Notes on Diophantine Geometry

Felipe Voloch and students

June 5, 2008

Rational Points on Curves of Genus Zero

An algebraic set over a field K is (the solution set of) a system of equations:

$$X : \begin{cases} f_1 = 0 \\ \quad \vdots \quad . \\ f_m = 0 \end{cases}$$

with $f_1, \ldots, f_m \in K[x_1, \ldots, x_n]$.

Let X be an irreducible algebraic set, i.e., $(f_1, \ldots, f_m)$ is a prime ideal. Next, let $R = K[x_1, \ldots, x_n]/(f_1, \ldots, f_m)$ and let $K(X)$ denote the field of fractions of R. Then the dimension of X is the transcendence degree of $K(X)$ over K:

$$\text{Tr deg}_K K(X) = \dim X.$$

X is a curve if $\dim X = 1$, that is, if some x_i is not in $\overline{K}$, and all other x_j are algebraic over $K(x_i)$.

We say that X, Y, irreducible algebraic sets, are birationally isomorphic if their function fields $K(X), K(Y)$ are isomorphic as field extensions of K.

Example 1. If $n = 2$ and $m = 1$, $f(x_1, x_2) = 0$, then this is a curve.

Now, we define the genus $g(X)$ of an irreducible curve X. Over a subfield of $\mathbb{C}$, the genus can be obtained from the topology of $X(\mathbb{C})$. An algebraic definition of genus is the dimension of the space of regular 1-forms on a smooth projective model. If X is a plane curve of degree d, then we have the following formula for the genus:

$$g(X) = \frac{1}{2}(d-1)(d-2) - \sum_{p \text{ singular}} \delta_p,$$

where, if the singularity is an ordinary singularity with m branches, then $\delta_p = \frac{1}{2}m(m-1)$. (So, δ_p depends on the singularity. There is an algorithm for computing it in general, but you won't find it in these notes.)

Background. Singular points are, for example, points $(x,\, y) \in \mathbb{C}^2$ with

$$f(x,\, y) = \frac{\partial f}{\partial x}\,(x,\, y) = \frac{\partial f}{\partial y}\,(x,\, y) = 0.$$

Example 2. For smooth (projective) plane curves of degree d, the genus is $\frac{1}{2}(d-1)(d-2)$. In particular

$$\begin{array}{rcl} g = 0 & \iff & d = 1,\, 2 \\ g = 1 & \iff & d = 3 \\ g > 1 & \iff & d \geq 4. \end{array}$$

Definition. An irreducible curve X is *parametrizable* (also, *rational*) over K if there exist $\varphi_1, \ldots, \varphi_n \in K(t)$ (not all constant) such that for all $j = 1, \ldots m$ we have $f_j(\varphi_1, \ldots, \varphi_n) = 0$.

Theorem 1. *A curve is parametrizable over K if and only if it has genus zero and a smooth point with coordinates in K.*

Proof. ($\Rightarrow$) If X is parametrizable then $K(X)$ embeds in $K(t)$. This is seen by considering the map $\alpha : K[x_1, \ldots, x_n] \to K(t)$ which sends $x_i \mapsto \varphi_i(t)$. Then $f_i \in \ker \alpha$, so that α induces a map $R = K[x_1, \ldots, x_n]/(f_1, \ldots, f_m) \to K(t)$. Thus, by Luroth's theorem, $K(X)$ is purely transcendental over K. X is therefore birationally isomorphic to a line, and so has genus zero and many smooth points in K.

($\Leftarrow$) A sketch of the proof in this direction: Use $g(X) = 0$ together with the smooth point P and the Riemann-Roch space $L(P)$ of functions whose only pole is a simple pole at P to get that $\dim L(P) = 2$. Then, we find a non-constant $f \in L(P)$, where $f : X \to \mathbb{P}^1$ has only one (simple) pole, so it has degree 1, making it a birational isomorphism. Thus, $f^{-1} : \mathbb{P}^1 \to X$ is a parametrization. $\square$

Example 3. Consider the curve $X : x^2 + y^2 = 1$. Then X has a point at $P = (1, 0)$. By the degree formula for the genus, $g(X) = 0$. We will give a parametrization of X working geometrically: Any line through P intersects

the curve in exactly one other point (unless it is tangent at P). The equation of a line through $(1,0)$ is given by $y = t(x-1)$. Substituting this into X for y and solving for x gives: $x = \frac{t^2-1}{t^2+1}$. Then, $y = t(x-1) = \frac{-2t}{t^2+1}$. This is our parametrization.

Assume K is perfect (e.g. has characteristic zero). By the genus formula and the fact that the genus is non negative, a cubic has at most one singularity. If a curve has a singular point in a field bigger than K, then its conjugates are also singular points so the curve must have other singular points. Therefore, we may conclude that an absolutely irreducible cubic with a singular point automatically has its singular point with coordinates in the ground field. The method used in the last example to find a parametrization works in this instance, too. You take the pencil of lines through the singular point, and because it is singular, this will give you a parametrization, hence lots of points. That is we get the following:

Corollary 2. *A singular cubic always has lots of points over the ground field.*

Example 4. Consider $X : y^2 = x^3 + x^2$. Then X has a singular point at the origin $P = (0,0)$. The equation of a line through $(0,0)$ is given by $y = tx$. Then, we get $x = t^2 - 1$, and so $y = t(t^2-1)$.

Example 5. But, $x^2+y^2 = -1$ has *no* solutions over $\mathbb{R}$. So, a smooth curve of degree 2 and genus 0, may have no points over $\mathbb{Q}$ or even $\mathbb{R}$. However, it does have points over $\mathbb{C}$.

Example 6. Another example is $x^2 + y^2 = 0$. But, this curve is reducible: $X = \{x = iy\} \bigcup \{x = -iy\}$.

Theorem 3. *Every curve of genus zero over K is birationally isomorphic to a conic.*

Proof. Ww will not give a proof, just remark that the proof uses the negative of the canonical divisor, which gives us a divisor of degree two on the curve. □

A conic is an absolutely irreducible curve of degree 2. Given by $f(x,y) = 0$ where deg $f = 2$.

If we are looking for rational solutions of an equation $f(x,y) = 0$ where deg $f = d$, we can also look at the homogenous polynomial of degree d in $x,\ y,\ z$ given by $z^d f(x/z, y/z)$. We have to be careful with $z = 0$.
A conic can be further simplified by diagonalization. So we can reduce the study of conics to equations of the form $ax^2 + by^2 + cz^2 = 0$ where absolute irreducibility is equivalent to $abc \neq 0$.
If $a,\ b,\ c \in \mathbb{Q}$ and we want to find out if $ax^2 + by^2 + cz^2 = 0$ has solutions, we can assume that $a,\ b,\ c \in \mathbb{Z}$ by clearing denominators. We can also assume that $a,\ b,\ c$ have no common factors.
If $a = m^2 \cdot a'$ then $ax^2 + by^2 + cz^2 = 0$ has a solution if and only if $a'x^2 + by^2 + cz^2 = 0$ has a solution (replace x by mx). In this way we can assume that a, b, c are square free.
Suppose there exists a prime p such that p divides both a and b. Then $a = a' \cdot p$ and $b = b' \cdot p$. If $ax^2 + by^2 + cz^2 = 0$ has a solution then

$$pa'x^2 + pb'y^2 + cz^2 \quad = \quad 0$$

$$a'(px)^2 + b'(py)^2 + pcz^2 \quad = \quad 0$$

has a solution. Proceeding in this way, I can eliminate common factors of any two of $a,\ b,\ c$.
Legendre's Theorem. *Suppose that $a,\ b,\ c \in \mathbb{Z}$ are nonzero, square free, and pairwise coprime. Then the equation $ax^2 + by^2 + cz^2 = 0$ has a solution in $\mathbb{Z}^3 - \{(0,0,0)\}$ if and only if the following two conditions are satisfied.*

(i) *$a,\ b,\ c$ are not all of the same sign.*

(ii) *For all odd primes $p \mid abc$ there is a solution to $ax^2 + by^2 + cz^2 \equiv 0 \bmod p$ where all of $x,\ y,\ z \not\equiv 0 \bmod p$*

Proof. ($\Uparrow$) If $p \mid abc$ assume that $p \mid a$. We are asuming that $\exists\ x_0,\ y_0, z_0 \not\equiv 0 \bmod p$ with $ax_0^2 + by_0^2 + cz_0^2 \equiv 0 \bmod p$ which is equivalent to $by_0^2 + cz_0^2 \equiv 0 \bmod p$. Let

$$u^2 = -\frac{b}{c} = \left(\frac{z_0}{y_0}\right)^2$$

As a polynomial,

$$\begin{aligned} ax^2 + by^2 + cz^2 &\equiv by^2 + cz^2 \bmod p \\ &\equiv c(z^2 - u^2y^2) \bmod p \\ &\equiv c(z - uy)(z + uy) \bmod p \end{aligned}$$

So for every odd prime $p \mid abc$ there are linear forms L_p and L'_p in $x,\ y,\ z$ with

$$ax^2 + by^2 + cz^2 \equiv L_p L'_p \bmod p$$

Also, for $p = 2$,

$$ax^2 + by^2 + cz^2 \equiv (ax + by + cz)^2 \bmod 2$$

So there is also L_2 and L'_2 such that

$$ax^2 + by^2 + cz^2 \equiv L_2 L'_2 \bmod 2$$

By the Chinese Remainder Theorem, there exist linear forms L and L'such that

$$ax^2 + by^2 + cz^2 \equiv LL' \bmod abc$$

Consider integers $x_0,\ y_0,\ z_0$ that satisfy the inequalities

$$0 \le x_0 \le \sqrt{|bc|}, 0 \le y_0 \le \sqrt{|ac|}, 0 \le z_0 \le \sqrt{|ab|}$$

Since $a,\ b,\ c$ are square free and coprime, we actually have

$$0 \le x_0 < \sqrt{|bc|}, 0 \le y_0 < \sqrt{|ac|}, 0 \le z_0 < \sqrt{|ab|}$$

How many such triples are there? The answer is greater than

$$\left(1 + \left\lfloor \sqrt{|bc|} \right\rfloor\right)\left(1 + \left\lfloor \sqrt{|ac|} \right\rfloor\right)\left(1 + \left\lfloor \sqrt{|ab|} \right\rfloor\right) > |abc|.$$

By the Pigeonhole Principle there exists distinct such triples $(x_0,\ y_0,\ z_0)$ and $(x_0',\ y_0',\ z_0')$ with

$$L(x_0,\ y_0,\ z_0) \ \equiv \ L(x_0',\ y_0',\ z_0') \text{mod } abc$$

which implies that

$$L(x_0 - x_0',\ y_0 - y_0',\ z_0 - z_0') \ \equiv \ 0 \text{ mod } abc$$

and consequently

$$a(x_0 - x_0')^2 + b(y_0 - y_0')^2 + c(z_0 - z_0')^2 \ \equiv \ 0 \text{ mod } abc$$

Let $x = x_0 - x_0',\ y = y_0 - y_0'$ and $z = z_0 - z_0'$. Then

$$x < \sqrt{|bc|}, y < \sqrt{|ac|}, z < \sqrt{|ab|}$$

and

$$ax^2 + by^2 + cz^2 \ \equiv \ 0 \text{ mod } abc$$

By condition (i) we may suppose without a loss of generality that $a < 0,\ b < 0$, and $c > 0$. This implies that $|abc| \ = \ abc$. As a result

$$\begin{aligned} ax^2 + by^2 + cz^2 \ &\leq \ cz^2 \ < abc \\ -(|a|x^2 + |b|y^2) \ &\leq \ ax^2 + by^2 + cz^2 \\ -2abc \ &< \ -(|a|x^2 + |b|y^2) \end{aligned}$$

so that

$$-2abc \ < \ ax^2 + by^2 + cz^2 \ < \ abc$$

and

$$ax^2 + by^2 + cz^2 \ = \ 0 \text{ or } -abc$$

If $ax^2 + by^2 + cz^2 = 0$, then we are done. We thus suppose that

$$ax^2 + by^2 + cz^2 = -abc$$

$$ax^2 + by^2 + c(z^2 + ab) = 0$$

Since a and b are squarefree and coprime, $z^2 + ab \neq 0$. The proof of the $\Uparrow$ direction is complete by the following polynomial identity.

$$a(xz+by)^2+b(yz-ax)^2+c(z^2+ab)^2 = (ax^2+by^2+c(z^2+ab))(z^2+ab) = 0$$

Proof. ($\Downarrow$) Suppose that $ax^2 + by^2 + cz^2 = 0$ where $x, y, z \in \mathbb{Z}$ are not all zero. Let p be an odd prime. If p divides x, y and z then

$$a\left(\frac{x}{p}\right)^2 + b\left(\frac{y}{p}\right)^2 + \left(\frac{z}{p}\right)^2 = 0$$

We may thus suppose that p does not divide one of x, y, or z. If p divides x and y but not z then it follows that p^2 divides cz^2 and therefore that p^2 divides c. c was assumed to be square free. This is a contradiction. So p can divide at most one of x, y, and z.

Suppose that p divides a and x but not y or z. From $ax^2 + by^2 + cz^2 = 0$ we have

$$a1^2 + by^2 + cz^2 \equiv 0 \bmod p$$

Suppose that p divides a and y but not x or z. Then

$$0 = ax^2 + by^2 + cz^2 \equiv cz^2 \bmod p$$

So p divides c. This is a contradiction since a and c are coprime. $\square$

New Topic: P-Adic Numbers

Let p be a prime number. For $x \in \mathbb{Q}, x \neq 0$ we can write

$$x = p^r \cdot \left(\frac{a}{b}\right)$$

with $a,\ b,\ r\ \in\ \mathbb{Z}$ and $p \nmid\ ab$.

The $p-$adic norm of x is defined as $|x|_p\ =\ p^{-r}$ and $|0|_p\ =\ 0$.
The $p-$adic distace from x to y is defined as $d_p(x,y)\ =\ |x-y|_p$.
Exercise: Prove that d_p is a metric.

$\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to the metric d_p.
$\mathbb{Z}_p$ is the completion of $\mathbb{Z}$ with respect to the metric d_p.
Exercise: Show that $\mathbb{Q}_p$ is a field, $\mathbb{Q} \subseteq \mathbb{Q}_p$ and $\mathbb{Z}_p$ is a ring, $\mathbb{Z} \subseteq \mathbb{Z}_p$.
Every element of $\mathbb{Q}_p$ is of the form

$$x\ =\ \sum_{n=n_0}^{\infty} a_n p^n$$

where $a_n\ \in\ \{\ 1,\ \ldots,\ p-1\ \}$, $a_{n_0}\ \neq\ 0$ and $|x|_p\ =\ p^{-n_0}$.
We note the **ultrametric inequality**. For $x,\ y\ \in\ \mathbb{Q}_p$,

$$|x+y|_p \leq \max\{\ |x|_p,\ |y|_p\ \}$$

$\mathbb{Z}_p$ is a local ring with maximal ideal (p).
$\dfrac{1}{1-p}\ =\ \sum\limits_{n=0}^{\infty} p^n\ \in\ \mathbb{Z}_p$. So $1-p$ is a unit.
Exercise: Show that for all $a \in \mathbb{Z},\ p \nmid\ a$, a is a unit in $\mathbb{Z}_p$.
$\dfrac{\mathbb{Z}_p}{(p^n)} \cong \dfrac{\mathbb{Z}}{p^n\mathbb{Z}}$
Exercise: Show that $\mathbb{Z}_p$ is isomorphic to

$$\begin{aligned} \lim_{\leftarrow} \frac{\mathbb{Z}}{p^n\mathbb{Z}}\ &:=\ \{(a_1,a_2,\ldots)\mid\ a_i \in \frac{\mathbb{Z}}{p^i\mathbb{Z}},\ a_{i+1} \equiv a_i \bmod p^i\ \} \\ &\subseteq\ \frac{\mathbb{Z}}{p\mathbb{Z}} \times \frac{\mathbb{Z}}{p^2\mathbb{Z}} \times \cdots \end{aligned}$$

Theorem. The following are equivalent.

(i) $f(x_1,\ldots,x_n)\ \in\ \mathbb{Z}[x_1,\ldots,x_n]$ such that $\forall\ r\ \exists$ solutions to $f(x_1,\ldots,x_n)\ \equiv\ 0 \bmod p^r, \quad x_i \in \mathbb{Z}$.

(ii) $\exists$ solutions to $f(x_1, \ldots, x_n) = 0$ with $x_i \in \mathbb{Z}_p$.

Proof. (i) $\Longrightarrow$ (ii)
For each r let $x_1^{(r)}, \ldots, x_n^{(r)} \in \mathbb{Z}$ with $f(x_1^{(r)}, \ldots, x_n^{(r)}) \equiv 0 \bmod p^r$. Since $\mathbb{Z}_p$ is compact $\exists$ a convergent subsequence for the $x_i^{(r)}$ and the limit satisfies $f(x_1, \ldots, x_r) = 0$
suitable for generalization.

Theorem 4. *A conic defined over $\mathbb{Q}$ has a $\mathbb{Q}$-rational point if and only if it has a $\mathbb{Q}_p$-rational point for all p, p prime or $p = \infty$.*

We will see that checking p-adic solubility is easy. Here are some (chronological) remarks.

Minkowski: A quadric (hypersurface of degree 2) has a point over $\mathbb{Q}$ if and only if it has point over $\mathbb{Q}_p$ for all p.

Meyer: A quadric of dim ≥ 4 always has points over $\mathbb{Q}_p$, if $p \neq \infty$(clearly we can always find a quadric with no real points).

Hasse: Generalized Legendre and Minkowski to number fields and function fields (global fields). He formulated what is now called the Hasse Principle: Solutions over $\mathbb{Q}_p$ for all p implies solution over $\mathbb{Q}$. It is not universally true but it is true for certain families of equations.

Definition. An absolute value on a field K is a map

$$|\cdot| : K \to \mathbb{R}$$

such that

1. $\forall x \in K, |x| \geq 0$ and $|x| = 0 \Leftrightarrow x = 0$.
2. $|xy| = |x||y| \qquad \forall x, y \in K$.
3. $|x + y| \leq |x| + |y| \qquad \forall x, y \in K$.

Example 7. The "usual" absolute value on $\mathbb{Q}$ is

$$|x|_\infty = \begin{cases} x, & \text{if} \quad x \geq 0 \\ -x, & \text{if} \quad x < 0 \end{cases}$$

$|\cdot|_p$ is the p-adic absolute value defined last lecture.

There is also the trivial absolute value :

$$|\cdot|_0 = \begin{cases} 1, & \text{if} \quad x \neq 0 \\ 0, & \text{if} \quad x = 0 \end{cases}$$

Definition. Two absoulte values on K are equivalent if they induce the same topology.

Theorem 5. *(Ostrowski) Every absolute value in $\mathbb{Q}$ is equivalent to $|\cdot|_p$ for some p, p prime, $p = \infty$ or $p = 0$.*

If $K/\mathbb{Q}$ is finite extension (i.e. K is a number field), then for each absolute value $|\cdot|$ on $\mathbb{Q}$ there is only a finite number of equivalence classes of absolute values on K that gives $|\cdot|$ when restricted to $\mathbb{Q}$. We denote by M_K the set of equivalence classes of absolute values on K. If $v \in M_K$, then, there exists p=prime,0 or ∞ such that $|x|_v = |x|_p \ \forall x \in \mathbb{Q}$. We say that $v|p$ (v divides p).

Product Formula: if $x \in \mathbb{Q}$ and $x \neq 0$, then

$$\prod |x|_p = 1$$

To see this, we write $x = \pm p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, $\alpha_i \in \mathbb{Z}$, p_i prime, and notice that

$$|x|_p = \begin{cases} 1 & \text{if} \quad p \neq p_i, \infty \\ p^{-\alpha_i} & \text{if} \quad p = p_i \\ p_1^{\alpha_1} \cdots p_r^{\alpha_r} & \text{if} \quad p = \infty \end{cases}$$

The product formula can be generalized to a number field K.

There is a choice of $n_v \in \mathbb{Z}$, for $v \in M_K$, such that $\forall x \in K$, $x \neq 0$

$$\prod_v |x|_v^{n_v} = 1$$

In $\mathbb{F}(t)$, where $\mathbb{F}$ is any field, there are absolute values corresponding to each monic irreducible polynomial in $\mathbb{F}[t]$ and another absolute value "at infinity". Choose $c > 1$ real number.

For $x = a/b$, $a, b \in \mathbb{F}[t]$ and $(a, b) = 1$, define

$$|x|_\infty = c^{\deg(a) - \deg(b)}$$

For instance, $|\frac{1}{t}|_\infty = \frac{1}{c}$.

Using valuation to define an absolute value, we have a way of writing the product formula eliminating the constant:

For $x = p^r \frac{a}{b} \in \mathbb{F}(t)$, $p \in \mathbb{F}[t]$ monic irreducible and $p \nmid ab$, we set

$v_p(x) = r$ and $|x|_p = c^{-v_p(x) \deg p}$ and then

$$\prod |x|_p = 1 \Leftrightarrow \prod c^{-v_p(x) \deg p} = 1 \Leftrightarrow \sum v_p(x) \deg p = 0$$

Notice that the last part is just expressing the fact that for any rational function we have # zeros=#poles.

The previous discussion was intended to introduce the following result.

Theorem 6. *(Hasse-Minkowski) If K is a global field then a quadric defined over K has K-rational points if and only if it has K_v-rational points for all $v \in M_K$.*

The next theorem will be proved later on.

Theorem 7. *Let X be an absolutely irreducible algebraic variety over a global field K. Then $X(K_v) \neq \emptyset$ for all but finitely many $v \in M_K$. Moreover, the exceptional v can be effectively listed.*

Theorem 8. *$f(x_1, \cdots, x_n) \in \mathbb{Z}[x_1, \cdots, x_n]$ non-constant and absolutely irreducible. Then for all but finitely many primes p, and for all $r \geq 0$, there exist solutions to*

$$f(x_1, \cdots, x_n) \equiv 0 \mod p^r$$

Definition. If $\mathcal{X}$ is a collection of varieties defined over a global field K, then we say that $\mathcal{X}$ satisfy the Hasse principle if $\forall X \in \mathcal{X}$

$$X(K) \neq \emptyset \Longleftrightarrow X(K_v) \neq \emptyset \qquad \forall v \in M_K$$

Big question: Which families satisfies the Hasse principle?

We know the following:

- Hasse-Minkowski: Quadrics satisfy the Hasse principle .
- Hooley, Heath Brown: Cubics in ≥ 8 variables satisfy the Hasse principle (over $\mathbb{Q}$).

Question: Which varieties in ≥ 3 variables do not satisfy the Hasse principle?

It is known that $3x^3 + 4y^3 + 5 = 0$ has points in $\mathbb{Q}_p$ for all p but does not have a rational point and there is an example with three variables as well. The case of cubics with $4, 5, 6$ and 7 variables is open.

Theorem 9. *Let $f \in \mathbb{Z}[x_1, \ldots, x_n]$ be absolutely irreducible. Then for all but finitely many primes p, there is a solution to the equation $f = 0$ in $\mathbb{Z}_p^n$.*

Remark. *The proof given below works for any global field.*

The proof will be given in three steps
Step 1: If $f \in \mathbb{Z}[x_1, \ldots, x_n]$ is absolutely irreducible, then $f \in (\mathbb{Z}/p\mathbb{Z})[x_1, \ldots, x_n]$ is absolutely irreducible for all but finitely many primes p.
Step 2: If f is absolutely irreducible in $(\mathbb{Z}/p\mathbb{Z})[x_1, \ldots, x_n]$ and p is large with respect to $\deg f$ and n, then the variety defined by $f = 0$ has a smooth point in $(\mathbb{Z}/p\mathbb{Z})^n$.
Step 3: If the variety defined by $f = 0$ has a smooth point in $(\mathbb{Z}/p\mathbb{Z})^n$, then it has a point in $\mathbb{Z}_p^n$.
Step 1: If $f \in \mathbb{Z}[x_1, \ldots, x_n]$ is absolutely irreducible, then $f \in (\mathbb{Z}/p\mathbb{Z})[x_1, \ldots, x_n]$ is absolutely irreducible for all but finitely many primes $p \in \mathbb{N}$.

Let $d = \deg f$. Fix $d \geq 2$ and $n \geq 1$. Let us consider a polynomial of degree d in n variables as a vector of its coefficients; in this way, we can identify the set of polynomials of degree d in n variables with the vector

space $V_{n,d}$ of dimension $N = \binom{n+d}{n}$. Under this identification, we define the map $\phi_k : V_{n,k} \times V_{n,d-k} \to V_{n,d}$, where $1 \leq k \leq d-1$, by $(g,h) \mapsto gh$, where g and h are polynomials in the same n variables with $\deg g = k$, $\deg g = n-k$, and gh is the product of g and h as polynomials. By the formula of multiplication of polynomials in terms of their coefficients, the image of ϕ_k is an algebraic set in the N-dimensional affine space $V_{n,d}$, so is the union U of the image of ϕ_k over $1 \leq k \leq d-1$. Therefore U is the set of common zeros $(c_1, \ldots, c_N)$ of some $F_1, \ldots, F_r \in \mathbb{Z}[y_1, \ldots, y_N]$. This means that f factors nontrivially if and only if $F_1 = \ldots = F_r = 0$ at $f \in V_{n,d}$, that is, the coefficients of f satisfies the polynomial equations $F_1 = \ldots = F_r = 0$ in N variables. In fact, the polynomial equations can be written explicitly in some case as the following exercise shows.

Exercise. *Let $f(x,y) = a_1x^2 + a_2xy + a_3y^2 + a_4x + a_5y + a_6$ be a polynomial of degree 2 over a field whose characteristic is not 2. Then f factors nontrivially if and only if*

$$\det \begin{pmatrix} a_1 & \frac{a_2}{2} & \frac{a_4}{2} \\ \frac{a_2}{2} & a_3 & \frac{a_5}{2} \\ \frac{a_4}{2} & \frac{a_5}{2} & a_6 \end{pmatrix} = 0$$

By the assumption that $f \in \mathbb{Z}[x_1, \ldots, x_n]$ is absolutely irreducible, there must be some F_i which does not vanish at f. Since the coefficients of F_i and f are all in $\mathbb{Z}$, $F_i(f)$ is a nonzero rational integer. Hence $F_i(f) \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$ for all but finitely many primes p, which implies that $f \in (\mathbb{Z}/p\mathbb{Z})[x_1, \ldots, x_n]$ is absolutely irreducible for those prime since the construction of $F_1, \ldots, F_r$ passes naturally through quotients.

Remark. *The classical algebraic geometry works only on algebraically closed fields, hence in the priori the coefficients of $F_1, \ldots, F_r$ are in $\bar{\mathbb{Q}}$. However the elimination theory ensure that we can get $F_1, \ldots, F_r$ in $\mathbb{Q}[y_1, \ldots, y_N]$, hence in $\mathbb{Z}[y_1, \ldots, y_N]$ by clearing denominators.*

There is a similar statement for smoothness: If the variety X is smooth, then X mod p is smooth for all but finitely many primes p.
Let X be defined by the polynomial equation $f(x_1, \ldots, x_n) = 0$. We say X is not smooth if there is $c = (c_1, \ldots, c_n)$ such that

$$f(c) = \frac{\partial f}{\partial x_i}(c) = 0, \qquad i = 1, \ldots, n.$$

For this to be true, there must be a relation among the coefficients of f. For cubics to be singular, it needs at least one condition for the coefficients; for

them to be reducible, it needs at least two conditions for the coefficients.
If X is smooth, primes p with X mod p smooth is called the primes of good reduction (associated with X).
Now let us get some geometric intuition about good or bad reductions. As mentioned in the beginning of semester, in order to see the geometry, we have to work on algebraically closed fields. Thus let F be an algebraically closed field and $R = F[t]$, $K = F(t)$. Since F is algebraically closed, the prime ideals in R are of the form $(t-c)R$ with $c \in F$. Thus the set of prime ideals in R can be identified with F. In this case, $F[t]$ plays the role of $\mathbb{Z}$, and F plays the role of the set of primes $p \in \mathbb{N}$. Now consider a polynomial $f \in R[x_1, \ldots, x_n]$, i.e. the coefficients of f are in $F[t]$. We write f as f_t to indicate the dependence. For any $c \in F$, the element $f \in (R/(t-c)R)[x_1, \ldots, x_n]$ is simply f_c; this corresponds the algebraic set V_c defined by $f_c = 0$ in the n-dimensional affine space. The primes of good reduction corresponds the points $c \in F$ such that V_c is smooth. In this context, one can show the set of all $c \in F$ such that V_c is not smooth is closed in the Zariski topology of F, hence is finite. Step 1 is the corresponding statement when $F[t]$ is replaced by $\mathbb{Z}$.
In general, if we do not assume that F is algebraically closed, the primes of $F[t]$ corresponds the monic irreducible polynomials, which can be identified with the Galois orbits of elements in the algebraic closure of F.

Step 2: If f is absolutely irreducible in $(\mathbb{Z}/p\mathbb{Z})[x_1, \ldots, x_n]$ and p is large with respect to $\deg f$ and n, then the variety defined by $f = 0$ has a smooth point in $(\mathbb{Z}/p\mathbb{Z})^n$.
To show this, we use the Lang-Weil estimate (which we do not prove):

Theorem 10. *Given $n \geq 1$, $d \geq 1$, there are constants $C(n,d)$, $C_1(n,d)$ such that for any primes q and any absolute irreducible $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ with degree d,*

$$|\#\{p \in \mathbb{F}_q^n | f(p) = 0\} - q^{n-1}| \leq C(n,d) q^{n-\frac{3}{2}} + C_1(n,d)$$

Hyperplane sections reduce to $n = 2$ which is due to Hasse-Weil. (Function field analogues of the Riemann Hypothesis)
Fact: $C(2,d) = (d-1)(d-2)$
To do Step 2, we want a solution $c \in (\mathbb{Z}/p\mathbb{Z})^n$ to $f = 0 \pmod p$ with $\frac{\partial f}{\partial x_i}(c) \neq 0 \pmod p$ for some i.
Lang-Weil gives that the number of solution to $f = 0 \pmod p$ is about p^{n-1}. Solutions to $f = 0 \pmod p$, $\frac{\partial f}{\partial x_1} = 0 \pmod p$ must satisfy $\mathrm{Res}_{x_n}(f, \frac{\partial f}{\partial x_1}) = 0$, a equation in $x_1, \ldots, x_{n-1}$). The latter one has about p^{n-2} solutions by Lang-Weil; and given one of its solution $x_1, \ldots, x_{n-1}$, there are at most d

values for x_n with $f(x_1, \ldots, x_n) = 0$. Hence we conclude the number of solutions to $f = \frac{\partial f}{\partial x_1} = 0 \pmod p$ is at most $d(p^{n-2} + C(n-1,d)p^{n-\frac{5}{2}} + C_1(n-1,d)$. For p large enough, this is less than $p^{n-1} - C(n,d)q^{n-\frac{3}{2}} - C_1(n,d)$, which is a lower bound of the number of solution to $f = 0 \pmod p$. Therefore, for p large enough, there exists a solution to $f = 0 \pmod p$ which is not a solutions to $\frac{\partial f}{\partial x_1} = 0 \pmod p$. Step 2 is done.

Under the given assumption, we have established the following consequences:
1. $f \in (\mathbb{Z}/p\mathbb{Z})[x_1, \ldots, x_n]$ is absolutely irreducible for all sufficiently large primes p.
2. For all sufficiently large primes p, the variety defined by $f = 0$ has a smooth point in $(\mathbb{Z}/p\mathbb{Z})^n$.

The final step is to turn the smooth point in $(\mathbb{Z}/p\mathbb{Z})^n$ of the variety defined by $f = 0$ to a p-adic point.

Essentially we want to prove Hensel's Lemma:

Lemma 1. *(Hensel) Suppose $f \in \mathbb{Z}[x]$ and $a \in \mathbb{Z}$ is such that $f(a) = 0 \pmod p$ and $f'(a) \neq 0 \pmod p$. Then there exists an $\alpha \in \mathbb{Z}_p$ such that $\alpha = a \pmod p$ and $f(\alpha) = 0$.*

Remark. *Note that the assumption $f(a) = 0 \pmod p$ is equivalent to $|f(a)|_p < 1$; the assumption $f'(a) \neq 0 \pmod p$ is equivalent to $|f'(a)|_p = 1$; the conclusion asserts that there exists an $\alpha \in \mathbb{Z}_p$ such that $|\alpha - a|_p < 1$ and $f(\alpha) = 0$. Therefore Hensel's Lemma is an analogue to the Newton's method of finding zeros of differentiable functions on the real line.*

First we prove by induction on n that there exist $a_n \in \mathbb{Z}$ such that $a_n = a_{n-1} \pmod{p^{n-1}}$ for $n \geq 2$, and $f(a_n) = 0 \pmod{p^n}$ and $f'(a_n) \neq 0 \pmod p$ for $n \geq 1$. Letting $a_1 = a$, we have the base case for free. As for inductive steps, we want to find $z \in \mathbb{Z}$ such that $f(a_{n-1} + zp^{n-1}) = 0$ and $f'(a_{n-1} + zp^{n-1}) \neq 0 \pmod p$, therefore we can put $a_n = a_{n-1} + zp^{n-1}$.

Write $f(x) = \sum_{i=0}^{d} c_i x^i$. Observe the equality

$$f(a_{n-1} + zp^{n-1}) = f(a_{n-1}) + f'(a_{n-1})zp^{n-1} + \frac{f''(a_{n-1})}{2!}(zp^{n-1})^2 + \cdots .$$

We claim $f(a_{n-1} + zp^{n-1}) \equiv f(a_{n-1}) + zp^{n-1}f'(a_{n-1}) \pmod{p^n}$ by showing

$\frac{f^{(k)}(c)}{k!} \in \mathbb{Z}$ for any $c \in \mathbb{Z}$ and $1 \leq k \leq d$. Note that

$$\frac{f^{(k)}(c)}{k!} = \sum_{i=k}^{d} \frac{i(i-1)\cdots(i-k+1)}{k!} c_i c^{i-k},$$

and that $\frac{i(i-1)\cdots(i-k+1)}{k!} = \binom{i}{k} \in \mathbb{Z}$, which proves the claim.

Now I want to find $z \in \mathbb{Z}$ such that $f(a_{n-1}) + zp^{n-1} f'(a_{n-1}) \equiv 0 \pmod{p^n}$. By inductive hypothesis $f(a_{n-1}) \equiv 0 \pmod{p^{n-1}}$, we write $f(a_{n-1}) = up^{n-1}$ for some $u \in \mathbb{Z}$. Therefore we aim to find $z \in \mathbb{Z}$ so that $(u + zf'(a_{n-1}))p^{n-1} = 0 \pmod{p^n}$, i.e. $u + zf'(a_{n-1}) = 0 \pmod{p}$. By inductive hypothesis $f'(a_{n-1}) \neq 0 \pmod{p}$, such $z \in \mathbb{Z}$ can be therefore found. Since

$$f'(a_{n-1} + zp^{n-1}) = f'(a_{n-1}) + f''(a_{n-1})zp^{n-1} + \frac{f^{(3)}(a_{n-1})}{2!}(zp^{n-1})^2 + \cdots$$

and we have shown that $\frac{f^{(k)}(c)}{k!} \in \mathbb{Z}$ for any $c \in \mathbb{Z}$ and $1 \leq k \leq \deg f$, we conclude that $\frac{f^{(k)}(a_{n-1})}{(k-1)!} \in \mathbb{Z}$ for $2 \leq k \leq \deg f$, and $f'(a_{n-1} + zp^{n-1}) = f'(a_{n-1}) \neq 0 \pmod{p}$. Therefore we put $a_n = a_{n-1} + zp^{n-1}$ and complete the inductive step.

Now we have a sequence $\{a_n\}_{n \geq 1}$ of integers with the stated properties. We claim $\{a_n\}_{n \geq 1}$ forms a Cauchy sequence in the p-adic norm. To see this, we apply the strong triangular inequality: for any $n > m$,

$$|a_n - a_m|_p = |\sum_{i=m}^{n-1} (a_{i+1} - a_i)|_p \leq \max\{|a_{i+1} - a_i|_p : m \leq i \leq n-1\} \leq p^{-m} \to 0$$

as $m \to \infty$. So there exists $\alpha \in \mathbb{Z}_p$ such that $a_n \to \alpha$ as $n \to \infty$, which implies $f(a_n) \to f(\alpha)$ as $n \to \infty$ since polynomials are continuous. We have also $f(a_n) = 0 \pmod{p^n}$, which implies $f(a_n) \to 0$ as $n \to \infty$, and therefore $f(\alpha) = 0$.

Example. $f(x) = x^2 + 1, \qquad p = 5$
$a_1 = a = 2$
$f(2) = 5 = 0$ *(mod 5)*
$f'(2) = 4 \neq 0$ *(mod 5)*
$a_2 = 2 + 5z_2$
$f(2 + 5z_2) = 5 + 2 \cdot 2 \cdot 5z_2 + 5^2 z_2^2 = 5(1 + 4z_2) + 5^2 z_2^2 = 0$ *(mod 5^2)* $\Rightarrow z_2 = 1$
$a_3 = 7 + 5^2 z_3$
$f(7 + 5^2 z_3) = 50 + 2 \cdot 7 \cdot 5^2 z_3 + 5^4 z_3^2 = 5^2(2 + 14z_3) + 5^4 z_3^2 = 0$ *(mod 5^3)*
$\Rightarrow z_3 = 2$

Question: How to write negative rational integer as p-adic numbers? Answer: For example, we have $-1 \equiv p^n - 1 = (p-1)(1+p+p^2+\ldots+p^{n-1}) \bmod p^n$. Thus as a p-adic number, $-1 = (p-1)(1+p+p^2+\ldots)$. Alternatively, using a bomb to kill an ant, we may apply Hensel's Lemma to the polynomial $x+1$ in order to write -1 a p-adic number.

To turn a solution $(a_1, \ldots, a_n) \in (\mathbb{Z}/p\mathbb{Z})^n$ of $f = 0$ and $\frac{\partial f}{\partial x_i} \neq 0$ for some i into a p-adic one, simply apply Hensel's Lemma to

$$f(a_1, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_n) \in \mathbb{Z}[x].$$

Then we have an $\alpha \in \mathbb{Z}_p$ such that $(a_1, \ldots, a_{i-1}, \alpha, a_{i+1}, \ldots, a_n)$ is a p-adic solution to $f = 0$. This completes the proof of Theorem **??**.

Examining the proof of Theorem **??**, we discuss how large the prime p needs to be in each step.

In Step 1, we want $f \in (\mathbb{Z}/p\mathbb{Z})[x_1, \ldots, x_n]$ to be absolutely irreducible. This require that p is so large that does not divide an integer which depends only on coefficients of f.

In Step 2, we want a smooth point in $(\mathbb{Z}/p\mathbb{Z})^n$ of the variety defined by $f = 0$. This require that p is so large in terms of the degree of f and the number of its variables that the Lang-Weil estimate gives a smooth solution of $f = 0$.

In Step 3, Hensel's Lemma can be applied for those primes $p \in \mathbb{N}$ which a smooth solution in $(\mathbb{Z}/p\mathbb{Z})^n$ is found in Step 2. This does not require the primes to be larger further.

Next, we investigate the question: How likely is it that an $f \in \mathbb{Z}[x_1, \ldots, x_n]$ has zeros in $\mathbb{Z}_p^n$ for all primes p?

Theorem 11. *For any $n \geq 1$, $d \geq 1$ and $H \geq 1$, let $A_{n,d,H}$ be the set of polynomials in $\mathbb{Z}[x_1, \ldots, x_n]$ with total degree d whose coefficients are no bigger than H in their absolute values; let $B_{n,d,H}$ be the set of polynomials in $A_{n,d,H}$ such that for any prime p they have a zero in Z_p^n. Then we have*

$$\lim_{H \to \infty} \frac{\#B_{n,d,H}}{\#A_{n,d,H}} > 0 \qquad \text{if } n \geq 2, d \geq 2 \text{ and } (n,d) \neq (2,2).$$

We count "bad" polynomials in each of three steps in the proof of Theorem **??**.

In Step 3, no bad polynomial is there.

In Step 1, for $n \geq 2, d \geq 2$ and $(n,d) \neq (2,2)$, the subspace of reducible polynomials has codimension at least 2 in the space of polynomials of total

degree d in n variables. So there are at least 2 numbers that need to be divisible by p in order for a polynomial in $\mathbb{Z}[x_1, \ldots, x_n]$ to be reducible in $(\mathbb{Z}/p\mathbb{Z})[x_1, \ldots, x_n]$. Thus the probability of a polynomial in $\mathbb{Z}[x_1, \ldots, x_n]$ being bad modulo p is no bigger than $\frac{1}{p^2}$. Equivalently, the probability of a polynomial in $\mathbb{Z}[x_1, \ldots, x_n]$ being good modulo p is no less than $1 - \frac{1}{p^2}$. Hence the probability of a polynomial in $\mathbb{Z}[x_1, \ldots, x_n]$ being good, i.e., good modulo any primes $p \in \mathbb{N}$, is no bigger than $\prod_p (1 - \frac{1}{p^2}) = \frac{6}{\pi^2} > 0$. Of course this is a heuristic argument.

In Step 2, given fixed n and d, all but finitely many primes $p \in \mathbb{N}$ are good for all polynomials in $\mathbb{Z}[x_1, \ldots, x_n]$ with total degree d. For each q of finitely many good primes, the probability of a polynomial in $\mathbb{Z}[x_1, \ldots, x_n]$ having a smooth zero is at least

$$\text{Prob}\left(f(0, \ldots, 0) = 0 \bmod q,\ \frac{\partial f}{\partial x_1}(0, \ldots, 0) \neq 0 \bmod q \right) = \frac{1}{q}(1 - \frac{1}{q}) > 0.$$

Again, this is a heuristic argument.

Conjecture 12. *Smooth hypersurfaces of degree d in n variables for $d \leq n$ and $n \geq 4$ satisfy the Hasse Principle.*

Conjecture 13. *Let $A_{n,d,H}$ be as in Theorem 11, and $B'_{n,d,H}$ be the set of polynomials in $A_{n,d,H}$ which admits a zero in $\mathbb{Q}^n$. Then*

$$\lim_{H \to \infty} \frac{\# B'_{n,d,H}}{\# A_{n,d,H}} = \begin{cases} C_{n,d} > 0 & \text{if } d \leq n \\ ? & \text{if } d = n+1 \\ 0 & \text{if } d \geq n+2. \end{cases}$$

No conjecture for $d = n + 1$. For $d \geq n + 2$, this conjecture is supported by the following heuristic argument:

Lemma 2. *If Λ is a lattice in $\mathbb{R}^n$, that is $\Lambda = \{a_1\lambda_1 + \ldots + a_n\lambda_n \mid a_i \in \mathbb{Z}\}$, where the λ_i are linearly independent, then:*

$$\#\{\lambda \in \Lambda \ :\ ||\lambda|| \leq H\} = cH^n + O(H^{n-1})$$

where:

$$c = \frac{\text{Vol}(S^n)}{\text{Vol}(\mathbb{R}^n/\Lambda)} \times \textit{Something that depends on the norm.}$$

Thus, letting $N = \binom{n+d}{d} - 1$, we have for $a \in \mathbb{Q}^n$, there exists some constant $c(a) > 0$ such that

$$\#\{f : |\text{coeff}(f)| \leq H, f(a) = 0\} = c(a)H^N + O(H^{N-1})$$

Using this lemma we see that:

$$\sum_{a \in A} \#\{f : |\text{coeff}(f)| \leq H, f(a) = 0\} = \sum_{a \in A} c(a)H^N + O(H^{N-1})$$

for A finite. If the error terms didn't matter this would give us:

$$\#\{f : |\text{coeff}(f)| \leq H, \exists a \in A, f(a) = 0\} \leq \sum_{a \in A} c(a)H^N$$

Now, for $d > n + 1$,

$$\sum_{a \in \mathbb{Q}^n} c(a) < \infty$$

and

$$\#\{f : |\text{coeff}(f)| \leq H\} \approx cH^{N+1}$$

so:

$$\frac{\#\text{f with solutions}}{\#\text{total}} \leq \frac{\sum_a c(a)H^N}{cH^{N+1}} = \frac{\sum_a c(a)}{cH}$$

which goes to 0 as $H \to \infty$.

Let K be a field. We will define n-dimensional projective space over K:

$$\mathbb{P}^n(K) = \{(a_0, \ldots, a_n) \in K^{n+1} : \exists i, a_i \neq 0\}/\sim$$

where the equivalence relation $\sim$ is defined by identifying $\mathbf{a} = (a_0, \ldots, a_n)$ and $\mathbf{b} = (b_0, \ldots, b_n)$, denoted $\mathbf{a} \sim \mathbf{b}$ if there exists $\lambda \in K^*$ such that $\mathbf{a} = \lambda\mathbf{b}$. The class of $(a_0, \ldots, a_n)$ is denoted $(a_0 : \ldots : a_n)$.

For example, when $K = \mathbb{Q}$ by the equivalence we see that we can represent every element of projective space as a vector of coprime integers in exactly 2 ways.

Suppose $f \in K[x_0, \ldots, x_n]$ is homogeneous of degree d, that is to say:

$$f(\lambda x_0, \ldots, \lambda x_n) = \lambda^d f(x_0, \ldots, x_n)$$

now if $\mathbf{a} \sim \mathbf{b}$ we have that $f(a) = \lambda^d f(b)$ thus:

$$f(a) = 0 \Leftrightarrow f(b) = 0$$

Thus the set of points in $\mathbb{P}^n(K)$ where f (homogeneous) vanishes is well defined. Thus we can make the following definition:

Definition 14. *A projective algebraic set is the set of common zeros of a collection of homogeneous polynomials.*

Let $\phi : K^n \hookrightarrow \mathbb{P}^n(K)$ be defined by $\phi(a_1, \ldots, a_n) = (1 : a_1 : \ldots : a_n)$.
If $f \in K[x_1, \ldots, x_n]$ is any polynomial define:

$$\overline{f} = f(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}) \in K[x_0, x_1, \ldots, x_n]$$

which is homogeneous. If $X = \{f_1 = \ldots = f_m = 0\} \subset \mathbb{A}^n$ then we can define the algebraic set $\overline{X} = \{\overline{f}_1 = \ldots = \overline{f}_n = 0\} \subset \mathbb{P}^n$ called the projective closure of X such that:

$$\phi(X(K)) = \overline{X}(K) \cap \phi(K^n)$$

The points of $\overline{X} - \phi(X)$ are called the points at infinity of $\overline{X}$.
Consider

$$f(x, y) = 0$$

so

$$\overline{f} = z^d f(\frac{x}{z}, \frac{y}{z})$$

and $\overline{f} = 0$ defines a curve in $\mathbb{P}^2$. The solutions to $\overline{f}(x, y, 0) = 0$ are points at infinity.

Example 15. *Consider:*

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

$$y^2 z = x^3 + axz^2 + bz^3$$

so the points at infinity correspond to $z = 0$ which implies $x^3 = 0$ or $x = 0$. So $(0 : y : 0) \sim (0 : 1 : 0)$ is the point at infinity.

A line in $\mathbb{P}^2(K)$ is the set of zeros of a linear homogeneous polynomial L.

Theorem 16. *Let $P, Q \in \mathbb{P}^2(K)$ $P \neq Q$ then there exists a unique line L that contains P and Q. Given L_1 and L_2 lines in $\mathbb{P}^2$ and $L_1 \neq L_2$ then there exists a unique point $P \in L_1 \cap L_2$.*

Proof. let $P = (a_0 : a_1 : a_2)$ and $Q = (b_0 : b_1 : b_2)$
then:

$$\det \begin{pmatrix} x_0 & x_1 & x_2 \\ a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 \end{pmatrix} = 0$$

is a line containing P and Q.

For the second part notice that the solutions to $\sum a_i x_i = 0$ and $\sum b_i x_i = 0$ is a 1-dimensional vector space, so this defines a unique point in $\mathbb{P}^2(K)$. □

If $X \subseteq \mathbb{P}^2$ is a cubic then given $P, Q \in X(K)$ there is a unique line $\overline{PQ}$ through them . Usually $\overline{PQ}$ meets $X(K)$ at a third point. (Also, usually the tangent at P also meets $X(K)$ in a new point). This allows us to usually produce new points from given points. The iteration of this process is known as the chord-tangent process.

Theorem 17. *(Mordell-Weil) Let X/K be a smooth cubic. If K is a global field then there exists a finite set $G \subseteq X(K)$ such that $X(K)$ can be obtained from G by the chord-tangent process.*

1 Elliptic curves

Definition: If K is a field then an elliptic curve E over K is a smooth irreducible projective curve of genus 1 with a point $P \in E(K)$

Question: Is it possible to decide if a curve of genus 1 over $\mathbb{Q}$ has a point over $\mathbb{Q}$?
Answer: There is a procedure which conjecturally works.

Proposition: Every elliptic curve over a field of characteristic $\neq 2, 3$ is isomorphic to a curve of the type

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

for some $a, b \in K, 4a^3 + 27b^2 \neq 0$ with the given point P mapping to $(0 : 1 : 0) = \mathcal{O}$.

Group law on E:

$\mathcal{O}$ is the identity, and if $P = (x, y)$ then $-P = (x, -y)$. By definition we have $\forall P$, $P + (-P) = \mathcal{O}$ and $P + \mathcal{O} = P$.

Let $P_1 = (x_1, y_1), P_2 = (x_1, y_1) \in E(K)$. If $x_1 \neq x_2$ then let

$$\alpha := \frac{y_1 - y_2}{x_1 - x_2}$$

otherwise (where $P_1 = P_2$)

$$\alpha := \frac{3x_1^2 + a}{2y_1}.$$

We then have $P_1 + P_2 = (x_3, y_3)$ where

$$\begin{aligned} x_3 &:= \alpha^2 - x_1 - x_2 \\ y_3 &:= -(\alpha(x_3 - x_1) + y_1) \end{aligned}$$

Geometrically the point $(x_3, -y_3)$ is the third point of intersection of the line passing through P_1 and P_2 with the elliptic curve. Substituting the equation of the line into the equation for E, we get

$$(\alpha(x - x_1) + y_1)^2 = x^3 + ax + b$$

which becomes

$$x^3 - \alpha^2 x^2 + \cdots = 0$$

since x_1, x_2, x_3 are the roots we get $x_1 + x_2 + x_3 = \alpha^2$ and so forth.

Also, $P + Q + R = \mathcal{O}$ iff P, Q, R are collinear.

One can prove associativity of the group law either by brute force computation or by using methods of classical geometry.

Two elliptic curves are isomorphic over an algebraically closed field if they have the same j-invariant. In other words, E is ismorphic to E' iff $j(E) = j(E')$, where

$$j(E) = \frac{1728a^3}{4a^3 + 27b^2},$$

so for example, changing x to $\lambda^{-2}x$ and y to $\lambda^{-3}y$ gives us $y^2 = x^3 + \lambda^4 ax + \lambda^6 b$ which is isomorphic to our original curve.

If $\Lambda \subseteq \mathbb{C}$ is a lattice, then $\mathbb{C}/\Lambda \cong E(\mathbb{C})$ under $z \mapsto (\wp(z), \wp'(z)/2)$, where

$$\wp(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda, \lambda \neq 0} \left(\frac{1}{(z+\lambda)^2} - \frac{1}{\lambda^2} \right).$$

Definition: An abelian variety is a smooth projective irreducible variety together with a (abelian) group law defined by rational functions in the coordinates.

(Elliptic curves are abelian varieties of dimension 1.)

The Mordell-Weil Theorem:

Theorem 18. *(Mordell-Weil): If K is a global field and A/K is an abelian variety then $A(K)$ is a finitely generated abelian group.*

Aside Question: Is the group law unique? No, because in any abelian group, given g_0 the map $(g, h) \mapsto g + h - g_0$ is a group law with identity g_0. But, other than that, yes.

Theorem 19. *If $f : A \to A'$ is a regular map of abelian varieties with $f(0) = 0$ then f is a group homomorphism.*

Aside Question: Can conics have a group structure? Yes, for example consider $xy = 1$ with $(x_1, y_1)(x_2, y_2) = (x_1 x_2, y_1 y_2)$. This only works for affine curves, not projective ones.

Aside Question: Are there other varieties with group laws, or non-abelian ones? Yes, known as group varieties. For example $GL_n \subseteq \mathbb{A}^{n^2}$, the set of $n \times n$ matrices with nonzero determinant.

In general, the analogue of the Mordell-Weil does not hold. For example, if X denotes the affine conic $xy = 1$ as above, $X(\mathbb{Q}) = \mathbb{Q}^\times$ is not finitely generated. But see the remark below.

Exercise: If $y^2 = x^3 + x^2$ (a nodal cubic) then $C_0(K) \cong K^\times$, and if $y^2 = x^3$ (a cuspidal cubic) then $C_0(K) \cong (K, +)$, where $C_0 := C - \{(0, 0)\}$. In other words, the same formulas define a group law for the given curves (with the groups mentioned) after we remove the singular point.

Remark: The first curve in the above exercise is an example of a semi-abelian

variety. For those, the integer points form a finitely generated group. This generalizes both the Mordell-Weil Theorem and the Dirichlet Unit Theorem.

Strategy for the proof of the Mordell-Weil Theorem:

Here we assume K is a global field throughout.

Step 1: First prove the Weak Mordell-Weil Theorem, which states: If $m \geq 2$ is an integer then $A(K)/mA(K)$ is finite, where $mA(K) := \{mP; P \in A(K)\}$.

Step 2: Use height functions: There exist $h : A(K) \to \mathbb{R}_{\geq 0}$ so that
(a) $\forall c > 0$, $\{P \in A(K); h(P) \leq c\}$ is finite
(b) $h(mP) = m^2 h(P) + O(1)$, $P \in A(K)$
(c) $\forall P_0 \in A(K), \exists c \in (P_0)$ such that $h(P + P_0) \leq 2h(P) + c(P_0)$.

Remark: For an elliptic curve over $\mathbb{Q}$, $h(x, y) = \log(\max\{|p|, |q|\})$ where $x = p/q$ with $p, q \in \mathbb{Z}$ and $(p, q) = 1$.

We claim Step 1 and Step 2 imply the Mordell-Weil Theorem:

Let $P_1, \ldots, P_r$ be representatives for the classes of $A(K)/mA(K)$. Given $Q \in A(K)$, $\exists i \in \{1, \ldots, r\}$ and $R \in A(K)$ so that $Q - P_i = mR$, giving $Q = mR + P_i$. Let $c = \max\{c(-P_1), \ldots, c(-P_r)\}$ constants from property (c) of the height functions, then

$$h(Q - P_i) = h(mR) = m^2 h(R) + c'$$

for some constant c' by property (b), and

$$m^2 h(R) + c' \leq 2h(Q) + c$$

by property (c). Hence

$$h(R) \leq \frac{2}{m^2} h(Q) + \frac{c - c'}{m^2}$$

so letting $c'' = (c - c')/m^2$ we have

$$\frac{2}{m^2} h(Q) + c'' \geq h(R)$$

so, choosing $\lambda, 2/m^2 < \lambda < 1$, either $h(R) < \lambda h(Q)$ or

$$h(Q)\left(\lambda - \frac{2}{m^2}\right) \leq c''.$$

Therefore we have $h(R) < \lambda h(Q)$ for some $\lambda < 1$, or $h(Q) \leq c'''$ where $c''' = c''/(\lambda - 2/m^2)$. Note that the restriction $h(Q) \leq c'''$ gives us a finite set.

Start with an arbitrary Q and put $Q' = R$ and repeat until we have $h(Q^{(k)}) \leq c'''$, that is,

$$\begin{array}{rcl} Q & = & mQ' + P_i \\ Q' & = & mQ'' + P_{i'} \\ & \vdots & \\ Q^{(k)} & & \end{array}$$

where $h(Q^{(k)}) \leq c'''$ which will happen eventually since otherwise $h(Q^{(i)}) \leq \lambda^i h(Q)$ which goes to 0 as i grows.

Since $Q = mQ' + P_i = m(mQ'' + P_{i'}) + P_i = m^2Q'' + mP_{i'} + P_i, \ldots$ we have

$$Q = m^k Q^{(k)} + \sum_{i=1}^{r} a_i P_i$$

therefore $\{P_1, \ldots, P_r\} \cup \{P; h(P) \leq c'''\}$, a finite set, generate $A(K)$.

Lemma 20. *Let K be a field of characteristic p, $p = 0$ or a prime number, A be an abelian variety over K, m be an integer with $m \geq 2$ and $p \nmid m$. Then $A[m] := \{P \in A | mP = 0\}$ is a finite set of points defined over a finite extension of K.*

Proof. For any abelian variety, the group law is defined by rational functions of coordinates, so $mP = P + P + \cdots + P$ is a rational function of P, and so $A[m]$ is an algebraic set. By algebraic geometry, we know $A[m]$ has a finite number of irreducible components, each defined over a finite extension of K. Let X be an irreducible component of $A[m]$, take a point $Q \in X$, then for any $P \in X$, we have $m(P - Q) = mP - mQ = 0 - 0 = 0$, which implies $X - Q \subseteq A[m]$, and $0 = Q - Q \in X - Q$.

Now consider the properties of $A[m]$ near $0 \in A$. Let $t_1, \ldots, t_n$ be local coordinates at 0, then near 0, the group law $\mu : A \times A \to A$ can be considered as a rational map $\mu = \mu(t_1, \ldots, t_n, t'_1, \ldots, t'_n)$ of the form

$$\mu = (F_1(t_1, \ldots, t_n, t'_1, \ldots, t'_n), \ldots, F_n(t_1, \ldots, t_n, t'_1, \ldots, t'_n)).$$

Since $0+0=0$, we have $F_i(0,\ldots,0,0,\ldots,0)=0$ for all $1\le i\le n$; since $t+0=0+t=t$, we have $F_i(t_1,\ldots,t_n,0,\ldots,0)=t_i$ and $F_i(0,\ldots,0,t_1',\ldots,t_n')=t_i'$, for all $1\le i\le n$. It follows that $F_i(t_1,\ldots,t_n,t_1',\ldots,t_n')=t_i+t_i'+$ higher order terms (as a power series) and hence, $m(t_1,\ldots,t_n)=(t_1,\ldots,t_n)+\cdots+(t_1,\ldots,t_n)=(mt_1+\text{higher order terms},\ldots,mt_n+\text{higher order terms})$. By assumption, $charK\nmid m$, so $m(t_1,\ldots,t_n)\neq 0$ for $(t_1,\ldots,t_n)$ close but unequal to 0, which implies 0 is an isolated point in $A[m]$.

Combine the two results, we see each irreducible component X must be a single point, so $A[m]$ is a finite set of points. □

Example. *Let A be an elliptic curve $y^2=x^3+ax+b$, $m=2$. By the addition on elliptic curves, a point $(x,y)\in A$ satisfies $2(x,y)=0$ if and only if $y=0$. So*

$$A[2]=\{(x,y)\in A|y=0\}\cup\{0\}=\{(x,0)|x^3+ax+b=0\}\cup\{0\}$$

consists of 4 points, each defined over the splitting field of x^3+ax+b over K.

Remark: Given this lemma and the Weak Mordell-Weil Theorem, we can prove Mordell-Weil Theorem by working in the extension of K which contains coordinates of $A[m]$. By the lemma, there exists L/K finite such that $A[m]\subseteq A(L)$ and we get that $A(L)/mA(L)$ is finite. Then using the height function, we can deduce $A(L)$ is finitely generated, so $A(K)\subseteq A(L)$ is also finitely generated.

Now suppose K is a field of characteristic p, $p=0$ or a prime number, A is an abelian variety over K, m is an integer with $m\ge 2$ and $p\nmid m$, and assume $A[m]\subseteq A(K)$. Denote the group $H=\mathrm{Hom}(\mathrm{Gal}(K^{sep}/K),A[m])$, then H has a bijection to the set of pairs (L,λ), where L/K is a finite Galois extension and λ is a group monomorphism from $\mathrm{Gal}(L/K)$ to $A[m]$. This bijection sends φ to $((K^{sep})^{\ker\varphi},\overline{\varphi})$. Define a map δ from $A(K)$ to H as follows: let $P\in A(K)$, choose $Q\in A(K^{sep})$ such that $mQ=P$, let $L=K(Q)$. We **Claim** that L/K is Galois, and the map $\lambda:\mathrm{Gal}(L/K)\to A[m]:\sigma\mapsto\sigma Q-Q$ is a group monomorphism. Now $(L,\lambda)\in H$, and is defined to be the image of P under δ. Then δ is a well-defined (independent of the choice of Q) group homomorphism, and $\ker\delta=mA(K)$. Henceforth, δ induces a homomorphism from $A(K)/mA(K)$ to H.

*Proof of **Claim**:* Firstly, suppose $\sigma\in\mathrm{Gal}(K^{sep}/K)$, then $m(\sigma Q)=\sigma(mQ)=\sigma(P)=P$, so $m(\sigma Q-Q)=P-P=0$, so $\sigma Q-Q\in A[m]\subseteq A(K)$, and so $\sigma Q=Q+(\sigma Q-Q)\in A(K(Q))=A(L)$. This shows L/K is Galois.

Secondly, for any $\sigma, \tau \in \mathrm{Gal}(L/K)$, we have $\lambda(\sigma\tau) = \sigma\tau Q - Q = \sigma\tau Q - \sigma Q + \sigma Q - Q = \sigma(\tau Q - Q) + (\sigma Q - Q) = \sigma(\lambda(\tau)) + \lambda(\sigma)$. As $\lambda(\tau)$ is an element in $A[m] \subseteq A(K)$, it is fixed by $\sigma \in \mathrm{Gal}(L/K)$, and so $\lambda(\sigma\tau) = \lambda(\tau) + \lambda(\sigma)$. Besides, suppose $\lambda(\sigma) = 0$, then $\sigma(Q) = Q \Longrightarrow L = K(Q)$ is fixed by $\sigma \Longrightarrow \sigma = 1$. This shows λ is a group monomorphism.

Our goal today is prove the Weak Mordell-Weil Theorem. Recall our map δ:

$$\delta : A(K) \longrightarrow \mathrm{Hom}(\mathrm{Gal}(K_{sep}/K), A[m]) = H$$

We can also identify H with the (a priori) set

$$\{(L, \lambda) : L/K \text{ Galois }, \lambda : \mathrm{Gal}(L/K) \hookrightarrow A[m]\},$$

(in fact, this set has a group structure), and we will often go back and forth between these two interpretations of H. We will also assume $A[m] \subseteq A(K)$. We defined δ by the following: given $P \in A(K)$, let Q be a point on our abelian variety such that $mQ = P$. Then we set $\lambda(\sigma) = \sigma Q - Q$ and $L = K(Q)$, where $K(Q)$ is the extension of K gotten by adjoining the coordinates of Q. We first want to prove some claims from last time.

Claim. *δ is independent of the choice of Q.*

Proof. Suppose Q, Q' satisfy $mQ = mQ' = P$. Then $m(Q - Q') = \mathcal{O}$, and by our assumption that $A[m] \subseteq A(K)$, we see that $Q - Q' \in A(K)$. This immediately tells us that $K(Q) = K(Q') = L$ since Q and Q' differ by an element of $A(K)$. Moreover for any $\sigma \in \mathrm{Gal}(L/K)$, $\sigma(Q - Q') = Q - Q'$. Rearranging, we find that for any $\sigma \in \mathrm{Gal}(L/K)$, $\sigma Q - Q = \sigma Q' - Q'$. Hence $\lambda(\sigma)$ is independent of Q, as is L. □

Claim. *λ is an injection.*

Proof. $\lambda(\sigma) = \mathcal{O}$ if and only if $\sigma Q = Q$ if and only if σ when restricted to L is the identity, i.e. σ is the identity in $\mathrm{Gal}(L/K)$. □

Claim. *δ is a homomorphism.*

Proof. Let $P = P_1 + P_2$. Choose Q_i such that $mQ_i = P_i$ for $i = 1, 2$. Let $Q = Q_1 + Q_2$, then $mQ = P$. Let $\lambda_i(\sigma) = \sigma Q_i - Q_i$ for $i = 1, 2$. Then

$$(\lambda_1 + \lambda_2)(\sigma) = \sigma Q_1 + \sigma Q_2 - Q_1 - Q_2 = \sigma(Q_1 + Q_2) - (Q_1 + Q_2) = \sigma Q - Q = \lambda(\sigma),$$

so $\lambda = \lambda_1 + \lambda_2$ as desired. □

Claim. $\ker \delta = mA(K)$.

Proof. We first show that $mA(K) \subseteq \ker\delta$: say $P \in mA(K)$, then there exists a $Q \in A(K)$ satisfying $mQ = P$, so let us choose this Q. Then $L = K$ so λ is the zero map, so $P \in \ker\delta$.

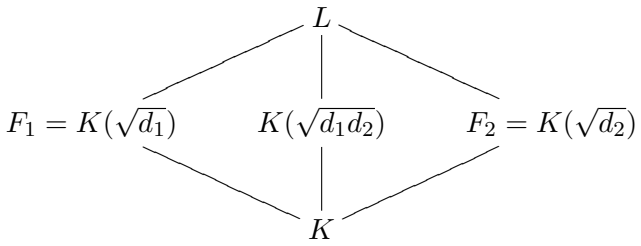
Now assume $P \in \ker\delta$, so $\lambda(\sigma) = \mathcal{O}$ for all σ. Then $\sigma Q = Q$ for all σ, hence $Q \in A(K)$ and, since $mQ = P$, we see that $P \in mA(K)$. □

Using this last claim, we see that $\delta : A(K)/mA(K) \hookrightarrow H$.

Example. Let $A = E : y^2 = x^3 + ax + b$ be an elliptic curve and $m = 2$. We are assuming that $E[2] \subseteq E(K)$, so the points of order 2 (i.e. those points with y-coordinate 0) are in $E(K)$. Thus our cubic factors over K:

$$y^2 = (x - e_1)(x - e_2)(x - e_3), \qquad e_i \in K.$$

As discussed last time, $E[2] = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. We want to know what extensions L/K are possible. Considering the possible maps $\mathrm{Gal}(L/K) \hookrightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and noting that $\mathrm{char}(K) \neq 2$, we readily see the only possible field diagram is



From this, the possible λ's are easily determinable. Noting that we can adjust $K(\sqrt{d})$ by a square (i.e. $K(\sqrt{d}) = K(\sqrt{r^2 d})$), we readily see that $H \cong K^\times/(K^\times)^2 \oplus K^\times/(K^\times)^2$, where $(K^\times)^2$ is the subgroup of squares in $K^\times$. Choosing the basis $\{(e_1, 0), (e_2, 0)\}$ for $E[2]$, for $(x, y) \neq (e_1, 0)$, $(e_2, 0)$, we see that

$$\delta : (x, y) \mapsto (x - e_1, x - e_2) \in E[2].$$

For $(x, y) = (e_1, 0)$, $(e_2, 0)$, one can readily work out δ by considering what to do in order to divide by 2. □

Remark. *In general, if $p \nmid m$, $A[m] = (\mathbb{Z}/m\mathbb{Z})^{2\dim A}$, so $H \cong (K^\times/(K^\times)^m)^{2\dim A}$.*

So far we had not assumed any conditions on our field K. We will now restrict our arguments to a global field K. Let M_K be the set of places (i.e. equivalence classes of absolute values) of K, K_v be the completion of K with respect to a place $v \in M_K$, $\mathcal{O}_v = \{x \in K_v : |x|_v \leq 1\} \subseteq K_v$, and $\mathcal{M}_v = \{x \in K_v : |x|_v < 1\}$ the unique maximal ideal in $\mathcal{O}_v$. By clearing

denominators, we can view A as being defined over $\mathcal{O}_v$ and reduce modulo $\mathcal{M}_v$ to get a variety A_v defined over the finite field $\mathcal{O}_v/\mathcal{M}_v$. If A_v is an abelian variety, we say A has *good reduction* at v; otherwise we say A has *bad reduction* at v.

We next define a set $S \subset M_K$ such that S contains the archimedean places, all places of bad reduction for A, and all places $v \mid m$ (i.e. $|m|_v < 1$). We claim without proof that S is finite. This can be shown by extending techiques from a previous lecture. We will need the following definitions to prove the Weak Mordell-Weil Theorem:

Definition 21. *Let K be a field, L/K a finite extension, and $|\cdot|$ an absolute value on L. We say that $|\cdot|$ is **unramified in** L if $\{|x| : x \in K\} = \{|x| : x \in L\}$.*

Definition 22. *A place $v \in M_K$ is **unramified in** L if for all $|\cdot|$ of L that are in the class of v when restricted to K are unramified in L.*

Example. Let $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{D})$ with D a square-free integer. Observe that for odd p, the p-adic absolute value in $\mathbb{Q}$ is ramified in $\mathbb{Q}(\sqrt{D})$ if and only if $p \mid D$. (We say $|\cdot|/\mathbb{Q}$ is **ramified** in L if there exists an absolute value in L that restricts to $|\cdot|$ in $\mathbb{Q}$ which is not unramified.) If $p \mid D$, $D = pc$ where $(c, p) = 1$ (since D is square-free). So $|\sqrt{D}|_p^2 = |D|_p = |pc|_p = 1/p$. Thus $|\sqrt{D}|_p = 1/\sqrt{p} \notin \{|x|_p : x \in \mathbb{Q}\} = p^{\mathbb{Z}} \cup \{0\}$. On the other hand if p does not divide D, then we have $|\sqrt{D}|_p = 1$. Thus $\{|x|_p : x \in \mathbb{Q}(\sqrt{D})\} = \{|x|_p : x \in \mathbb{Q}\}$. We also note that 2 ramifies in $\mathbb{Q}(\sqrt{D})$ if and only if D is even or $D \equiv 3 \pmod 4$. □

We will make use of the following important theorem:

Theorem 23. *If $P \in A(K)$, $mQ = P$. Then $K(Q)/K$ is unramified outside of S.*

Note that S depends on the abelian variety A and the field K. So as you vary $P \in A(K)$, the theorem tells us that the extensions $K(Q)/K$ are *all* unramifiied outside the *same* set S. We will also need the following theorem:

Theorem 24 (Hermite)**.** *If K is a global field, $S \subset M_K$ finite, $d \geq 2$ an integer (with $p \nmid d$ if $p = charK > 0$), then the set $\{L/K : L$ unramified outside of $S, [L : K] = d\}$ is finite.*

Theorem 25. *Theorem 23 and 24 imply the Weak Mordell-Weil Theorem.*

Proof. By Theorem 23, if $P \in A(K)$, $K(Q)$ is unramified outside of S for any $mQ = P$. We also know that $[K(Q) : K] \leq \#A[m]$. Then by Theorem 24, there are only finitely many choices for such $K(Q)$ and only finitely many $\lambda : \mathrm{Gal}(K(Q)/K) \hookrightarrow A[m]$. Thus the image of δ is finite. Thus $A(K)/mA(K)$ is finite, giving us the Weak Mordell-Weil Theorem. $\square$

Thus we are only left with proving Theorems 1 and 2. We will only do the case of an elliptic curve over $\mathbb{Q}$ and $m = 2$, leaving the general case to one of the standard texts.

Proof of Theorem 1. We have

$$E : y^2 = x^3 + ax + b = (x - e_1)(x - e_2)(x - e_3)$$

where we may assume without loss of generality that $e_i \in \mathbb{Z}$ (performing a change of coordinates if necessary). As discussed before,

$$\delta(x, y) = (x - e_1, x - e_2) \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \times \mathbb{Q}^\times/(\mathbb{Q}^\times)^2.$$

Considering the possible linear change of variables, we observe that a point (x, y) on E must be of the form $(u/z^2, v/z^3)$ with$u, v, z \in \mathbb{Z}$ and $(u, z) = 1$, $(v, z) = 1$. Thus

$$x - e_i = \frac{u - e_i z^2}{z^2}.$$

So if p is an odd prime ($2 \in S$ since $m = 2$) which ramifies in $\mathbb{Q}(Q)$, then $p \mid (u - e_i z^2)$. (Note that we do not know if $u - e_i z^2$ is square-free, so we do not have an if and only if in the previous statement.) Plugging $(x, y) = (u/z^2, v/z^3)$ into the equation for E, we get

$$v^2 = (u - e_1 z^2)(u - e_2 z^2)(u - e_3 z^2).$$

Say $p \mid (u - e_1 z^2)$ but $p \nmid (u - e_2 z^2)(u - e_3 z^2)$, then an even power of p divides exactly $(u - e_1 z^2)$, since $p \mid v^2$. So p does not ramify in $\mathbb{Q}(\sqrt{x - e_1})$.

So the primes that ramify divide two of the factors of the cubic. So suppose without loss of generality that $p \mid (u - e_1 z^2)$ and $p \mid (u - e_2 z^2)$. Then $p \mid (e_1 - e_2) z^2$. But if $p \mid z$, then $p \mid u$, but this cannot happen since $(z, u) = 1$. Thus $p \nmid z$, hence $p \mid (e_1 - e_2)$. So the primes that ramify in $\mathbb{Q}(Q)$ are contained inside the set

$$S = \{2, \infty\} \cup \underbrace{\left\{ p : p \mid \prod_{i \neq j} (e_i - e_j) \right\}}_{\text{primes of bad reduction}}.$$

Thus $\mathbb{Q}(Q)$ is unramified outside of S. $\square$

Proof of Theorem 2. We want to count the number of quadratic extensions of $\mathbb{Q}$ unramified outside of $S = \{2, p_1, \ldots, p_r\}$. These extensions are those $\mathbb{Q}(\sqrt{D})$ such that D is square-free and for all $p \notin S$, $p \not| D$. Thus for $\epsilon_i = 0, 1$,

$$D = \pm \prod_{p_i \in S} p_i^{\epsilon_i}.$$

There are finitely many such D, so there are finitely many extensions $\mathbb{Q}(D)$. $\square$

The general case of these theorems requires finiteness of class numbers and Dirichlet's Unit Theorem, but we will leave it at that.

We now assume that K is a global field, and M_K the set of places of K. Then for $v \in M_K$, we let K_v represent the corresponding completion. We can now look at the induced maps

$$\delta_v : A(K_v)/mA(K_v) \to H_{K_v}$$

and notice that we obtain a commutative diagram:

$$\begin{array}{ccc} \delta : A(K)/mA(K) & \longrightarrow & H_K \\ \downarrow & & \downarrow \\ \delta_v : A(K_v)/mA(K_v) & \longrightarrow & H_{K_v} \end{array}$$

We now define a new group. Let

$$S_m := \{h \in H_K \mid h \in Im(\delta_v) \text{ for all } v \in M_K\}.$$

Because of the diagram above, note that elements in $A(K)/mA(K)$ are in S_m, and in particular, δ induces an injective map $0 \to A(K)/mA(K) \hookrightarrow S_m$.

Theorem 26. *S_m is finite.*

Proof. While we do not go through the proof of this theorem here, it follows from much the same argument as the proof of the finiteness of $A(K)/mA(K)$. $\square$

Define

$$\text{Sha}_m = S_m/\delta(A(K)).$$

We want to figure out how to compute $A(K)$. In order to do this, we need to compute $A(K)/mA(K)$. It turns out that S_m is computable, but it's hard

to determine the image of $A(K)/mA(K)$ in S_m, as it is not clear how to decide if an element of S_m actually comes from $A(K)/mA(K)$. It turns out that there is a way around this.

Let l be a prime, $l \neq p$ if $\mathrm{char}K = p > 0$. Then the following commutative diagram holds:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A(K)/lA(K) & \longrightarrow & S_l & \longrightarrow & \mathrm{Sha}_l & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & A(K)/l^nA(K) & \longrightarrow & S_{l^n} & \longrightarrow & \mathrm{Sha}_{l^n} & \longrightarrow & 0 \end{array}$$

We can look at the image of $S_{l^n} \to S_l$, which is a subgroup of S_l containing the image of $A(K)/lA(K)$. (Note: For this to make sense, we need to define $H_K, \delta, S_{l^n}, \ldots$ even when $A[l^n] \not\subset A(K)$, which can be done using Galois cohomology).

Descent "algorithm"

We may now use the above to compute the image of $A(K)/lA(K)$ in S_l in the following manner. Consider two distinct parallel processes.

1. Compute elements of $A(K)$ and map them to S_l. In this manner, we will build up a larger and larger picture of the image of $A(K)/lA(K)$ in S_l.

2. Compute S_{l^n} and map it to S_l for $n = 1, 2, 3, \ldots$. In this manner, we will find smaller and smaller subgroups of S_l containing the image of $A(K)/lA(K)$.

At some point, it is our hope that the subgroups obtained by following these two processes will be the same. That is, there will come a point where we can no longer build up our subgroup as in part 1, or restrict the subgroup further, as we are doing in part 2. At this point, we will have found the exact image of $A(K)/lA(K)$ in S_l as desired.

Theorem 27. *The descent "algorithm" will work if* $|\,\mathrm{Sha}_{l^m}\,|$ *is bounded as* $m \to \infty$.

Consider

$$\mathrm{Sha}_{l^\infty} := \varprojlim_n \mathrm{Sha}_{l^n}\,.$$

We define the Tate-Shafarevich group by $\mathrm{Sha} = \bigoplus_l \mathrm{Sha}_{l^\infty}$.

Conjecture 28 (Tate-Shafarevich)**.** Ш *is finite.*

If this conjecture indeed holds true in all cases, then our algorithm is always valid. For now, the conjecture is known to be true only for some elliptic curves over $\mathbb{Q}$ of small rank.

Example. *Consider the abelian variety A over $K = \mathbb{Q}$ given by $y^2 = (x - e_1)(x - e_2)(x - e_3)$ where $e_i \in \mathbb{Z}$. Let $m = 2$. Then the map δ is given by:*

$$\begin{array}{rccc} \delta: & A(\mathbb{Q}) & \to & \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \oplus \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \\ & (x,y) & \mapsto & (x-e_1, x-e_2) \end{array}$$

Let μ be the restriction of the map δ to the first coordinate. That is,

$$\begin{array}{rccc} \mu: & A(\mathbb{Q}) & \to & \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \\ & (x,y) & \mapsto & x-e_1 \end{array}$$

We want to know what it means if $b \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ is in the image of μ. First off, we know that $b \in Im(\mu)$ if and only if there exists some $(x,y) \in E(\mathbb{Q})$ with $x - e_1 = bu^2$ for some $u \in \mathbb{Q}^\times$. That is, there exists some solution to the equation

$$y^2 = bu^2(bu^2 - e_1 + e_2)(bu^2 - e_1 + e_3).$$

Letting $v = \frac{y}{u}$, this is the same as the statement that $b \in Im\ (\mu)$ if and only if the equation

$$v^2 = b(bu^2 + e_1 - e_2)(bu^2 + e_1 - e_3) \qquad (*)$$

has a solution $(u,v) \in \mathbb{Q}^2$. Consider the set S_2. We know $b \in S_2$ (i.e., $b \in \mu(A(\mathbb{Q}_p))$ for all p) if and only if the above equation $(*)$ has points in $\mathbb{Q}_p$ for all p. In this example, $Ш_2$ *measures how much bigger S_2 is than $Im(\mu)$. Specifically,* $Ш_2$ *is the set of equations $y^2 = bu^2(bu^2 - e_1 + e_2)(bu^2 - e_1 + e_3)$ for varying b which have solutions in $\mathbb{Q}_p$ for all p "modulo" the set of these equations that have solutions in $\mathbb{Q}$. What this means for us is that*

$Ш_2 = 0 \iff$ *the Hasse Principle holds for this particular set of equations.*

For every curve C of genus 1 over a field K, one can associate an elliptic curve E/K called its Jacobian. If K is a global field and $C(K_v) \neq \emptyset$ for all $v \in M_K$, then C can be viewed as an element of $Ш(E/K)$. $Ш(E/K) = 0$ if and only if the Hasse Principle holds for curves of genus 1 over K with Jacobian E. If the conjecture of Tate and Shafarevich above holds then failure of the Hasse Principle is measured by a finite quantity.

Suppose C/K has genus 1. If $C(K_v) = \emptyset$ for some v, then $C(K) = \emptyset$. On the other hand, if $C(K_v) \neq \emptyset$ for all $v \in M_K$, then $[C] \in \text{Sha}(E/K)$. It follows that we have

$$C(K) \neq \emptyset \iff [C] = 0.$$

If $\text{Sha}(E/K)$ is finite, then we can verify whether $[C] = 0$ by a finite computation. To do this, we use a bilinear pairing (known as the Cassels pairing)

$$\beta : \text{Sha} \times \text{Sha} \to \mathbb{Q}/\mathbb{Z}$$

which is known to be nondegenerate if Sha is finite. From this pairing, we get $[C] = 0 \iff \beta([C], g) = 0$ for all $g \in \text{Sha}$. Note that this is true only for curves of genus 1, not for those of higher genus. It does, however, end up generalizing to "principal homogeneous spaces of abelian varieties."

Heights

Recall: To complete our proof of the Mordell-Weil Theorem, we need a function

$$h : A(K) \to [0, \infty)$$

such that

(i) For all $c > 0$, $\{P \in A(K) : h(P) \leq c\}$ is finite,

(ii) $h(mP) = m^2 h(P) + O(1)$,

(iii) $\forall P_0 \in A(K), \exists c(P_0) > 0, h(P + P_0) \leq 2h(P) + c(P_0)$.

By definition, an abelian variety is in projective space, so it is natural to start with heights defined on projective space $\mathbb{P}^n(K)$. For the remainder of these notes, let K denote a global field (i.e. a finite extension of $\mathbb{Q}$ or $\mathbb{F}_q(x)$) and let M_K be the set of places of K. Then for each $v \in M_K$ we choose an absolute value $|\cdot|_v$ and number n_v such that the product formula holds for all $x \in K^*$. This means that for all $x \in K^*$,

$$\prod_v |x|_v^{n_v} = 1.$$

If $a \in \mathbb{P}^n(K)$, write $a = (a_0 : \cdots : a_n)$. Then we define

$$h(a) = \sum_v n_v \log \max_{0 \leq i \leq n} \{|a_i|_v\}.$$

Remark: Sometimes the function

$$H(a) = \prod_v \max_{0 \le i \le n} \{|a_i|_v\}^{n_v}$$

is used. These heights are related by $h(a) = \log H(a)$.

Lemma: If $a \sim b$, then $h(a) = h(b)$.

Proof: By definition, $a \sim b$ if there exists some $\lambda \in K^*$ such that $a_i = \lambda b_i$ for each i. We then observe that

$$\begin{aligned}\max_{0\le i\le n}\{|a_i|_v\} &= \max_{0\le i\le n}\{|\lambda|_v|b_i|_v\} \\ &= |\lambda|_v \max_{0\le i\le n}\{|b_i|_v\}.\end{aligned}$$

Summing each side over all $v \in M_K$, we have

$$h(a) = h(b) + \sum_v n_v \log|\lambda|_v.$$

However, the sum on the right vanishes by the product formula:

$$\begin{aligned}\sum_v n_v \log|\lambda|_v &= \log\left(\prod_v |\lambda|_v^{n_v}\right) \\ &= \log 1 = 0.\end{aligned}$$

■

Example: $K = \mathbb{Q}$.

Every point $a \in \mathbb{P}^n(\mathbb{Q})$ can be represented by $a = (a_0 : \cdots : a_n)$ with $a_i \in \mathbb{Z}, \gcd(a_0, \ldots, a_n) = 1$. If p is prime, then we have that, for this representation,

$$\max_{0\le i\le n}\{|a_i|_p\} = 1.$$

To see this, note that there must be some a_i not divisible by p. For this a_i, $|a_i|_p = 1$. For the rest, we note that each other a_j is of the form $a_j = p^s m$ with $p \not| m$ and $s \ge 0$, so $|a_j| = p^{-s} \le 1$. Hence we see that

$$h(a) = \log \max_{0\le i\le n}\{|a_i|_\infty\}.$$

Theorem: If K is a global field, given integers $n, c \geq 1$, the set

$$\{a \in \mathbb{P}^n(K) \,:\, h(a) \leq c\}$$

is finite.

Before we give the proof of this theorem, the following two propositions are left as exercises:

Proposition 1: Define $h(\alpha) = h(1 : \alpha)$ for $\alpha \in K$. Then, for $\alpha_1, \ldots, \alpha_n \in K$ we have

$$\max_{0 \leq i \leq n} \{h(\alpha_i)\} \leq h((1 : \alpha_1 : \cdots : \alpha_n)) \leq h(\alpha_1) + \cdots + h(\alpha_n).$$

Proposition 2: For $p/q \in \mathbb{Q}$, $\gcd(p, q) = 1$

$$h(p/q) = \max\{\log |p|_\infty, \log |q|_\infty\}.$$

We also adopt the following notation:

Notation: $\log^+ x := \log \max\{1, x\}$.

Proof of Theorem: We handle the case where K is a finite extension of $\mathbb{Q}$ (the case for function fields is similar). Using the first proposition, we may reduce the problem to demonstrating that each set

$$\{\alpha \in K \,:\, h(\alpha) \leq c\}$$

is finite. If $\alpha \in K$, let $m_\alpha(x) \in \mathbb{Z}[x]$ be its minimal polynomial. It is then enough to show a bound for the coefficients of $m_\alpha(x)$ if $h(\alpha) \leq c$. Since each finite extension of $\mathbb{Q}$ is contained in some Galois extension, we may assume that $K/\mathbb{Q}$ is Galois. Then $m_\alpha(x)$ divides the polynomial

$$\prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} (x - \sigma(\alpha)).$$

It is then enough to bound the heights of the coefficients of this polynomial, i.e. the symmetric functions in $\{\sigma(\alpha) : \sigma \in \mathrm{Gal}(K/\mathbb{Q})\}$. Defining

$$\beta = \sum_{i_1 \leq \cdots \leq i_k} \sigma_{i_1}(\alpha) \cdots \sigma_{i_k}(\alpha),$$

we note that

$$h(\beta) = \sum_{p \leq \infty} \log^+ |\beta|_p.$$

We then estimate each $|\beta|_p$. If $v|p$, then

$$\begin{aligned} |\beta|_p &= |\beta|_v \\ &= \left| \sum_{i_1 \leq \cdots \leq i_k} \sigma_{i_1}(\alpha) \cdots \sigma_{i_k}(\alpha) \right|_v \\ &\leq \sum_{i_1 \leq \cdots \leq i_k} |\sigma_{i_1}(\alpha) \cdots \sigma_{i_k}(\alpha)|_v \\ &= \sum_{i_1 \leq \cdots \leq i_k} |\sigma_{i_1}(\alpha)|_v \cdots |\sigma_{i_k}(\alpha)|_v . \end{aligned}$$

Since the function $|\sigma_{i_j}(\cdot)|_v$ is yet another absolute value restricting to $|\cdot|_p$ on $\mathbb{Q}$, label it $|\cdot|_{v_{i_j}}$. Continuing our estimates,

$$\begin{aligned} \sum_{i_1 \leq \cdots \leq i_k} |\sigma_{i_1}(\alpha)|_v \cdots |\sigma_{i_k}(\alpha)|_v &= \sum_{i_1 \leq \cdots \leq i_k} |\alpha|_{v_{i_1}} \cdots |\alpha|_{v_{i_k}} \\ &\leq \binom{n}{k} \max\{1, |\alpha|_{v_1}, \ldots, |\alpha|_{v_n}\}^k. \end{aligned}$$

By the strong triangle inequality, we don't need the combinatorial coefficient in the non-archimedean case. Combining the estimates at each place,

$$\begin{aligned} h(\beta) &= \sum_{p \leq \infty} \log^+ |\beta|_p \\ &\leq \binom{n}{k} + k \sum_{p \leq \infty} \log \max_{v_i, \ldots, v_n | p} \{1, |\alpha|_{v_1}, \ldots, |\alpha|_{v_n}|\} \\ &\leq \binom{n}{k} + k h(\alpha). \end{aligned}$$

■

There is a stronger version of the theorem due to Northcott:

Theorem: For fixed integers $d, n \geq 1$, the set

$$\{a \in \mathbb{P}^n(\overline{\mathbb{Q}}) \,:\, [\mathbb{Q}(a) : \mathbb{Q}] \leq d, h(a) \leq c\}$$

is finite.

In defining the height h on $\mathbb{P}^n(\overline{\mathbb{Q}})$, it is necessary to make the right choice of $|\cdot|_v, n_v$ such that if $a \in \mathbb{P}^n(K)$ and L/K, then $h(a)$ is the same value regardless whether it is computed in K or L.

Theorem: Suppose K is a global field, $\phi_0, \ldots, \phi_r \in K[x_0, \ldots, x_n]$ are homogeneous all of degree d. Then, on the set of $a \in \mathbb{P}^n(K)$ such that some $\phi_i(a) \neq 0$, define the function Φ by

$$\Phi : (a_0 : \cdots : a_n) \mapsto (\phi_0(a) : \cdots : \phi_r(a)) \in \mathbb{P}^r(K).$$

Then $h(\Phi(a)) \leq h(a) + O(1)$.

Proof: By definition,

$$h(\Phi(a)) = \sum_v n_v \log \max_{0 \leq i \leq r} |\phi_i(a)|_v.$$

If we write $\phi_i(a)$ as

$$\phi_i(a) = \sum_{d_1 + \cdots + d_n = d} c^i_{d_0, \ldots, d_n} a_0^{d_0} \cdots a_n^{d_n},$$

then we have

$$\begin{aligned} \log |\phi_i(a)|_v &\leq \log \left(\sum_{d_1 + \cdots d_n = d} |c^i_{d_0, \ldots, d_n}|_v |a_0|_v^{d_0} \cdots |a_n|_v^{d_n} \right) \\ &\leq \log k_v + d \log \left(\max_{0 \leq i \leq n} \{|a_i|_v\} \right) + \log \binom{n+d}{d} \end{aligned}$$

Here $k_v = \max |c^i_{d_0,\ldots,d_n}|_v$. It is clear that, for all but finitely many v, $\log k_v = 0$. As before, the combinatorial term is not necessary in the non-archimedean case. The result follows by summing over v. ■

Remark: If $(\phi_0, \ldots, \phi_r) = (x_0, \ldots, x_n)^k$, then $h(\Phi(a)) = dh(a) + O(1)$.

Heights on Abelian Varieties

We want $h : A(K) \to [0, \infty)$ (with K a global field) such that

1. $\{P : h(P) \leq c\}$ is finite for all c,
2. $h(mP) = m^2 h(P) + O(1)$,
3. $\forall P_0 \in A(K)$, $\exists c(P_0)$ such that $h(P + P_0) \leq 2h(P) + c(P_0)$.

We defined a height function $h : \mathbb{P}^n \to [0, \infty)$. As $A \hookrightarrow \mathbb{P}^n$, we get a height function on A. It satisfies 1 automatically. We proved "$h(\Phi(a)) \leq dh(a) + O(1)$." This implies 3 and $h(mP) \leq m^2 h(P) + O(1)$ (multiplication by m is a degree m^2 polynomial map). We will only show this for elliptic curves and $m = 2$.

To get the lower bound on 2 requires some extra geometric properties of the embedding $A \hookrightarrow \mathbb{P}^n$; namely, the map $P \mapsto -P$ is induced by a linear transformation of $\mathbb{P}^n$.

Remark. *Different embeddings $A \hookrightarrow \mathbb{P}^n$ give different heights.*

We will do the proof in detail now for elliptic curves and $m = 2$:

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

$P_0 = (x_0, y_0)$, $P = (x, y)$, $h((x, y)) = h((1 : x : y))$. The equation $y^2 = x^3 + ax + b$ implies $3h(x) = 2h(y) + O(1)$. It is sufficient to work with $h(x)$; i.e. with the function $(x, y) \mapsto h(x)$.

We start with property 3. $P + P_0$ has x-coordinate given by

$$\begin{aligned}\left(\frac{y - y_0}{x - x_0}\right)^2 - (x + x_0) &= \frac{(y - y_0)^2 - (x + x_0)(x^2 - 2xx_0 + x_0^2)}{(x - x_0)^2} \\ &= \frac{x^3 + ax + b - 2yy_0 + y_0^2 - (x^3 - x^2x_0 - xx_0^2 + x_0^3)}{(x - x_0)^2} \\ &= \frac{2yy_0 - y_0^2 + ax + b + x^2x_0 + xx_0^2 - x_0^3)}{(x - x_0)^2}.\end{aligned}$$

The numerator and denominator have degree 2 in x and degree 1 in y. So "$h(\Phi(a)) \leq dh(a) + O(1)$" gives 3.

Now 2. The x-coordinate of $2P$ is given by

$$\left(\frac{3x^2+a}{2y}\right)^2 = \frac{(3x^2+a)^2 - 8xy^2}{4y^2}$$
$$= \frac{(3x^2+a)^2 - 8x(x^3+ax+b)}{4(x^3+ax+b)} = \frac{A(x)}{B(x)},$$

where $\deg A = 4$, $\deg B = 3$; so "$h(\Phi(a)) \leq dh(a) + O(1)$" gives $h(2P) \leq 4h(P) + O(1)$. Now we just need to show $h(2P) \geq 4h(P) + O(1)$

$$h(2P) = h\left(\frac{A(x)}{B(x)}\right) = \sum_v n_v \log\left(\max\left\{|A(x)|_v, |B(x)|_v\right\}\right)$$

likewise,

$$h(P) = h(x) = \sum_v n_v \log\left(\max\left\{|x|_v, 1\right\}\right).$$

Assume $|x|_v > 1$,

$$\begin{aligned}
|A(x)|_v &= \left|a_0x^4 + a_1x^3 + \cdots + a_n\right|_v \\
&= \left|x^4\right|_v \left|a_0 + a_1x^{-1} + \cdots + a_nx^{-4}\right|_v \\
&\geq |x|_v^4 \left(|a_0|_v - |x|_v^{-1}\left|a_1 + \cdots + a_nx^{-3}\right|_v\right) \\
&\geq |x|_v^4 \left(|a_0|_v - C_v\right),
\end{aligned}$$

for some constant C_v. Thus, $\log\left(|A(x)|_v\right) \geq 4\log(|x|_v) + C_v'$. Note in the non-archimedean case, we can take $C_v = 1$ using the strong triangle inequality. Also $|a_0|_v$ is almost always 1 (that is, all but finitely many are 1). Likewise for B, we have $|B(x)|_v \leq |x|_v^3 + C_v$; so for those v with $|x|_v > 1$, we get

$$\log\left(\max\left\{|A(x)|_v, |B(x)|_v\right\}\right) \geq 4\log(|x|_v) + C_v',$$

where the C_v' are almost always 0.

Now look at $|x|_v \leq 1$. Then $\log\left(\max\left\{|x|_v, 1\right\}\right) = 0$; so we want to show $\log\left(\max\left\{|A(x)|_v, |B(x)|_v\right\}\right) \geq C_v'$ with $C_v' = 0$ for all but finitely many v. Now $B(x) = 4f(x)$ (where $f(x) = x^3 + ax + b$) and $A(x) = (f'(x))^{1/2} - 2xf(x)$.

Claim. $(A(x), B(x)) = 1$.

Proof. If $p(x)|B(x)$ then $p(x)|f(x)$. If also $p(x)|A(x)$, then $p(x)|f'(x)$. But $(f(x), f'(x)) = 1$, since $f(x)$ has distinct roots (as we are working on an elliptic curve). □

Then $\exists u(x), v(x) \in K[x]$ such that $u(x)A(x) + v(x)B(x) = 1$. Hence

$$\begin{aligned} 1 &= |u(x)A(x) + v(x)B(x)| \\ &\leq C_v'' \max\left\{|A(x)|_v, |B(x)|_v\right\} \qquad C_v'' = 1 \text{ for almost all } v, \end{aligned}$$

(the non-archimedean case). So $\max\left\{|A(x)|_v, |B(x)|_v\right\} \geq C_v'$.

This gives us our desired height function; so we have proven the Mordell-Weil Theorem.

Néron-Tate canonical height

The *canonical height* is a positive-definite quadratic form on $A(\overline{K})$ modulo torsion; $\hat{h}(mP) = m^2\hat{h}(P)$, and $\hat{h}(P) = 0$ if and only if P is torsion.

Néron's approach:

$$\hat{h}(P) = \sum_v \lambda_v(P).$$

Tate's approach:

$$\hat{h}(P) = \lim_{n\to\infty} \frac{h(2^n P)}{4^n}.$$

We have $h(2P) \sim 4h(P)$, which implies $\frac{h(2P)}{4} \sim h(P)$; thus

$$\left\{\frac{h(2^n P)}{4^n}\right\} \quad \text{is a Cauchy sequence.}$$

Formally, you get $\hat{h}(2P) = 4\hat{h}(P)$; one needs to prove it works for all values of m.

Remark. *Now everytime you have a positive-definite quadratic form on a finitely generated abelian group Γ of rank r means that you can embed Γ in $\mathbb{R}^r$ in such a way that the quadratic form is the restriction of $\sum x_i^2$. This leads to many geometric question about the resulting lattice.*

Open Problems

1. What is the "shape" of the Lattice? (square, skew, etc.)

2. Finding lower bounds for the smallest positive value of $\hat{h}(P)$ for $P \in A(K)$. (There is a conjecture of Lang in this direction.)

3. Are there elliptic curves E over $\mathbb{Q}$ with rank $E(\mathbb{Q})$ of arbitrarily large values? (The largest known is something like 28.)

4. How often is the rank large? More generally, what is the distribution of ranks?

5. For elliptic curves, there is a bound $C(K)$ such that $\#\left(E(K)\right)_{\text{tors}} \leq C(K)$ for all E/K. Does the corresponding statement hold for abelian varieties of fixed dimension? (It is known that $C(\mathbb{Q}) = 16$. Note for number fields $C(K)$ depends on $[K : \mathbb{Q}]$.)

6. Birch and Swinnerton-Dyer Conjecture (to be discussed)

Remark. *Some key facts about the proof of* $C(\mathbb{Q}) = 16$. *Let* $Y_1(m)$ *be the set of isomorphism classes of pairs* (E, P), *where* E *is an elliptic curve* $P \in E$ *is of order* m. *It turns out that* $Y_1(m)$ *is an algebraic curve; It has a map to* $\mathbb{A}^1$ *via the* j*-invariant which comes from* $(E, P) \mapsto E$. *One finds that* $Y_1(m)(\mathbb{Q})$ *is finite if the genus of* $Y_1(m)$ *is at least* 2. *For* m *large, the set is actually empty. Proving* $C(\mathbb{Q}) = 16$ *is extremely difficult.*

Let K be a global field. A/K will be an abelian variety of dimension n, M_K the set of places of K, and S the set of places of bad reduction and archimedean places.

Suppose v is a non-archimedean place, with corresponding absolute value $|\cdot|_v$ and completion K_v. Let $\mathcal{O}_v$ denote the ring of integers $\{x \in K_v : |x|_v \leq 1\}$ and M_v the unique maximal ideal $\{x \in K_v : |x|_v < 1\}$. Note that $\mathcal{O}_v/M_v$ is a finite field; we will write q_v for its cardinality. We can view the equations defining A/K as equations over K_v; for all but finitely many v's, these equations are in $\mathcal{O}_v$. We can look at the same equations in $\mathcal{O}_v/M_v$.

We say v is *of good reduction* if we get from A an abelian variety A_v over $\mathcal{O}_v/M_v$.

Theorem (Weil). *Fix* $v \notin S$. *There exists a polynomial* $P_v(T) \in \mathbb{Z}[T]$ *such that*

$$P_v(T) = \prod_{i=1}^{2n}(1 - \alpha_i T)$$

where the $\alpha_i \in \mathbb{C}$ *have* $|\alpha_i| = q_v^{\frac{1}{2}}$*, and such that over the finite field* $\mathbb{F}_{q_v^m}$*, for all* $m \geq 1$ *we have*

$$\#A_v(\mathbb{F}_{q_v^m}) = \prod_{i=1}^{2n}(1 - \alpha_i^m).$$

Proof. This is a consequence of Weil's proof of the Riemann Hypothesis for function fields, and is not given here.

Example. Elliptic curves E/K $(n = 1)$. Here

$$\#E_v(\mathbb{F}_{q_v}) = (1 - \alpha_1)(1 - \alpha_2) = 1 - (\alpha_1 + \alpha_2) + \alpha_1\alpha_2.$$

Now $P_v(T) = (1 - \alpha_1 T)(1 - \alpha_2 T) \in \mathbb{Z}[T]$, because of the above theorem. It follows that if $\alpha_1 \notin \mathbb{R}$ then $\alpha_2 = \overline{\alpha_1}$, and so $\alpha_1\alpha_2 = |\alpha_1|^2 = q_v$. If $\alpha_1 \in \mathbb{R}$, then $\alpha_2 \in \mathbb{R}$ and α_1, $\alpha_2 = \pm q_v^{\frac{1}{2}}$. If their signs differed, plugging back into $\#E_v(\mathbb{F}_{q_v})$ would give $1 - q_v$, contradicting $\#E_v(\mathbb{F}_{q_v}) \geq 0$. We therefore deduce that $\alpha_1 = \alpha_2$, and $\alpha_1\alpha_2 = q_v$. Hence $\#E_v(\mathbb{F}_{q_v}) = 1 - (\alpha_1 + \alpha_2) + q_v$, and we note that $|\alpha_1 + \alpha_2| \leq |\alpha_1| + |\alpha_2| = 2q_v^{\frac{1}{2}}$.

We can give an interpretation of $P_v(T)$ as a characteristic polynomial. Let l be a prime not dividing q_v. Then $A_v[l^k] \subset A_v(\overline{\mathbb{F}}_{q_v})$ is a $\mathbb{Z}/l^k$-module of rank $2n$. The Frobenius automorphism ϕ (which generates $Gal(\overline{\mathbb{F}}_{q_v}/\mathbb{F}_{q_v})$) acts on $A_v[l^k]$. $P_v(T) = det(1 - T\phi)$, so essentially, $P_v(T)$ is the characteristic polynomial of the Frobenius automorphism.

Definition. $L(A/K, s)$, a function of the complex variable s, is given by

$$L(A/K, s) := \prod_{v \notin S} P_v(q_v^{-s})^{-1} \underbrace{\prod_{v \in S}(\text{other stuff})}_{\Psi}$$

where Ψ is entire and nonvanishing for $Re(s) \geq 1$.

Exercise. This product converges for $Re(s) > \frac{3}{2}$.

In the case of elliptic curves over $\mathbb{Q}$, we obtain

$$L(E/K, s) = \prod_p (1 - a_p p^{-s} + p^{1-2s})^{-1}$$

where $1 - a_p + p = \#E_p(\mathbb{F}_p)$, and $|a_p| \leq 2p^{\frac{1}{2}}$. Although L is strictly only defined for $Re(s) > \frac{3}{2}$, we can heuristically consider $L(E/\mathbb{Q}, 1)$. This is

$$\prod_p (1 - a_p p^{-1} + p_{-1})^{-1} = \prod_p (\frac{p - a_p + 1}{p})^{-1} = \prod_p \frac{p}{\#E_p(\mathbb{F}_p)}.$$

From the latter expression, if $\#E_p(\mathbb{F}_p) > p$ "often enough", then $L(E/\mathbb{Q}, 1) = 0$.

We now examine whether the existence of many rational points forces the existence of many points mod p. Empirically, it has been observed that

$$\prod_{p \le x} \frac{\#E_p(\mathbb{F}_p)}{p} \longrightarrow \infty \Leftrightarrow E(\mathbb{Q}) \text{ is infinite.}$$

Indeed, if this is the case, then the product grows proportionally to $(\log x)^r$, where $r = \text{rank}_{\mathbb{Z}} E(\mathbb{Q})$.

Conjecture (Birch, Swinnerton-Dyer).
(1) *$L(A/K, s)$ has an analytic continuation to $\mathbb{C}$.*
(2) *$ord_{s=1} L(A/K, s) = rank_{\mathbb{Z}} A(K) (= r)$.*
(3) $\lim_{s \to 1} (s-1)^{-r} L(A/K, s) = \frac{R |\text{Sha}| \prod_{v \in S} c_v}{|A(K)_{tor}||A^*(K)_{tor}|}$,

where the regulator $R = \text{vol}(\frac{\mathbb{R}^r}{(A(K)/A(K)_{\text{tor}})}$ with respect to canonical height, $\text{Sha} = \text{Sha}(A/K)$ is the Tate-Shafarevich group, the c_v depend on Ψ above, $A(K)_{\text{tor}}$ is the subgroup of $A(K)$ consisting of points of finite order, and A^* is the dual abelian variety to A, which we don't define. For elliptic curves, $A^* = A$.

Remarks. The stronger condition $(1\frac{1}{2})$, $L(A/K, 2-s) = \pm L(A/K, s)$ is known for abelian varieties (over number fields) having "many endomorphisms" by Hecke, Deuring, Taniyama-Shimura and others.

Statement (2) implies that the sign in $(1\frac{1}{2})$ is equal to $(-1)^r$.

Statements (1) and $(1\frac{1}{2})$ are known for elliptic curves over $\mathbb{Q}$ from Wiles' proof of Fermat's Last Theorem.

The statements (1) and $(1\frac{1}{2})$ are known for abelian varieties over function fields. If $K/\mathbb{F}_q(t)$, then $L(A/K, s)$ is a polynomial in q^{-s} (Weil, Dwork, Grothendieck).
For elliptic curves over $\mathbb{Q}$, $\text{ord}_{s=1} L(A/\mathbb{Q}, s) \le 1$ implies statement (2) (Rubin, Kolyvagin, Gross-Zagier, ...)
If K is a function field, then $\text{rank}_{\mathbb{Z}} A(K) \le \text{ord}_{s=1} L(A/K, s)$, with equality iff Sha is finite. In this case, (2) implies (3) (Tate, ..., Kato-Trihan).

We start with a theorem, which was conjectured by Mordell.

Theorem 29. *If K is a global field and C/K is a curve of genus ≥ 2, then $C(K)$ is finite except if K is a function field over $\mathbb{F}_q$ and C is defined over $\mathbb{F}_q$.*

Remark. *In particular, if K is a number field, then $C(K)$ is finite. The number field case is solved by Faltings in 1983. The function field case was done by Samuel in the 60's.*

Before we embark on the arithmetic of curves we need to do some geoemtry. We begin by defining divisors and Jacobians.

Suppose F is algebraically closed and C/F is a smooth irreducible projective curve. In general $C(F)$ is not finite.

Definition 30. *A divisor on C is a formal sum $D := \sum_{P \in C(F)} n_P P$ where $n_P : C(F) \to \mathbb{Z}$ is supported on finitely many points.*

Given two divisors $D = \sum_P n_P P, D' = \sum_P n'_P P$ define $D + D' := \sum_P (n_P + n'_P)P$. Denote the set of all divisors on C by $\mathrm{Div}(C)$. In other words, $\mathrm{Div}(C)$ is a free abelian group generated by $C(F)$.

We also define a map $\deg : \mathrm{Div}(C) \to \mathbb{Z}$ by $\deg(D) := \sum_P n_P$ where $D = \sum_P n_P P$. Set $\mathrm{Div}^0(C) := \ker(\deg)$.

Recall that the function field $F(C)$ is defined as a field of fractions of

$$R := F[x_1, \ldots, x_n]/(f_1, \ldots, f_m)$$

where $f_1 = \cdots = f_m = 0$ is a system of equations for a non-empty affine open subset of C. For example, if C is defined by $f(x, y) = 0$ then $R = F[x, y]/(f(x, y))$ and $F(C)$ is a field of fractions of R.

Let $h \in F(C)$. Define $(h) \in \mathrm{Div}(C)$ by

$$(h) := \sum_P \mathrm{ord}_P(h) P$$

where $\mathrm{ord}_P(h)$ is the order of zero or pole of h at P. We have the following fact.

Proposition 31. *$\deg((h)) = 0$ for any $h \in F(C)$, that is, any function has as many zeros as poles with multiplicities.*

Verify this for a couple of examples. If $F = \mathbb{C}$, then C is a compact Riemann surface. Take any function $h \in F(C)$, that is, a meromorphic function on the surface. Then there are only finitely many zeros and poles

on C. We can take a closed path γ on C enclosing a disk that does not contain any zeros or poles of h. By the residue theorem we have that

$$0 = \int_\gamma \frac{dh}{h} = \sum_P \mathrm{ord}_P(h).$$

If $C = \mathbb{P}^1$, then $F(C) = F(x)$. For $h = \frac{A(x)}{B(x)}$, we have $\mathrm{ord}_\infty(h) = \deg(B) - \deg(A)$ hence the proposition holds.

Definition 32. *Prin*$(C) := \{(h) : h \in F(C)\}$.

Remark. *By proposition 1,* $Prin(C) \subset Div^0(C) \subset Div(C)$. *Also for any* $h_1, h_2 \in F(C)$, $(h_1 h_2) = (h_1) + (h_2)$.

We are now in position to define the Jacobian of C.

Definition 33. *The Jacobian of* C *is the group* $Div^0(C)/Prin(C)$.

Definition 34. *We say divisors* D, D' *on* C *are linearly equivalent if* $D - D' \in Prin(C)$ *and denote* $D \sim D'$ *if those are equivalent. In other words,* $D \sim D'$ *if and only if there exists* $h \in F(C)$ *so that* $D - D' = (h)$.

Here are a couple of examples.

Suppose $D \in \mathrm{Div}^0(\mathbb{P}^1)$. Then D is a form of $\sum_{\alpha \in F} n_\alpha [\alpha] + n_\infty [\infty]$. Note that $\sum n_\alpha + n_\infty = 0$. Define a function

$$h := \prod_{\alpha \in F} (x - \alpha)^{n_\alpha}.$$

Then $(h) = D$ and this implies that $\mathrm{Jac}(\mathbb{P}^1) = 0$.

Now consider an elliptic curve $E : y^2 = x^3 + ax + b$. We claim that $\mathrm{Jac}(E) \cong E(F)$. The isomorphism is given by $E(F) \ni P \mapsto P - O \in \mathrm{Jac}(E)$ where O is the point at ∞ on E. This map is well-defined because $P - O \in \mathrm{Div}^0(E)$. We are going to show first that this is surjective. Later we will see that this is injective and a homomorphism.

Let $P, Q \in E$ and L be the line $\overline{PQ}$. Then by definition,

$$(L) = P + Q + R - 3O$$

unless the line L is vertical, where R is another intersection point on E by L. Hence

$$P + Q - 2O \sim O - R \sim \overline{R} - O$$

where $\overline{R} = -R$ in the group law on E. Therefore

$$P + Q \sim \overline{R} + O.$$

This can be used iteratively on a divisor to trade two arbitrary points by a pair of points one of which is O. Let $D = \sum n_i P_i - \sum m_i P_i$ where $n_i, m_i > 0$ and $\sum n_i = \sum m_i$. Then, applying this procedure gives:

$$D \sim \left(Q + \left(\sum n_i - 1\right) O\right) - \left(R + \left(\sum m_i - 1\right) O\right) = Q - R$$

Now, $Q - R \sim Q + \overline{R} - 2O \sim O - P \sim \overline{P} - O$. This shows that our map is surjective.

We begin with letting F be algebraically closed with characteristic not 2 or 3. We saw for an elliptic curve E, $E(F) \to \operatorname{Jac} E$, where $P \mapsto P - \mathcal{O}$, is surjective (and the proof can be extended to show it is a homomorphism). We now show it is injective. So we need to show that if $P \neq \mathcal{O}$ then $P - \mathcal{O} \not\sim 0$; that is, there is no function h on E with $(h) = P - \mathcal{O}$. Note:

$$\begin{array}{ll} F(E) = F(x,y) & \text{(degree 2 since } y = \sqrt{x^3 + ax + b}\text{)} \\ \Big| 2 & \\ F(x) & \end{array}$$

Thus $F(E) = \{r(x) + ys(x) : r(x), s(x) \in F(x)\}$ so we may write $h(x,y) = \frac{a(x)+yb(x)}{c(x)}$, with $\gcd(a,b,c) = 1$ (by getting a common denominator and cancelling common factors).

We claim that if h has no poles in the affine part of E then c is a constant. To see this, suppose $\deg(c) \geq 1$. Then $\exists \alpha \in F$ with $c(\alpha) = 0$. Let β satisfy $\beta^2 = f(\alpha)$ (where $f(x) = x^3 + ax + b$) so the points $(\alpha, \pm\beta) \in E$. If h has no pole at $(\alpha, \pm\beta)$, the numerator must vanish; so $a(\alpha) \pm b(\alpha)\beta = 0$. Since it must hold for both $(\alpha, +\beta)$ and $(\alpha, -\beta)$, we can add both equations to deduce $a(\alpha) = 0$, and so $b(\alpha)\beta = 0$.

If $\beta \neq 0$, then $b(\alpha) = 0$; implying that $(x - \alpha)$ is a common factor to a, b, and c, contradiction. If $\beta = 0$ then $f(\alpha) = 0$. So $y^2 = f(x) = (x-\alpha)g(x)$. We have $\operatorname{ord}_{(\alpha,0)}(x - \alpha) = 2$ and $\operatorname{ord}_{(\alpha,0)} y = 1$, so $a(x) = (x-\alpha)^r a_1(x)$ and $\operatorname{ord}_{(\alpha,0)}(a(x)) = 2r \geq 2$ and similarly for b. In particular, their orders are even. If $\operatorname{ord}_{(\alpha,0)}(h) \geq 0$ then $\operatorname{ord}(a + by) \geq \operatorname{ord}(c)$, so $\min\{\operatorname{ord}(a), \operatorname{ord}(b)\} \geq \operatorname{ord}(c)$. But $\operatorname{ord}(b) > 0$ implies $b(\alpha) = 0$, contradiction as above. So $\operatorname{ord}(b(\alpha)y) = \operatorname{ord}(b) + \operatorname{ord}(y) = \operatorname{ord}(y) = 1$. Thus we have $1 \geq 2$, contradiction.

Thus we have $h = a + yb$ for $a, b \in F[x]$. Now the $\operatorname{ord}_{\mathcal{O}} a = -2 \deg a$ and $\operatorname{ord}_{\mathcal{O}} by = -2 \deg b - 3$ (the latter follows since $y^2 = f(x)$ the $\operatorname{ord}_{\mathcal{O}} x = -2$ and $\operatorname{ord}_{\mathcal{O}} y = -3$). Now $-1 = \operatorname{ord}_{\mathcal{O}} h = \min\{-2 \deg a, -2 \deg b - 3\}$ for $a, b \neq 0$. [If $a = 0$ or $b = 0$, we have a term not appearing in the minimum.] We get a contradiction, and this shows injectivity.

Example. *Let $y^2 = f(x)$ with $\deg f(x) = 5$ and f has distinct roots. It is a fact that this gives a curve of genus 2. $f(x) - (ax^2 + bx + c)$ has 5 zeroes say $\alpha_1, \ldots, \alpha_5$. Say $\beta_i = -(a\alpha_i^2 + b\alpha_i + c)$ and $P_i = (\alpha_i, \beta_i)$. Then $(h) = P_1 + P_2 + \cdots + P_5 - 5P_\infty$, where $h(x, y) = y + (ax^2 + bx + c)$.*

Now given P_1, P_2, P_3, we can choose a, b, c so that $P_1 + P_2 + P_3 - 3P_\infty \sim 2P_\infty - (P_4 + P_5)$ is the relation given by h.

Using these kinds of relations, we can trade three points for two points and prove that every divisor D, $\deg D = 0$, is linear equivalent to a divisor of the form $P_1 + P_2 - 2P_\infty$.

Define $C^{(2)} = C \times C/S_2$ (i.e. mod out by switching coordinates); this is the set of unordered pairs. Hence we have a map $\Phi : C^{(2)} \to \mathrm{Jac}(C)$ given by $\{P_1, P_2\} \mapsto P_1 + P_2 - 2P_\infty$, which is surjective.

Unfortunately, it is not injective. The divisor of $(x - \alpha)$ is $(\alpha, \beta) + (\alpha, -\beta) - 2P_\infty$ (where $\beta^2 = f(\alpha)$). Hence all the pairs of the form $\{(\alpha, \beta), (\alpha, -\beta)\}$ gives $\mathcal{O}$ under Φ. It turns out that this is the only source of non-injectivity. The other points in $C^{(2)}$ uniquely represent a point in $\mathrm{Jac}(C)$. [In algebraic geometry terms, Φ is a birational map and $\mathrm{Jac}(C)$ is the blow-down of $C^{(2)}$ along a curve.]

For curves of genus 2, the Jacobian is a surface. In general the Jacobian of a curve of genus g is an algebraic variety of dimension g. In fact, $\mathrm{Jac}(C)$ is projective and, since it has a group law, it is an abelian variety. Moreover, $\mathrm{Jac}(C)$ is birational to $C^{(g)} := C^g/S_g$, where $\{P_1, \ldots, P_g\} \mapsto P_1 + \cdots + P_g - gP_0$ for some fixed P_0. The sources of non-injectivity are more complicated, but it is a collection of blow-downs.

Example. *If $F = \mathbb{C}$ and $C/\mathbb{C}$ you can choose $\omega_1, \ldots, \omega_g$ linear independent holomorphic differential forms on C with $\mathrm{Jac}(C) \to \mathbb{C}^g/L$, where L is a lattice, given by $P_1 + \cdots + P_g - gP_0 \mapsto \sum_{i=1}^g \left(\int_{P_0}^{P_i} \omega_1, \ldots, \int_{P_0}^{P_i} \omega_g \right)$; the lattice is $\left\{ \left(\int_\gamma \omega_1, \ldots, \int_\gamma \omega_g \right) : \gamma \in \pi_1(C(\mathbb{C})) \right\}$.*

Back to a global field

Suppose K is a global field and C/K is a smooth curve of genus g. Write $F = \overline{K}$. We can view C as a curve over F and get $\mathrm{Jac}(C)$ which is an abelian variety. It turns out that $\mathrm{Jac}(C)$ is defined over K.

We have $\mathrm{Jac}(C)(K)$ is a subgroup of $\mathrm{Jac}(C)(F)$. Suppose $D = \sum n_i P_i$ is a divisor and K is perfect. Take $\sigma \in \mathrm{Gal}(F/K)$ and $P_i \in C(F)$. Note σ acts on points by acting on coordinates and gives another point in C, since C is defined over K. Thus σ can act on D by $\sigma(F) = \sum n_i \sigma(P_i)$.

Definition. *We say D is defined over K if $\sigma(D) \sim D$ for all $\sigma \in \mathrm{Gal}(F/K)$*

It can be shown that $\mathrm{Jac}(C)(K)$ is exactly the set of equivalence classes of divisors of degree zero defined over K.

Example. *For $g = 1$, $\mathrm{Jac}(E) = E$ over F. It turns out $\mathrm{Jac}(E)(K) = E(K)$, since $\sigma(P) - \mathcal{O} = \sigma(P - \mathcal{O}) \sim P - \mathcal{O}$ (that is using the fact that $\mathcal{O}$ is rational) implies $\sigma P \sim P$. Which can be shown to imply $\sigma(P) = P$. If this happens for all $\sigma \in \mathrm{Gal}(F/K)$, we have $P \in E(K)$.*

If C is curve of genus 1 with no rational points, we get $\mathrm{Jac}(C) = E$ is an elliptic curve E/K with E and C isomorphic over F.

Example. *Consider $g = 2$. Let $y^2 = f(x)$, where $\deg f = 5$. Assume P_0 is a rational point at ∞. Now $\mathrm{Jac}(C) = \{[P_1 + P_2 - 2P_0] : P_1, P_2 \in C(F)\}$; note $\sigma(P_1) + \sigma(P_2) - 2P_0 = \sigma(P_1 + P_2 - 2P_0) \sim P_1 + P_2 - 2P_0$ "usually" implies $\sigma(P_1) + \sigma(P_2) = P_1 + P_2$. If $\sigma(P_i) = P_2$ for $i = 1, 2$ for all σ then $P_i \in C(K)$. Unfortunately this need not always happen. For example, we could have $\sigma(P_1) = P_2$ and $\sigma(P_2) = P_1$, which would occur if $P_1 \in C(L)$ where $[L : K] = 2$ and P_2 is the galois conjugate of P_1; we have*

$$\mathrm{Jac}(C)(K) = \{[P_1 + P_2 - 2P_0] : P_1, P_2 \in C(K)\} \cup \bigcup_{[L:K]=2} \left\{[P + \overline{P} - 2P_0] : P \in C(L)\right\}$$

where $\overline{P}$ denotes the conjugate of P. We have a case of this example: If $y^2 = (x^2 + 1)(x^3 + 2)$ and $P = (i, 0) \in C(\mathbb{Q}(i))$; so $(i, 0) + (-i, 0) - 2P_0 \in \mathrm{Jac}(C)(\mathbb{Q})$.

• **Last time:**

C/K curve of genus $g \geq 2$. We constructed an abelian variety $J = \mathrm{Jac}(C)$ also defined over K and of dimension g.

If $P_0 \in C(K)$ then we have a map

$$\alpha : C \longrightarrow J$$

$$P \mapsto P - P_0$$

Remark: We can use any divisor D_0 with $deg(D_0) = 1$ and get a map

$$\alpha : C \longrightarrow J$$

$$P \mapsto P - D_0$$

So $C(K) \subseteq J(K)$. Mordell-Weil implies that $J(K)$ is a finitely generated abelian group when K is a global field. Does it help to understand $C(K)$?

•**Today:**

Theorem*(Chabauty '38) If K is a number field and $rank_{\mathbb{Z}} J(K) < g$, then $C(K)$ is finite.*

(We use p-adic analysis to prove it)

We can embed K in $\mathbb{Q}_p$ for some prime p. Let's study $J(\mathbb{Q}_p)$ first.

Lemma *There exists a neighborhood of $0 \in J(\mathbb{Q}_p)$ which is isomorphic (as a p-adic analytic group) to $\mathbb{Z}_p^g$.*

More precisely, there are local coordinates $t_1, ..., t_g$ near 0 and power series $\lambda_1, ..., \lambda_g$ in $t_1, ..., t_g$ converging in some neighborhood U of 0 such that $P, Q \in U, P = (t_1(P), ..., t_g(P))$, etc., then $\lambda_i(t_1(P+Q), ..., t_g(P+Q)) = \lambda_i(t_1(P), ..., t_g(P)) + \lambda_i(t_1(Q), ..., t_g(Q))$.

Assume the Lemma for a while.

Proof of Theorem: Let $P_1, ..., P_r$ be generators of the free part of $J(K), r < g$. Replace P_i, if necessary, by $p^m P_i$ so that without loss of generality $P_i \in U$. Consider the vectors

$$\begin{matrix} (\lambda_1(P_1), & \cdots & , \lambda_g(P_1)) \\ \vdots & & \vdots \\ (\lambda_1(P_r), & \cdots & , \lambda_g(P_r)) \end{matrix}$$

There exist $a_1, ...a_g \in \mathbb{Z}_p$ not all zero such that

$$\sum a_i \lambda_i(P_j) = 0, j = 1, ..., r$$

Let $\lambda = \sum a_i \lambda_i$ which is an analytic function on U. By construction $\lambda(P_i) = 0, i = 1, .., r$ and by the lemma λ is linear in a neighborhood of 0. So $\lambda(P) = 0$ for any $\mathbb{Z}$-linear combination of the $P_i's$.

If $Q \in J(K)$ then $p^m Q \in U$ for some large m. $\lambda(Q) = \frac{1}{p^m}\lambda(p^m Q) = 0$. Suppose by contradiction that $C(K)$ is infinite. $C(K) \subseteq C(\mathbb{Q}_p)$ is compact (C is projective). Hence there is an accumulation point P_0. Take $P_1 \in C(K)$ such that $P_1 - P_0 \in U$. If $P \in C(K)$ is close enough to P_0 then $P - P_0, P_1 - P_0 \in U$ gives $P_1 - P_0 \in J(K) \cap U$. Thus $\lambda(P - P_1) = 0$. But λ is a an analytic function and C is 1-dimensional. So λ can only have finitely many zeros in C, unless the function $\psi : P \mapsto \lambda(P - P_1)$ is identically zero.

If $\psi \not\equiv 0$ we get only finitely many $P's$, contradicting the fact that P_0 was an accumulation point of $C(K)$.

If $\psi \equiv 0$, then $\lambda(P - P_1) = 0, \forall P \in C(K), P - P_1 \in U$. If $Q_1, ..., Q_g \in C(\mathbb{Q}_p)$ are near P_1,

$$\sum \lambda(Q_i - P_1) = 0$$

Now $Q_1 + ... + Q_g - gP_1$ cover an open set of $J(\mathbb{Q}_p)$ as $Q_1, ..., Q_g$ vary. So $\lambda \equiv 0$, a contradiction.$\square$

Idea of Proof of Lemma: Given $P \in J$, translation by P ($Q \mapsto Q+P$) gives a map $\tau_P : J \longrightarrow J$ such that $0 \mapsto P$. The derivative

$$d\tau_P : T_0 J \longrightarrow T_P J$$

is an isomorphism. Therefore the dual spaces $(T_0 J)^*$ and $(T_P J)^*$ are also isomorphic.

Given an element of $(T_0 J)^*$ say v we get a 1-form on J, given by $\omega = (d\tau_P)^*(v)$ i.e., for each P an element of $(T_P J)^*$. We have $\tau_P^* \omega = \omega$. The function

$$\lambda : P \mapsto \int_0^P \omega$$

is linear in P. In fact,

$$\int_0^{P+Q} \omega = \int_0^P \omega + \int_P^{P+Q} \omega = \int_0^P \omega + \int_0^Q \tau_P^* \omega = \int_0^P \omega + \int_0^Q \omega$$

Since $\dim(T_0 J) = g$, we get a g-dimensional set of $\lambda' s$.$\square$

Example: $C : y^2 = f(x), deg(f) = 5, g = 2$

Holomorphic differentials on C are generated by $\frac{dx}{y}, \frac{xdx}{y}$. If $t = \frac{x^2}{y}$ we can represent x, y as Laurent series in t.

$$\int_{P_\infty}^P \frac{dx}{y}$$

is a power series in t. Take $\alpha : C \longrightarrow J$. If ω is a differential on J, then $\alpha^* \omega$ is a differential on C.

$$\int_{P_\infty}^P \alpha^* \omega = \int_{\alpha(P_\infty)}^{\alpha(P)} \omega$$

(integrals on J transfer to integrals on C)

Let K be a field of characteristic $p > 0$. Let $f(x_1, x_2, \ldots, x_n) \in K[x_1, x_2, \ldots, x_n]$ given by

$$f(x_1, x_2, \ldots, x_n) = \sum a_{i_1, i_2, \ldots i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}.$$

Define

$$f^{(p)}(x_1, x_2, \ldots, x_n) = \sum a^p_{i_1, i_2, \ldots i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}.$$

If X/K is a variety, X is the set of zeros of $f_1, f_2, \ldots, f_m \in K[x_1, x_2, \ldots, x_n]$. Define $X^{(p)}$ to be the set of common zeroes of $f_1^{(p)}, f_2^{(p)}, \ldots, f_m^{(p)}$. There is a map $F : X \to X^{(p)}$ given by $(x_1, x_2, \ldots, x_n) \mapsto (x_1^p, x_2^p, \ldots, x_n^p)$ because $(f(x_1, x_2, \ldots, x_n))^p = f^{(p)}(x_1^p, x_2^p, \ldots, x_n^p)$. (Follows from the fact that $(x + y)^p = x^p + y^p$ in characteristic p).

Remark. *If X is defined over $\mathbb{F}_p$, then $X^{(p)} = X$. If X is defined over $\mathbb{F}_{p^m}$, then, if we define $X^{(p^2)} = (X^{(p)})^{(p)}$, etc. then $X^{(p^m)} = X$, and we get a map $F^m : X \to X$ via*

$$X \to X^{(p)} \to X^{(p^2)} \to \cdots \to X^{(p^m)}$$

.

Let A/K be an abelian variety. Then we have the map $F : A \to A^{(p)}$. We also have the map $[p] : A \to A$ defined by $P \mapsto pP$. Fact: There is a map $V : A^{(p)} \to A$ such that $[p] = V \circ F$.

Remark. *If $\Phi : X \to Y$ is an onto map of varieties over K, we have an injection of function fields $K(Y) \hookrightarrow K(X)$. Then the map Φ is separable if $K(X)/K(Y)$ is separable.*

Definition. *An abelian variety A is called ordinary if V is separable.*

Theorem 35. *If K is a global field of characteristic $p > 0$ and C/K is a curve of genus $g \geq 2$ such that C is not defined over K^p and $J = \mathrm{Jac}(C)$ is ordinary, then $C(K)$ is finite.*

Proof. Mordell-Weil implies that $J(K)$ is finitely generated, so $J(K)/pJ(K)$ is finite. If $C(K) = \emptyset$, we are done. If not, we have $\alpha : C \to J$ defined by $P \mapsto P - P_0$. We can assume $C \subseteq J$. So $C(K) = C \cap (J(K))$. If $C(K)$ is infinite, then there is $P_1 \in J(K)$ such that $C \cap (P_1 + pJ(K))$ is infinite. Define $\Phi : J^{(p)} \to J$ by $\Phi(P) = V(P) + P_1$. Define $C' = \Phi^{-1}(C)$, so that C' is a curve on $J^{(p)}$. Now we have $P \in P_1 + pJ(K) \Leftrightarrow$ there is $Q \in J(K)$ such that $P = P_1 + pQ = P_1 + V(F(Q)) = \Phi(F(Q)) \Leftrightarrow \Phi^{-1}(P) \in F(J(K))$. But $F(J(K)) = J^{(p)}(K^p)$. So $C \cap (P_1 + pJ(K)$ infinite $\Rightarrow C' \cap J^{(p)}(K^p)$ is infinite. $J^{(p)}$ is defined over K^p. It can be shown that $C' \cap J^{(p)}(K^p)$ being infinite implies C' is defined over K^p. But using the fact that J is ordinary, we can show C' defined over K^p implies C defined over K^p, giving a contradiction. □

Remark. *The natural hypothesis for the Mordell conjecture is that C is not defined over $\mathbb{F}_q$. It can be shown that this is equivalent to C not defined over*

K^{p^m} for some $m \geq 1$: If K is a global field of characteristic p, $\bigcap_{m\geq 1} K^{p^m} = \mathbb{F}_q$. The proof can be adapted to deal with this more general situation.

What happens over finite fields: Consider $C/\mathbb{F}_q$, with $q = p^f$. Let K be a global field of characteristic p wth constant field $\mathbb{F}_q$. Suppose $P \in C(K) - C(\mathbb{F}_q)$. We can consider $F^{fm}(P) \in C(K)$, and we get infinitely many points with $m = 1, 2, \ldots$.

Example. *$C : y^2 = x^5 + 1$ over $\mathbb{F}_3$. Take $K = \mathbb{F}_3(t, s)$ where $s^2 = t^5 + 1$. Then $(t^{3^m}, s^{3^m}) \in C(K)$.*

In place of $J(K)$, we could have used any subgroup $\Gamma \subseteq J(K^{sep})$ with the property that $\Gamma/p\Gamma$ is finite (e.g., one can take Γ to be the group of prime to p torsion points in $J(K^{sep})$. A special case of the Manin-Mumford conjecture says that $C \cap J_{tor}$ is finite.

Another example that one can take is to embed $J(K)$ in $J(K_v)$ for a completion K_v of K and take $\overline{J(K)}$ in $J(K)$. (In the case of number fields, the Chabauty argument proves that $\overline{J(K)} \cap C$ is finite if $J(K) \subseteq J(K_v)$ and $\mathrm{rk}(J(K)) < \mathrm{genus}(C)$). In characteristic p, $\overline{J(K)} \subseteq J(K_v)$ is always "small", where "big" means that it "contains a neighborhood of 0," and "small" means not "big." In characteristic 0, $\overline{J(K)} \subseteq J(K_v)$ is "small" if v is non-Archimedean and $\mathrm{rk}(J(K)) < \mathrm{genus}(C)$. Otherwise, it is usually "big."

Conjecture. *Let K be a global field and A/K an Abelian variety. If $X \subset A$ is a closed algebraic set defined over K, then*

$$\prod_{v\in M_K} X(K_v) \cap \overline{A(K)} = \overline{X(K)}$$

Here M_K ist the set of places of K and $\overline{S}$ represents the closure of the set S in the product topology of $\prod_{v\in M_K} A(K_v)$ where each $A(K_v)$ is endowed with the v-adic metric topology.

Remark. *In other words, the conjecture says that if we are given a sequence $P_n \in A(K)$, $n = 1, 2...$, such that for all $v \in M_K$, there exists $Q_v \in X(K_v)$ with $P_n \longrightarrow Q_v$ in the v-adic topology then there exists a sequence $\{R_n\} \subset X(K)$ with $R_n \longrightarrow Q_v$ in the v-adic topology.*

Also notice that if $X(K)$ is finite then $\overline{X(K)} = X(K)$, so we get a stronger conclusion, namely: there exists a $R \in X(K)$ such that $Q_v = R$, for all $vinM_K$.

We'll sketch the proof of this conjecture in characteristic p under the following assumptions:

- X is a curve with Genus$(X) \geq 2$, which is not defined over K^p, A is an ordinary abelian variety and the set $\{P \in A(K^{sep}) | \exists n \geq 1, p^n P = 0\}$ is finite.

Recall that in this case the Mordell conjecture was proved by writing

$$A(K) = \cup_{i=1}^{n} (pA(K) + P_i)$$

where P_i, $i = 1, 2, ..., n$, are coset representatives of $A(K)/pA(K)$. Therefore

$$X \cap A(K) = \cup_{i=1}^{n} (X \cap (pA(K) + P_i))$$

So we are left to show that each intersection $X \cap (pA(K) + P_i)$ is finite. This is done by first noticing that $pA(K) = V(F(A(K))) = V(A^{(p)}(K^p))$, where V is the dual of the Frobenius map. Let's define a map Φ by $\Phi(P) = V(P) + P_i$ and assume, by contradiction, that $X \cap (pA(K) + P_i)$ is infinite. So $\Phi^{-1}(X) \cap A^{(p)}(K^p)$ is infinite. This would imply, after some work, that $\Phi^{-1}(X)$ is defined over K^p. And so X is defined over K^p, contradicting our previous assumption.

Also notice that the same proof would work if we replace $A(K)$ by its closure in $A(K_v)$ and work with K_v^p instead of K_v, since $K_v^p \cap K = K^p$. Taking another careful look at this proof, one sees that we're really proving that:

(*) There exists a finite set $Z \subset X$ such that $P_n \in A(K)$ and $P_n \longrightarrow P_v \in X(K_v)$ in $A(K_v)$ then $\lim P_n \in Z$.

Namely, there exists a set Z_1 such that $X \cap pA(L) \subset Z$ for any L/K separable extension. Z corresponds to the finitely many cosets of $\overline{A(K)}$ in $p\overline{A(K)}$.

This condition implies that

$$\prod_{v \in M_K} X(K_v) \cap \overline{A(K)} = \prod_{v \in M_K} Z(K_v) \cap \overline{A(K)}$$

which reduces the proof of the conjecture in dimension 1 to proving it in dimension zero. The case of dimension zero requires an extra argument. The condition $\{p \in A(K^{sep}) | \exists n \geq 1, p^n P = 0\}$ is finite comes in the proof of the zero dimensional case.

Let's now take a look at the zero characteristic case and assume the condition $\operatorname{rank}(A(K)) < \dim A$ of Chabauty's theorem. In this case we construct $\lambda : A(K_v) \longrightarrow K_v$ analytic with $A(K) \subset \lambda^{-1}(0)$, but $X \cap \lambda^{-1}(0)$ is finite. $Z_v = X \cap \lambda^{-1}(0)$ has the property (*). Unfortunately Z_v depends on v in characteristic zero, so we cannot reduce the 1-dimensional case to the 0-dimensional one.

Suppose instead that $\operatorname{rank}(A(K)) < \dim A - 1$, then you can construct $\lambda_1, \lambda_2 : A(K_v) \longrightarrow$ linearly independents, with $A(K) \subset \lambda_i^{-1}(0)$. Define $Z_v = X \cap \lambda_1^{-1} \cap \lambda_2^{-1}$.

Conjecture (Stoll)**.** *In this situation, there is a finite set Z independent of v with $Z_v \subset Z$, for all v*

If this is true then the reduction of the 1-dimensional case to the 0-dimensional case works in zero characteristic.