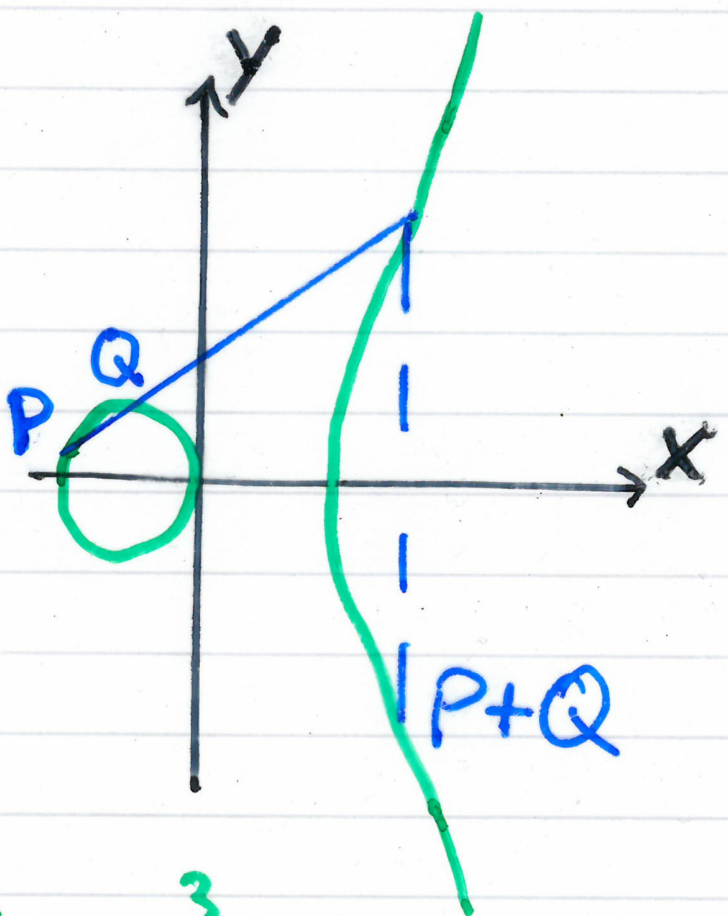
Elliptic curves

We fix K as one of the fields $\mathbb{R}$ (real numbers), $\mathbb{C}$ (complex numbers), $\mathbb{Q}$ (rational numbers), $\mathbb{F}_{p^r}$ (finite field of p^r elements), $p>3$ prime.

Definition. Let x^3+ax+b with $a,b\in K$ be a cubic polynomial without multiple roots. An elliptic curve over K is the set of points (x,y) with $x,y\in K$ which satisfy the equation

$$y^2=x^3+ax+b$$

together with a single element denoted O and called the „point at infinity".



$y^2=x^3-x$ over $\mathbb{R}$

The number of generators of infinite order is called the rank of an elliptic curve over $\mathbb{Q}$.

The Birch and Swinnerton-Dyer conjecture (Millenium Prize problem, 1,000,000 U.S. \$):
The rank of an elliptic curve E over $\mathbb{Q}$ equals the L-function of E at the point 1.

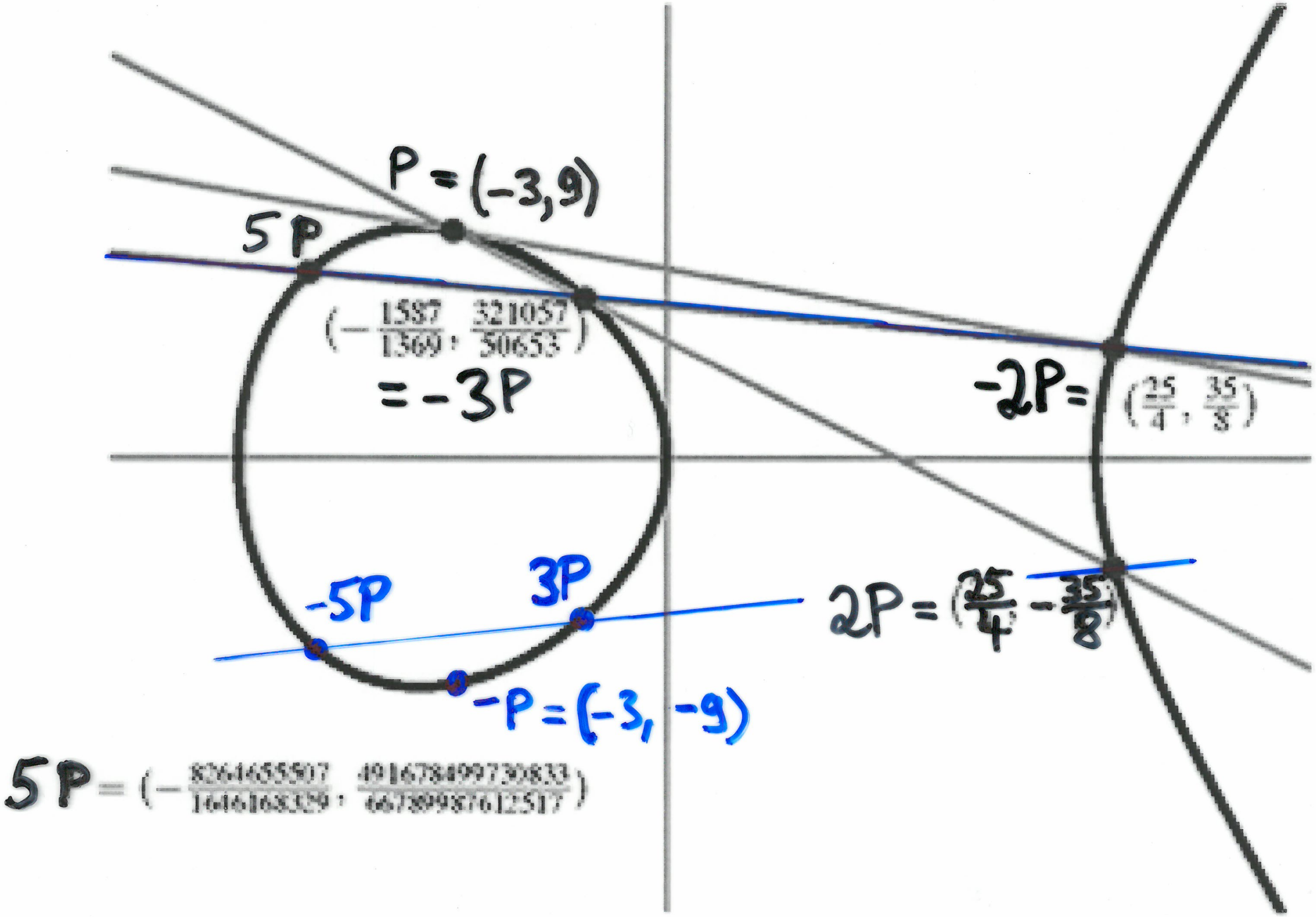
Exercise. Find the order of $P=(2,3)$ on $y^2=x^3+1$.

Integral points on elliptic curves

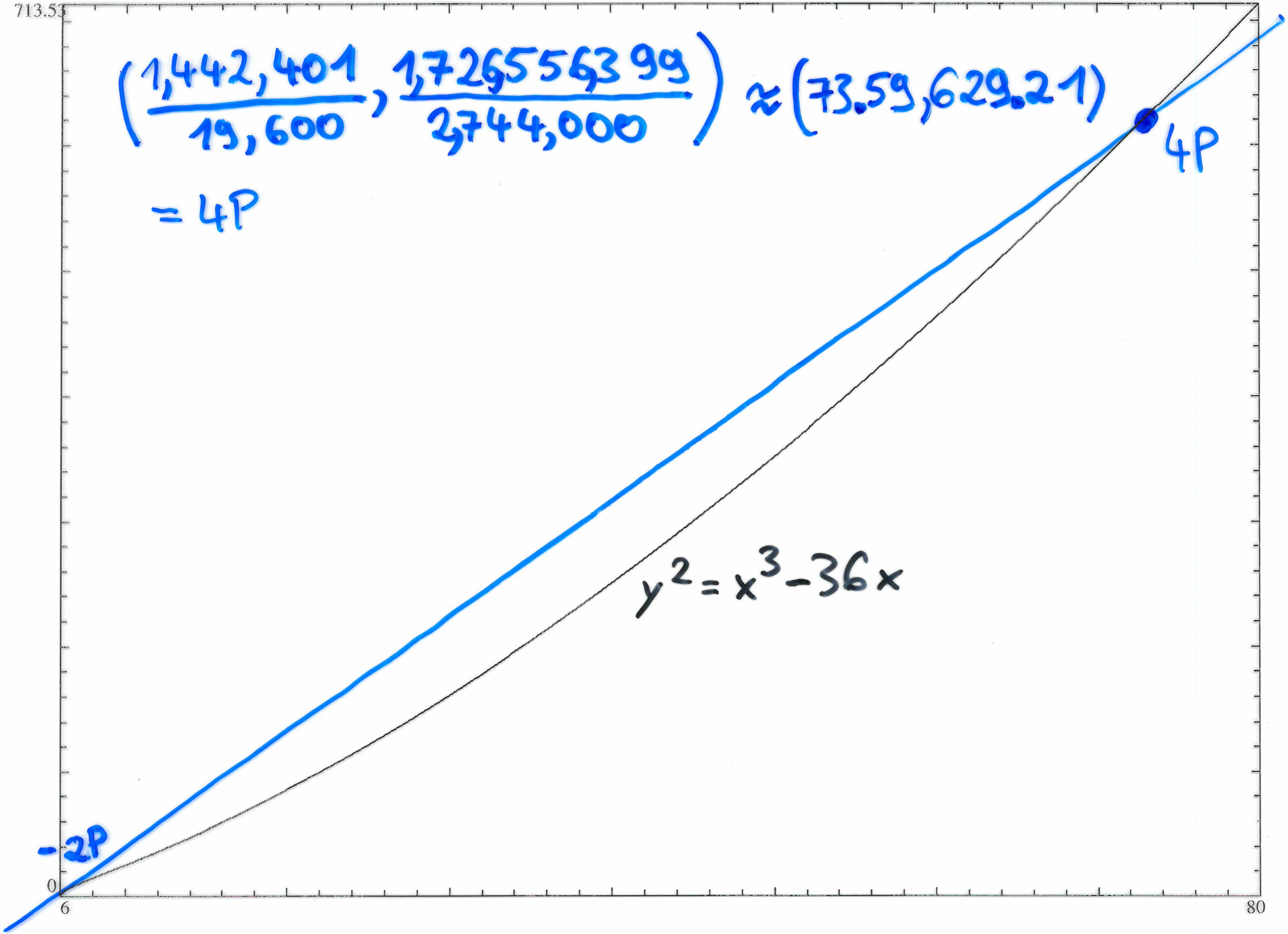
On the elliptic curve $y^2=x^3+27x-62$, the only points with $x\in\mathbb{Z}$ and $y\in\mathbb{Z}$ are $(2,0)$ and $(28844402, \pm 154914585540)$.

It took big research efforts to prove that there are no other such points. In fact, if $n>1$ and both $6n^2-1$ and $12n^2+1$ are odd primes then $y^2=x^3+(36n^2-9)x-2(36n^2-5)$ has only the integral point $(2,0)$ [Yang and Fu 2011].

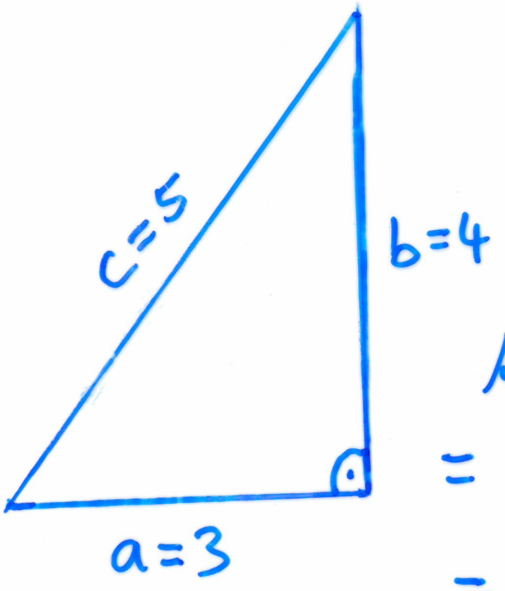
$$y^2 = x^3 - 36x$$



$P = (-3, 9)$
$5P$
$\left(-\frac{1587}{1369}, \frac{321057}{50653}\right)$
$= -3P$
$-2P = \left(\frac{25}{4}, \frac{35}{8}\right)$
$2P = \left(\frac{25}{4}, -\frac{35}{8}\right)$
$3P$
$-5P$
$-P = (-3, -9)$
$5P = \left(-\frac{8264655507}{1646168329}, \frac{491678499730833}{66789987612517}\right)$


713.53
0
6
80
$\left(\frac{1,442,401}{19,600}, \frac{1,726,556,399}{2,744,000}\right) \approx (73.59, 629.21)$
$= 4P$
$4P$
$-2P$
$y^2 = x^3 - 36x$

Right-angled triangles and elliptic curves



$$a^2+b^2=c^2$$

$$3^2+4^2=5^2$$

$$9+16=25$$

Area of the triangle

$= \frac{1}{2}$ (Area of the rectangle a b)

$= \frac{1}{2} a\cdot b = 6$

„Which other natural numbers $n \in \mathbb{N}$ are the area of a right-angled triangle with rational side lengths?"

is equivalent to the question

„Is the rank of the elliptic curve $y^2 = x^3 - n^2 x$ greater than zero?"

because:

$n = \frac{1}{2} a\cdot b$ and we can set $x = \left(\frac{c}{2}\right)^2$ and $y = \frac{(b^2-a^2)\cdot c}{8}$.

Then $y^2 = \frac{b^4-2a^2b^2+a^4}{64}c^2 = \frac{(b^2+a^2)^2}{64}c^2 - \frac{4a^2b^2}{64}c^2$

$= \frac{c^6}{2^6} - \left(\frac{ab}{2}\right)^2 \frac{c^2}{2^2} = x^3 - n^2 x$ as claimed.