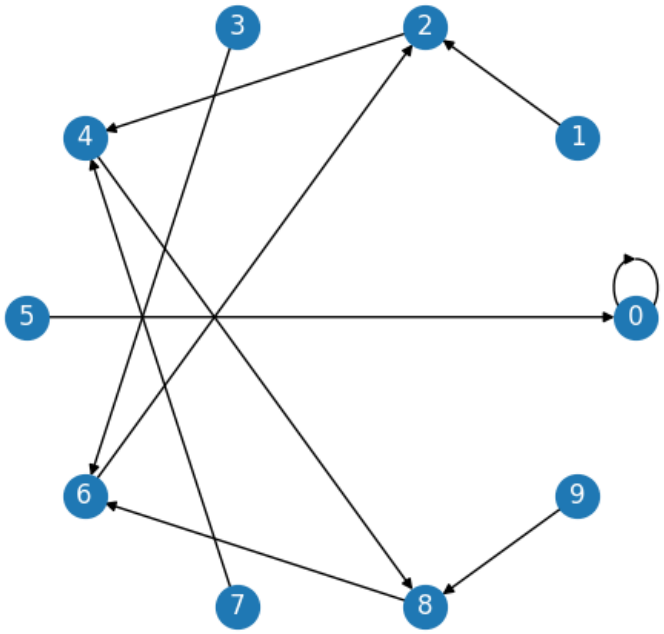
9. Малая теорема Ферма

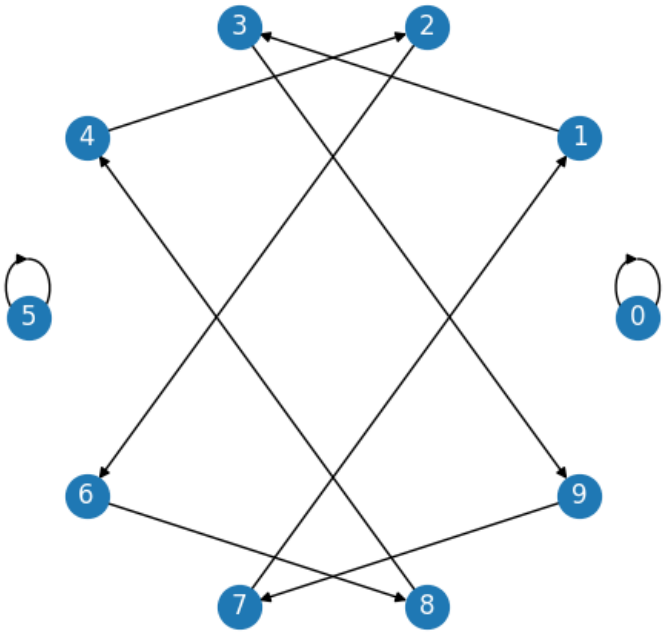
Мы уже обращали внимание на то, что последние цифры степеней двойки (и вообще любого числа) с какого-то момента повторяются по циклу: 1, 2, 4, 8, 6, 2, 4, 8, 6, 2, 4, 8, 6 ... (первая единица в цикл не входит, а дальше повторения по четыре). Сейчас мы посмотрим на это подробнее, для чего нарисуем схему переходов.



На этой схеме из каждого остатка по модулю 10 идёт стрелка, соответствующая умножению его на 2 (по модулю 10)

9.1 Найдите на этой картинке упомянутый цикл.

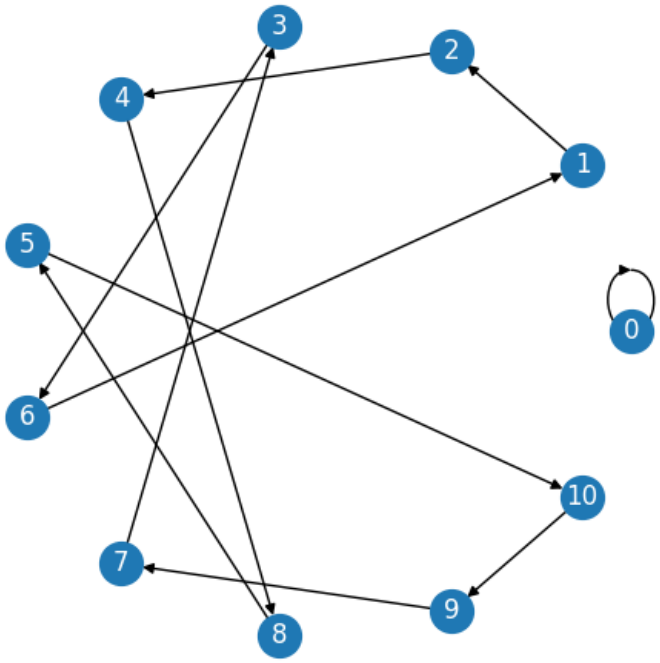
▷ Надо пройти по стрелкам, начиная с 1. ◁



9.2 Сколько циклов и какой длины есть в графе умножения остатков по модулю 10 на 3 на рисунке? Как будут меняться последние цифры степеней тройки?

▷ Видны два цикла длины 1 (если число кончается на 0 или на 5, то умножение на 3 не меняет последней цифры) и два цикла длины 4. Один из них соответствует последним цифрам степеней тройки: 1, 3, 9, 7, 1, 3, 9, 7, 1 ... и далее по циклу. ◁

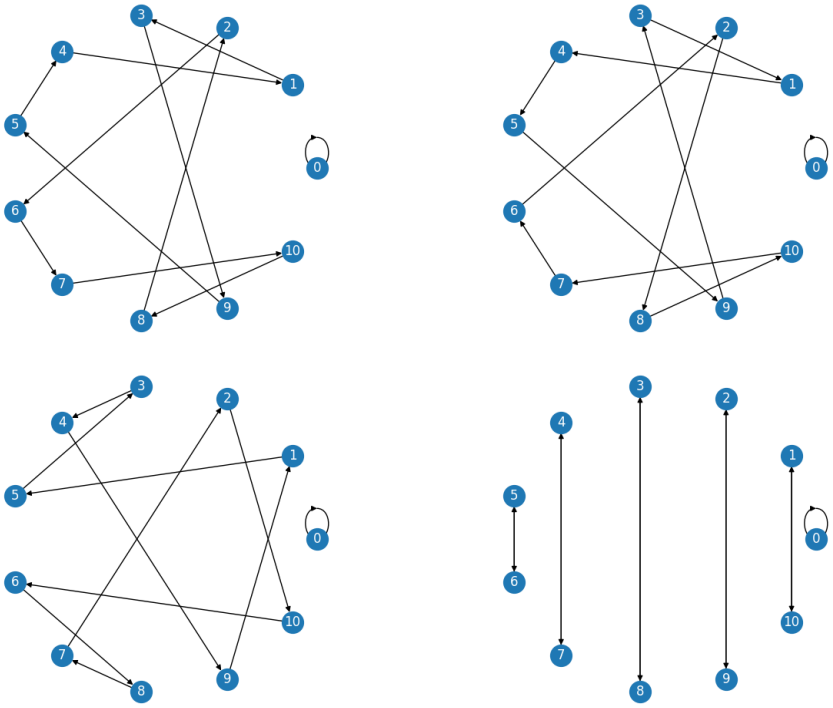
Мы уже обсуждали, что простые модули ведут себя более регулярно (все остатки, кроме нуля, обратимы, можно сокращать и т.п.). Вот один из графов умножения для простого модуля 11.



9.3 На что мы умножаем на этом рисунке? Какой будет период в последовательности остатков? Найдите $2^{179} \bmod 11$, глядя на эту картинку.

▷ Чтобы узнать, на что мы умножаем, надо посмотреть, куда переходит стрелка из 1, так что умножаем мы на 2. Там получается один цикл длины 10 (помимо цикла длины 1 из одного нуля, который есть всегда), так что 2^{180} по модулю 11 равно $2^0 = 1$, а 2^{179} будет предыдущим по циклу, то есть 6. ◁

По тому же модулю 11 можно нарисовать графы умножения на другие числа (слева направо множители 3 и 4 в верхнем ряду, 5 и 10 в нижнем).



9.4 Рассматривая эти картинки, можно заметить некоторые закономерности и понять, отчего так получается. Почему, скажем, две верхние картинки так похожи друг на друга (надо присмотреться, чтобы заметить, что стрелки ведут в противоположные стороны)? Почему последняя картинка состоит из отрезков (циклов длины 2, туда-сюда?

▷ Если сначала умножить на 3, а потом на 4 (или в другом порядке), то мы умножим на $12 \equiv 1 \pmod 1$1, то есть вернёмся в исходную точку. Поэтому стрелки обратны.

Умножая на 10, мы всё равно что умножаем на -1 (поскольку $-1 \equiv 10 \pmod 1$)1, а второе умножение на -1 возвращает в исходную точку. ◁

Теперь докажем некоторые общие свойства графов умножения на данное a по простому модулю p.

9.5 Докажите, что из каждой вершины выходит одна стрелка и в каждую вершину входит одна стрелка.

▷ То, что выходит одна стрелка, доказывать не требуется — так мы рисовали стрелки (из x ведёт стрелка в ax и только). А вот то, что в каждое y входит ровно одна стрелка, надо доказать. Другими словами, надо

доказать, что для любого y (и любого простого p и любого a, не равного 0 по модулю p уравнение $ax \equiv y$ (относительно x) имеет единственное решение. А это мы уже видели (умножая слева на обратный элемент a^{-1}, мы получаем, что $x = a^{-1}y$). ◁

9.6 Покажите, что стрелки разбиваются на несколько циклов.

• Стрелка, ведущая из вершину в неё саму же, считается циклом длины 1 (из одной вершины).

▷ Это следует из предыдущей задачи. Пойдём по стрелкам — рано или поздно мы должны попасть в вершину, где уже были. Но это может быть только начальная вершина (потому что иначе в неё будет две стрелки: одна уже нарисована ранее, одна новая. Значит, цикл замкнётся (и эти вершины уже больше ни с кем не связаны, так как все выходящие и входящие стрелки есть). ◁

9.7 У нас был граф умножения на 2 по модулю 10, и там вершина 1 не входила в цикл. Не противоречит ли это утверждению предыдущей задачи? Где не проходят наши рассуждения?

▷ Нет, потому что 2 не взаимно просто с 10 и не имеет обратного, поэтому в вершину могут входить несколько стрелок (скажем, в вершину 2 входят стрелки из 1 и 6). ◁

9.8 Покажите, что для простого модуля p в графе умножения на $a \neq 0 \pmod p$ все циклы имеют одинаковую длину (кроме тривиального цикла из одного нуля)

▷ Для этого полезно записать элементы цикла, начинающиеся с какого-то $b \neq 0$, с помощью формулы:

$$b \to ba \to ba^2 \to ba^3 \to \ldots$$

Цикл зациклится, когда мы дойдём (впервые) до $ba^m = b$. При каком m это случится? Можно сократить на b (умножить на обратный к b) и увидеть, что нам нужно минимальное m, при котором $a^m = 1$ (точнее следовало бы написать $a^m \equiv 1 \pmod p$, поскольку равенство и умножение понимаются по модулю p). А это m не зависит от b, так что все циклы одинаковы. ◁

Минимальное m, для которого $a^m \equiv 1 \pmod p$ (при простом p и $a \not\equiv 0 \pmod p$), называется *порядком* элемента a по модулю p.

Теперь всё готово для доказательства *малой теоремы Ферма*.

9.9 Докажите, что если p — простое число и $a \not\equiv 0 \pmod{p}$, то $x^{p-1} \equiv 1 \pmod{p}$.

▷ Мы знаем, что граф умножения на a без нуля разбивается на циклы одинаковой длины, равной порядку m элемента a. Значит, $p-1$ (общее число элементов в циклах) делится на m (длину цикла). Поскольку $a^m \equiv 1$ и $p-1$ кратно m. то и $a^{p-1} \equiv 1 \pmod{p}$. ◁

▷ Это тот же самый Ферма, что и с $x^n + y^n \neq z^n$, но теорема другая («малая», а не «последняя» или «великая») — и тут Ферма, возможно, действительно знал доказательство, хотя и не опубликовал: в его письме от 1640 года говорится, что он мог бы послать доказательство, если не бы не опасался быть многословным. Доказательство было опубликовано Эйлером в 1736 году (почти что через сто лет). ◁

Умножив равенство $a^{p-1} \equiv 1 \pmod{p}$ ещё раз на a, мы замечаем, что $a^p \equiv a \pmod{p}$. Теперь оговорку про то, что a не делится на p, можно убрать (потому что для этого случая равенство верно по очевидным причинам), и мы можем сформулировать малую теорему Ферма так: *для любого простого p и для любого целого a разность $a^p - a$ делится на p.*

- Для этого утверждения можно предложить и другие доказательства.

9.10* Пусть p — простое число и $a \not\equiv 0 \pmod{p}$. Докажите, что произведение $A = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1)$ по модулю p

(а) умножится на a^{p-1} и

(б) не изменится,

если все сомножители умножить на a, и выведите отсюда малую теорему Ферма.

▷ Первая часть очевидна (надо просто сгруппировать все множители a в начале). Вторая следует из того, что при такой замене (x на ax) мы пройдём из всех вершин по стрелкам, и по-прежнему останется произведение всех ненулевых остатков, хотя и в другом порядке. Ведь в каждую вершину входит ровно одна стрелка. Поскольку $a^{p-1}A \equiv A \pmod{p}$, то можно сократить на A (заметим, что A не равно нулю по модулю p как произведение ненулевых элемнетов) и получить $a^{p-1} \equiv 1 \pmod{p}$. ◁

В предыдущей задаче мы доказали теорему Ферма, но так и не узнали, чему равно это самое $A \equiv (p-1)! \pmod{p}$. На этот вопрос отвечает *теорема Вильсона*: при простых p выполнено сравнение $(p-1)! \equiv -1 \pmod{p}$. Другими словами, *при простых p число $(p-1)!+1$ делится на p.*

9.11* Докажите теорему Вильсона.

▷ Разобьём все ненулевые остатки по модулю p на пары, объединив остаток с обратным, то есть включив в одну пару x, y, если $xy = 1$. Есть два остатка, обратных самому себе (1 и $-1 = p-1$), они так и останутся без пары, а остальные сомножите, сгруппировавшись в пары, дадут -1, что и требовалось доказать.

Видите пробел в этом рассуждении? Сгруппировать в пары можно (обратный единственный, поэтому каждый элемент войдёт только в одну пару), но почему только два элемента обратны самому себе? Вдруг найдётся ещё какой-то x, для которого $x^2 = 1$ по модулю p? Но тогда $x^2 - 1 = (x-1)(x+1)$ делится на p, так что одна из скобок должна делиться на p. Отсюда видно, что других таких нет, и доказательство завершается.

Ещё одна поправка: если $p = 2$, то 1 и -1 это один и тот же остаток, так что нельзя сказать, что непарных остатков 2. Но и в этом случае $(2-1)! + 1 = 2$ делится на 2. ◁

▷ Видимо, формулировка этого утверждения известна давно (похоже, что её знал уже Ибн аль-Хайсам, X–XI век), а доказательство предложил Лагранж в 1771. Так что Вильсон, кажется, тут скорее не по делу (возможно, он переоткрыл её формулировку). ◁

9.12* Покажите, что для любого составного p утверждение теоремы Вильсона неверно.

▷ Пусть q — простой делитель p. Тогда q входит в произведение для $(p-1)!$, поэтому $(p-1)!$ делится на q, а $(p-1)! + 1$ даёт остаток 1 при делении на q и не делится на q (и тем более на p). ◁

Вот ещё два доказательства малой теоремы Ферма, правда, использующие некоторые сведения из комбинаторики.

9.13* При простом p и любых целых a и b выполнено такое утверждение:

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

Выведите из него малую теорему Ферма.

▷ Вывести можно так: $(a+b+c)^p \equiv ((a+b)^p + c^p) \equiv a^p + b^p + c^p$, и аналогично для большего числа слагаемых. Поэтому и $(1+1+\ldots 1)^p \equiv 1^p + 1^p + \ldots + 1^p \pmod{p}$ при любом числе m слагаемых, поэтому $m^p \equiv m \pmod{p}$ (второй вариант формулировки теоремы).

А само утверждение следует из того, что все биномиальные коэффициенты $C_p^i = \frac{p!}{i!(p-i)!}$ содержат p в числителе, но не в знаменателе, поэтому после сокращения общих простых множителей p останется. ◁

▷ Отображение $x \mapsto x^p$ называют *гомоморфизмом Фробениуса* (для полей характеристики p). ◁

9.14* Пусть есть n разных букв. Мы их пишем (одну букву можно использовать и несколько раз, и вообще не использовать) в вершинах правильного p-угольника разными способами, причём не различаем способы, отличающиеся лишь поворотом. Покажите, что число разных способов равно $n + (n^p - n)/p$. Выведите отсюда теорему Ферма.

▷ Если бы вращать не разрешалось, то было бы n^p вариантов. Объединим варианты, отличающиеся вращениями, в одну группу. Будет n групп по одному варианту (во всех вершинах одна буква), а остальные группы будут по p вариантов (многоугольник можно повернуть p способами), откуда и получается ответ.

Видите пробел в этом рассуждении? Где мы использовали, скажем, что p простое? Надо проверить, что если использованы две разные буквы, то никакой поворот не переводит многоугольник в себя. Если бы переводил, то можно было бы его повторять, пока не получится поворот на одну вершину (поскольку по простому модулю всякий ненулевой остаток обратим).

Теорема Ферма вытекает из этого подсчёта, потому что число вариантов целое. ◁

• С помощью теоремы Ферма можно доказать, что некоторое число составное. Например, 12 составное, потому что $5^{11} \bmod 12 = 5$ (а не 1, как должно быть по теореме Ферма, будь 12 простым). Это выглядит глупо — мы доказываем очевидное с помощью неочевидного, но как ни странно, это имеет некоторый смысл. А именно, для больших чисел это может быть сильно проще, чем разлагать на множители. Скажем, можно проверить, что для $n = 2^{512}+1$ и $a = 3$ теорема Ферма не выполнена: используя домашний компьютер и несложную программу, можно почти мгновенно понять, что $a^{n-1} \bmod n$ равно

13387457852131866017809974335626508736765841341908171621341620739066502578 7-
93457441078230804865246011339933833061458906559278633032869468345609327807927612

(число разбито на две строки), так что $n = 2^{512} + 1$ составное, но чтобы разложить n на множители, домашнего компьютера может и не хватить. (А некоторые составные — по теореме Ферма — числа вообще никто раскладывать на множители не умеет.) На разнице между сложностью задач проверки простоты и разложения на множители основана вычислительная криптография.

Числа $2^1+1, 2^2+1, 2^4+1, 2^8+1, 2^{16}+1, 2^{32}+1$,... называются «числами Ферма». Он предположил, что они все простые, посмотрев на первые пять — но Эйлер обнаружил делитель 641 для числа $2^{32} + 1$, так что это число составное, Ферма ошибся. Пока что других простых чисел Ферма, кроме этих пяти, не обнаружено,

и вообще мало что известно. Бесконечно ли много простых среди чисел Ферма? Бесконечно ли много составных? Эти вопросы остаются открытыми.

Теорема Ферма касается простых модулей, но аналогичное утверждение есть и для составных; его называют *теоремой Эйлера*. Рассуждения остаются почти без изменений, но нужно рассматривать не все остатки по данному модулю n, а только взаимно простые с n. Вспомним их основные свойства.

9.15 (а) Докажите, что если $a \equiv b \pmod{n}$, то $\text{НОД}(a,n) = \text{НОД}(b,n)$. В частности, взамная простота с n определяется остатком по модулю m. (б) Докажите, что остаток a взаимно прост с модулем n тогда и только тогда, когда он обратим по модулю n (и в этом случае обратный тоже взаимно прост с n). (в) Докажите, что произведение двух взаимно простых с n остатков (по модулю n) взаимно просто с n.

▷ (а) Это мы знаем ещё из алгоритма Евклида: добавление кратного n не меняет наибольшего общего делителя с n. (б) Обратный к a остаток x по модулю n можно найти, решая уравнение $ax+ny=1$. Наоборот, если $ax \equiv 1 \pmod{n}$, то $ax+ny=1$ для некоторого n, поэтому a и n взаимно просты. (в) Мы знаем, что произведение двух чисел, взаимно простых с n, тоже взаимно просто с n (например, потому, что ни в том, ни в другом нет общих множителей с n). Можно заметить также, что произведение двух обратимых элементов обратимо (и обратным будет произведение обратных). ◁

Число остатков по модулю n, взаимно простых с n, называют *функцией Эйлера* от n и обозначают $\varphi(n)$.

9.16 Чему равно $\varphi(p)$ для простого p? Чему равно $\varphi(p^k)$ для степени простого числа p?

▷ В обоих случаях надо считать остатки (от 0 до $p-1$ или от 0 до p^k-1), не делящиеся на p (взаимно просты с p те числа, которые не делятся на p). Другими словами нужно пропускать каждое p-е число, начиная с нуля. В первом случае пропускается только 0, во втором случае $p^k/p = p^{k-1}$ чисел, остаётся $\varphi(p) = p-1$ и $\varphi(p^k) = p^k - p^{k-1}$ взаимно простых остатков. ◁

Теперь у нас всё готово для теоремы Эйлера.

9.17 Докажите теорему Эйлера: если остаток a взаимно прост с модулем n, то $a^{\varphi(n)} \equiv 1 \pmod{n}$.

• Если n простое, то все остатки, кроме нуля, с ним взаимно просты, а $\varphi(n) = n - 1$, так что получается в точности малая теорема Ферма.

▷ Нарисуем граф умножения на a по модулю n, но оставим в нём из вершин только взаимно простые с n. По-прежнему из каждой вершины ведёт по стрелке (потому что при умножении на a взаимная простота сохраняется, см. задачу 15). Остатки обратимы, поэтому решать уравнение $ax \equiv b \pmod{n}$ можно умножением на обратный. Значит, в каждую вершину входит только одна стрелка, и стрелки разбиваются на циклы. Как и раньше, цикл, начинающийся с b, имеет вид $b \to ba \to ba^2 \to \ldots$, и замыкается, когда $a^m = 1$ (здесь мы снова должны сослаться на обратимость), поэтому все циклы равной длины. Общее число вершин теперь $\varphi(n)$, поэтому $\varphi(n)$ делится на длину цикла, откуда и следует требуемое утверждение. ◁

9.18* Сколько решений имеет сравнение $x^2 \equiv 1 \pmod{pq}$, если p и q — различные простые числа? Найдите все решения при $p = 7$, $q = 5$.

▷ По китайской теореме об остатках нам надо искать отдельно решения этого сравнения по модулю p и по модулю q. Для простых модулей мы уже видели, что решений два: 1 и -1. (Если $x^2 - 1$ делится на p, то $(x-1)(x+1)$ делится на p.) Теперь два решения по одному модулю надо комбинировать с двумя решениями по другому модулю. Например, при $pq = 35$ получатся не только комбинации 1 и $-1 \equiv 34$, но и остаток x, для которого $x \equiv 1 \pmod{5}$ и $x \equiv -1 \pmod{7}$, то есть $x \equiv 6 \pmod{35}$, а также другой остаток x, для которого $x \equiv -1 \pmod{5}$ и $x \equiv 1 \pmod{7}$, то есть $x \equiv 29 \pmod{35}$. ◁

9.19* Докажите, что функция Эйлера мультипликативна: если m и n взаимно просты, то $\varphi(mn) = \varphi(m)\varphi(n)$.

▷ Тут полезна китайская теорема об остатках. Каждому остатку по модулю mn соответствует пара остатков: по модулю m и по модулю n, и наоборот (китайская теорема об остатках). При этом взаимно простым с mn остаткам соответствуют пары, в которых остатки взаимно просты с m и n соответственно: число не имеет общих делителей с mn тогда и только тогда, когда у него нет общих делителей ни с m, ни с n. А таких пар будет $\varphi(m)\varphi(n)$. ◁

Это рассуждение годится при $m, n > 1$. Вообще $\varphi(1)$ это некоторый особый случай, и мы положим $\varphi(1) = 1$ — для того, в частности, чтобы предыдущая задача была верна при всех m, n, включая 1.

9.20* Покажите, что для любого числа $n > 2$ выполняется тождество $\sum_{d|n} \varphi(d) = n$ (где сумма берётся по всем делителям числа n).

• Например, $\varphi(1) + \varphi(2) + \varphi(3) + \varphi(6) = 1 + 1 + 2 + 2 = 6$. А для простого p мы получаем $\varphi(1) + \varphi(p) = 1 + (p - 1) = p$. Напомним, что мы считаем $\varphi(1)$ равным 1.

▷ Все остатки по модулю n можно разбить на группы, объединив в одну группу те, у которых равный наибольший общий делитель с n. Например, одну группу образуют остатки, взаимно простые с n, и в этой группе по определению $\varphi(n)$ остатков.

А сколько будет остатков x (будем считать, от 0 до $n - 1$), для которых НОД $(x, n) = 2$? Если n нечётно, то их совсем не будет. А если n чётно (и равно $2m$ при $m = n/2$)? Тогда эти остатки равны $2y$, где $0 \leqslant k < m$. Для всех таких $2y$ число 2 будет общим делителем с m, но не обязательно наибольшим: мы знаем, что НОД $(2y, 2m) = 2$ НОД (y, m), и поэтому нам нужны только те, для которых НОД $(y, m) = 1$. А их будет $\varphi(m)$.

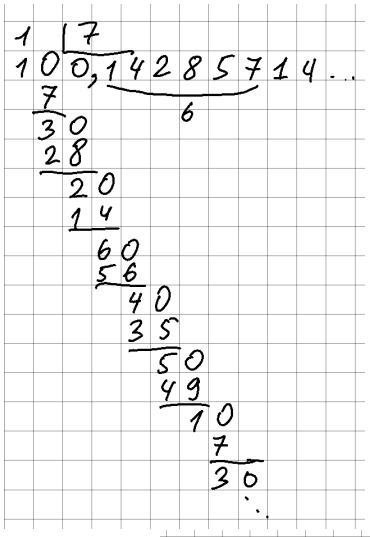
Аналогичное рассуждение показывает, что остатков x по модулю n, для которых НОД $(x, n) = d$,

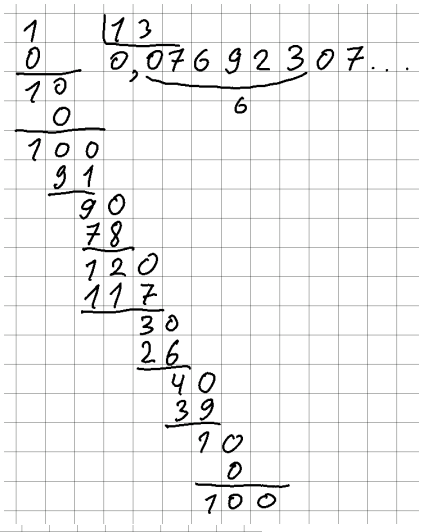
- ровно $\varphi(n/d)$, если d делит n;
- не существует, если d не делит n.

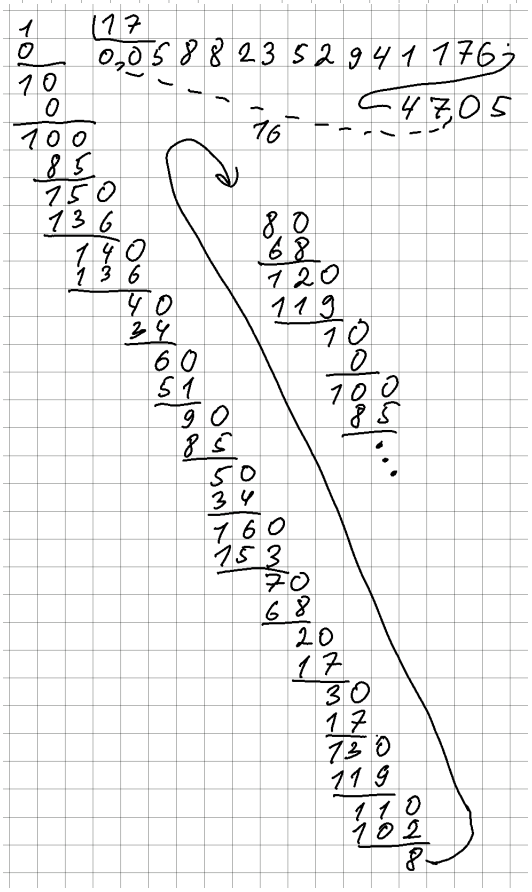
(Тут надо отдельно проверить случай $d = n$, потому что $\phi(1)$ определялось особо, но там ровно один остаток 0 годится.)

Осталось записать утверждение о том, что общее число остатков во всех группах равно n. ◁

С распространением калькуляторов благородное искусство деления уголком постепенно утрачивается, но когда-то оно было одним из базовых навыков в курсе арифметики. С его помощью можно было получать результат деления в виде бесконечной десятичной дроби.







9.21* Каким образом выполняется деление с остатком? Почему при делении целых чисел получается всегда периодическая дробь? Докажите, что в дроби $1/p$, где p — простое число, период начинается с самого начала (сразу после нуля), а длина этого периода является делителем $p-1$.

• В наших примерах 6 делит $7-1$ (для 1/7), а также 6 делит $13-1$ (для 1/13), наконец, 16 делит $17-1$ (для 1/17).

▷ Глядя на примеры, мы видим, что происходит вот что. Текущий остаток (под горизонтальной чертой, вначале 1) умножается на 10 (приписывается нуль). Затем полученное число делится на p (делитель, он справа в уголке), неполное частное добавляется к дроби, а с остатком процесс повторяется.

Ясно, что все остатки не больше делителя, так что их конечное число, и они должны начать повторяться. Как только повторится остаток, всё дальнейшее тоже повторится. Значит, получается периодическая дробь (в которой какая-то группа цифр повторяется вновь и вновь). Не обязательно эта группа начинается с нуля: например, $1/6 = 0{,}16666\ldots$.

Но если делитель — простое число, то период начинается с самого начала. Почему? Можно заметить, остаток каждый раз умножается на 10 по модулю p, поэтому движение будет по циклу в графе умножения на 10 по модулю p. Мы знаем, что для простого модуля все вершины разбиваются на циклы одинаковой длины, и длина эта является делителем $p-1$, и одновременно периодом нашей десятичной дроби.

Остаётся один последний вопрос: может быть, у дроби есть и меньший период? Ведь цифры в частном могут повториться, даже если остатки не повторяются. (Например, в 1/17 период равен 16, и многие цифры входят несколько раз — иногда даже подряд.) Тут можно сослаться на то, что у любой последовательности символов длина *наименьшего* периода является делителем длины любого периода (иначе разделим с остатком, и остаток будет меньше — а периоды тоже образуют идеал). Поэтому, даже если бы период в частном был бы меньше периода в остатках, то он был бы его делителем и ничего бы не нарушилось. Но на самом деле период в частном и период в остатках одинаковы. Проще всего (хотя и не вполне строго) это объяснить так: дробь с какого-то места является десятичным представлением соответствующего остатка, делённого на p, и если с двух мест дроби одинаковы, то и остатки одинаковы. ◁

9.22* Пусть p — простое число. Сумму дробей

$$\frac{1}{1}+\frac{1}{2}+\ldots+\frac{1}{p-1}$$

привели к общему знаменателю. Докажите, что числитель полученной дроби делится на p.

- Например, при $p = 5$ получается

$$\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\frac{1}{4} = \frac{2\cdot 3\cdot 4 + 1\cdot 3\cdot 4 + 1\cdot 2\cdot 4 + 1\cdot 2\cdot 3}{1\cdot 2\cdot 3\cdot 4} = \frac{24+12+8+6}{24} = \frac{50}{24} = \frac{25}{12},$$

и 25 делится на 5.

▷ Посмотрим на вычисления, сделанные при приведении к общему знаменателю. Мы умножаем числители и знаменатели дробей на ненулевые выражения (как в обычном смысле, так и по модулю p), потом их складываем, потом сокращаем на ненулевые выражения (ненулевые, поскольку в знаменателе нет кратных p). Поэтому на это можно смотреть как на корректное вычисление в остатках по модулю p. Слева получится сумма всех обратных величин к ненулевым остаткам, то есть сумма всех ненулевых остатков, которые группируются на пары, в сумме равные нулю (1 и $p-1$, 2 и $p-2$ и так далее; заметим, что $p-1$ чётное число). Поэтому и правая часть равна 0, то есть числитель дроби равен нулю по модулю p, что и требовалось доказать. ◁