10. Натуральные числа a, b, n таковы, что $a - k^n$ кратно $k - b$ для любого натурального числа $k \neq b$. Докажите, что $a = b^n$.

Степени числа a по модулю p

Для любого целого числа a, не кратного простому p, рассмотрим числа 1, a, a^2, …, a^{p-1}. Ни одно из них не кратно p. Поскольку ненулевых остатков от деления на p существует всего $p-1$ штук, а мы рассматриваем p чисел, то какие-то два из них дают один и тот же остаток:

$$a^r \equiv a^s \pmod p,$$

где $0 \le r < s < p$. Сокращая на a^r, получаем:

$$a^{s-r} \equiv 1 \pmod p,$$

т. е. остаток от деления числа a^{s-r} на p равен 1. Значит, последовательность остатков от деления степеней числа a на p – периодическая.

Упражнения

11. а) Пусть число n нечетно и не кратно 5. Докажите, что существует кратное n число, записываемое одними единицами. б) Если целое число a и натуральное n взаимно просты, то существует такое k, что сумма $1 + a + a^2 + \ldots + a^k$ кратна n. Докажите это.

12. а) Докажите, что для любого натурального n числа $8^n + 1$ и $5 \cdot 4^n + 1$ – составные. б) Существует бесконечно много составных чисел вида $10^n + 3$. Докажите это. (Неизвестно, существует ли бесконечно много простых чисел вида $10^n + 3$.) в) Пусть a, b, c – натуральные числа, $b > 1$. Докажите, что среди чисел вида $ab^n + c$ бесконечно много составных.

Что такое порядок?

Наименьшее натуральное число k, для которого $a^k \equiv 1 \pmod p$, называют *порядком* (не кратного p) числа a по модулю p.

Очевидно, числа a, a^2, …, $a^k (\equiv 1)$ дают при делении на p разные остатки, а дальше последовательность периодична: $a^{k+1} \equiv a$, $a^{k+2} \equiv a^2$, … При этом

$$a^k \equiv a^{2k} \equiv a^{3k} \equiv \ldots \equiv 1 \pmod p,$$

а другие степени числа a не сравнимы с 1 по модулю p.

Если вместо простого числа p вы рассмотрите любое натуральное число n, то аналогичным образом сможете доказать следующую важную теорему.

Теорема 2. *Если целое число a взаимно просто с натуральным числом n, то существует бесконечно много таких натуральных m, что $a^m - 1$ кратно n. Все они являются кратными наименьшего из них (которое называют порядком числа a по модулю n).*

Упражнения

13. Если целое число a взаимно просто с натуральным n и если $a^r \equiv a^s \equiv 1 \pmod n$, то $a^{\text{НОД}(r,s)} \equiv 1 \pmod n$. Докажите это.

14. Зная, что порядок числа $a = 10$ по модулю $p = 19$ равен 18, выясните, при каких k число $\underbrace{11\ldots1}_{k}$ кратно 19.

15. Если число 1000…01 кратно 19, то оно кратно 13. Докажите это.

Разбиение на циклы

Пусть целое число a не кратно простому p и пусть k – порядок числа a по модулю p. Как при помощи k сформулировать малую теорему Ферма? А вот как: $p - 1$ кратно k. (Т.е. $p - 1 = km$ для некоторого натурального m; сравнение $a^{p-1} \equiv 1$ получается из сравнения $a^k \equiv 1$ возведением в m-ю степень.)

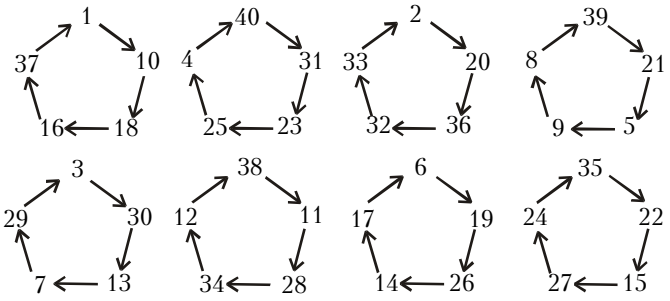

Рис.2

Теорема 3. *Порядок k не кратного простому p целого числа a является делителем числа $p - 1$.*

Доказательство. Идея в том, что все $p - 1$ ненулевых остатков от деления на p мы разобьем на циклы вида $\{x, ax, \ldots, a^{k-1}x\}$. Каждый такой цикл состоит из k остатков. Например, при $p = 41$ и $a = 10$ разбиение изображено на рисунке 2, на котором стрелочкой показано действие операции умножения на 10 («по модулю 41», т.е. мы каждый раз не только умножаем на 10, но и берем остаток от деления на 41).[6]

В общем случае, проведя от каждого ненулевого остатка x стрелочку к остатку от деления на p числа ax, мы получим рисунок, на котором из каждого ненулевого остатка выходит одна стрелочка и к каждому ненулевому остатку ведет тоже одна стрелочка (если бы к какому-то остатку y вели стрелочки от x_1 и x_2, то выполнялись бы сравнения $ax_1 \equiv y \equiv ax_2 \pmod p$, откуда $x_1 \equiv x_2 \pmod p$, так что $x_1 = x_2$).

Теорема 3 доказана.

Теорема Эйлера

Рассмотрев вместо простого p любое натуральное число n, аналогичным образом можно доказать, что порядок (по модулю n) взаимно простого с n целого числа a – делитель числа $\varphi(n)$. При этом $a^{\varphi(n)} \equiv 1 \pmod n$. Последнее утверждение, как вы помните, носит имя Леонарда Эйлера.

Упражнения

16. Существует ли такое натуральное число k, что сто последних цифр десятичной записи числа 3^k совпадают со ста последними цифрами числа 7^k?

17. Если a и b – взаимно простые натуральные числа, то $a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod{ab}$. Докажите это.

18. Существует бесконечно много натуральных чисел n, для которых $2^n + n^2$ кратно 100. Докажите это.

19. Для любого простого числа p существует бесконечно много чисел вида $2^n - n$, кратных p. Докажите это.

20. а) Последние две цифры квадрата любого натурального числа и его 22-й степени совпадают: $n^2 \equiv n^{22} \pmod{100}$. Докажите это. б) Докажите, что $n^{103} \equiv n^3 \pmod{1000}$ для любого целого числа n.

21. Докажите, что последние цифры чисел вида а) n^n; б) n^{n^n} (n – натуральное) образуют периодическую последовательность, и найдите длину ее наименьшего периода.

22. Найдите четыре последние цифры числа а) 3^{1999}; б) 2^{1999}; в) $2^{3^{2000}}$.

---

[6] Эти циклы тесно связаны с разложениями обыкновенных дробей со знаменателем 41 в периодические десятичные дроби (см. статью Л. Семеновой «Периодические дроби» в «Кванте» №2).