24.03.2019

Множество классов образуют кольцо.

1. Элементы кольца можно исследовать.
2. Элементы кольца можно перемножать.
3. (a + b)\*c = ac + bc

***Обозначение***: Zm (или Z/mZ) — кольцо остатков по mod m (включает и множество 1, 2,…,m‑1, и операции «+», «\*»).

Пример:

(1000000 + 11\*12\*13)\*1000000 mod 7 = ?

1000000 = 100\*100\*100 = 2\*2\*2 mod 7 = 8 = 1

1000000 = (-1)\*(-1) mod 7 = 1, т.к. 1001 = 7\*11\*13

11\*12\*13 = (-3)\*(-2)\*(-1) mod 7 = -6 = 1 mod 7

Итого: (1000000 + 11\*12\*13)\*1000000 = (1 + 1)\*1 mod 7 = 2

**Признаки делимости:**

1. mod 3, mod 9

10 = 1 mod 3 / mod 9

anan-1…a0 10 = an\*10n +…+a0 = an\*1n +…+a0 mod 3 / mod 9 = an+…+a0 = ϕ(x)

где ϕ(x) — сумма цифр числа

Итого, x = ϕ(x) mod 3 / mod 9

Следствие, x ⁝ 3 ↔ ϕ(x) ⁝ 3, x ⁝ 9 ↔ ϕ(x) ⁝ 9

1. mod 11

10 = -1 mod 11

x = anan-1…a0 10 = an\*10n +…+a0 = a0 – a1 + a2 – a3 +…± an

x = a0 – a1 + a2 – …

Пример:

57121 = 1 – 2 +1 -7 +5 mod 11 = -2 = 9 mod 11

1. mod 7

anan-1…a0 10 = a2a1a0 + 1000\* a5a4a3 + 10003\* a8a7a6 +…

Пример:

1273957121 = 121 – 957 + 273 – 1 mod 7 = -4 = 3 mod 7

1. mod 2 / mod 5 / mod 10

10 = 0 mod mod 2 / mod 5 / mod 10

x = anan-1…a0 10 = a0 mod 2 / mod 5 / mod 10

**Системы вычетов**

***Определение***: Полная система вычетов mod m — это множество M, такое что оно состоит из чисел, которые имею все возможные остатки по модулю m, т.е

1. для любого r (остаток) существует x ϵ M: x mod m = r (0 ≤ r < m)
2. для любого x ≠ y ϵ M, x mod m ≠ y mod m

Пример:

mod 5: {0, 1, 2, 3, 4} или {-2, -1, 0, 1, 2} или {0, 2, 4, 6, 8}

***Утверждение***: 1) Множество {0, 1, 2,…, m-1} —полная система вычетов (ПСВ). 2) В ПСВ всего m элементов.

***Утверждение***: Для любого c ϵ M, где М — ПСВ mod m, справедливо: 1) М + с = {x + c | x ϵ M } — ПСВ, 2) М\*с = {x\* c | x ϵ M } — ПСВ, если (c, m) = 1.

Доказательство:

Обозначим М + с как M’, М\*с как M’’.

Проверим определения.

1. Для любого r (0 ≤ r < m), рассмотрим y ϵ M: y mod m = (r – c) mod m (такой y есть, т.к. M — ПСВ).

y + c ϵ M’ и y ± c = (r –c + c) mod m = r

Следовательно, y + c подходит, он ϵ M’ и имеет нужный остаток r.

1. Для любых x, y ϵ M’, x ≠ y, проверим, что x ≠ y mod m.

Это верно, т.к. x + c ≠ y + c, т.к. x ≠ y mod m, ч.т.д.

Пример:

M = {0, 1, 2, 3} — ПСВ mod 4

M + 5 = {5, 6, 7, 8}

Другое доказательство:

Проверим вторую часть определения.

Почему все остатки есть в M’?

В M’ ровно m чисел и (по второму определению) и они имеют разные остатки → они имеют все возможные остатки.

Теперь про умножение.

* Для любых x, y ϵ M’’, x ≠ y, проверим, что x = y mod m.

Докажем от противного.

Пусть x\*c = y\*c, тогда сократим на с, т.к. (c, m) = 1.

Получаем x = y — *противоречие*.

* Из соображений количества |M’’| = m → M — содержит все остатки.

Пример:

M = {-2, -1, 0, 1, 2} — ПСВ mod 5

c = 3, (c, m) = 1

M” = {-6, -3, 0, 3, 6} — ПСВ mod 5

**Следствие о делимости**

Пусть a, b, m ϵ Z, (a, m) = 1, m ≥ 2.

Тогда существует x, такое что ax = b mod m.

*\*Замечание*: x — частное от деления b на a mod m.

Доказательство:

Рассмотрим a\*M, где M = {0, 1, 2,…, m-1} — ПСВ.

a\*M содержит y = b mod m, где y — это ax (x ϵ M). Т.е. x — ответ, ч.т.д.

Пример:

5x = 1 mod 11

M = {0, 1,.., 9, 10} — ПСВ mod 11

5M = {0, 5,…, 45, 50}

45 mod 11 = 1 → x = 9

Замечание:

Мы поняли, что mod m всегда можно поделить на любое взаимно простое число.

Ответ по mod m единственный, т.к в а\*M = {0, а, 2а,…, а\*(m-1)} все остатки разные.