в) (М1510) Докажите, что существует бесконечно много таких составных чисел n, что $3^{n-1}-2^{n-1}$ кратно n.

63. Докажите, что если n – составное число и $1^{n-1}+2^{n-1}+\ldots+(n-1)^{n-1}\equiv -1 \pmod n$, то n – число Кармайкла. (Воспользовавшись списком чисел Кармайкла, не превосходящих 10^{16}, можно при помощи компьютера проверить, что не существует ни одного удовлетворяющего этому сравнению числа, не превосходящего 10^{16}. Существуют ли такие числа, большие 10^{16}, мы не знаем.)

Приложения

Бином Ньютона

Малую теорему Ферма легко доказать по индукции, если использовать формулу бинома Ньютона. Мы сделаем это для натуральных чисел a, оставив случай отрицательных чисел читателю.

Пусть сначала $p=3$. *База индукции*: $1^3-1=0$ делится на 3. *Переход*: если для некоторого числа a уже доказали, что a^3-a кратно 3, то

$$(a+1)^3-(a+1)=$$
$$=a^3+3a^2+3a+1-(a+1)\equiv$$
$$\equiv a^3+1-a-1=a^3-a\equiv 0 \pmod 3.$$

Аналогично для $p=5$: база очевидна $\left(1^5-1\equiv 0 \pmod 5\right)$, а для перехода используем формулу

$$(a+1)^5=a^5+5a^4+10a^3+10a^2+5a+1.$$

Видите, коэффициенты при a^4, a^3, a^2 и a кратны 5. Поэтому

$$(a+1)^5\equiv a^5+1 \pmod 5,$$

откуда и следует возможность индукционного перехода:

$$(a+1)^5-(a+1)\equiv$$
$$\equiv a^5+1-a-1=a^5-a \pmod 5.$$

Упражнение 64. Докажите индукцией по a малую теорему Ферма для а) $p=2$; б) $p=7$.

Займемся общим случаем. Формула бинома имеет вид

$$(a+1)^p=a^p+pa^{p-1}+\frac{p(p-1)}{2}a^{p-2}+$$
$$+\frac{p(p-1)(p-2)}{3!}a^{p-3}+\ldots$$
$$\ldots+\frac{p(p-1)}{2}a^2+pa+1.$$

Коэффициенты

$$C_p^1=p, C_p^2=p(p-1)/2,\ \ldots$$
$$\ldots C_p^k=p(p-1)\ldots(p-k+1)/k!,\ldots$$
$$\ldots C_p^{p-1}=p$$

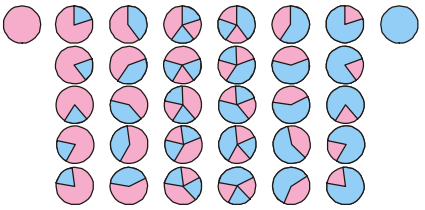
кратны простому числу p. Поэтому $(a+1)^p\equiv a^p+1 \pmod p$, что и требовалось:

$$(a+1)^p-(a+1)\equiv$$
$$\equiv a^p+1-a-1=a^p-a \pmod p.$$

Упражнение 65. Если n составное, то хотя бы один из биномиальных коэффициентов C_n^{n-2}, C_n^2, …, C_n^k, …, C_n^{n-1} не кратен n. Докажите это.

Комбинаторное доказательство

На рисунке изображены все 32 способа раскраски в два цвета круга, который разделен на 5 равных секторов. Среди



них выделяются два способа – когда весь круг синий и когда он весь красный. А остальные разбиты на 6 групп по 5 раскрасок, получающихся одна из другой поворотом.

Задача. Сколькими способами можно раскрасить a разными красками круг, разбитый на p одинаковых секторов, где p – простое число? (Каждый сектор окрашивается одной краской; не обязательно использовать все краски; две раскраски, совпадающие при повороте круга, считаются одинаковыми.)

Решение. Очевидно, можно все сектора покрасить одной краской. Таких способов столько же, сколько красок, т.е. a способов.

А вот из любой другой раскраски поворотами можно получить p разных раскрасок (считая и саму эту раскраску: она получается поворотом на 0°). Значит, ответ таков:

$$a+\frac{a^p-a}{p}.$$

Поскольку количество способов не бывает дробным, число a^p-a обязано нацело делиться на p.

Упражнение 66. Сколькими способами можно раскрасить a разными красками круг, разбитый а) на p^2 секторов, где p – простое число? б) на pq секторов, где p, q – простые числа, $p\neq q$? (Каждый сектор окрашиваем одной краской; не обязательно использовать все краски; две раскраски, совпадающие при повороте круга, считаем одинаковыми.)

Как строят большие простые числа?

Как помнит читатель первой части статьи, для криптографической системы RSA нужны большие (лучше всего – длиной в несколько сот цифр) простые числа. Наиболее эффективным средством построения таких чисел сейчас является метод, основанный на следующей лемме.

Лемма. *Пусть q – нечетное простое число, r – четное натуральное, $n=qr+1$. Если существует такое целое число a, что $a^{n-1}\equiv 1 \pmod n$ и $НОД\left(a^r-1,n\right)=1$, то каждый простой делитель p числа n удовлетворяет сравнению $p\equiv 1 \pmod{2q}$.*

Доказательство. Обозначим порядок числа a по модулю p буквой k. Поскольку $a^{n-1}\equiv 1 \pmod p$ и $a^{(n-1)/q}\not\equiv 1 \pmod p$, то k делится на q. В силу теоремы 3, $p-1$ делится на k. Следовательно, $p-1$ делится на q. Кроме того, $p-1$ четно. Лемма доказана.

Следствие. *Если выполнены условия леммы и $r\le 4q+2$, то n – простое число.*

Доказательство. Пусть n равняется произведению не менее чем двух простых чисел. Поскольку каждое из них не меньше $2q+1$, получаем противоречие:

$$(2q+1)^2\le n=qr+1\le 4q^2+2q+1.$$

Покажем теперь, как, имея большое простое число q, можно пытаться строить существенно большее простое число n. Выберем случайным образом четное число r на промежутке $q<r\le 4q+2$ и положим $n=qr+1$. Затем проверим n на отсутствие малых простых делителей, перепробовав малые простые числа.[3] Если при этом выяснится, что n – составное, то следует выбрать новое значение r и повторить вычисления.

Если же есть надежда, что n простое, то можно случайным образом выбрать число a и проверить, выполнены ли для него соотношения $a^{n-1}\equiv 1 \pmod n$ и $НОД\left(a^r-1,n\right)=1$. Если выполнены, то можно утверждать, что n простое (заметьте: $n>q^2$, так что число n записывается примерно вдвое большим количеством цифр, чем q). Если же нет, то можно взять другое значение a, и так далее.

В настоящий момент нет доказательства того, что этот алгоритм сработает и тем более – что он сработает достаточно быстро. Однако на практике он позволяет строить большие (порядка 10^{300}) простые числа.

---

[3] *В этом месте мы чуть лукавим: следует не только делить на малые простые числа, но и применять более хитрые методы проверки на простоту. Хотя эти методы основаны на малой теореме Ферма и по сути сводятся к тому, что если для некоторого a, взаимно простого с n, число a^{n-1} не сравнимо с 1 по модулю n, то n составное, подробное обсуждение завело бы нас слишком далеко в бурно развивающуюся область теории чисел и вычислительной математики.*