Кольца вычетов

Опр: 1. Сравнимость целых чисел по модулю $m \in \mathbb{N}$: $k \equiv l \pmod{m}$, если $k - l \,\vdots\, m$ (то есть разность чисел $k - l$ делится на m). Эквивалентным образом: k и l имеют одинаковые остатки при делении на m.

Опр: 2. Класс вычетов числа $k \in \mathbb{Z}$ по модулю m (вычет числа k по модулю m) это множество:

$$k \mod m = \{l \in \mathbb{Z} \colon l \equiv k \pmod{m}\} = \{l = k + m{\cdot}n \colon n \in \mathbb{Z}\} = k + m{\cdot}\mathbb{Z}$$

где $m{\cdot}\mathbb{Z}$ - это множество всех целых чисел кратных m.

Обозначение: $k \mod m = \overline{k}$.

Основные свойства классов вычетов

1) В одном классе вычетов все числа сравнимы между собой по модулю m, поскольку имеют один и тот же остаток при делении на m;
2) Числа из разных классов вычетов несравнимы по модулю m, поскольку имеют разные остатки при делении на m;
3) Разные классы вычетов между собой не пересекаются;
4) Любое целое число попадает в какой-то класс вычетов, то есть все классы вычетов по модулю m образуют разбиение $\mathbb{Z}$ на попарно непересекающиеся подмножества;

Множество классов вычетов по модулю m обозначается как $\mathbb{Z}_m = \left\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\right\}$. Графически это множество можно представить так:

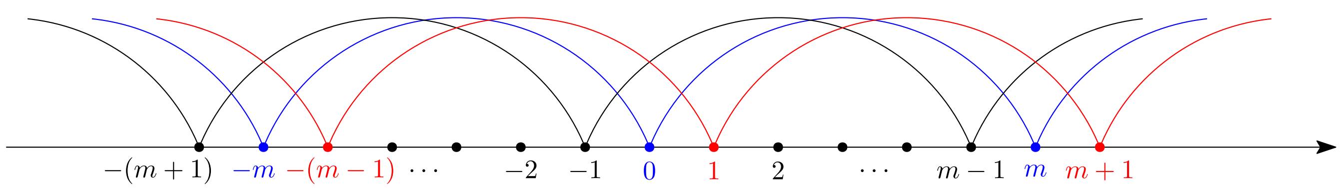

Рис. 1: Геометрическое изображение классов вычетов.

Или же “свернуть” в окружность длины m, то тогда все элементы из одного и того же класса вычетов попадут в одну и ту же точку на окружности:

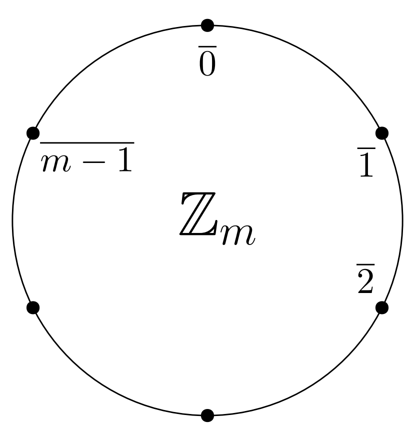

Рис. 2: Геометрическое изображение классов вычетов в виде окружности.

Таким образом, прямая превратилась в окружность. Точка $\overline{0}$ - класс вычетов нуля и так далее до класса $\overline{m-1}$, а дальше снова вернемся в класс вычетов $\overline{0}$. Таким образом, разумнее изображать точками на окружности, плюс отсюда становится ближе терминология кольца вычетов.

Опр: 3. Определим операции над вычетами следующим образом:

1) **Сумма вычетов**: $\overline{k}+\overline{l}=\overline{k+l}$;
2) **Произведение вычетов**: $\overline{k}\cdot\overline{l}=\overline{k\cdot l}$;

Утв. 1. (**Корректность определения**) Операции над вычетами определены однозначно (то есть не зависят от выбора представителей классов вычетов).

□ Пусть $k'\equiv k$, $l'\equiv l \Rightarrow k'=k+m\cdot r$, $l'=l+m\cdot s$, тогда:

1) $k'+l'=k+l+m\cdot(r+s)\equiv k+l$;
2) $k'\cdot l'=k\cdot l+m\cdot r\cdot l+k\cdot m\cdot s+m^2\cdot r\cdot s=k\cdot l+m\cdot(r\cdot l+k\cdot s+m\cdot r\cdot s)\equiv k\cdot l$;

■

Пример: Рассмотрим $\mathbb{Z}_5=\left\{\overline{0},\overline{1},\overline{2},\overline{3},\overline{4}\right\}$: $\overline{3}+\overline{4}=\overline{7}=\overline{2}$, $\overline{3}\cdot\overline{2}=\overline{6}=\overline{1}$.

Свойства операций в $\mathbb{Z}_m$ определяются свойствами операций в $\mathbb{Z}$. В частности из этих свойств вытекает, что $\mathbb{Z}_n$ - коммутативное, ассоциативное кольцо с единицей (кольцо вычетов по модулю m).

Отметим, что в кольце целых чисел нет делителей нуля, тогда как в кольце вычетов они могут быть.

Пример: Рассмотрим $\mathbb{Z}_6$: $\overline{3}\cdot\overline{2}=\overline{0}$, то есть в кольце вычетов могут быть делители нуля.

Утв. 2. Для делителей нуля кольца вычетов $\mathbb{Z}_m$ будет верно следующее:

1) $\overline{k}\in\mathbb{Z}_m$ - делитель нуля $\Leftrightarrow k \not\vdots\, m$ и k,m - имеют общие делители больше 1;
2) $\overline{k}\in\mathbb{Z}_m^\times \Leftrightarrow k,m$ - взаимно просты, то есть не имеют общих делителей больших 1;

Rm: 1. Из утверждения видно, что любой элемент кольца вычетов это либо ноль, либо делитель нуля, либо обратимый элемент.

□

1) ($\Rightarrow$) $\overline{k}$ - делитель нуля $\Leftrightarrow \overline{k}\neq\overline{0}\wedge\exists\,\overline{l}\neq 0\colon \overline{k}\cdot\overline{l}=\overline{0}$. Переформулируем эти свойства:

$$\overline{k}\neq\overline{0}\Leftrightarrow k\not\vdots\, m$$

$$\exists\,\overline{l}\neq 0\colon \overline{k}\cdot\overline{l}=\overline{0}\Leftrightarrow \exists\, l\not\vdots\, m\colon k\cdot l\,\vdots\, m\Rightarrow (k,m)>1$$

то есть k и m имеют общие делители больше 1. Если бы k не имело общих делителей с m, а произведение делилось бы на m, то $l\,\vdots\, m$, что не так по условию.

($\Leftarrow$) Пусть верно:

$$k\not\vdots\, m,\ k=k'\cdot d,\ m=m'\cdot d,\ m>d=(k,m)>1$$

Возьмем $l=m'<m$, тогда $k\cdot l=k'\cdot d\cdot m'=k'\cdot m\Rightarrow k\cdot l\,\vdots\, m\Rightarrow\overline{k}$ - делитель нуля;

2) ($\Rightarrow$) $\overline{k} \in \mathbb{Z}_m^\times \Rightarrow \overline{k} \neq \overline{0} \wedge \overline{k}$ - неделитель нуля (т.к. они необратимы) $\Leftrightarrow k \not\vdots\, m \wedge (k, m) = 1$, то есть числа k и m не имеют общих делителей больше 1 $\Leftrightarrow$ k и m - взаимно просты.

   ($\Leftarrow$) Пусть верно: $\overline{k} \neq \overline{0}$ и $\overline{k}$ - неделитель нуля. Рассмотрим множество произведений:
$$\left\{\overline{k}\cdot\overline{0}, \overline{k}\cdot\overline{1}, \overline{k}\cdot\overline{2}, \ldots, \overline{k}\cdot\overline{m-1}\right\}$$
   таких произведений будет m штук. Более того, $\overline{k}\cdot\overline{i} = \overline{k}\cdot\overline{j} \Rightarrow \overline{i} = \overline{j}$, поскольку на неделители нуля можно сокращать. Следовательно, все такие произведения будут различными и верно равенство:
$$\left\{\overline{k}\cdot\overline{0}, \overline{k}\cdot\overline{1}, \overline{k}\cdot\overline{2}, \ldots, \overline{k}\cdot\overline{m-1}\right\} = \left\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\right\}$$
   В частности, $\exists\, \overline{l} \in \mathbb{Z}_m \colon \overline{k}\cdot\overline{l} = \overline{1} \Rightarrow \overline{k}$ - обратим;

■

Следствие 1. $\mathbb{Z}_m$ - поле $\Leftrightarrow$ m - простое число.

□ $\mathbb{Z}_m$ - поле $\Leftrightarrow \mathbb{Z}_m^\times = \mathbb{Z}_m \setminus \{\overline{0}\} \Leftrightarrow \forall k = 1, 2, \ldots, m-1$ - взаимно просты с m, то есть $(m, k) = 1$. Это как раз и означает, что m - простое число. ■

Пример: $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ является полем.

Утв. 3. В $\mathbb{Z}_m$ верно свойство: $\underbrace{\overline{1} + \overline{1} + \ldots + \overline{1}}_{m} = \overline{0}$.

□ Очевидно: $\underbrace{\overline{1} + \overline{1} + \ldots + \overline{1}}_{m} = \overline{m} = \overline{0}$. ■

Это необычное для полей свойство, например в $\mathbb{R}$ сложение единиц бесконечно растёт.

Опр: 4. Пусть K - произвольное поле, назовем его характеристикой $\operatorname{char} K$ наименьшее число $p \in \mathbb{N}$ такое, что: $\underbrace{1 + 1 + \ldots + 1}_{p} = 0$ в K. Если такого p не существует, то $\operatorname{char} K = 0$.

Примеры характеристик полей:

1) $\operatorname{char} \mathbb{Q} = 0$, $\operatorname{char} \mathbb{R} = 0$, $\operatorname{char} \mathbb{Z} = 0$;
2) Пусть p - простое, тогда $\operatorname{char} \mathbb{Z}_p = p$;

Утв. 4. Характеристика любого поля это либо 0, либо простое число.

□ Пусть $\operatorname{char} K = p > 0$ и предположим, что $p = k\cdot l$, где $1 < k, l < p$. Рассмотрим следующие суммы:
$$\underbrace{1 + 1 + \ldots + 1}_{k} \neq 0, \underbrace{1 + 1 + \ldots + 1}_{l} \neq 0$$
Но если мы их переменожим, то получим:
$$(\underbrace{1 + 1 + \ldots + 1}_{k})\cdot(\underbrace{1 + 1 + \ldots + 1}_{l}) = \underbrace{1\cdot 1 + 1\cdot 1 + \ldots + 1\cdot 1}_{k\cdot l} = \underbrace{1 + 1 + \ldots + 1}_{p} = 0$$
Таким образом, два ненулевых элемента дали 0 $\Rightarrow$ в поле K есть делители нуля $\Rightarrow$ противоречие с тем, что в поле нет делителей нуля, так как все ненулевые элементы обратимы. ■

Утв. 5. Пусть $\operatorname{char} K = p > 0$, тогда верно следующее:

$$\forall x, y \in K\colon (x+y)^p = x^p + y^p$$

$\square$ Раскроем скобки по формуле бинома Ньютона:

$$(x+y)^p = x^p + C_p^1 x^{p-1} y^1 + \ldots + C_p^k x^{p-k} y^k + \ldots + y^p$$

Рассмотрим k-ое слагаемое в такой сумме:

$$C_p^k x^{p-k} y^k = (\underbrace{1+1+\ldots+1}_{C_p^k}) \cdot x^{p-k} \cdot y^k$$

Поскольку p - простое, при $k \neq p$ или $k \neq 0$, будет верно:

$$C_p^k = \frac{p!}{k!(p-k)!} \Rightarrow p! \,\vdots\, p,\ k!(p-k)! \not\vdots\, p \Rightarrow C_p^k \,\vdots\, p,\ 0<k<p \Rightarrow$$

$$\Rightarrow (\underbrace{1+1+\ldots+1}_{C_p^k}) = (\underbrace{1+1+\ldots+1}_{p}) + \ldots + (\underbrace{1+1+\ldots+1}_{p}) = 0 + \ldots + 0 = 0,\ 0<k<p \Rightarrow$$

$$\Rightarrow C_p^k x^{p-k} y^k = (\underbrace{1+1+\ldots+1}_{C_p^k}) \cdot x^{p-k} \cdot y^k = 0 \cdot x^{p-k} \cdot y^k = 0,\ 0<k<p \Rightarrow$$

$$\Rightarrow (x+y)^p = x^p + C_p^1 x^{p-1} y^1 + \ldots + C_p^k x^{p-k} y^k + \ldots + y^p = x^p + 0 + \ldots + 0 + \ldots + 0 + y^p = x^p + y^p$$

$\blacksquare$

Следствие 2. Если $\operatorname{char} K = p > 0$, то тогда будет верно:

$$\forall x_1, \ldots, x_n,\ (x_1 + \ldots + x_n)^p = x_1^p + \ldots + x_n^p$$

$\square$ Доказательство идёт индукцией по числу слагаемых. Для $n = 2$ мы уже доказали, пусть верно для $n-1$, тогда:

$$(x_1 + \ldots + x_{n-1} + x_n)^p = ((x_1 + \ldots + x_{n-1}) + x_n)^p = (x_1 + \ldots + x_{n-1})^p + x_n^p = x_1^p + \ldots + x_{n-1}^p + x_n^p$$

$\blacksquare$

Теорема 1. (**Малая теорема Ферма**) Пусть p - простое число, тогда $\forall n \in \mathbb{Z}$, $n^p \equiv n \pmod p$.

$\square$ На языке вычетов по модулю p надо доказать следующее:

$$\forall n \in \mathbb{Z}_p,\ \overline{n}^p = \overline{n}$$

По предыдущему следствию будет верно:

$$\overline{n} = \underbrace{\overline{1} + \ldots + \overline{1}}_{n} \Rightarrow \overline{n}^p = \underbrace{\overline{1}^p + \ldots + \overline{1}^p}_{n} = \underbrace{\overline{1} + \ldots + \overline{1}}_{n} = \overline{n}$$

$\blacksquare$

Комплексные числа

Система комплексных чисел это некоторое расширение системы действительных чисел. Исторически расшерение чисел можно представить так:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$$

В $\mathbb{N}$ не всегда выполнимо вычитание $\Rightarrow \mathbb{Z}$, но в $\mathbb{Z}$ не всегда выполнимо деление $\Rightarrow \mathbb{Q}$, но не все длины измеримы (стороны в рациональных числах, но диагонали уже нет, например) $\Rightarrow \mathbb{R}$, но в $\mathbb{R}$ не всегда разрешимы квадратные уравнения.

Хочется уметь извлекать квадратные корни из отрицательных чисел. Для этого достаточно уметь извлекать корень из -1: $\sqrt{-1} \Rightarrow \forall d < 0$ можно извлечь квадратный корень:

$$\sqrt{d} = \sqrt{-1}\cdot\sqrt{|d|}$$

Мы пришли к задаче расширения $\mathbb{R}$ до такой системы, в которой существует $\sqrt{-1}$ и не добавлено ничего лишнего (выполнялись все арифметические операции в этой системе и не выходило за её рамки).

Опр: 5. Полем комплексных чисел называется поле $\mathbb{C}$, обладающее следующими свойствами:

1) $\mathbb{R} \subset \mathbb{C}$;
2) $i \in \mathbb{C}\colon i^2 = -1$, этот элемент называется мнимой единицей;
3) **Условие минимальности**: Если K - подполе: $\mathbb{R} \subseteq K \subseteq \mathbb{C}$, $i \in K \Rightarrow K = \mathbb{C}$;

Rm: 2. Заметим, что это аксиоматическое определение. Похожим образом мы определяли группы.

Такое определение оставляет открытым вопрос, а существует ли такое поле? А если существует, то сколько таких полей? Пока мы отложим вопросы о существовании и единственности этого поля и изучим его структуру. После чего будет легче ответить на вопросы о существовании и единственности.

Опр: 6. Алгебраической формой записи комплексного числа $z \in \mathbb{C}$ называется запись вида:

$$z = x + iy,\ z \in \mathbb{C},\ x, y \in \mathbb{R}$$

где число $x \in \mathbb{R}$ называется действительной частью комплексного числа $z \in \mathbb{C}$ и обозначается $\operatorname{Re}(z) = x$, а число $y \in \mathbb{R}$ называется мнимой частью комплексного числа $z \in \mathbb{C}$ и обозначается $\operatorname{Im}(z) = y$.

Утв. 6. $\forall z \in \mathbb{C}$, $\exists!\, x, y \in \mathbb{R}\colon z = x + iy$.

$\square$
(**Существование**): Рассмотрим множество $K = \{z = x + iy \mid x, y \in \mathbb{R}\}$.

1) $\mathbb{R} \subseteq K$, поскольку это так при $y = 0$;
2) $i \in K$ при $x = 0$, $y = 1$;
3) Пусть $z = x + iy$, $z' = x' + iy' \in K$, докажем что их сумма, произведение также лежат в K:

$$z \pm z' = x + iy \pm x \pm iy' = (x \pm x') + i(y \pm y') \in K$$

$$z\cdot z' = (x + iy)\cdot(x' + iy') = x\cdot x' + iy'\cdot x + iy\cdot x' + i^2 y\cdot y' = (x\cdot x' - y\cdot y') + i(y\cdot x' + y\cdot x')$$

Таким образом, множество замкнуто относительно операций сложения, вычитания и умножения. В частности:

$$(x+iy)(x-iy)=x^2+y^2\in\mathbb{R},\, x>0\vee y>0\Rightarrow (x+iy)(x-iy)>0$$

Следовательно, если $z=x+iy\neq 0$, то есть $x\neq 0$ или $y\neq 0$, то z^{-1} будет иметь вид (это число всегда существует в поле для $z\neq 0$):

$$z^{-1}=\frac{x}{x^2+y^2}-i\frac{y}{x^2+y^2}\Rightarrow z^{-1}\in K$$

Следовательно, K - это подполе. По свойству минимальности $K=\mathbb{C}$;

(**Единственность**): Пусть $z=x+iy=x'+iy'\in\mathbb{C}$, тогда:

$$x-x'=i(y'-y)\Rightarrow (x-x')^2=i^2(y'-y)^2=-1\cdot(y'-y)^2=-(y'-y)^2$$

$$0\leq (x-x')^2=-(y'-y)^2\leq 0\Rightarrow (x-x')^2=(y'-y)^2=0\Rightarrow x-x'=y'-y=0\Rightarrow x=x',\, y=y'$$

$\blacksquare$

Rm: 3. Единственность записи комплексного числа в алгебраической форме означает, что комплексное число взаимнооднозначно задается парой действительных чисел. Далее это поможет нам доказать существование поля комплексных чисел.