопросы.

1) Докажите, что любое натуральное число можно представить в виде произведения простых чисел. Единственно ли это представление?

2) Докажите, что любой многочлен из кольца $k[x]$ можно представить в виде произведения простых многочленов. Единственно ли это представление?

3) На какие множители можно разложить многочлен из $\mathbb{C}[x]$?

4) На какие множители можно разложить многочлен из $\mathbb{R}[x]$?

5) Сформулируйте лемму Гаусса для $\mathbb{Z}[x]$. Какие она имеет следствия?

6) Сформулируйте критерий Эйзенштейна для многочленов из $\mathbb{Z}[x]$.

Практические вопросы.

1) Разложите на множители 245650. Укажите множитель, который имеет кратность 3.

2) Найдите наибольший общий делитель чисел $4335, 4913, 476$.

3) Задайте идеал $(4335, 4913, 476)$ в Sage и проверьте, что он является главным идеалом, порожденным наибольшим общим делителем, найденным выше.

4) Докажите, что числа 13 и 17 простые и подберите такие целые числа u и v, что $13u + 17v = 1$.

5) Разложите многочлен

$$x^6 + 8x^5 + 25x^4 + 40x^3 + 40x^2 + 32x + 16$$

на множители как многочлен из a.) $\mathbb{C}[x]$, b.) $\mathbb{R}[x]$, c.) $\mathbb{Q}[x]$, d.) $\mathrm{GF}(3)[x]$.

6) Найдите множитель кратности 3 у многочлена

$$x^6 - 5x^5 + 10x^4 - 12x^3 + 11x^2 - 7x + 2$$

кольца $\mathbb{Q}[x]$.

7) Найдите все рациональные корни уравнения

$$16x^6 - 32x^5 + 40x^4 - 40x^3 + 25x^2 - 8x + 1 = 0.$$

Укажите их кратность.

8) Разложите на множители $(x^2+4)^3(x^2-4)$ в кольцах $\mathbb{Q}[x]$, $\mathbb{R}[x]$ и $\mathbb{C}[x]$. В каких кольцах разложения совпадают?

9) Разложите на множители $(2x^3 + x - 1)^3(x - 1)(x + 2)^2$ в кольцах $\mathbb{Q}[x]$ и $\mathbb{Z}[x]$. Чем отличаются эти разложения?