Задача. Бобу требуется по заданной точке P эллиптической кривой найти 2017-кратную точку, т.е. сумму 2017 экземпляров P. В распоряжении Боба — операции сложения, вычитания, удвоения и утроения точек. Бобу нужно организовать вычисления, затратив как можно меньше операций. Например, с помощью представления $2017 = 3^7 - 2 \cdot 3^4 - 3^2 + 1$ Боб может найти кратную точку за 11 операций: 7 утроений, 1 удвоение, 2 вычитания и 1 сложение. Можно ли еще быстрее?

Решение. Вычисления описываются схемой — ориентированным графом без циклов. Дуги не заходят в единственную вершину схемы, ее называют листом. В остальные вершины заходит либо одна, либо две дуги. Эти вершины помечаются кодами операций — удвоения, утроения, сложения, вычитания. В вершины удвоения и утроения заходит одна дуга, в вершины сложения и вычитания — две. На лист схемы подается число 1, это число перемещается по дугам в следующие вершины. Если числа на входных дугах некоторой вершины определены, то к этим числам применяется операция вершины, результат операции перемещается по выходным дугам дальше. В некоторой вершине должно появиться искомое число $n = 2017$, на этом вычисления заканчиваются. Ничего не изменится, если на вход схемы вместо числа 1 подать точку P. Только теперь в вершинах вместо чисел i будут вычисляться кратные точки iP, а ожидать следует появления точки nP.

Размер схемы — это число ее вершин-операций. Размер не изменится, если перестроить схему, заменив в ней все удвоения на сложения одинаковых операндов. Будем рассматривать дальше только схемы без удвоений.

Схемы можно строить для произвольных целых n. Пусть $C(n)$ — минимальный размер схемы для вычисления n (*схемная сложность* n). Можно легко получить следующие факты:

1) $C(n) = 0$ только для $n = 1$;

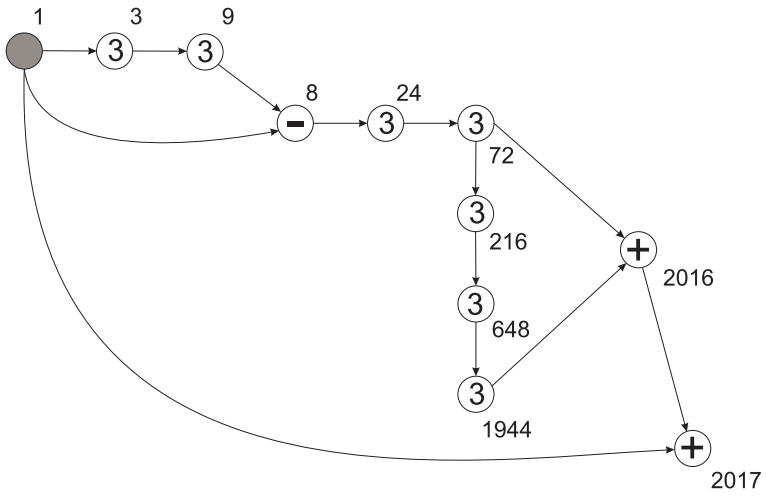
2) $C(n) = 1$ только для $n = 0, 2, 3$;

3) $C(n) = 2$ только для $n = -1, 4, 5, 6, 9$;

4) $C(n) \geq \log_3 n$, причем нижняя граница достижима.

Но нахождение $C(n)$ для общего n является непростой задачей.

Докажем, что $C(2017) = 10$. Во-первых, $C(2017) \leq 10$. Действительно, число 2017 можно вычислить за 10 операций с помощью следующей схемы:



Эту схему можно описать равенством $2017 = 3^5(3^2-1)+3^2(3^2-1)+1$ или еще компактнее: $2017 = (3^5+3^2)(3^2-1)+1$.

Во-вторых, $C(2017) \geq 10$. Действительно, предположим, что имеется схема для вычисления 2017 размера $c \leq 9$ и пусть в ней используется d операций сложения и вычитания. С помощью этой схемы нельзя вычислить число, большее $(d+1)3^{c-d}$. Отсюда $d \leq 3$. С учетом того, что число 2017 — простое, схема должна строиться на представлении этого числа выражением одного из следующих форм:

$$
\begin{aligned}
&3^u \pm 3^v,\\
&(3^u \pm 3^v)3^w \pm 3^x,\\
&(3^u \pm 3^v)(3^w \pm 3^x) \pm 3^y,\\
&((3^u \pm 3^v)3^w \pm 3^x)3^y \pm 3^z.
\end{aligned}
$$

Прямыми расчетами убеждаемся, что может быть реализовано выражение только 3-й формы и только следующими 4-мя способами:

$$
\begin{aligned}
2017 &= (3^4+3)(3^3-3)+1,\\
2017 &= (3^4-3^2)(3^3+1)+1,\\
2017 &= (3^5-1)(3^2-1)+3^4,\\
2017 &= (3^5+3^2)(3^2-1)+1.
\end{aligned}
$$

Ни одно из найденных представлений не дает схему размера $c \leq 9$. □