Теория делимости

Пусть A - область целостности (коммутативное, ассоциативное кольцо с единицей без делителей нуля). И пусть $a, b \in A,\ a, b \neq 0$.

Опр: 1. Мы говорим, что a делится на b и соответственно b делит элемент a, если:

$$\exists\, c \in A\colon a = b{\cdot}c$$

Обозначение: $a \,\vdots\, b \Rightarrow a$ делится на b, $b \mid a \Rightarrow b$ делит a.

Опр: 2. Если $a \,\vdots\, b$ и $b \,\vdots\, a$, то говорят, что a и b - ассоциированные элементы.
Обозначение: $a \sim b$.

Утв. 1. (**Свойства отношения ассоциированности**):

1) $a \sim b \Leftrightarrow a = b{\cdot}u$, где $u \in A^{\times}$ (то есть обратимый элемент кольца A);

   □
   ($\Rightarrow$) По определению:
   $$a \sim b \Rightarrow a \,\vdots\, b \wedge b \,\vdots\, a \Rightarrow a = b{\cdot}u,\ b = a{\cdot}v = b{\cdot}u{\cdot}v$$
   Поскольку мы находимся в кольце без делителей нуля, то на ненулевой множитель b можно сократить и мы получим:
   $$1 = u{\cdot}v \Rightarrow u, v \in A^{\times}$$
   ($\Leftarrow$) Если верно $a = b{\cdot}u$, $u \in A^{\times}$, то домножив на обратный к u, получим:
   $$a{\cdot}u^{-1} = b{\cdot}u{\cdot}u^{-1} = b \Rightarrow a \,\vdots\, b \wedge b \,\vdots\, a \Rightarrow a \sim b$$
   ■

2) Ассоциированность является отношением эквивалентности на множестве A без нуля (рефлексивность, симметричность, транзитивность);

   □

   (1) $a \sim a$ - очевидно, поскольку $a = a{\cdot}1$;

   (2) $a \sim b \Rightarrow a = b{\cdot}u,\ u \in A^{\times} \Rightarrow b = a{\cdot}u^{-1},\ u^{-1} \in A^{\times} \Rightarrow b \sim a$;

   (3) $a \sim b \sim c \Rightarrow a = b{\cdot}u,\ b = c{\cdot}v,\ u, v \in A^{\times} \Rightarrow a = c{\cdot}v{\cdot}u,\ v{\cdot}u \in A^{\times} \Rightarrow a \sim c$;

   ■

3) Ассоциированность не влияет на делимость: пусть $a \sim a'$, $b \sim b'$ тогда: $a \,\vdots\, b \Leftrightarrow a' \,\vdots\, b'$;

   □ Заметим, что в силу того, что отношение ассоциированности симметрично, то достаточно доказать утверждение в одну сторону. По условию:
   $$a \sim a' \Rightarrow a = a'{\cdot}u,\ u \in A^{\times},\ b \sim b' \Rightarrow b = b'{\cdot}v,\ v \in A^{\times}$$
   Пусть известно, что $a \,\vdots\, b$, то есть $a = b{\cdot}c$, тогда:
   $$a = a'{\cdot}u = b{\cdot}c = b'{\cdot}v{\cdot}c \Rightarrow a' = b'{\cdot}(v{\cdot}c{\cdot}u^{-1}) \Rightarrow a' \,\vdots\, b'$$
   ■

Все вопросы теории делимости можно рассматривать с точностью до замены любых элементов на ассоциированные с ними. Далее, будем рассматривать все вопросы с точностью до ассоциированности.

Примеры ассоциированных элементов:

1) $A = \mathbb{Z}$, тогда $a \sim b \Leftrightarrow a = \pm b$, поскольку обратные элементы в кольце целых чисел это лишь ± 1;
2) $A = K[x]$, K - поле, тогда $f \sim g \Leftrightarrow f = \lambda \cdot g$, $\lambda \in K^{\times}$, поскольку обратимыми многочленами в кольце многочленов являются только ненулевые константы;

Опр: 3. Пусть $a, b \in A$, $a, b \neq 0$, тогда наибольшим общим делителем (НОД) элементов a и b называется такой их общий делитель $d \in A$, $d \neq 0$, который делится на все остальные общие делители:

1) $d \mid a$ и $d \mid b$;
2) $\forall c \in A \setminus \{0\}$, если $c \mid a$, $c \mid b \Rightarrow c \mid d$;

Обозначение: $d = \text{НОД}(a, b) = (a, b)$.

Опр: 4. Элементы a и b из A взаимно просты, если $(a, b) = 1$, то есть a и b не имеют общих делителей, кроме обратимых элементов.

Утв. 2. НОД(a, b) определён однозначно, с точностью до ассоциированности (если существует).

□ Пусть d и d' - два НОД элементов a и b, по свойству 1), оба эти элемента делят a и b, но тогда по свойству 2) НОД делится на все остальные общие делители $\Rightarrow d \,\vdots\, d'$ и $d' \,\vdots\, d \Rightarrow$ они ассоциированы:

$$(a, b) = d,\ (a, b) = d' \Rightarrow a \,\vdots\, d,\ b \,\vdots\, d,\ a \,\vdots\, d',\ b \,\vdots\, d' \Rightarrow d \,\vdots\, d',\ d' \,\vdots\, d \Rightarrow d \sim d'$$

■

Евклидовы кольца

Теперь хотелось бы вернуться к вопросам существования и найти для каких колец, любые два элемента обладают НОД. Укажем один класс колец, который удовлетворяет этому свойству.

Опр: 5. Целостное кольцо A называется евклидовым, если задана функция:

$$N \colon A \setminus \{0\} \to \mathbb{Z}_{+} = \{0, 1, 2, \dots\}$$

называемая евклидовой нормой, со свойствами:

1) **Монотонность**: $N(a \cdot b) \geq N(a)$, причем равенство верно только в том случае, если $b \in A^{\times}$;
2) **Деление с остатком**:

$$\forall a, b \in A,\ b \neq 0,\ \exists\, q, r \in A \colon a = b \cdot q + r,\ N(r) < N(b) \wedge r = 0$$

Rm: 1. Условие 1) в силу коммутативности целостного кольца справедливо и для b:

$$N(a \cdot b) = N(b \cdot a) \geq N(b)$$

Более того, равенство возможно при $b \in A^{\times}$, поскольку:

$$N((a \cdot b) \cdot b^{-1}) = N(a \cdot b \cdot b^{-1}) = N(a \cdot 1) = N(a) \geq N(a \cdot b)$$

Rm: 2. На самом деле в условии 2) можно опустить условие про $r = 0$, если договориться считать, что норма нуля равна минус бесконечности: $N(0) = -\infty$.

Лемма 1. $N(ab) = N(a) \Leftrightarrow b \in A^\times$.

□
($\Leftarrow$) Уже показали выше: $b \in A^\times \Rightarrow N((ab)b^{-1}) = N(a) \geq N(ab) \geq N(a)$.

($\Rightarrow$) Предположим, что $b \notin A^\times$ и что $a \not\vdots\, ab$. Если $a = abc \Rightarrow a(bc - 1) = 0$. По определения нормы:

$$a, b \neq 0 \Rightarrow bc - 1 = 0 \Rightarrow bc = 1 \Rightarrow b \in A^\times$$

Тогда a можно разделить на ab:

$$\exists\, q, r \in A\colon a = ab{\cdot}q + r,\ r \neq 0,\ N(r) < N(ab) \Rightarrow r = a - ab{\cdot}q = a(1 - b{\cdot}q) \Rightarrow$$

$$\Rightarrow N(r) = N(a{\cdot}(1 - bq)) \geq N(a) \wedge N(r) < N(ab) \Rightarrow N(a) < N(ab)$$

Получаем противоречие с первым свойством нормы. ■

Примеры евклидовых колец:

1) $A = \mathbb{Z}$, $N(a) = |a|$;
2) $A = K[x]$, K - поле, $N(f) = \deg(f)$;

Упр. 1. Кольцо гауссовых чисел $K[i] = \{z = x + iy \in \mathbb{C} \mid x, y \in \mathbb{Z}\}$ - решетка точек с целыми координатами в $\mathbb{C}$. Доказать, что это евклидово кольцо, с нормой $N(z) = |z|^2 = x^2 + y^2$.

Утв. 3. В евклидовом кольце $\forall a, b \neq 0$, $\exists\,(a, b)$.

□ Основано на алгоритме Евклида:

(1) $a = b{\cdot}q_1 + r_1$ - делим элемент a с остатком на элемент b.
Если $r_1 = 0$, то алгоритм Евклида заканчивается и мы останавливаемся.
Если $r_1 \neq 0$, то делаем второй шаг;

(2) $b = r_1{\cdot}q_2 + r_2$ - делим элемент b с остатком на элемент r_1.
Если $r_2 = 0$, то алгоритм Евклида заканчивается и мы останавливаемся.
Если $r_2 \neq 0$, то делаем третий шаг;

(3) $r_1 = r_2{\cdot}q_3 + r_3$ - делим элемент r_1 с остатком на элемент r_2.
И так далее;

⋮

k) $r_{k-1} = r_k{\cdot}q_{k+1} + r_{k+1}$;

⋮

s) $r_{s-2} = r_{s-1}{\cdot}q_s + r_s$, $r_s \neq 0$;

s+1) $r_{s-1} = r_s{\cdot}q_{s+1}$;

Основной вопрос - почему процесс остановится? Заметим, что норма каждого следующего остатка меньше нормы предыдущего, по свойству евклидовой нормы:

$$N(b) > N(r_1) > N(r_2) > \ldots > N(r_k) > N(r_{k+1}) > \ldots$$

Норма это целое неотрицательное число, она не может уменьшаться бесконечно $\Rightarrow$ рано или поздно, процесс оборвётся. Пусть мы остановились на шаге $s+1$, тогда $r_{s+1} = 0$ и алгоритм останавливается.

Докажем,что $r_s = (a, b)$:

1) Из последнего шага видно, что $r_s \mid r_{s-1}$. Поднимаясь по строчкам выше, мы видим:

$$r_s \mid r_s, r_{s-1} \Rightarrow r_s \mid r_{s-2} = r_{s-1}{\cdot}q_s + r_s \Rightarrow r_s \mid r_{s-2}, r_{s-1} \Rightarrow r_s \mid r_{s-3} = r_{s-2}{\cdot}q_{s-1} + r_{s-1} \Rightarrow \ldots \Rightarrow$$

$$\Rightarrow r_s \mid r_{k+1}, r_k \Rightarrow r_s \mid r_{k-1} \Rightarrow \ldots \Rightarrow r_s \mid r_2, r_1 \Rightarrow r_s \mid b \Rightarrow r_s \mid b, r_1 \Rightarrow r_s \mid a$$

2) Покажем, что r_s делится на любой другой общий делитель. Пусть $c \mid a, b$, тогда:

$$c \mid r_1 = a - b{\cdot}q_1 \Rightarrow c \mid b, r_1 \Rightarrow c \mid r_2 = b - r_1{\cdot}q_2 \Rightarrow \ldots \Rightarrow$$

$$\Rightarrow c \mid r_{k-1}, r_k \Rightarrow c \mid r_{k+1} = r_{k-1} - r_k{\cdot}q_{k+1} \Rightarrow \ldots \Rightarrow c \mid r_s = r_{s-2} - r_{s-1}{\cdot}q_s$$

Таким образом, $r_s = (a, b)$. ■

Следствие 1. (**Из алгоритма Евклида**) $\exists\, u, v \in A\colon (a, b) = u{\cdot}a + v{\cdot}b$.

□ Докажем, что $\forall k \geq 0$, $r_k = u_k{\cdot}a + v_k{\cdot}b$, в частности верно и для $r_s = (a, b)$. Индукцией по k:

<u>База индукции</u>: $k = 0 \Rightarrow r_0 = b = 0{\cdot}a + 1{\cdot}b$, $k = 1 \Rightarrow r_1 = a - q_1{\cdot}b = 1{\cdot}a - q_1{\cdot}b$.

<u>Шаг индукции</u>: Пусть все остатки $r_1, \ldots, r_k$ уже представили в требуемом виде, рассмотрим r_{k+1}:

$$r_{k+1} = r_{k-1} - r_k{\cdot}q_{k+1} = u_{k-1}{\cdot}a + v_{k-1}{\cdot}b - (u_k{\cdot}a + v_k{\cdot}b){\cdot}q_{k+1} =$$

$$= (u_{k-1} - u_k{\cdot}q_{k+1}){\cdot}a + (v_{k-1} - v_k{\cdot}q_{k+1}){\cdot}b = u_{k+1}{\cdot}a + v_{k+1}{\cdot}b$$

При $k = s$, получаем $(a, b) = u_s{\cdot}a + v_s{\cdot}b$. ■

Простые и неприводимые элементы

Основная задача теории делимости это выяснение, когда один элемент кольца делится на другой, другими словами, как элементы нашего кольца раскладываются на множители.

<u>**Тривиальное разложение на множители**</u>: $\forall a \in A$, $a = (a{\cdot}u){\cdot}u^{-1}$, $u \in A^\times$. Такие разложения всегда существуют, их очень много и они не интересны с точки зрения теории делимости.

Вопрос заключается в том, можно ли как-то разложить элемент нетривиальным способом (в произведение двух необратимых множителей)?

Опр: 6. Элемент $p \in A$ называется простым, если $p \neq 0$, $p \notin A^\times$ и $\nexists$ разложения $p = a{\cdot}b$, где $a, b \notin A^\times$.

Примеры простых элементов:

1) $A = \mathbb{Z} \Rightarrow$ простые элементы в $\mathbb{Z}$ это $\pm p$, где p - натуральное простое число;

2) $A = K[x]$, где K - поле, простые элементы - это многочлены $p \neq 0$, $\deg(p) > 0$, для которых не существует разложения $p = f{\cdot}g$, где $0 < \deg(f), \deg(g) < \deg(p)$, то есть многочлен p не должен разлагаться в произведение многочленов меньшей степени;

Опр: 7. Многочлен называется неприводимым, если он не разлагается в произведение многочленов меньшей степени, то есть это простой элемент кольца многочленов.

Rm: 3. Простой элемент $p \in A$ имеет ровно 2 делителя, с точностью до ассоциированности: p и 1. Это так, поскольку если мы разложили простой элемент p на два множителя $p = a{\cdot}b$, то один из множителей должен быть обратимым. Пусть $b \in A^\times \Rightarrow b \sim 1$, $p \sim a$ и делитель a это тоже самое, с точностью до ассоциированности, что и делитель p. При этом, $p \not\sim 1$, так как $p \notin A^\times$.

Лемма 2. Пусть A - евклидово кольцо и $p \in A$ - простой элемент, тогда: $a{\cdot}b \,\vdots\, p \Rightarrow a \,\vdots\, p \vee b \,\vdots\, p$.

$\square$ Рассмотрим (a, p). По определению:

$$(a,p) \mid p \Rightarrow (a,p) = p \vee (a,p) = 1$$

Если $a \,\vdots\, p$, то мы доказали требуемое. Если $(a, p) = 1$, то:

$$(a,p) = u{\cdot}a + v{\cdot}p \Rightarrow b = u{\cdot}ab + v{\cdot}pb,\ ab \,\vdots\, p \wedge pb \,\vdots\, p \Rightarrow b \,\vdots\, p$$

$\blacksquare$

Следствие 2. Если $a_1{\cdot}\ldots{\cdot}a_k \,\vdots\, p$, то $\exists\, i\colon a_i \,\vdots\, p$.

$\square$ Индукцией по k:

База индукции: $k = 2 \Rightarrow$ лемма.

Шаг индукции: Если $a_1{\cdot}\ldots{\cdot}a_{k-1}{\cdot}a_k = (a_1{\cdot}\ldots{\cdot}a_{k-1}){\cdot}a_k \,\vdots\, p$, то по лемме $a_k \,\vdots\, p \vee a_1{\cdot}\ldots{\cdot}a_{k-1} \,\vdots\, p$. В первом случае a_k делится на p, во втором случае по предположению индукции $\exists\, i < k\colon a_i \,\vdots\, p$. $\blacksquare$

Основная теорема арифметики в евклидовых кольцах

Теорема 1. (**Основная теорема арифметики в евклидовых кольцах**) В евклидовом кольце A, $\forall a \neq 0$, $a \notin A^\times$, $\exists$ разложение:

$$a = p_1{\cdot}\ldots{\cdot}p_m$$

где p_i - простые элементы. Причём разложение единственное, с точностью до перестановки множителей и их замены на ассоциированные.

$\square$

Существование: Индукцией по $N(a)$:

База индукции: $N(a) = n_0$ - наименьшее значение нормы необратимых элементов в кольце A. Следовательно, элемент a - прост, иначе $a = b{\cdot}c$, $b, c \in A^\times$ и тогда $N(a) = N(bc) > N(b), N(c)$ - по монотонности евклидовой нормы и мы получаем противоречие с тем, что $N(a) = n_0$. Следовательно, a разлагается в разложение из самого себя.

Шаг индукции: Возьмем произвольный элемент a с любой нормой. Либо элемент a прост и тогда существование доказано, либо он не прост и тогда $a = b{\cdot}c$, $b, c \in A^\times$, где $N(b), N(c) < N(a)$. Тогда по предположению индукции b и c можно разложить в произведение простых элементов:

$$b = p_1{\cdot}\ldots{\cdot}p_k,\ c = p_{k+1}{\cdot}\ldots{\cdot}p_m$$

где $p_1, p_2, \dots, p_m$ - это простые элементы. Перемножая их, мы получаем разложение для элемента a:

$$a = p_1 \cdot \ldots \cdot p_m$$

Единственность: Пусть у нас есть два разложения $a \in A$ на простые элементы:

$$a = p_1 \cdot \ldots \cdot p_m = q_1 \cdot \ldots \cdot q_n$$

Без ограничения общности, будем считать, что $m \leq n$. Докажем, что на самом деле $m = n$ и после перенумерации множителей, $p_i \sim q_i$, $\forall i$. Будем вести индукцию по числу множителей m в разложении:

База индукции: $m = 1 \Rightarrow a = p_1$ - простое $\Rightarrow n = 1$, $a = q_1 \Rightarrow p_1 = q_1$.

Шаг индукции: Рассмотрим последний множитель в разложении: $p_m \mid a = q_1 \cdot \ldots \cdot q_n \Rightarrow \exists\, i \colon p_m \mid q_i$. После перенумерации, для удобства можно считать, что $p_m \mid q_n$. Поскольку это простые множители, тогда $p_m \sim q_n$, так как p_m - необратимый элемент $\Rightarrow p_m \sim q_n \Rightarrow q_n = p_m \cdot u$, $u \in A^\times$. Подставим:

$$a = p_1 \cdot \ldots \cdot p_{m-1} \cdot p_m = q_1 \cdot \ldots \cdot q_{n-1} \cdot u \cdot p_m \Rightarrow p_1 \cdot \ldots \cdot p_{m-1} = q_1 \cdot \ldots \cdot q_{n-2} \cdot (q_{n-1} \cdot u)$$

где мы можем поделить на p_m, поскольку находимся в целостном кольце. Итого, мы снова получили два разложения на простые множители, но по предположению индукции $n-1 = m-1 \Rightarrow n = m$ и после перенумерации будет верно:

$$p_1 \sim q_1,\ \ldots,\ p_{m-2} \sim q_{n-2},\ p_{m-1} \sim q_{n-1} \cdot u \sim q_{n-1}$$

Таким образом, единственность доказана. ■

Следствие 3. (**Основная теорема арифметики целых чисел**) $\forall n \in \mathbb{N}$, $n > 1$, $\exists!$ разложение:

$$n = p_1 \cdot \ldots \cdot p_m$$

где p_i - простые числа. Причём разложение единственное с точностью до перестановки множителей.

Rm: 4. Поскольку простые элементы кольца целых чисел это с точностью до знака - простые натуральные числа, а n - само натуральное, то все знаки можно убрать и ассоциированности не возникает, так как все множители положительны.

Следствие 4. $\forall f \in K[x]$, K - поле, $\deg(f) > 0$, $\exists$ разложение:

$$f = p_1 \cdot \ldots \cdot p_m$$

где p_i - неприводимые многочлены. Причём разложение единственное с точностью до перестановки множителей и умножению их на ненулевые константы.

Факториальные кольца

Опр: 8. Целостное кольцо A называется факториальным, если $\forall a \in A$, $a \neq 0$, $a \notin A^\times$ можно разложить в произведение простых множителей единственным образом, с точностью до перестановки множителей и их замены на ассоциированные элементы.

Rm: 5. Коротко можно сказать, что целостное кольцо факториально, если в нём выполняется теорема о разложении. То есть теорема по существу говорит, что евклидовы кольца - факториальны.

Следствие 5. Евклидовы кольца - факториальны.

Rm: 6. Но не все факториальные кольца - евклидовы.

Rm: 7. В частности кольцо $K[x]$ над полем K и кольцо $\mathbb{Z}$ - это факториальные кольца.

В факториальном кольце A все вопросы теории делимости сводятся к разложению на простые множители. Например, хотим выяснить, когда один элемент делится на другой.

Пусть $a, b \in A$, $a, b \neq 0$, $a, b \notin A^\times$. Разложим каждое на простые так, чтобы ассоциированные множители были сгруппированы, вынеся обратимые множители перед произведением:

$$a = u \cdot p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_s^{k_s},\ u \in A^\times,\ \forall i = \overline{1, s},\ k_i \geq 0$$

где p_i - простые и попарно не ассоциированные. Аналогично для b:

$$b = v \cdot p_1^{l_1} \cdot p_2^{l_2} \cdot \ldots \cdot p_s^{l_s},\ v \in A^\times,\ \forall i = \overline{1, s},\ l_i \geq 0$$

Причём можно считать, что $p_1, \ldots, p_s$ - одинаковые у a и b.

Утв. 4. В условиях выше, верно:

$$a \vdots b \Leftrightarrow \forall i = \overline{1, s},\ k_i \geq l_i$$

$\square$

($\Leftarrow$) Если $\forall i = \overline{1, s}$, $k_i \geq l_i$, то $a = b \cdot u \cdot v^{-1} \cdot p_1^{k_1 - l_1} \cdot \ldots \cdot p_s^{k_s - l_s} \Rightarrow a \vdots b$.

($\Rightarrow$) Если $a \vdots b$, то $a = b \cdot c = v \cdot p_1^{l_1} \cdot p_2^{l_2} \cdot \ldots \cdot p_s^{l_s} \cdot c = v \cdot p_1^{l_1} \cdot p_2^{l_2} \cdot \ldots \cdot p_s^{l_s} \cdot q_1 \cdot \ldots \cdot q_t$, где q_j - простые множители. Но в силу разложения a и единственности разложения с точностью до перестановки множителей и ассоциированности мы имеем:

$$u \cdot p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_s^{k_s} = v \cdot p_1^{l_1} \cdot p_2^{l_2} \cdot \ldots \cdot p_s^{l_s} \cdot q_1 \cdot \ldots \cdot q_t \Rightarrow \forall j = \overline{1, t},\ \exists\, i \in \overline{1, s} \colon q_j \sim p_i \Rightarrow$$

$$\Rightarrow q_1 \cdot \ldots \cdot q_t = w \cdot p_1^{m_1} \cdot \ldots \cdot p_s^{m_s},\ w \in A^\times \Rightarrow \forall i = \overline{1, s},\ k_i = l_i + m_i \Rightarrow k_i \geq l_i$$

$\blacksquare$

Опр: 9. Пусть $a, b \in A$, $a, b \neq 0$, тогда наименьшим общим кратным (НОК) элементов a и b называется такой наименьший элемент $m \in A$, $d \neq 0$, который делится на a и b без остатка:

1) $a \mid m$ и $b \mid m$;
2) $\forall c \in A \setminus \{0\}$, если $a \mid c$, $b \mid c \Rightarrow m \mid c$;

Обозначение: $m = \text{НОК}(a, b) = [a, b]$.

Таким образом, вопрос делимости одного элемента на другой сводится к сравнению показателя степеней. Например, наибольший общий делитель - НОД(a, b):

$$(a, b) = p_1^{\min(k_1, l_1)} \cdot \ldots \cdot p_s^{\min(k_s, l_s)}$$

и наименьшее общее кратное - НОК$[a, b]$:

$$[a, b] = p_1^{\max(k_1, l_1)} \cdot \ldots \cdot p_s^{\max(k_s, l_s)}$$