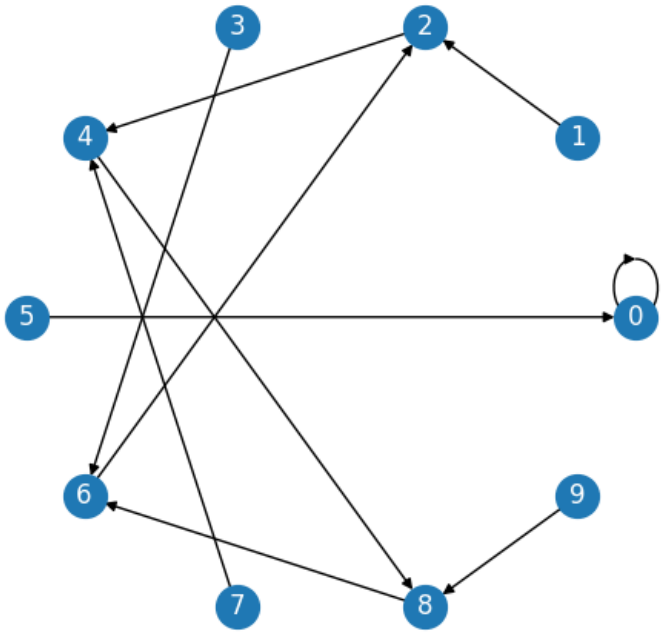
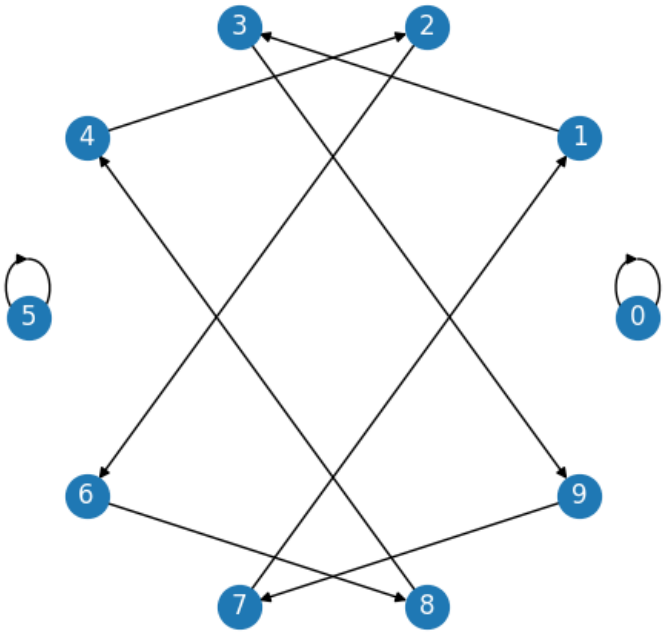
9. Малая теорема Ферма

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.



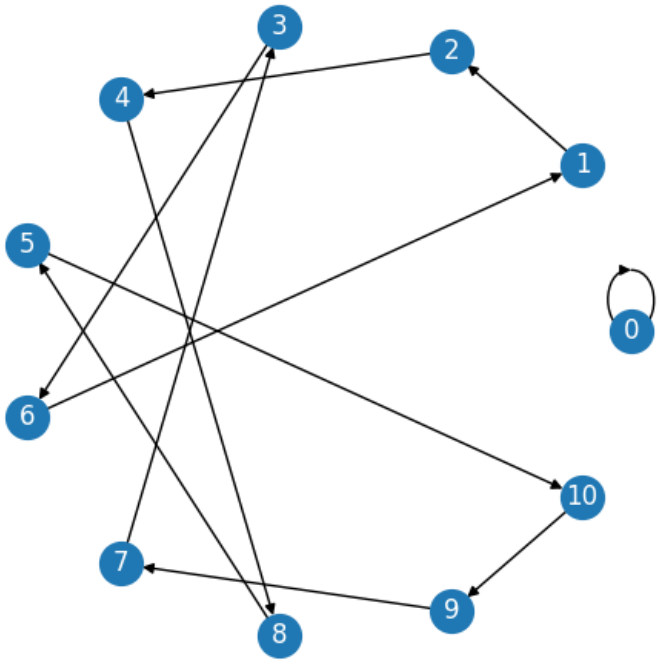
На этой схеме из каждого остатка по модулю 10 идёт стрелка, соответствующая умножению его на 2 (по модулю 10)

9.1 Найдите на этой картинке упомянутый цикл.



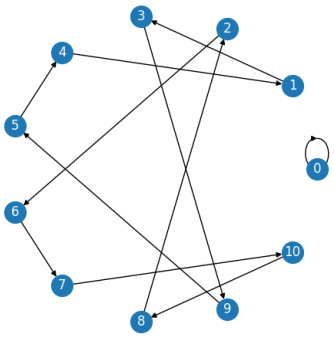
9.2 Сколько циклов и какой длины есть в графе умножения остатков по модулю 10 на 3 на рисунке? Как будут меняться последние цифры степеней тройки?

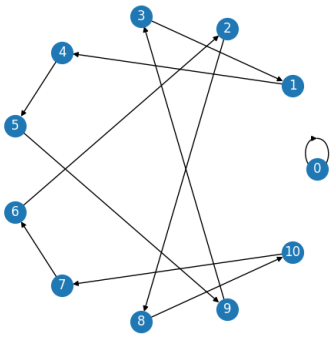
Мы уже обсуждали, что простые модули ведут себя более регулярно (все остатки, кроме нуля, обратимы, можно сокращать и т.п.). Вот один из графов умножения для простого модуля 11.

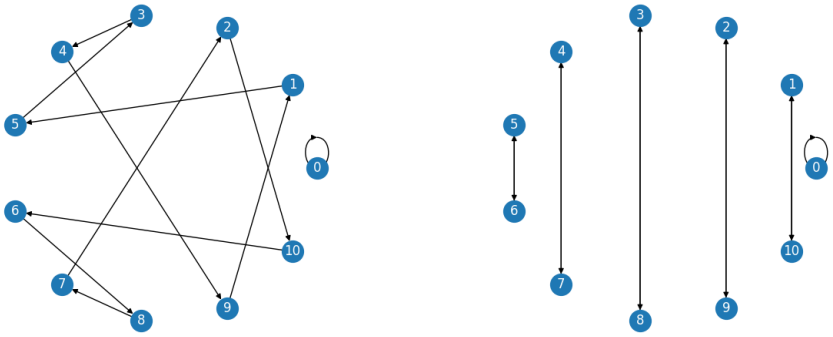


9.3 На что мы умножаем на этом рисунке? Какой будет период в последовательности остатков? Найдите $2^{179} \bmod 11$, глядя на эту картинку.

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?

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.

9.6 Покажите, что стрелки разбиваются на несколько циклов.

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

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?

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)

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

▷ 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.

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.

▷ 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.

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.

▷ 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.

• 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 (a) Докажите, что если $a \equiv b \pmod n$, то НОД$(a, n) =$ 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.

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?

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.

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

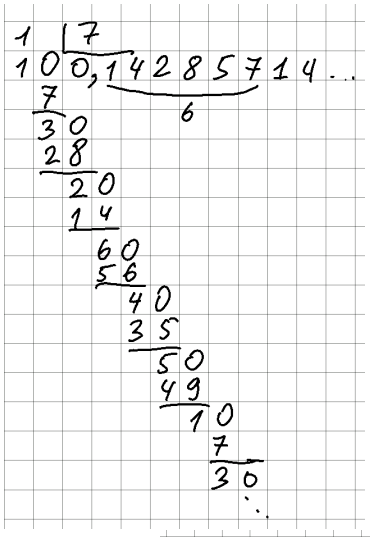
9.19* Докажите, что функция Эйлера мультипликативна: если m и n взаимно просты, то $\varphi(mn) = \varphi(m)\varphi(n)$.

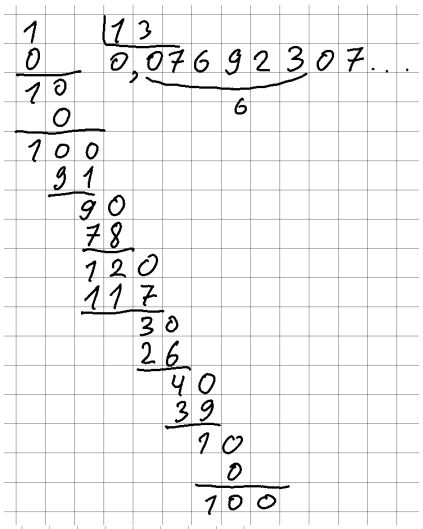
Это рассуждение годится при $m, n > 1$. Вообще $\varphi(1)$ это некоторый особый случай, и мы положим $\varphi(1) = 1$ — для того, в частности, чтобы предыдущая задача была верна при всех m, n, включая 1.

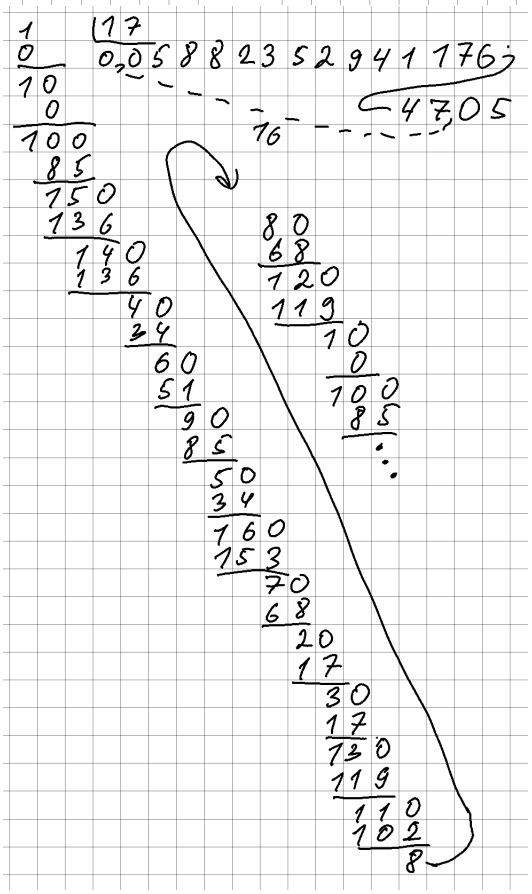
9.20* Покажите, что для любого числа $n > 2$ выполняется тождество $\sum_{d|n} \varphi(d) = n$ (где сумма берётся по всем делителям числа n).

• 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.

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).

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

$$\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}=\frac{2\cdot3\cdot4+1\cdot3\cdot4+1\cdot2\cdot4+1\cdot2\cdot3}{1\cdot2\cdot3\cdot4}=\frac{24+12+8+6}{24}=\frac{50}{24}=\frac{25}{12},$$

и 25 делится на 5.