Лекции по курсу

Математические основы криптологии

Университет ИТМО

Преподаватель: Петтай Павел Пээтерович

Лекция 1

0. Простейшие свойства арифметических операций на множестве целых чисел.

Договоримся, что в рамках данного курса, если не оговорено противное, *всюду речь идёт о целых числах*.

Вспомним некоторые свойства операций сложения и умножения (на множестве целых чисел $\mathbb{Z}$).

1. $\boxed{\forall a,b\ a+b=b+a}$ - коммутативность сложения
2. $\boxed{\forall a,b,c\ (a+b)+c=a+(b+c)}$ - ассоциативность сложения
3. $\boxed{\exists 0\ \forall a\quad 0+a=a+0=a}$ - существование нейтрального по сложению элемента (нуля)
4. $\boxed{\forall a\ \exists -a\quad a+(-a)=(-a)+a=0}$ - существование противоположного элемента (элемента, обратного по сложению)
5. $\boxed{\forall a,b\ a\cdot b=b\cdot a}$ - коммутативность умножения
6. $\boxed{\forall a,b,c\ (a\cdot b)\cdot c=a\cdot(b\cdot c)}$ - ассоциативность умножения
7. $\boxed{\exists 1\ \forall a\quad 1\cdot a=a\cdot 1=a}$ - существование нейтрального по умножению элемента (единицы)
8. $\boxed{\forall a,b,c\quad a\cdot(b+c)=a\cdot b+a\cdot c}$ и $\boxed{\forall a,b,c\quad (b+c)\cdot a=b\cdot a+c\cdot a}$ - дистрибутивность умножения относительно сложения.

Выполнение всех этих свойств говорит о том, что $(\mathbb{Z},+,\cdot)$ - *коммутативное кольцо с единицей*.

Отсюда легко выводятся различные простые свойства целых чисел. Например,

9. $\boxed{\forall a\in\mathbb{Z}\ a\cdot 0=0\cdot a=0}$.

Доказательство.

$$a\overset{'7'}{=}a\cdot 1\overset{'3'}{=}a\cdot(1+0)\overset{'8'}{=}a\cdot 1+a\cdot 0\overset{'7'}{=}a+a\cdot 0\Rightarrow -a+a=-a+(a+a\cdot 0)\overset{'4','2'}{\Leftrightarrow}$$

$$\overset{'4','2'}{\Leftrightarrow}0=(-a+a)+a\cdot 0\overset{'4'}{\Leftrightarrow}0=0+a\cdot 0\overset{'3'}{\Leftrightarrow}0=a\cdot 0\overset{'5'}{\Leftrightarrow}0=0\cdot a\quad .$$ **Ч.т.д.**

10. $\boxed{\forall a \in \mathbb{Z}\ (-1)\cdot a = a\cdot(-1) = -a}$.

Доказательство.

$$0 \overset{'9'}{=} 0\cdot a \overset{'4'}{=} (1+(-1))\cdot a \overset{'8'}{=} 1\cdot a + (-1)\cdot a \overset{'7'}{=} a + (-1)\cdot a \Rightarrow -a + 0 = -a + (a + (-1)\cdot a) \overset{'3','2'}{\Leftrightarrow}$$

$$\overset{'3','2'}{\Leftrightarrow} -a = (-a + a) + (-1)\cdot a \overset{'4'}{\Leftrightarrow} -a = 0 + (-1)\cdot a \overset{'3'}{\Leftrightarrow} -a = (-1)\cdot a \ .$$ **Ч.т.д.**

11. $\boxed{\forall a \in \mathbb{Z}\ -(-a) = a}$

Доказательство. В Свойстве “4” элементы a и $-a$ симметричны. **Ч.т.д.**

12. $\boxed{(-1)\cdot(-1) = 1}$

Доказательство.

$a\cdot((-1)\cdot(-1)) \overset{'6'}{=} (a\cdot(-1))\cdot(-1) \overset{'10'}{=} (-a)\cdot(-1) \overset{'10'}{=} -(-a) \overset{'11'}{=} a$, подставляя сюда $a = 1$, получим: $1 = 1\cdot((-1)\cdot(-1)) \overset{'7'}{=} (-1)\cdot(-1)$. **Ч.т.д.**

13. $\boxed{\forall a,b \in \mathbb{Z}\ (-a)\cdot(-b) = a\cdot b}$

Доказательство.

$$(-a)(-b) \overset{'10'}{=} (a\cdot(-1))((-1)\cdot b) \overset{'6'}{=} (a\cdot((-1)\cdot(-1)))\cdot b \overset{'12'}{=} (a\cdot 1)\cdot b \overset{'7'}{=} a\cdot b \ .$$ **Ч.т.д.**

14. $\boxed{\forall a,b \in \mathbb{Z}\ a\cdot(-b) = (-a)\cdot b = -(a\cdot b)}$

Доказательство.

$$a\cdot b + a\cdot(-b) \overset{'8'}{=} a\cdot(b+(-b)) \overset{'4'}{=} a\cdot 0 \overset{'9'}{=} 0 \Rightarrow -(a\cdot b) + (a\cdot b + a\cdot(-b)) = -(a\cdot b) + 0 \overset{'2','3'}{\Leftrightarrow}$$

$$\overset{'2','3'}{\Leftrightarrow} (-(a\cdot b) + a\cdot b) + a\cdot(-b)) = -(a\cdot b) \overset{'4'}{\Leftrightarrow} 0 + a\cdot(-b)) = -(a\cdot b) \overset{'3'}{\Leftrightarrow} -(a\cdot b) \overset{'4'}{\Leftrightarrow} a\cdot(-b)$$

Тогда, по доказанному, $(-a)\cdot b \overset{'5'}{=} b\cdot(-a) = -(b\cdot a) \overset{'5'}{=} -(a\cdot b)$. **Ч.т.д.**

15. $\boxed{\forall a,b,c\in\mathbb{Z}\quad a\cdot(b-c)=a\cdot b-a\cdot c}$ и $\boxed{\forall a,b,c\in\mathbb{Z}\quad (b-c)\cdot a=b\cdot a-c\cdot a}$ - дистрибутивность умножения относительно вычитания

Доказательство.

Вспомним, что $b-c=b+(-c)$ *по определению операции вычитания*. А тогда,

$$a\cdot(b-c)=a\cdot(b+(-c))\overset{'8'}{=}a\cdot b+a\cdot(-c)\overset{'14'}{=}a\cdot b+(-(a\cdot c))=a\cdot b-(a\cdot c)$$

$$(b-c)\cdot a=(b+(-c))\cdot a\overset{'8'}{=}b\cdot a+(-c)\cdot a\overset{'14'}{=}b\cdot a+(-(c\cdot a))=b\cdot a-(c\cdot a)\text{. }\textbf{Ч.т.д.}$$

1. Делимость в кольце целых чисел.

Опр.1.1. Говорят, что *число* a *делится на число* b (*кратно числу* b) и пишут $a\vdots b$, если существует такое единственное число c, что $a=b\cdot c$.

Итак, $\boxed{a\vdots b\Leftrightarrow\exists!c\ \ a=b\cdot c}$.

Опр.1.1'. Если существует такое единственное число c, что $a=b\cdot c$, то говорят также, что *число* b *делит число* a и пишут $b\,|\,a$.

Опр.1.2. *Разделить число* a *на число* b (без остатка), значит представить число a в виде $a=b\cdot c$.

Естественно задаться вопросом, верно ли, что любое число можно разделить на любое? Не сложно понять, что ответ на этот вопрос отрицательный. Попробуем, например, разделить число 3 на число 2. Т.к. произведение только положительных чисел является положительным числом, то результат деления тоже должен быть положительным числом. Сложение с положительным числом увеличивает сумму. Отсюда следует, что умножение положительного числа на большее положительное вернёт больший результат. В самом деле, если $c>b$, то есть $x>0$ такой что $c=b+x$, тогда при $a>0$ имеем: $a\cdot c=a\cdot(b+x)=ab+ax>ab$. Заметим, что $2\cdot1=2<3$, $2\cdot2=4>3$, тогда при $b>2$ по доказанному $2\cdot b>2\cdot2=4>3$. Итак, мы показали, что не существует такого целого числа c, что $3=c\cdot2$, значит 3 разделить на 2 не удастся.

Утверждение 1.1. *Никакое число не делится на ноль***.**

Доказательство. Предположим, что некоторое число $a \vdots 0$, при этом $a \neq 0$. Это значит, что существует такое c, что $a = 0 \cdot c = 0$, но $a \neq 0$ - противоречие. Теперь попробуем разделить 0 на 0. Это значит, что существует такое c, что $0 = 0 \cdot c = 0$. Это верно при любых c, в этом случае результатом деления 0 на 0 будет является любое число, т.е. нет единственности (деление не будет операцией). Таким образом, 0 тоже нельзя разделить на 0. **Ч.т.д.**

Утверждение 1.2. *Если* $\exists c\ a = bc$ *и* $b \neq 0$*, то такое число* c *единственно.*

Доказательство. Если $b > 0$, то при $x < c$ $bx < bc = a$, при $x > c$ $bx > bc = a$. Таким образом, при $x \neq c$ $bx \neq a$. Если $b < 0$, то при $x < c$ $bx > bc = a$, при $x > c$ $bx < bc = a$. Таким образом, при $x \neq c$ $bx \neq a$. **Ч.т.д.**

Следствие 1.1. При $b = 0$ по Утверждению 1.1, делимость на b невозможна, при $b \neq 0$ *для доказательства делимости* $a \vdots b$ достаточно доказать (например, предъявить явно) существование такого c, что $a = bc$, т.е. *единственность можно не доказывать*.

Свойства делимости

Свойство 1.1.

а.) $\boxed{\forall a \neq 0\ a \vdots a}$	б.) $\boxed{\forall a \neq 0\ a \vdots (-a)}$	в.) $\boxed{\forall a\ \ a \vdots 1}$	г.) $\boxed{\forall a\ \ a \vdots (-1)}$

Доказательство. а.) $a = a \cdot 1$, б.) $a = (-a) \cdot (-1)$, в.) $a = 1 \cdot a$, г.) $a = (-1) \cdot (-a)$ **Ч.т.д.**

Свойство 1.2. *Если среди чисел* $a_1, a_2, ..., a_n$ *хоть одно число кратно* d*, то и произведение* $a_1 \cdot a_2 \cdot ... \cdot a_n$ *кратно* d.

Доказательство. Пусть $a_i \vdots d$, т.е. $a_i = bd$ В силу коммутативности и ассоциативности умножения чисел, множитель d передвигаем вперёд перед произведением. **Ч.т.д.**

Свойство 1.3. (транзитивность отношения делимости)

$\boxed{a \vdots b \wedge b \vdots c \Rightarrow a \vdots c}$

Доказательство. $a \vdots b \Leftrightarrow \exists d_1\ a = bd_1$, $b \vdots c \Leftrightarrow \exists d_2\ b = cd_2$. Тогда
$a = bd_1 = (cd_2)d_1 = c(d_2 d_1) \Rightarrow a \vdots c$. **Ч.т.д.**

Свойство 1.4.

$$\boxed{a \vdots c \wedge b \vdots d \Rightarrow (ab) \vdots (cd)}$$

Доказательство. $a \vdots c \Leftrightarrow \exists x\, a = cx$, $b \vdots d \Leftrightarrow \exists y\, b = dy$. Тогда

$$ab = (cx)(dy) \overset{ас-ть}{=} c((xd)y) \overset{ком-ть}{=} c((dx)y) \overset{ас-ть}{=} (cd)(xy) \Rightarrow ab \vdots (cd).$$ **Ч.т.д.**

Свойство 1.5. Если $a = b + c$ и в этом равенстве два числа делятся на число d, то третье число также делится на число d.

Доказательство. Если $a \vdots d$ и $b \vdots d$, то существуют k_1 и k_2, такие что $a = d \cdot k_1$ и $b = d \cdot k_2$. Подставляя в исходное равенство, получим:

$d \cdot k_1 = d \cdot k_2 + c \Leftrightarrow d \cdot k_1 - d \cdot k_2 = c \Leftrightarrow d(k_1 - k_2) = c \Rightarrow c \vdots d$.

Случай $a \vdots d$ и $c \vdots d$ разбирается в точности так же.

Если $b \vdots d$ и $c \vdots d$, то существуют k_1 и k_2, такие что $b = d \cdot k_1$ и $c = d \cdot k_2$. Подставляя в исходное равенство, получим:

$a = d \cdot k_1 + d \cdot k_2 \Rightarrow a = d(k_1 + k_2) \Rightarrow a \vdots d$. **Ч.т.д.**

Замечание 1.1. Доказанное свойство легко обобщается на случай суммы любого количества слагаемых: *в равенстве* $a_1 + a_2 + ... + a_n = b$ *есть* n *чисел кратных* d *в том и только том случае, когда все входящие в равенство числа кратны* d. Доказательство практически аналогично доказательству Свойства1.5. и остаётся читателю в качестве несложного упражнения.

Пример.1 Пусть $246 = 66 + x$, тогда, т.к. $246 \vdots 6$ и $66 \vdots 6$, то $x \vdots 6$.

Пример.2 Пусть $247 = 66 + x$, тогда т.к. $247 \not\vdots 6$, а $66 \vdots 6$, то $x \not\vdots 6$ (если бы $x \vdots 6$, то по Свойству 1.4, $247 \vdots 6$, что не верно).

Свойство 1.6.

$$\boxed{\forall n \in \mathbb{N}\ a \vdots b \Rightarrow a^n \vdots b^n}$$

Доказательство. Достаточно n раз применить Свойство 1.4. Например,

$a \vdots b \wedge a \vdots b \overset{Св-во\,1.4}{\Rightarrow} (a \cdot a) \vdots (b \cdot b) \Leftrightarrow a^2 \vdots b^2$. Теперь

$a \vdots b \wedge a^2 \vdots b^2 \overset{Св-во\,1.4}{\Rightarrow} (a \cdot a^2) \vdots (b \cdot b^2) \Leftrightarrow a^3 \vdots b^3$. Тогда

$a \vdots b \wedge a^3 \vdots b^3 \overset{Св-во\,1.4}{\Rightarrow} (a \cdot a^3) \vdots (b \cdot b^3) \Leftrightarrow a^4 \vdots b^4$ и т.д. **Ч.т.д.**

Замечание 1.2. Данное простое свойство можно было доказывать разными способами. Например, можно необходимое количество раз воспользоваться свойствами коммутативности и ассоциативности умножения (а значит

множители можно переставлять в произведении, как хочется). Тогда $a \vdots b \Leftrightarrow \exists c\ a = bc$, следовательно, $a^n = (bc)^n = b^n \cdot c^n \Rightarrow a^n \vdots b^n$.

Свойство 1.7.

$\boxed{a \vdots b \wedge |a| < |b| \Rightarrow a = 0}$, иными словами, *меньшее по модулю число не может делиться на большее по модулю за исключением случая, когда меньшее по модулю число - ноль.*

Доказательство. $a \vdots b \Rightarrow \exists c\ a = bc \Rightarrow |a| = |bc| = |b| \cdot |c|$. Тогда $|b| \cdot |c| < |b| \Leftrightarrow |b| \cdot |c| - |b| < 0 \Leftrightarrow |b|(|c| - 1) < 0$. Т.к. $a \vdots b$, $b \neq 0 \Rightarrow |b| > 0$, следовательно, $|c| - 1 < 0 \Leftrightarrow |c| < 1$, но $c \in \mathbb{Z}$, значит $c = 0$, но тогда $a = b \cdot c = b \cdot 0 = 0$. **Ч.т.д.**

Опр.1.3. Числа a и b называются *ассоциированными*, если $a \vdots b$ и $b \vdots a$.

Свойство 1.8. $\boxed{a \vdots b \wedge b \vdots a \Rightarrow |a| = |b|}$ (ассоциированные числа либо совпадают, либо отличаются только знаком, т.е. являются противоположными).

Приведём два разных доказательства.

Доказательство 1. $a \vdots b \Leftrightarrow \exists c\ a = bc$, $b \vdots a \Leftrightarrow \exists d\ b = ad$. Объединяя вместе, получим, что $a = bc = (ad)c = a(dc)$, т.к. $b \vdots a$, то $a \neq 0$, следовательно, обе части равенства можно сократить на a и получить $1 = dc$. Если $|d| = 0 \vee |c| = 0$, то равенство невозможно. Если $|d| \geq 2$, то $1 = |1| = |dc| = |d| \cdot |c| \geq 2|c| \geq 2 \cdot 1 = 2$ - противоречие. Значит $|d| = 1$, а тогда $|b| = |ad| = |a| \cdot |d| = |a| \cdot 1 = |a|$. **Ч.т.д.**

Доказательство 2. Если $|a| = |b|$, то $a = b$ или $a = -b$, в каждом из этих случаев при $a \neq 0$ и $b \neq 0$ верно $a \vdots b \wedge b \vdots a$ в силу Свойства 1.1. Покажем, что другие случаи невозможны. Если $|a| < |b|$, то, т.к. $a \vdots b$, по Свойству 1.7. $a = 0$, что противоречит тому, что $b \vdots a$. Аналогично, если $|a| > |b|$, то, т.к. $b \vdots a$, по Свойству 1.7. $b = 0$, что противоречит тому, что $a \vdots b$. **Ч.т.д.**

Следствие 1.2. $\boxed{a,b \in \mathbb{N} \wedge a \vdots b \wedge b \vdots a \Rightarrow a = b}$

Свойство 1.9. Среди любых n подряд идущих целых чисел ровно одно кратно n.

Доказательство. Заметим, что раз речь идёт об n подряд идущих целых числах, то модуль разности любых двух из них меньше n. Пусть речь идёт о числах $a_1, a_2, ..., a_n$, где $\forall k \in \mathbb{N}\ k < n \rightarrow a_{k+1} = a_1 + k$. Предположим, что среди данных чисел хотя бы два числа кратны n, пусть это числа a_i и a_j, т.е. $\exists c_i\ \exists c_j\ a_i = nc_i \wedge a_j = nc_j$. Но тогда

$|a_i - a_j| = |nc_i - nc_j| = n|c_i - c_j| < n \Rightarrow |c_i - c_j| < 1 \Rightarrow |c_i - c_j| = 0 \Rightarrow c_i = c_j \Rightarrow a_i = a_j$ - противоречие.

Теперь докажем существование. Пусть b - максимальное число, кратное n среди чисел, меньших a_1. Если $b + n < a_1$, то это противоречит максимальности числа b, следовательно, $b + n \geq a_1$. В свою очередь, $b < a_1$, т.е. $b \leq a_1 - 1$, а тогда $b + n \leq (a_1 - 1) + n = a_1 + n - 1 = a_n$ Следовательно, $b + n \in \{a_1, a_2, ..., a_n\}$. Т.к. $b \vdots n$, то и $b + n \vdots n$, т.е. одно из чисел $a_1, a_2, ..., a_n$ кратно n. **Ч.т.д.**

Пример. Среди чисел -123, -122, -121, -120, -119, -118, -117 ровно одно число кратно 7 (конкретно, число -119).

2. Деление с остатком.

Как мы увидели, далеко не всегда одно число делится на другое. Возникает естественное желание ввести некоторый аналог делимости, применимый всегда.

Опр.2.1. *Разделить число a на число b с остатком*, значит представить число a в виде $\boxed{a = bq + r}$, где $\boxed{0 \leq r < |b|}$, при этом число a называют *делимым*, число b - *делителем*, число q - *частным*, а число r - *остатком*.

Например, $17 = 5 \cdot 3 + 2$, т.е. частным от деления 17 на 3 является 5, а остатком - число 2.

В свою очередь, $-17 = (-6) \cdot 3 + 1$, т.е. частным от деления числа -17 на число 3 является число -6, а остатком – число 1. Несмотря на то, что равенство $-17 = (-5) \cdot 3 - 2$ является верным, оно не является делением с остатком.

Возникают естественные вопросы: всегда ли можно разделить одно число на другое с остатком (возможно, равным нулю), определены ли частное и остаток единственным образом? Оказывается, если делимое отлично от нуля, то ответ на оба вопроса положительный.

Утверждение 2.1. *Никакое число нельзя разделить на ноль с остатком***.**

Доказательство. Предположим, что некоторое число a делится на 0 с остатком. Это значит, что существуют такие целые q и r, что $a = 0 \cdot q + r$, где $0 \le r < |0| = 0$ - противоречие. **Ч.т.д.**

Теорема 2.1. $\boxed{\forall a\ \forall b\ b \neq 0 \to \exists!(q,r)\ \ a = bq + r \wedge 0 \le r < |b|}$ - *Любое число можно разделить с остатком на любое ненулевое число, при этом частное и остаток определены однозначно***.**

Доказательство. Докажем существование. Пусть $b > 0$, тогда по аксиоме Архимеда, найдётся такое целое число q, что $bq \le a$, а $b(q+1) > a$. Иными словами, в качестве q мы берём самое большое число, такое, что $bq \le a$. Тогда, раз $bq \le a$, то $a = bq + r$, где $r \ge 0$. Раз $a < b(q+1)$, то

$a = bq + r < b(q+1) = bq + b \Rightarrow r < b = |b|$.

Пусть теперь $b < 0$, тогда по аксиоме Архимеда, найдётся такое целое число q, что $bq \le a$, а $b(q-1) > a$ (раз $q - 1 < q$ и $b < 0$, то $(q-1)b > qb \Leftrightarrow bq < b(q-1)$). Иными словами, в качестве q мы берём самое маленькое число, такое, что $bq \le a$. Тогда, раз $bq \le a$, то $a = bq + r$, где $r \ge 0$. Раз $a < b(q-1)$, то $a = bq + r < b(q-1) = bq - b = bq + (-b) = bq + |b| \Rightarrow r < |b|$.

Теперь докажем единственность.

Предположим, что есть хотя бы две пары подходящих частного и остатка, т.е. $a = bq_1 + r_1,\ 0 \le r_1 < |b|$ и $a = bq_2 + r_2,\ 0 \le r_2 < |b|$, где $(q_1, r_1) \neq (q_2, r_2)$. Вычитая соответствующие части равенств, получим:

$0 = a - a = (bq_1 + r_1) - (bq_2 + r_2) = b(q_1 - q_2) + r_1 - r_2 \Leftrightarrow r_2 - r_1 = b(q_1 - q_2) \Rightarrow$

$\Rightarrow |r_2 - r_1| = |b(q_1 - q_2)| = |b| \cdot |q_1 - q_2|$, но, т.к. $0 \le r_1 < |b|$ и $0 \le r_2 < |b|$, то

$-|b| < r_2 - r_1 < |b| \Rightarrow |r_2 - r_1| < |b|$, а тогда

$|b| \cdot |q_1 - q_2| < |b| \Leftrightarrow |q_1 - q_2| < 1 \Rightarrow q_1 - q_2 = 0 \Leftrightarrow q_1 = q_2$. Наконец,

$r_1 = a - bq_1 \overset{q_1 = q_2}{=} a - bq_2 = r_2$ - противоречие. **Ч.т.д.**