Вариант №29. Поиск базовой точки выполнялся 352 секунды на компьютере со следующими характеристиками: процессор – i5-8250U, частота 3.40 ГГц, объем ОЗУ – 8 ГБ.

Поиск базовой точки

In[3]:=
```
a = 0; b = 44; c = 18; p = 1086161;
RankMin = Floor[2 * p / 3]; XMin = Floor[p / 2];
```

In[5]:=
```
Timing[FindPoint[p, a, b, c, XMin, RankMin]]
```

```
P={543082, 199071}.
            x=543082 ≥ Floor[p/2]=543080.
            Порядок точки=1085767 ≥ 2p/3=724107 и является простым числом.
            Эллиптическая кривая y^2=x^3+0*x^2+44*x+36 - гладкая. i=18
```

Out[5]=
```
{352.093750, Null}
```

Проверка

In[9]:=
```
y = 199071; x1 = 543082; i = 18;
```

In[18]:=
```
Mod[y^2, p]
```

Out[18]=
```
678956
```

In[19]:=
```
Mod[x1^3 + a * x1^2 + b * x1 + c + i, p]
```

Out[19]=
```
678956
```

In[20]:=
```
PrimeQ[1085767]
```

Out[20]=
```
True
```