Числа на окружности

Для любых трех стоящих подряд чисел a, b, c рисунка 1 разность $b^2 - ac$ кратна 11. И это не случайный курьез, а частный случай общей конструкции: взяв первообразный корень g по простому модулю p, рассмотрим геометрическую прогрессию g, g^2, … …, g^{p-2}, g^{p-1} и выпишем вдоль окружности остатки от деления ее членов на p. (Рисунок 1 иллюстрирует случай $g = 2$ и $p = 11$, заставка к статье – случай $g = 6$ и $p = 13$.)

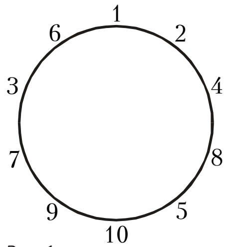

Рис.1

Дело вот в чем: если числа a, b, c образуют геометрическую прогрессию, то выполнено равенство $b^2 = ac$. (А поскольку мы заменяли числа на их остатки от деления на p, то вместо равенств получаем сравнения по модулю p.)

Итак, когда мы докажем, что по простому модулю p существует первообразный корень [4], то одновременно докажем и возможность такого расположения чисел 1, 2, …, $p - 1$ вдоль окружности, при котором для любых трех стоящих подряд чисел a, b, c разность $b^2 - ac$ кратна p.

Упражнение 3. Пусть n – составное. Можно ли так расположить числа 1, 2, …, $n - 1$ вдоль окружности, чтобы для любых трех стоящих подряд чисел a, b, c разность $b^2 - ac$ была кратна n?

Степени двойки по модулю 17

Рассмотрим остатки от деления степеней двойки на 17 (табл.4).

Таблица 4

n	1	2	3	4	5	6	7	8
$2^n (\mathrm{mod}\, 17)$	2	4	8	16	15	13	9	1

Зацикливание произошло слишком рано: $2^8 \equiv 1 \pmod{17}$. Поэтому не все ненулевые остатки от деления на 17 – остатки от деления степеней двойки. Например, в нижней строке таблицы 4 нет числа 5, так что разность $2^n - 5$ не кратна 17 ни при каком натуральном n.

Упражнения

4. Докажите, что ни при каком натуральном n число $1719^n - 3$ не кратно 17.

5. Среди чисел вида $2^n - 3$ бесконечно много чисел, кратных 5, и бесконечно много чисел, кратных 13, но нет ни одного числа, кратного 65 (= 5 · 13). Докажите это.

Степени тройки по модулю 17

Давайте начнем не с двойки, а с тройки и, не забывая переходить к остатку от деления на 17, будем умножать, умножать и умножать на три: 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1. Мы получили все 16 возможных ненулевых остатков от деления на 17. Значит, 3 – первообразный корень по модулю 17.

Не для каждого простого числа p в качестве первообразного корня годятся 2 или 3. Например, легко проверить, что

$$2^{11} \equiv 1 \equiv 3^{11} \pmod{23},$$

так что ни 2, ни 3 не являются первообразными корнями по модулю 23. (А вот –2 и –3, как можно убедиться, являются.)

Упражнение 6. Найдите наименьшее простое число p, для которого существует a, не сравнимое по модулю p ни с одним из чисел –1, 0, 1 и такое, что ни a, ни $-a$ не являются первообразными корнями по модулю p.

Когда $a^m - 1$ делится на $a^k - 1$?

От числовых примеров перейдем к более абстрактным рассуждениям. Прежде всего напомним формулы сокращенного умножения:

$$a^2 - 1 = (a-1)(a+1),$$

$$a^3 - 1 = (a-1)(a^2 + a + 1),$$

и вообще,

$$a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \ldots + a + 1).$$

Теорема 1. *Если a, k, m – натуральные числа, $a > 1$, то $a^m - 1$ делится на $a^k - 1$ в том и только том случае, когда m делится на k.*

Доказательство. Если $m = kn$, то

$$a^m - 1 = (a^k - 1)(a^{k(n-1)} + a^{k(n-2)} + \ldots + a^k + 1).$$

Обратно, если m не делится на k, то разделим m на k с остатком:

$$m = kn + r,$$

где $0 < r < k$, и рассмотрим равенство

$$a^{kn+r} - 1 = a^{kn+r} - a^r + a^r - 1 = a^r(a^{kn} - 1) + (a^r - 1).$$

Число $a^r - 1$ не делится на $a^k - 1$, поскольку $0 < a^r - 1 < a^k - 1$. Теорема доказана.

Упражнения

7. Если число $a^n - 1$ простое, $a > 1$ и $n > 1$, то $a = 2$ и n – простое. Докажите это. (Не при всяком простом p число $2^p - 1$ простое: например, $2^{11} - 1 = 2047 = 23 \cdot 89$. Простые числа вида $2^p - 1$ называют *числами Мерсенна* [5]. В настоящий момент известно 38 чисел Мерсенна и неизвестно, конечно или бесконечно их множество. В 1997 году было найдено число Мерсенна $2^{2976221} - 1$, а 1 июня 1999 года нашли наибольшее из известных на сегодняшний день: $2^{26972593} - 1$.)

8. Если $a^n + 1$ – простое число, a, n – натуральные числа, $a > 1$, то a четно и n – степень числа 2. Докажите это. (Простые числа вида $2^{2^n} + 1$ называют *числами Ферма*. Их известно всего пять: $2^{2^0} + 1 = 3$, $2^{2^1} + 1 = 5$, $2^{2^2} + 1 = 17$, $2^{2^3} + 1 = 257$ и $2^{2^4} + 1 = 65537$. Существуют ли другие, неизвестно. Неизвестно и то, конечно или бесконечно множество простых чисел вида $p = a^2 + 1$.)

9. а) Число $2^n - 1$ делится на $2^m + 1$ тогда и только тогда, когда n делится на $2m$. Докажите это. б) Для каких натуральных чисел m существует такое натуральное n, что $2^n + 1$ делится на $2^m - 1$?

[4] *А мы это докажем, хотя и не в этом номере журнала.*

[5] *Марен Мерсенн (1588–1648) занимался математикой, теорией музыки, физикой и философией. Он был товарищем Р. Декарта по учебе в иезуитском колледже и членом монашеского ордена минимов. Мерсенн сыграл выдающуюся роль как организатор науки. Он состоял в переписке с Р. Декартом, Ж. Робервалем, Б. Паскалем, Х.Гюйгенсом, Б.Кавальери, Б.Френиклем де Бесси, Дж.Валлисом и др. Вокруг него образовался кружок ученых, который стал основой для создания Парижской Академии наук (1666 год).*