Proof of Nagell-Lutz theorem.

$E: y^2 = x^3 + ax + b \quad / \mathbb{Q}$. General equation: $y^2 = x^3 + ax^2 + bx + c$.

Let $f(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$ over the complex numbers,

$$= x^3 - \underbrace{(\alpha_1+\alpha_2+\alpha_3)}_{a} x^2 + \underbrace{(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)}_{b} x \underbrace{- \alpha_1\alpha_2\alpha_3}_{c}$$

$$D = (\alpha_1-\alpha_2)^2(\alpha_1-\alpha_3)^2(\alpha_2-\alpha_3)^2$$

$$= -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$$

There exists polynomials $r(x)$ and $s(x)$ so that

$$D = r(x) f(x) + s(x) f'(x)$$

and $r(x)$, $s(x)$ have integer coefficients.

$$\begin{cases} r(x) = (18b - 6a^2)x \\ \quad -(4a^3 - 15ab + 27c) \\ s(x) = (2a^2 - 6b)x^2 \\ \quad + (2a^3 - 7ab + 9c)x \\ \quad + (a^2 b + 3ac - 4b^2) \end{cases}$$

Now the doubling formula says: for P with $y \neq 0$, $2P$ is not at ∞ and.

$P(x_1, y_1) \mapsto 2P = (x_2, y_2)$, $\quad x_2 = \lambda^2 - a - 2x_1$ where $\lambda = \dfrac{f'(x_1)}{2y_1}$

Assume P and $2P$ have integers coefficients:

then $\lambda^2 = x_2 + a + 2x_1 \in \mathbb{Z}$, so $\lambda \in \mathbb{Z}$, and $2y_1 \mid f'(x_1)$.

Now use $D = r(x_1)\underbrace{f(x_1)}_{y_1 \mid f(x_1)} + s(x_1)\underbrace{f'(x_1)}_{y_1 \mid f'(x_1)} \Rightarrow y_1 \mid D$.

Lemma. Let $P(x_1, y_1)$ be a point on our cubic curve $E: y^2 = x^3 + ax^2 + bx + c$ such that P and $2P$ have integer coordinates. Then either $y = 0$ or $y \mid D$.

Proof of Nagell-Lutz theorem part II.

- Points of finite order have integer coordinates.

Definition: **valuation.** Let m an integer ($m \in \mathbb{Z}$) and p a prime.

The VALUATION of m at p is the order (or multiplicity) of p in the factorization of m, in other words, the largest integer v such that

$$p^v \mid m, \quad p^{v+1} \nmid m.$$

The definition extends to $\mathbb{Q}$: $m, n \in \mathbb{Z}$, $\frac{m}{n} \in \mathbb{Q}$, $\mathrm{val}_p\left(\frac{m}{n}\right) = \mathrm{val}_p(m) - \mathrm{val}_p(n)$, the valuation at the denominator is positive.

We can write $\frac{m}{n} = \frac{m'}{n'} p^{\mathrm{val}_p(m/n)}$ and m', n' are coprime to p.

To show that a rational $m = m_n/m_d$ is actually an integer, we will show that m_d is not divisible by any prime $p \geq 2$, hence the denominator is 1.

Let $P(x,y) \in E(\mathbb{Q})$. Say p divides the denominator of x,

$$x = \frac{m}{n p^{v_p(x)\mu}} \quad \text{and} \quad y = \frac{u}{w p^{v_p(y)\sigma}}, \quad m, n, u, w \text{ coprime to } p.$$
$$\mu, \sigma > 0.$$

$y^2 = x^3 + ax^2 + bx + c$:

$$\frac{u^2}{w^2 p^{2\sigma}} = \frac{m^3}{n^3 p^{3\mu}} + a\frac{m^2}{n^2 p^{2\mu}} + b\frac{m}{n p^{\mu}} + c$$
$$= \frac{m^3 + a m^2 n p^{\mu} + b m n^2 p^{2\mu} + c n^3 p^{3\mu}}{n^3 p^{3\mu}}$$

look at the numerator mod p: this is $m^3 \bmod p$ and $\gcd(m,p) = 1$ by assumption. Hence the numerator is coprime to p. (because $\mu > 0$)

On the left-hand-side, w^2, u^2 are coprime to p.

$$\mathrm{val}_p\left(\frac{u^2}{w^2 p^{2\sigma}}\right) = 2\sigma = \mathrm{val}_p\left(\frac{m^3 + a m^2 n p^{\mu} + \dots}{n^3 p^{3\mu}}\right) = 3\mu$$

$$\Rightarrow 2\sigma = 3\mu > 0. \qquad \Rightarrow 2 \mid \mu, \ 3 \mid \sigma,$$

Hence $\sigma = 3\nu$ and $\mu = 2\nu$ for some $\nu > 0$ integer.

If we start with $\sigma > 0$, we arrive exactly at the same point: $\sigma = 3\nu$ and $\mu = 2\nu$ for $\nu > 0$

Hence if p divides the denominator of x or y, then it divides both, and

$$p^{3\nu} \mid \text{denom}(y), \quad p^{2\nu} \mid \text{denom}(x).$$

We define $E(p^\nu) = \{(x,y) \in E(\mathbb{Q}) : \text{ord}_p(x) \leq -2\nu \text{ and } \text{ord}_p(y) \leq -3\nu\}$

$$E(\mathbb{Q}) \supset E(p) \supset E(p^2) \supset E(p^3) \supset \dots$$

and let $\mathcal{O} \in E(p^\nu)$ for all ν.

→ We want to show that $P(x,y) \notin E(p)$.

↓ We will show that $E(p^\nu)$ are subgroups.
→ $E(p^\nu)$ is stable by addition, dbl, subtraction

First we need a change of variables.

$t = \frac{x}{y}$ and $s = \frac{1}{y}$

$y^2 = x^3 + ax^2 + bx + c$ becomes

$$\frac{1}{y} = \frac{x^3}{y^3} + a\frac{x^2}{y^2} + b\frac{x}{y} + \frac{c}{y^3}$$

$$\Leftrightarrow s = t^3 + a s t^2 + b s^2 t + c s^3$$

inverse change of variables: $y = 1/s$ and $x = t/s$.

$\mathcal{O}$ in (x,y) $\leftrightarrow$ $(0,0)$ in (t,s)

$(x,0)$ does not have a correspondance in (t,s) : we miss the points of order 2.

Let $\mathcal{L}$ a line in the (x,y) plane: $y = \lambda x + \mu \Leftrightarrow \frac{y}{\mu y} = \frac{\lambda}{\mu}\frac{x}{y} + \frac{\mu}{\mu y} \Leftrightarrow \frac{1}{\mu} = \frac{\lambda}{\mu}t + \dots$

$$\Leftrightarrow s = -\frac{\lambda}{\mu}t + \frac{1}{\mu}.$$

Let's add $P(t_1, s_1)$ and $Q(t_2, s_2)$ on $\mathcal{C}$: $t^3 + a s t^2 + b s^2 t + c s^3 - s = 0$

(P): $t_1^3 + a s_1 t_1^2 + b s_1^2 t_1 + c s_1^3 - s_1 = 0$

(Q): $t_2^3 + a s_2 t_2^2 + b s_2^2 t_2 + c s_2^3 - s_2 = 0$

$(P)-(Q)$: $t_1^3 - t_2^3 + a(s_1 t_1^2 - s_2 t_2^2) + b(s_1^2 t_1 - s_2^2 t_2) + c(s_1^3 - s_2^3) - (s_1 - s_2) = 0.$

$$= (t_1 - t_2)(t_1^2 + t_1 t_2 + t_2^2) + a\left((t_1^2 - t_2^2)(s_1) + t_2^2(s_1 - s_2)\right) + b\left((t_1 - t_2)s_1^2 + t_2(s_1^2 - s_2^2)\right)$$

$$+ c(s_1 - s_2)(s_1^2 + s_1 s_2 + s_2^2) - (s_1 - s_2) = 0.$$

divide by $t_1 - t_2$:

$$(t_1^2 + t_1 t_2 + t_2^2) + a\left((t_1 + t_2)s_1 + t_2^2 \frac{(s_1 - s_2)}{t_1 - t_2}\right) + b\left(s_1^2 + t_2 \frac{(s_1 - s_2)(s_1 + s_2)}{t_1 - t_2}\right)$$

$$+ c(s_1 - s_2)(s_1^2 + s_1 s_2 + s_2^2) - (s_1 - s_2) = 0.$$

Addition on the ~~line~~ curve

$$s_1 - s_2 = (t_1 - t_2)(t_1^2 + t_1 t_2 + t_2^2) + a\big((t_1 - t_2)(t_1 + t_2)\, s_1 + t_2^2 (s_1 - s_2)\big)$$
$$+ b\big((t_1 - t_2)(\cancel{t_1 + t_2})\, s_1^2 + t_2 (s_1 - s_2)(s_1 + s_2)\big) + c\,(s_1 - s_2)(s_1^2 + s_1 s_2 + s_2^2)$$

$$\frac{s_1 - s_2}{t_1 - t_2} = t_1^2 + t_1 t_2 + t_2^2 + a\left((t_1 + t_2)\, s_1 + t_2^2 \frac{s_1 - s_2}{t_1 - t_2}\right)$$
$$+ b\left((\cancel{t_1 + t_2})\, s_1^2 + t_2 \frac{s_1 - s_2}{t_1 - t_2}(s_1 + s_2)\right) + c \frac{s_1 - s_2}{t_1 - t_2}(s_1^2 + s_1 s_2 + s_2^2)$$

$$\frac{s_1 - s_2}{t_1 - t_2} - a t_2^2 \frac{s_1 - s_2}{t_1 - t_2} + b t_2 (s_1 + s_2) \frac{s_1 - s_2}{t_1 - t_2} + c \frac{s_1 - s_2}{t_1 - t_2}(s_1^2 + s_1 s_2 + s_2^2)$$

$$= t_1^2 + t_1 t_2 + t_2^2 + a(t_1 + t_2) s_1 + b(\cancel{t_1 + t_2}) s_1^2$$

$$\frac{s_1 - s_2}{t_1 - t_2}\left(1 - a t_2^2 - b t_2 (s_1 + s_2) - c(s_1^2 + s_1 s_2 + s_2^2)\right) = \dots$$

$$\frac{s_1 - s_2}{t_1 - t_2} = \frac{t_1^2 + t_1 t_2 + t_2^2 + a(t_1 + t_2) s_1 + b(\cancel{t_1 + t_2}) s_1^2}{(1) - a t_2^2 - b t_2 (s_1 + s_2) - c(s_1^2 + s_1 s_2 + s_2^2)}$$

the denominator mod p is (1) as if $p^i \mid t_i$, $p^{3i} \mid s_i$, the denominator is 1.

in other words, $\lambda = \frac{s_1 - s_2}{t_1 - t_2}$ has ~~finitely~~ non-negative valuation at p (after simplifying the fraction)

Hence λ is well-defined.

Now the addition: $\mathcal{L}$ through P_1 and P_2 intersects $\mathcal{C}$ in a 3rd point P_3.

$\mathcal{L}: s = \lambda(t - t_1) + s_1$ $\qquad \lambda = \frac{s_2 - s_1}{t_2 - t_1}$

$\frac{s_2 - s_1}{t_2 - t_1}(t - t_1) + s_1$ $\qquad (t - t_1)(t - t_2)(t - \tilde{t}_3) = t^3 - (t_1 + t_2 + \tilde{t}_3) t^2 + \dots$ lower terms

$$s = t^3 + a s t^2 + b s^2 t + c s^3$$

$$\frac{s_2 - s_1}{t_2 - t_1}(t - t_1) + s_1 = t^3 + a\left(\frac{s_2 - s_1}{t_2 - t_1}(t - t_1) + s_1\right) t^2 + b\left(\frac{s_2 - s_1}{t_2 - t_1}(t - t_1) + s_1\right)^2 t + c\left(\frac{s_2 - s_1}{t_2 - t_1}(t - t_1) + s_1\right)$$

Let's write it in terms of t. → cubic equation.

$$t^3 + a(\lambda t - \lambda t_1 + s_1) t^2 + b(\lambda^2 (t^2 - 2 t_1 t + t_1^2) + s_1^2 + 2 s_1 \lambda (t - t_1)) t + c\left(\lambda^3 (t - t_1)^3 + \text{lower terms}\right)$$

$$(t^3 + a\lambda t^2 + b\lambda^2 t^3 + c\lambda^3 t^3) + \text{lower terms in } t.$$

$$1 + a\lambda + b\lambda^2 + c\lambda^3 = -t_1 - t_2 - \tilde{t}_3 \to -\tilde{t}_3 = 1 + a\lambda + b\lambda^2 + c\lambda^3 + t_1 + t_2$$

$\mathcal{C}$: $s = t^3 + a s t^2 + b s^2 t + c s^3$

$\mathcal{L}$: $s = \frac{s_2 - s_1}{t_2 - t_1}(t - t_1) + s_1$ and $\mathcal{L}(t_1, s_1)$ is true, $\mathcal{L}(t_2, s_2)$ is true.

$\mathcal{L}$: $s = \lambda t - \lambda t_1 + s_1$ (λ and we just saw that the denominator of λ is coprime to p.)

$s^2 = (\lambda t + s_1 - \lambda t_1)^2 = \lambda^2 t^2 + 2\lambda t(s_1 - \lambda t_1) + (s_1 - \lambda t_1)^2$

$\mathcal{L} \cap \mathcal{C}$: $s^2 = \lambda^2(t^2 - 2tt_1 + t_1^2) + s_1^2 + 2\lambda(t - t_1)s_1 = \lambda^2 t^2 + 2\lambda t s_1 + \text{constant term}$. $-2\lambda^2 t_1 t$

$s^3 = [illegible]_1 (\lambda t + s_1 - \lambda t_1)^3 = \lambda^3 t^3 + 3\lambda^2 t^2(s_1 - \lambda t_1) + \text{lower terms}$ $3\lambda t(s_1 - \lambda t_1)^2 + (s_1 - \lambda t_1)^3$

$t^3 + a(\lambda(t - t_1) + s_1)t^2 + b(\lambda^2 t^2 + 2\lambda t(s_1 - \lambda t_1) + (s_1 - \lambda t_1)^2)t$

$+ c(\lambda^3 t^3 + 3\lambda^2 t^2(s_1 - \lambda t_1) + 3\lambda t(s_1 - \lambda t_1)^2 + (s_1 - \lambda t_1)^3) - (\lambda(t - t_1) + s_1) = 0.$

$t^3 + a\lambda t^3 + b\lambda^2 t^3 + c\lambda^3 t^3 + a(-\lambda t_1 + s_1)t^2 + b(2\lambda(s_1 - \lambda t_1))t^2 + c \cdot 3\lambda^2 t^2(s_1 - \lambda t_1)$

$+ \text{lower term in } t = 0.$

$(1 + a\lambda + b\lambda^2 + c\lambda^3)t^3 + (a(-\lambda t_1 + s_1) + b(2\lambda(s_1 - \lambda t_1)) + 3c\lambda^2(s_1 - \lambda t_1))t^2 + \cdots = 0$

$(1 + a\lambda + b\lambda^2 + c\lambda^3)t^3 + (s_1 - \lambda t_1)(a + 2b\lambda + 3c\lambda^2)t^2 + \cdots = 0$

coprime to p.

we divide by the leading coefficient to get a monic polynomial:

$t^3 + \underbrace{(s_1 - \lambda t_1)}_{\beta} \frac{a + 2b\lambda + 3c\lambda^2}{1 + a\lambda + b\lambda^2 + c\lambda^3} t^2 + \cdots = 0.$

$(t - t_1)(t - t_2)(t - t_3)$

$\to t_1 + t_2 + t_3 = (\lambda t_1 - s_1)\frac{a + 2b\lambda + 3c\lambda^2}{1 + a\lambda + b\lambda^2 + c\lambda^3} = t^3 - (t_1 + t_2 + t_3)t^2 + \cdots$

$t_3 = (\lambda t_1 - s_1)\frac{a + 2b\lambda + 3c\lambda^2}{1 + a\lambda + b\lambda^2 + c\lambda^3} - t_1 - t_2$

by assumption, $p \mid t_1$ and $p \mid t_2$, and we obtained previously that $p \mid \lambda$ but $p \nmid$ denominator(λ).
(but $p \nmid$ denominator(t_1), $p \nmid$ denominator(t_2))

more precisely: $\lambda = \frac{s_1 - s_2}{t_1 - t_2} = \frac{t_1^2 + t_1 t_2 + t_2^2 + a(t_1 + t_2)s_1 + b s_1^2}{1 - a t_2^2 - b t_2(s_1 + s_2) - c(s_1^2 + s_1 s_2 + s_2^2)}$

$p^i \mid t_1$, $p^j \mid t_2$

$= \frac{t_1'^2 p^{2i} + p^{i+j} t_1' t_2' + p^{2j} t_2^2 + a p^i (t_1 + t_2 p^{j-i}) p^{3i} s_1' + b p^{6i} s_1'^2}{\text{denom coprime to } p} = p^{2i} \cdot \text{something}.$

$\to \text{val}_p(\lambda) \geq 2\,\text{val}_p(t_1)$.

$\text{val}_p(\lambda t_1 - s_1) = 3\,\text{val}_p(t_1)$.

$$t_3 = (\lambda t_1 - s_1)\,\frac{a+2b\lambda+3c\lambda^2}{1+a\lambda+b\lambda^2+c\lambda^3} - t_1 - t_2$$

and we showed that $\mathrm{val}_p(t_3) \geq \mathrm{val}_p(t_1)$.

more precisely:

$$t_1+t_2+t_3 = (\lambda t_1 - s_1)\,\frac{a+2b\lambda+3c\lambda^2}{1+a\lambda+b\lambda^2+c\lambda^3} \quad \text{has valuation at } p \geq 3\,\mathrm{val}_p(t_1) \geq 3.$$

$$P_1 + P_2 = (-t_3, -s_3)$$

Doubling: what is λ? $\mathcal{C}$: $s = t^3 + a s t^2 + b s^2 t + c s^3$.

$\Leftrightarrow \quad t^3 + a s t^2 + b s^2 t + c s^3 - s = 0.$

$$\frac{\partial \mathcal{C}}{\partial t} = 3t^2 + 2as t + bs^2$$

$$\frac{\partial \mathcal{C}}{\partial s} = at^2 + 2bst + 3cs^2 - 1$$

$$\frac{\partial \mathcal{C}/\partial t}{\partial \mathcal{C}/\partial s} = \frac{\partial s}{\partial t} = -\frac{3t^2+2ast+bs^2}{1-at^2-2bst-3cs^2} = -\lambda$$

$$\lambda = \frac{3t_1^2+2at_1s_1+bs_1^2}{1-at_1^2-2bt_1s_1-3cs_1^2}$$ same formula with $t_1=t_2$ as before (uses

$$\frac{t_1^2+t_1t_2+t_2^2+a(t_1+t_2)+s_1+bs_1^2}{1-at_2^2-bt_2(s_1+s_2)-c(s_1^2+s_1s_2+s_2^2)}$$

(in conclusion for addition and doubling, one has the same λ and t_3 s_3;

and $t_1+t_2+t_3 \equiv 0 \bmod p^{3v}$