1. Делимость

Напомним, что множество целых чисел обозначается $\mathbb{Z}$, множество натуральных чисел обозначается $\mathbb{N}$.

Определение. *Пусть a, b — целые числа. Тогда будем говорить, что a делится на b (или b делит a, или a кратно b), если существует такое c, что $a = bc$. Число a называется делимым, b — делителем, a число c — частным.*

Формула $a \vdots b$ читается как «a делится на b», а формула $b \mid a$ читается как b делит a. Формула $b \nmid a$ читается как b не делит a.

Пример. *6 делится на 2 т.к.* $6 = 2 \cdot 3$. *Значит,* $6 \vdots 2$ *или* $2 \mid 6$.

Отметим некоторые свойства простых чисел.

1) Если $a \vdots b$ и $b \vdots c$, то $a \vdots c$.

2) Если $a \vdots c$ и $b \vdots c$, то $a + b \vdots c$ и $a - b \vdots c$.

3) Если $c \mid a$ и $c \nmid b$, то $c \nmid a + b$.

4) Если $a \vdots b$, то $ac \vdots bc$, для любого целого c, отличного от нуля.

Определение. *Натуральное число a называется составным, если $a = b \cdot c$, где b и c — натуральные числа, и $a \neq b$ и $a \neq c$. Натуральное число отличное от единицы называется простым, если оно не является составным.*

Заметим, что, если a и b натуральные числа, и a делится на b, то $a \geq b$.

Лемма (О простом делителе.)**.** *У любого натурального числа, большего 1, существует простой делитель.*

Доказательство. Пусть n — произвольное натуральное число, большее единицы. Рассмотрим множество натуральных делителей n, больших единицы. Они все не больше n и не меньше двух. Значит, их конечное число. Значит, среди них можно найти наименьший. Пусть p — это наименьший делитель числа n, больший единицы.

Докажем, что p — простое. Пусть это не так. Тогда $p = b \cdot c$, где b и c — натуральные числа отличные от p. Тогда b и c отличны от единицы. Если бы, скажем, b равнялось единице, то тогда c равнялось бы p, что не так. Но тогда b — натуральное число, большее единицы и меньшее p, которое делит p, а значит и n. Это противоречит нашему предположению, что p — наименьший делитель n. □

Здесь мы использовали интуитивно понятный факт, что из конечного набора чисел можно выбрать наименьшее. Давайте обратим внимание, что из бесконечного набора чисел выбрать наименьшее не всегда возможно. Полезно помнить следующий пример. Рассмотрим следующий бесконечный набор чисел $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots, \frac{1}{n} \ldots$. Среди чисел из этого набора наименьшего нет.

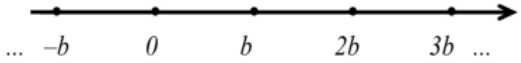
2. Деление с остатком. Наибольший общий делитель. Алгоритм Евклида.

Теорема. *Для любых целых чисел a и b, таких, что $b \neq 0$, найдутся такие целые числа q и r, что*

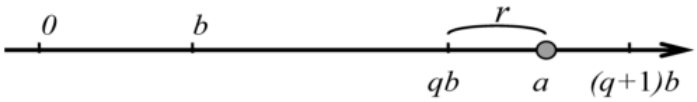
$$a = b \cdot q + r \quad \textit{где} \quad 0 \leq r \leq |b|.$$

Определение. *В этом случае число q называется частным, а число r — остатком от деления a на b.*

Доказательство. Пусть b — некоторое целое число. Отметим на числовой оси целые числа, делящиеся на b.



Теперь отметим на той же числовой оси число a. Оно попадет в единственный полуинтервал между двумя выделенными числами, кратными b. Пусть это числа qb и $(q+1)b$. Тогда число $r = a - qb$ есть целое число, удовлетворяющее неравенствам $0 \leq r \leq |b|$.



Пример. *Разделим 17 на 5 с остатком. Имеем* $17 = 5 \cdot 3 + 2$. *Тогда частное* $q = 3$, *а остаток* $r = 2$.

Деление с остатком помогает найти наибольший общий делитель двух чисел.

Определение. *Наибольшим общим делителем двух целых чисел a и b называется наибольшее натуральное число d, которое делит и a, и b. Наибольший общий делитель обозначают либо как НОД(a, b), либо как (a, b).*

Наименьшим общим кратным двух целых чисел a и b называется наименьшее натуральное число k, которое делится и на a, и на b. Наименьшее общее кратное обозначают либо как НОК(a, b), либо как $[a, b]$.

Определение. *Если* $(a, b) = 1$, *то говорят, что числа взаимно просты.*

Отметим важное свойство наибольшего общего делителя.

Теорема.

$$(a, b) = (a - b, b).$$

Доказательство. Если число d является общим делителем a и b, то d является общим делителем и чисел $a - b$ и b, и наоборот. Таким образом множество общих делителей у пар чисел a,b и $a - b$,b совпадают. Значит, совпадают и НОДы. □

Следствие. *Разделим число a на b с остатком: $a = bq + r$. Тогда $(a, b) = (r, b)$.*

Доказательство. Действительно,

$$(a, b) = (a - b, b) = (a - 2b, b) = \ldots = (a - qb, b) = (r, b).$$

□

На этом свойстве основан **алгоритм Евклида** для нахождения наибольшего общего делителя чисел a и b.

Разделим сначала a на b с остатком. Тогда

$$a = bq_1 + r_1.$$

При этом $(a, b) = (r_1, b)$, и $0 \leq r_1 < |b|$. Далее разделим b на r_1:

$$b = r_1 q_2 + r_2.$$

Опять же, $(a,b)=(r_1,b)=(r_1,r_2)$, и $0\le r_2<r_1<|b|$. Далее разделим r_1 на r_2

$$r_1=r_2q_3+r_3,$$

при этом $(a,b)=(r_1,r_2)=(r_3,r_2)$, и $0\le r_3<r_2<r_1<|b|$. Далее будем продолжать делить остаток, полученный на предыдущем шаге, на остаток, полученный на новом шаге. Остатки становятся все меньше и меньше. Поэтому на некотором шаге деление произойдет без остатка

$$r_{n-1}=r_nq_{n+1}.$$

Мы видим, что $(a,b)=(r_{n-1},r_n)$. Но $(r_{n-1},r_n)=r_n$, так как r_{n-1} делится на r_n. Таким образом мы нашли наибольший общий делитель.

Пример. *Найдем с помощью алгоритма Евклида НОД(132, 75).*

$$132=75\cdot1+57;$$
$$75=57\cdot1+18;$$
$$57=18\cdot3+3;$$
$$18=3\cdot6.$$

Число 3 *— это последний ненулевой остаток, который мы получили. Поэтому*

$$(132,57)=3.$$

Из алгоритма Евклида следует важно утверждение

Теорема. *Для любых двух целых чисел a и b найдутся такие целые числа u и v такие, что $(a,b)=au+bv$.*

Доказательство. Действительно, будем по очереди выражать остатки r_1,r_2,r_3,r_n через a и b. Мы имеем:

$$a=bq_1+r_1,$$
$$b=r_1q_2+r_2,$$
$$r_1=r_2q_3+r_3,$$
$$\dots$$
$$r_{n-1}=r_nq_{n+1}.$$

Тогда

$$r_1=a-bq_1,$$
$$r_2=b-r_1q_2=b-(a-bq_1)q_2=a(-q_2)+b(1+q_1q_2),$$
$$\dots$$

И так далее. Мы последовательно получаем выражения $r_i=u_ia+v_ib$, где u_i,v_i — целые числа. Но так как $(a,b)=r_n$, то в итоге мы получим выражение для НОДа. □

Пример. *В предыдущем примере мы нашли, что* $(132,75)=3$. *Выразим тройку через 132 и 75. Итак имеем:*

$$132=75\cdot1+57\quad\Rightarrow57=132-75,$$
$$75=57\cdot1+18\quad\Rightarrow18=75-57=75-(132-75)=2\cdot75-132,$$
$$57=18\cdot3+3\quad\Rightarrow3=57-18\cdot3=(132-75)-(2\cdot75-132)\cdot3=4\cdot132-7\cdot75.$$

И так, $(132,75)=4\cdot132-7\cdot75$.

3. Основная теорема арифметики.

Перед тем, как перейти к основной теореме арифметики, мы докажем следующее вспомогательное утверждение.

Лемма. *Пусть a — натуральное число, и $a = b \cdot c$, где b и c — тоже натуральные числа. И пусть некоторое простое число p делит a. Тогда либо b, либо c делится на p.*

Доказательство. Предположим, что b не делится на p. Тогда $(p, b) = 1$, т.к. у p нет других делителей кроме p и 1. Тогда существуют такие целые числа u и v, что

$$1 = u \cdot p + v \cdot b.$$

Домножим это равенство на c. Получим

$$c = u \cdot p \cdot c + v \cdot b \cdot c = u \cdot p \cdot c + v \cdot a.$$

Числа $u \cdot p \cdot c$ и $v \cdot a$ делятся на p. Значит и $u \cdot p \cdot c + v \cdot a$ делится на p. Получаем, что c делится на p. □

Следствие. *Пусть произведение целых чисел $a_1 \cdot a_2 \cdot a_3 \cdot \ldots \cdot a_n$ делится на простое число p. Тогда одно из чисел a_i делится на p.*

Доказательство. Пусть a_1 не делится на p. Тогда число $a_2 \cdot a_3 \cdot \ldots \cdot a_n$ делится на p. Если a_2 не делится на p, то $a_3 \cdot \ldots \cdot a_n$. И так далее рано или поздно мы получим, что какое-то a_i делится на p. (В крайнем случае это будет a_n). □

Теперь мы готовы сформулировать и доказать следующую теорему.

Теорема (Основная теорема арифметики)**.** *Каждое натуральное число a, большее 1, можно представить в виде произведения $a = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n$, где $p_1, p_2, p_3 \ldots p_n$ — простые числа. Это представление единственно с точностью до перестановки множителей.*

Доказательство. 1) Существование. Будем доказывать, что такое разложение существует, по индукции.

База индукции. $a = 2$. Тогда a само является простым.

Шаг индукции. Пусть теперь мы знаем, что такое разложение существует для всех натуральных чисел, меньших a. По лемме о простом делителе, существует такое простое число p, что $a = p \cdot b$. Так как $b \leq a$, то для b найдутся такие простые числа $p_1, p_2 \ldots p_n$, что $b = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n$. Но тогда $a = p \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_n$. Это и есть искомое разложение.

2) Докажем теперь единственность разложения на простые множители. Предположим, что некоторые натуральные числа имеют два разложения на простые множители. Возьмем наименьшее такое число a. Тогда $a = p_1 \cdot p_2 \cdot \ldots \cdot p_n = q_1 \cdot q_2 \cdot \ldots \cdot q_m$, где $p_1, \ldots p_n, q_1, \ldots q_m$ — простые числа. Но тогда $q_1 \cdot q_2 \cdot \ldots \cdot q_m$ делится на p_1. Пользуясь леммой, доказанной выше, мы делаем вывод, что какое-то q_i делится на p_1. Но это значит, что $q_i = p_1$, так как оба числа простые. Тогда мы можем сократить равенство $p_1 \cdot p_2 \cdot \ldots \cdot p_n = q_1 \cdot q_2 \cdot \ldots \cdot q_m$ на p_1 и получить, что $p_2 \cdot p_3 \cdot \ldots \cdot p_n = q_1 \cdot q_2 \cdot \ldots \cdot q_m$ (справа уже нет q_i). Но число $p_2 \cdot p_3 \cdot \ldots \cdot p_n$ меньше чем a и тоже имеет два разложения на простые множители. Мы приходим к противоречию с выбором a. □

Как правило, когда раскладывают число на простые множители, не записывают одно и тоже простое число несколько раз, а пишут его один раз, возведенным в степень. Например, вместо $2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3$ пишут $2^4 \cdot 3^2$. На всякий случай приведем пример.

Пример. *Число* $360 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 = 2^3 \cdot 3^2 \cdot 5$.

С помощью разложения на простые множители можно находить НОДы и НОКи чисел. Пусть есть два натуральных числа a и b. Разложим их на простые множители

$$a = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots p_n^{a_n}, \quad b = p_1^{b_1} p_2^{b_2} \cdot p_n^{b_n},$$

где $p_1, p_2, \ldots p_n$ — различные простые числа, $a_1, \ldots, a_n, b_1, \ldots b_n$ — целые неотрицательные числа. Если какое-то простое число, которое входит в разложение числа a не входит в разложение b, то соответствующая степень этого простого числа в разложении b равна нулю и наоборот.

Тогда имеем

$$(a, b) = p_1^{\min\{a_1,b_1\}} p_2^{\min\{a_2,b_2\}} \cdot \ldots \cdot p_n^{\min\{a_n,b_n\}},$$
$$[a, b] = p_1^{\max\{a_1,b_1\}} p_2^{\max\{a_2,b_2\}} \cdot \ldots \cdot p_n^{\max\{a_n,b_n\}}.$$

Пример. *Пусть* $a = 360 = 2^3 \cdot 3^2 \cdot 5$, *и* $b = 588 = 2^2 \cdot 3 \cdot 7^2$. *Тогда*

$$(a, b) = 2^2 \cdot 3, \quad [a, b] = 2^3 \cdot 3^2 \cdot 5 \cdot 7^2.$$

4. Простые числа.

Теперь мы выведем некоторые основные свойств простых чисел.

Теорема. *Простых чисел бесконечно много.*

Доказательство. Предположим противное, что их конечное число. Пусть это числа $p_1, p_2, \ldots p_n$. Тогда рассмотрим следующее число:

$$a = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n + 1.$$

С одной стороны оно не делится ни на одно из чисел среди $p_1, p_2, \ldots, p_n$. Но это значит, что число a — простое. Мы получаем противоречие с тем, что $p_1, \ldots, p_n$ — все простые числа. □

Что нужно сделать, чтобы проверить, что число просто?

Теорема. *Если натуральное число* n *не делится ни на одно простое число, не превосходящее* $\sqrt{n}$, *то* n *— простое.*

Доказательство. Предположим, что n — составное. Тогда в разложении n на простые числа есть хотя бы два простых числа (возможно повторяющихся). Т.е. $n = p_1 \cdot p_2 \cdot b$, где p_1, p_2 — простые, а b — натуральное. Число n делится на p_1 и p_2. Значит $p_1 > \sqrt{n}$ и $p_2 > \sqrt{n}$. Но тогда

$$n = p_1 \cdot p_2 \cdot b > \sqrt{n} \cdot \sqrt{n} \cdot b = n \cdot b > n.$$

Мы получаем, что $n > n$, чего не может быть. Противоречие. □

Легко доказать, что числа n^2 имеют остатки только 0 и 1 при делении на 3. Возможно простые числа, тоже обладают каким-то похожим свойством? Оказывается, что нет.

Теорема (Дирихле)**.** *Пусть* $(d, r) = 1$. *Тогда в последовательности чисел* $kd + r$ *бесконечно много простых числе.*

Доказательство этой теоремы очень трудное. Мы докажем эту теорему в случае, когда $d = 3, r = 2$.

Теорема. *В последовательности числе* $3k + 2$ $(k = 1, 2, \ldots)$ *бесконечно много простых чисел.*

Доказательство. Доказательство похоже на доказательство теоремы о бесконечно простых чисел. Пусть среди чисел $3k+2$ только конечное число простых. Пусть это числа $p_1, p_2, \dots p_n$. Число 2 имеет вид $3k+2$, поэтому можно считать, что $p_1 = 2$. Рассмотрим число

$$a = 3 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n + 2.$$

Оно не делится на ни на 2, ни на числа $p_2, \dots p_n$. Число a должно быть составным, иначе мы получили еще одно простое число вида $3k+2$. Значит

$$a = q_1 \cdot q_2 \cdot \ldots q_m, \text{ , где } q_1, q_2, \dots, q_m\text{- простые.}$$

Числа $q_1, q_2, \dots q_m$ не делятся на 3. Они не могут иметь остаток 2 при делении на 3, т.к. иначе они совпадали с какими-то из чисел $p_1, , p_n$, а a не делится на эти числа. Значит,

$$q_1 = (3k_1+1),\ q_2 = (3k_2+1), \dots, q_m = (3k_m+1).$$

Но произведении таких чисел имеет остаток 1 при делении на 3, число a имеет остаток 2. Противоречие. □

Интуитивно кажется, что простые числа должны встречаться все реже и реже, когда мы рассматриваем все большие и большие числа. В некотором смысле, это правда.

Теорема. *Для любого натурального N есть N последовательных натуральных чисел, среди которых нет простых.*

Доказательство. Рассмотрим числа $(N+1)!+2, (N+1)!+3, \dots, (N+1)!+(N+1)$. Каждое из них составное ($(N+1)!+2$ делится на 2, $(N+1)!+3$ делится на 3, и т.д.). Их N штук. □

У нас возникли факториалы. Давайте обсудим, как $n!$ раскладывается на простые множители.

Теорема. *Просто число p входит в разложение на простые множители числа $n!$ в степени*

$$\frac{n}{p} + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \dots.$$

(Здесь скобочки $[a]$ означают целую часть от числа a, т.е. наибольшее целое число, которое меньше a. Например, $\left[3\frac{17}{19}\right] = 3$.)

5. Где верна основная теорема арифметики? Пример Яглома. Пример Гильберта.

Умножать и делить можно не только числа. Например, мы видели, что можно делить многочлены. Множество многочленов обозначается $\mathrm{R}[x]$.

Многочлен f делиться на многочлен g, если существует такой многочлен h, что $f = g \cdot h$.

Какие многочлены являются аналогами простых чисел? Это неприводимые многочлены.

Определение. *Многочлен f называется неприводимым, если его нельзя представить в виде произведения многочленов $g \cdot h$, каждый из которых имеет ненулевую степень.*

Напомним, что многочлены нулевой степени - это только константы, т.е. многочлены, в которые не входит x. Например, $7, \frac{1}{2}, -3$ — это многочлены нулевой степени.

Таким образом, неприводимые многочлены - это те, которые нельзя представить в виде произведения многочленов, каждый из которых отличен от константы.

Вы можете убедиться, что для многочленов тоже верна основная теорема арифметики. Каждый многочлен однозначно раскладывается в произведение неприводимых.

Может быть, основная теорема арифметики верна всегда, когда есть деление и умножение? Следующий пример показывает, что это не так. Следующая конструкция называется **примером Яглома.**

Рассмотрим множество четных чисел. Четные числа можно складывать и умножать привычным образом. Но, если мы хотим рассматривать только четные числа, то когда мы говорим о делимости, то стоит требовать, чтобы частное тоже было четным числом.

Определение (определение делимости в примере Яглома)**.** *Четное число a делится на четное число b, если есть такое четное число c, что $a = b \cdot c$.*

Таким образом число 6 не делится на 2. $6 = 3 \cdot 2$, но 3 не является четным числом. Определение простого и составного числа остается тем же, что и для целых чисел. Число 6 будет простым.

Теорема. *Все четные числа, кратные 4, являются составными, а все некратные — простыми.*

Доказательство. Если число n делится на 4, то n можно представить в виде $n = 4k$, где k — целое. Тогда $n = 2 \cdot 2k$. Числа 2, и $2k$ — четные. Значит, n — составное.

Пусть теперь n — четное число, которое не делится на 4. Но произведение двух четных чисел дает число, делящиеся на 4. Поэтому n нельзя представить в виде произведения двух четных чисел, и n — простое. □

Рассмотрим число 36. С одной стороны, $36 = 6 \cdot 6$, причем 6 — простое. С другой, $36 = 18 \cdot 2$, где 18 и 2 тоже простые. Значит, 36 можно разложить двумя способами на простые, и в примере Яглома основаня теорема арифметики неверна.

Еще один пример множества, где есть умножение, но неверна основная теорема арифметики, называется **примером Гильберта.**

Рассмотрим множество чисел, имеющих остаток 1 при делении на 4, т.е. числа вида $4k + 1$, где k — произвольное целое число. Давайте убедимся, что произведение чисел, имеющих остаток 1 при делении на 4, дает число, тоже имеющее остаток 1 при делении на 4. Действительно,

$$(4k + 1) \cdot (4l + 1) = 16kl + 4k + 4l + 1 = 4(4kl + k + l) + 1.$$

Давайте выпишем несколько чисел из примера Гильберта и поймем, какие из них являются простыми, а какие составными.

$$1, 5, 9, 13, 17, 21, 25, 29, 33.$$

Число 1 не является ни простым, ни составными. Число 5 будет простым, т.к. оно в принципе не раскладывается в произведение двух чисел. По той же причине простыми будут числа 13, 17, 29. Число 9 можно представить как $3 \cdot 3$. Но 3 имеет остаток 3 при делении на 4, а не 1. Поэтому 3 не принадлежит множеству рассматриваемых чисел. Поэтом в примере Гильберта число 9 тоже простое. Аналогично 21 и 33 тоже простые. А число 25 равно $5 \cdot 5$, причем 5 имеет остаток 1 при делении на 4. Значит, 25 — составное.

Давайте рассмотрим число $441 = 3^2 \cdot 7^2$. Оно имеет остаток 1 при делении на 4. Как его можно разложить на простые множители в примере Гильберта? Во-первых, $441 = 9 \cdot 49$. И 9, и 49 имеют остаток 1 при делении на 4. Легко убедиться, что они простые. Значит, мы получили первое разложение. Но в тоже время $441 = 21 \cdot 21$. Число 21 тоже простое. Поэтому мы получили еще одно разложение. Основная теорема арифметики не верна и в примере Гильберта.

6. Диофантовы уравнения

Диофантовыми уравнениями называются уравнения, в которых вы ищите целые решения. Сейчас мы поговорим о линейных диофантовых уравнениях.

Пусть дано уравнение

$$ax + by = c,$$

где числа a, b, c — целые числа, и решения (т.е. пары x и y, которые удовлетворяют уравнению) нас интересуют тоже целые. Такие уравнения называются *линейными диофантовыми уравнениями.* Как его решить?

Если число c не делится на (a, b), то это уравнение не имеет решений, т.к. справа стоит число, которое делится на (a, b), а слева нет. Если же число c делится на (a, b), то все коэффициенты (т.е. числа a, b, c) можно разделить на (a, b). И тогда получим уравнение, у которого коэффициенты взаимно простые. Давайте проиллюстрируем это на примерах.

Уравнение $2x + 4y = 5$, не имеет решений, т.к. число слева делится на 2, а 5 не делится на 2.

Рассмотрим уравнение $12x + 8y = 20$. НОД(12, 8) $= 4$. Разделим уравнение на 4. Получим $3x + 2y = 5$. У этого уравнения коэффициенты 3 и 2 взаимно простые.

Таким образом достаточно научиться решать уравнения вида $ax+by = c$, где $(a, b) = 1$. Давайте для начала рассмотрим уравнение $ax + by = 1$. Но ведь у нас есть следствие из алгоритма Евклида, которое говорит, что НОД чисел a и b можно выразить как $au + bv$, где u и v — целые числа. Значит, если мы возьмем $x = u, y = v$ мы получим решение.

Пример. *Рассмотрим уравнение* $13x + 19y = 1$. *Применим алгоритм Евклида к 13 и 19.*

$$19 = 13 + 6,$$

$$13 = 6 \cdot 2 + 1.$$

Выразим НОД(13, 19). Из первого равенства получаем $6 = 19-13$, *из второго* $1 = 13-6\cdot 2$. *Подставляем выражение для 6 в выражение для 1.* $1 = 13-(19-13)\cdot 2 = 13-2\cdot 19+2\cdot 13 = 3 \cdot 13 - 2 \cdot 19$. *Значит, если положить* $x = 3$, *а* $y = -2$, *то получим решение.*

Что делать, если a или b отрицательное? На самом деле, все тоже самое.

Пример. *Решим уравнение* $17x - 5y = 1$. *Применяем алгоритм Евклида к 17 и 5.*

$$17 = 5 \cdot 3 + 2,$$

$$5 = 2 \cdot 2 + 1.$$

Отсюда $2 = 17-5\cdot 3,\ 1 = 5-2\cdot 2$. *Значит,* $1 = 5-2\cdot(17-5\cdot 3) = 5-2\cdot 17+6\cdot 5 = 7\cdot 5-2\cdot 17$. *Возъмем* $x = -2, y = -7$. *Тогда* $17x - 5y = 17 \cdot (-2) - 5 \cdot (-7) = -2 \cdot 17 + 7 \cdot 5 = 1$.

Что делать, если в правой части не один, а какое-то целое число c? Нужно просто умножить найденное решение для единицы на c.

Пример. *Попробуем решить уравнение* $13x + 19y = 23$. *Мы только что видели, что пара чисел* $x = 3, y = -2$, *является решением уравнения* $13x + 19y = 1$. *Но если мы возъмем* $x = 3 \cdot 23, y = -2 \cdot 23$, *то получим, что* $13x + 19y = 13 \cdot 3 \cdot 23 + 19 \cdot (-2) \cdot 23 = 23(13 \cdot 3 + 19 \cdot (-3)) = 23 \cdot 1 = 23$.

Итак, мы научились находить некоторое решение уравнений вида $ax + by = c$. Нашли ли мы все решения? Легко видеть, что нет. Пусть пара чисел x_0, y_0 — какое-то решение уравнения $ax + by = c$. Рассмотрим числа $x = x_0 + b \cdot k$ и $y = y_0 - a \cdot k$, где k — некоторое целое число. Подставим их в уравнение. Получим:

$$ax + by = a(x_0 + b \cdot k) + b(y_0 - a \cdot k) = ax_0 + a \cdot b \cdot k + by_0 - a \cdot b \cdot k = ax_0 + by_0 = c.$$

Пример. *Посмотрим на уравнение* $17x - 5y = 3$. *Мы видели, что пара* $x = -2, y = -7$, *является решением уравнения* $17x - 5y = 1$. *Но тогда пара* $x_0 = -6, y_0 = -21$, *является решением уравнения* $17x - 5y = 3$. *Но тогда числа* $x = x_0 + b \cdot k = -6 + (-5) \cdot k$, $y = y_0 - a \cdot k = -21 - 17 \cdot k$, *тоже будут решениями для произвольного целого числа* k. *Т.е. мы получаем пары*

$$x = -6, y = -21 \ (k = 0),$$
$$x = -11, y = -38 \ (k = 1),$$
$$x = -1, y = -4 \ (k = -1)$$

и т.д.

Нашли ли мы теперь все решения уравнения? Оказывается, да.

Теорема. *Пусть пара целых чисел* x_0, y_0 *является решением уравнения* $ax + by = c$, *где* a, b, c *— целые числа и* $(a, b) = 1$. *Тогда произвольное решение имеет вид* $x = x_0 - b \cdot k$, $y = y_0 + a \cdot k$, *где* k *— некоторое целое число.*

Доказательство. Так как пара чисел x_0, y_0 является решением, то верно равенство

$$ax_0 + by_0 = c.$$

Пусть пара чисел x_1, y_1 также является решением, т.е.

$$ax_1 + by_1 = c.$$

Вычтем из первого равенства второе. Получим

$$ax_0 + by_0 - ax_1 - by_1 = c - c,$$

т.е.

$$ax_0 - ax_1 + by_0 - by_1 = 0.$$

Вынося a и b за скобки получаем

$$a(x_0 - x_1) + b(y_0 - y_1) = 0;$$

Перенесем второе слагаемое в правую часть.

$$a(x_0 - x_1) = -b(y_0 - y_1)$$

Мы видим, что $a(x_0 - x_1)$ делится на b. Но так как a и b взаимно простые числа, то это значит, что $x_0 - x_1$ делится на b. Таким образом $x_0 - x_1 = k \cdot b$, для некоторого целого k, т.е. $x_0 - k \cdot b = x_1$ (перенесли x_1 направо, а $k \cdot b$ налево). Но тогда

$$a(x_0 - x_1) = a \cdot k \cdot b = -b(y_0 - y_1).$$

Сократим на b.

$$a \cdot k = -(y_0 - y_1) = -y_0 + y_1;$$

Отсюда $y_1 = y_0 + a \cdot k$ (перенесли y_0 налево). Резюмируя, мы получили, что существует такое целое k, что $x_1 = x_0 - k \cdot b$, а $y_1 = y_0 + k \cdot a$. Что и требовалось.

□

Скажем пару слов о решении линейных диофантовых уравнений с большим количеством неизвестных. Нам понадобится определение.

Определение. *Наибольшим общим делителем совокупности целых чисел $a_1, a_2, \ldots, a_n$ называется такое наибольшее целое число, которое делит все числа $a_1, a_2, a_3, \ldots a_n$.*

Обозначается $(a_1, a_2, a_3, \ldots, a_n)$.

Например, $(6, 10, 15) = 1$.

Теорема. *Рассмотрим уравнение $a_1x_1 + a_2x_2 + a_3x_3 + \ldots + a_nx_n = 1$, где $a_1, a_2, \ldots, a_n$ — целые числа. Тогда оно имеет целочисленное решение (т.е. набор целых чисел $x_1, x_2, \ldots, x_n$, которые удовлетворяют равенству) тогда и только тогда, когда $(a_1, a_2, \ldots, a_n) = 1$.*

Доказательство. Если $(a_1, a_2, \ldots a_n) = d \neq 1$, то при любых целых $x_1, x_2, \ldots, x_n$ выражение $a_1x_1 + a_2x_2 + \ldots + a_nx_n$ делится на d и не может равняться 1. Т.е. в этом случае решений нет.

Докажем, что если $(a_1, a_2, \ldots a_n) = 1$, то решения есть. Сделаем это с помощью индукции по n. В качестве базы индукции возьмем $n = 2$. Этот случай мы уже рассматривали. Докажем шаг индукции. Пусть утверждение верно для $n - 1$, докажем его для n. Пусть $(a_1, a_2, \ldots, a_{n-1}) = d$. Рассмотрим уравнение

$$a_1x_1 + a_2x_2 + \ldots + a_{n-1}x_{n-1} = d.$$

Сократим его на d. Получим уравнение

$$b_1x_1 + b_2x_2 + \ldots + b_{n-1}x_{n-1} = 1,$$

где $b_1 = \frac{a_1}{d}, b_2 = \frac{a_2}{d} \ldots$. По предположению индукции, это уравнение имеет решение пусть это числа $y_1, y_2, \ldots y_{n-1}$. Но тогда эти числа будут и решениями уравнения $a_1x_1 + a_2x_2 + \ldots + a_{n-1}x_{n-1} = d$.

Наибольший общий делитель чисел d и a_n равен 1 (иначе $(a_1, \ldots a_n) \neq 1$). Значит, есть такие целые числа u и v, что $du + a_nv = 1$. При этом $a_1y_1 + a_2y_2 + \ldots a_{n-1}y_{n-1} = d$. Подставляя это выражение для d в предыдущее равенство, получим.

$$(a_1y_1 + a_2y_2 + \ldots + a_{n-1}y_{n-1})u + a_nv = 1.$$

Раскроем скобки.

$$a_1y_1u + a_2y_2u + \ldots + a_{n-1}y_{n-1}u + a_nv = 1.$$

Но это значит, что если взять $x_1 = y_1u, x_2 = y_2u, \ldots, x_{n-1} = y_{n-1}u, x_n = v$, то получим, что

$$a_1x_1 + a_2x_2 + \ldots + a_{n-1}x_{n-1} + a_nx_n = 1.$$

Но это значит, что мы нашли решение. □

Чтобы не перегружать наших юных читателей, вопрос о нахождении всех решений уравнения $a_1x_1 + a_2x_2 + \ldots + a_nx_n = 1$ рассматривать не будем.

7. Сравнения по модулю. Арифметика остатков.

Определение. *Пусть n — натурально число, большее 1. Тогда будем говорить, что целое число a сравнимо с целым числом b по модулю n, если a и b имеют одинаковые остатки при делении на n.*

Обозначают это так: $a \equiv b \ (mod\ n)$ (a сравнимо с b по модулю n). Или $a \equiv b \ (n)$ или $a \equiv_n b$. Иногда, если из контекста понятно о каком n идет речь, пишут просто $a \equiv b$.

Например,

$$27 \equiv 12 \ (mod\ 5), \quad 2193 \equiv_2 12343.$$

Сформулируем пару простых свойств сравнения по модулю. Пусть $a \equiv_n b$ и $c \equiv_n d$. Тогда

1) $a + c \equiv_n b + d$.

2) $a - c \equiv_n b - d$.

3) $a \cdot c \equiv_n b \cdot d$.

4) $a^k \equiv_n b^k$.

Пример. *Какой остаток при делении на 13 имеет число* 27^{100}*? Легко видеть, что* $27 \equiv_{13} 1$. *Значит,* $27^{100} \equiv 1^{100} = 1$. *Т.е.* 27^{100} *имеет остаток 1.*

А какой остаток при делении на 15 дает число 74^{1812}*? Заметим, что* $74 \equiv_{15} -1$. *Действительно,* $74 = 15 \cdot 4 + 14$, *и* $-1 = -15 + 14$. *Поэтому они имеют одинаковые остатки. Значит,* $74^{1812} \equiv (-1)^{1812} = 1$. *Значит, число* 74^{1812} *тоже имеет остаток 1 при делении на 15.*

Найдем остаток при делении на 17 от числа $84^{100!} \cdot 35^{999} + 17001$. *Мы видим, что* $84 \equiv_{17} -1$, *т.е.* $84^{100!} \equiv 1$, *т.к.* $100!$ — *четное число.* $35^{999} \equiv 1^{999} = 1$, *а* $17001 \equiv 1$. *Значит,* $84^{100!} \cdot 35^{999} + 17001 \equiv 1 \cdot 1 + 1 = 2$.

С помощью сравнений можно доказывать признаки делимости.

Теорема. *Число* $\overline{a_n a_{n-1} \dots a_1 a_0}$ *имеет такой же остаток при делении на 3 как и число* $a_n + a_{n-1} + a_{n-2} + \dots + a_1 + a_0$. *В частности, число* $\overline{a_n a_{n-1} \dots a_1 a_0}$ *делится на 3 тогда и только тогда, когда число* $a_n + a_{n-1} + a_{n-2} + \dots + a_1 + a_0$ *делится на 3.*

Доказательство. Заметим, что $10 \equiv_3 1$. Т.е. $10^k \equiv_3 1^k = 1$ для любого натурального k. Поэтому

$$\overline{a_n a_{n-1} \dots a_1 a_0} = 10^n a_n + 10^{n-1} a_{n-1} + 10^{n-2} a_{n-2} + \dots + 10 a_1 + a_0 \equiv_3 a_n + a_{n-1} + a_{n-2} + \dots + a_1 + a_0.$$

□

Аналогично доказывается признак делимости на 9.

Теорема. *Число* $\overline{a_n a_{n-1} \dots a_1 a_0}$ *имеет такой же остаток при делении на 9 как и число* $a_n + a_{n-1} + a_{n-2} + \dots + a_1 + a_0$. *В частности, число* $\overline{a_n a_{n-1} \dots a_1 a_0}$ *делится на 9 тогда и только тогда, когда число* $a_n + a_{n-1} + a_{n-2} + \dots + a_1 + a_0$ *делится на 9.*

Также легко выводится признак делимости на 11.

Теорема. *Число* $\overline{a_n a_{n-1} \dots a_1 a_0}$ *имеет такой же остаток при делении на 11 как и число* $a_0 - a_1 + a_2 - a_3 + \dots (-1)^n a_n$. *В частности, число* $\overline{a_n a_{n-1} \dots a_1 a_0}$ *делится на 11 тогда и только тогда, когда число* $a_0 - a_1 + a_2 - a_3 + \dots (-1)^n a_n$ *делится на 11.*

Доказательство. Заметим, что $10 \equiv_{11} -1$. Т.е. $10^k \equiv (-1)^k$, для любого натурального k. Поэтому

$$\overline{a_n a_{n-1} \dots a_1 a_0} = a_0 + 10 a_1 + 10^2 a_2 + 10^3 a_3 + \dots + 10^n a_n \equiv_{11} a_0 - a_1 + a_2 - a_3 + \dots + (-1)^n a_n.$$

□

Из-за того, что $10 \equiv_7 3$ такого же простого признака делимости как на 3, 9 или 11 не получается. Но заметим, что $1001 = 7 \cdot 13 \cdot 11$. Поэтому $1000 = 1001 - 1 \equiv_7 -1$. Поэтому для произвольного числа $\overline{a_n a_{n-1} \dots a_1 a_0}$ мы получаем:

$$\overline{a_n \dots a_3 a_2 a_1 a_0} = \overline{a_2 a_1 a_0} + 1000 \cdot \overline{a_5 a_4 a_3} + 1000^2 \cdot \overline{a_8 a_7 a_6} + \dots \equiv_7 \overline{a_2 a_1 a_0} - \overline{a_5 a_4 a_3} + \overline{a_8 a_7 a_6} - \dots$$

Отсюда получаем признак делимости на 7.

Теорема. *Число $\overline{a_n \dots a_3 a_2 a_1 a_0}$ имеет такой же остаток при делении на 7 как и число $\overline{a_2 a_1 a_0} - \overline{a_5 a_4 a_3} + \overline{a_8 a_7 a_6} - \dots$. В частности, $\overline{a_n \dots a_3 a_2 a_1 a_0}$ делится на 7 тогда и только тогда, когда $\overline{a_2 a_1 a_0} - \overline{a_5 a_4 a_3} + \overline{a_8 a_7 a_6} - \dots$ делится на 7.*

Пример. *Найдем остаток от деления на 7 числа 9245384. Мы имеем:*

$$9245384 \equiv_7 384 - 245 + 9 = 148 = 7 \cdot 20 + 1 \equiv_7 1.$$

Но можно подойти к этому вопросу с другой стороны. Как отмечалось выше, $10 \equiv_7 3$. Поэтому справедливо следующее:

$$\overline{a_n a_{n-1} \dots a_1 a_0} = 10 \cdot \overline{a_n a_{n-1} \dots a_1} + a_0 \equiv_7 3 \cdot \overline{a_n a_{n-1} \dots a_1} + a_0.$$

В принципе, мы получили еще один признак делимости на 7. Число $\overline{a_n a_{n-1} \dots a_1 a_0}$ делится на 7 тогда и только тогда, когда $3 \cdot \overline{a_n a_{n-1} \dots a_1} + a_0$ делится на 7. Однако легко видеть, что этот признак неудобен. Чтобы им пользоваться, приходится умножать порой достаточно большие числа на 3. Можно ли от этого избавиться? Мы хотим выяснить, когда имеет место равенство:

$$3 \cdot \overline{a_n a_{n-1} \dots a_1} + a_0 \equiv_7 0.$$

Для этого заметим, что $3 \cdot 5 = 15 \equiv_7 1$. А значит, если мы умножим все сравнение на 5, то получим

$$5 \cdot 3 \cdot \overline{a_n a_{n-1} \dots a_1} + 5 \cdot a_0 \equiv_7 \overline{a_n a_{n-1} \dots a_1} - 2 \cdot a_0 \equiv_7 0$$

(Здесь мы воспользовались тем, что $5 \equiv_7 -2$.) Таким образом мы получили теорему.

Теорема. *Число делится на 7 тогда и только тогда, когда $\overline{a_n a_{n-1} \dots a_1} - 2 \cdot a_0$ делится на 7.*

При этом стоит отметить, что остатки от деления на 7 у чисел $\overline{a_n a_{n-1} \dots a_0}$ и $\overline{a_n a_{n-1} \dots a_1} - 2 \cdot a_0$ могут не совпадать.

Пример. *Выясним делится ли на 7 число 896. Для этого посмотрим на число $89 - 2 \cdot 6 = 89 - 12 = 77$. Очевидно, что оно делится на 7. Значит, и число 896 делится на 7.*

Давайте на остаток от деления на 7 числа 271. Нехитрые вычисления показывают, что $271 = 266 + 5 = 7 \cdot 38 + 5$. Однако число $27 - 2 = 25$ имеет остаток 4 при делении на 7.

Когда мы выводили признак делимости на 7, мы воспользовались тем, что для числа 3 нашлось число 5 такое, что $3 \cdot 5 \equiv_7 1$. В каких случаях такие числа можно найти?

Чтобы ответить на этот вопрос, давайте определим операции сложения и умножения на множестве остатков при делении на некоторое целое число n.

Пусть r_1, r_2 — остатки при делении на число n. Тогда суммой остатков $r_1 + r_2$ называется такой остаток r_3, что $r_1 + r_2 \equiv_n r_3$, а произведением остатков r_1 и r_2 называется такой остаток r_4, что $r_1 \cdot r_2 \equiv_n r_4$. Ниже приведены таблицы сложения и умножения по модулю 6.

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Таблица сложения по модулю 6

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Таблица умножения по модулю 6

Таблица сложения устроена просто. В первой строчки там стоят числа $0, 1, 2 \dots 6$ подряд. Вторая строчка отличается от первой сдвигом на одну клеточку налево. Третья отличается от второй еще одним сдвигом налево, и и.д.

Таблица умножения устроена сложнее. Мы видим, что не в каждой строчке встречаются все возможные остатки. В частности, в строках, соответствующих 2, 3, 4 нету единицы. Почему? Это можно легко объяснить. Если произведение чисел $a \cdot b$ имеет остаток 1 при делении на 6, что числа a и b должны быть взаимно простыми с шестью. Но 2, 3, 4 имеют общие делители с 6. Оказывается, верна следующая теорема.

Теорема. *Пусть n — натуральное число, а число a — целое. Тогда существует такое целое число b, что $a \cdot b \equiv_n 1$ тогда и только тогда, когда $(a, n) = 1$.*

Доказательство. Из алгоритма Евклида следует, что $(a, n) = 1$ тогда и только тогда, когда существуют такие целые числа u, v, что $a \cdot u + n \cdot v = 1$. Но это эквивалентно тому, что $a \cdot u \equiv_n 1$. □

Благодаря этой теорем можно легко решать линейные уравнения по модулю некоторого числа. Пусть мы хотим найти все такие x, что $a \cdot x + c \equiv_n 0$, причем $(a, n) = 1$. Тогда мы находим такое число b, что $a \cdot b \equiv_n 1$. Умножим левую и правую часть нашего сравнения на b. Получим:

$$b \cdot a \cdot x + b \cdot c \equiv_n 0$$

Отсюда получаем:

$$x + b \cdot c \equiv_n 0,$$

т.е.

$$x \equiv -b \cdot c.$$

Значит, $x = -b \cdot c + k \cdot n$, где k — произвольное целое число.

Пример. *Давайте решим сравнение $5x - 3 \equiv_7 0$. Получаем $5x \equiv 3$. Заметим, что $5 \cdot 3 \equiv 1$. Поэтому, домножив левую и правую часть сравнения на 3, получим $x \equiv 3 \cdot 3 \equiv 2$.*

8. Малая теорема Ферма

Теорема. *Пусть p — простое число, и пусть x не делится на p. Тогда $x^{p-1} \equiv_p 1$.*

Перед тем как доказывать теорему, докажем лемму о колоде карт.

Лемма. *Пусть $(a, n) = 1$. Тогда числа $a, 2a, 3a, \dots, (n-1)a, na$ имеют различные остатки при делении на n.*

Доказательство. Предположим, что это не так. Т.е. у каких-то двух чисел ia и ja одинаковые остатки (i, j — целые числа, можно считать, что $i > j$). Тогда $ia \equiv_n ja$. Это равносильно тому, что $ia - ja \equiv 0$, т.е. $(i-j)a \equiv 0$. Так как a взаимно просто с n, то это означает, что $i - j$ должно делится на n. Но $0 < i - j < n$. Противоречие. □

Отметим еще, что так как в наборе чисел $a, 2a, 3a, \ldots na$ ровно n чисел, а всевозможных остатков при делении на n тоже n, то среди чисел $a, 2a, \ldots na$ встречаются все остатки при делении на n. Но так как na очевидно имеет остаток 0 при делении на n, то в наборе чисел $a, 2a, \ldots (n-1)a$ встречаются все ненулевые остатки при делении на n.

Теперь докажем саму теорему.

Доказательство. Так как x не делится на p, и $(x, p) = 1$, то среди чисел $x, 2x, \ldots, (p-1)x$ встречаются все ненулевые остатки при делении на p. Поэтому произведение

$$x \cdot 2x \cdot 3x \ldots (p-1)x$$

сравнимо с произведением

$$1 \cdot 2 \cdot 3 \ldots (p-1).$$

Поэтому имеем:

$$x \cdot 2x \cdot 3x \ldots (p-1)x \equiv x^{p-1} \cdot (p-1)! \equiv (p-1)!.$$

Заметим, что число $(p-1)!$ не делится на p. Поэтому в последнем сравнении на него можно сократить. Получим:

$$x^{p-1} \equiv 1.$$

Что и требовалось. □