Периодичность остатков

Мы заняты делом,
отвлечься не можем:
мы числа в тетради
все множим и множим.
А.Котова

Остатки от деления на 11

Какие остатки дают степени двойки при делении на 11? Посмотрите на таблицу 1.

Таблица 1

n	1	2	3	4	5	6	7	8	9	10	11	12
2^n	2	4	8	16	32	64	128	256	512	1024	2048	4096
$2^n \pmod{11}$	2	4	8	5	10	9	7	3	6	1	2	4

Дальше можно не продолжать: $2^{10+n} = 2^{10} \cdot 2^n \equiv 1 \cdot 2^n = 2^n \pmod{11}$, остатки будут повторяться с периодом 10. Между прочим, средняя строка таблицы излишняя: в нижней строке каждое следующее число – это остаток от деления на 11 удвоенного предыдущего числа.

Как бы то ни было, $2^{10} \equiv 1 \pmod{11}$. Ничего удивительного в этом нет, это всего лишь частный случай малой теоремы Ферма. Интереснее другое: в нижней строке таблицы 1 присутствуют все ненулевые остатки от деления на 11. Например, $3 \equiv 2^8$, $5 \equiv 2^4$, $7 \equiv 2^7$, $10 \equiv 2^5 \pmod{11}$.

Другими словами, для любого целого числа a, не кратного 11, существует такое s, что

$$a \equiv 2^s \pmod{11}.$$

А сейчас – внимание:

$$a^{10} \equiv \left(2^s\right)^{10} = \left(2^{10}\right)^s \equiv 1^s = 1 \pmod{11}.$$

Таким образом, при $p = 11$ мы проверили малую теорему Ферма не только для $a = 2$, но для любого ненулевого остатка a. Красиво и неожиданно, не правда ли?

Упражнение 1. Рассматривая степени двойки, докажите малую теорему Ферма для а) $p = 13$; б) $p = 19$.

Что такое первообразный корень?

Число g называют *первообразным корнем* по простому модулю p, если числа g, g^2, …, g^{p-1} дают разные (ненулевые) остатки при делении на p. Другими словами, g – первообразный корень, если для любого целого числа a, не кратного числу p, существует такое s, что $a \equiv g^s \pmod{p}$.

Упражнение 2. а) Какие из чисел 1, 2, 3, 4 являются первообразными корнями по модулю 5? б) Какие целые числа являются первообразными корнями по модулю 7?

Число 2 – первообразный корень по модулю 11

В разделе «Таблицы умножения» первой части статьи, как помните, мы составили таблицу умножения по модулю 11. Тот факт, что 2 – первообразный корень, позволяет нам так переставить ее столбцы и строки, что таблица приобретет гораздо более внятный вид (табл.2).

Если $a \equiv g^s$ и $b \equiv g^t$, то $ab \equiv g^s g^t = g^{s+t} \pmod{11}$. Это

Таблица 2

×	1	2	4	8	5	10	9	7	3	6
1	1	2	4	8	5	10	9	7	3	6
2	2	4	8	5	10	9	7	3	6	1
4	4	8	5	10	9	7	3	6	1	2
8	8	5	10	9	7	3	6	1	2	4
5	5	10	9	7	3	6	1	2	4	8
10	10	9	7	3	6	1	2	4	8	5
9	9	7	3	6	1	2	4	8	5	10
7	7	3	6	1	2	4	8	5	10	9
3	3	6	1	2	4	8	5	10	9	7
6	6	1	2	4	8	5	10	9	7	3

Таблица 3

+	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

сводит умножение по модулю 11 к сложению по модулю 10 (именно по этому модулю рассматриваются числа s и t). Давайте рассмотрим таблицу сложения по модулю 10 (табл.3).

Таблицы 2 и 3 очень похожи! Математик сказал бы, что мультипликативная [1] группа вычетов $\boldsymbol{Z}_{11}^*$ (ее элементы – ненулевые классы вычетов по модулю 11) *изоморфна* аддитивной [2] группе $\boldsymbol{Z}_{10}$ вычетов по модулю 10. Наивно говоря, изоморфизм – это взаимно однозначное отображение, сохраняющее операцию.[3] Например, изоморфизм между $\boldsymbol{Z}_{10}$ и $\boldsymbol{Z}_{11}^*$ можно установить, сопоставив каждому из чисел $s = 0, 1, \ldots, 9$ число 2^s. При этом сумме $s + t \pmod{10}$ будет, как мы уже говорили, сопоставлено произведение $2^s \cdot 2^t \pmod{11}$.

---

[1] *От латинского «умножать».*
[2] *От латинского «складывать».*
[3] *Точное определение изоморфизма можно найти, например, в «Алгебре» Ван дер Вардена (М.: Наука, 1976).*