Chabauty-Kim

Xiang Li

1 Apply to $\mathbb{G}_m(\mathbb{Z})$

Fix a prime $p \in \mathbb{Z}$. For any prime $l \in \mathbb{Z}$, consider the diagram

$$\begin{tikzcd}
\mathbb{G}_m(\mathbb{Z}) \arrow[r] \arrow[d, "j"] & \mathbb{G}_m(\mathbb{Z}_l) \arrow[d, "j_l"] \\
H^1(G_{\mathbb{Q}}, \mathbb{Q}_p(1)) \arrow[r, "\mathrm{loc}_l"] & H^1(G_l, \mathbb{Q}_p(1))
\end{tikzcd} \tag{1}$$

Proposition 1.1. *Let K be a field of characteristic 0. Then the the Kummer map $\mathbb{G}_m(K) = K^\times \to H^1(G_K, \mathbb{Q}_p(1))$ can be identified with the natural map*

$$K^\times \to K^\times \otimes \mathbb{Q}_p := \left(\varprojlim_n K^\times/(K^\times)^{p^n} \right) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

Proof. We have short exact sequence

$$0 \longrightarrow \mu_{p^n} \longrightarrow \mathbb{G}_m \xrightarrow{\times p^n} \mathbb{G}_m \longrightarrow 0$$

which induces long exact sequence of Galois cohomology on $\overline{K}$ points

$$\mu_{p^n} \longrightarrow \overline{K}^\times \xrightarrow{\times p^n} \overline{K}^\times \longrightarrow H^1(G_K, \mu_{p^n}(\overline{K})) \longrightarrow H^1(G_K, \overline{K}^\times)$$

By Hilbert 90, $H^1(G_K, \overline{K}^\times) = 0$. So the above long exact sequence gives us the following short exact sequence

$$0 \longrightarrow K^\times/(K^\times)^{p^n} \longrightarrow H^1(G_K, \mu_{p^n}(\overline{K})) \longrightarrow 0$$

So

$$K^\times/(K^\times)^{p^n} \simeq H^1(G_K, \mu_{p^n}(\overline{K})).$$

By taking the limit $n \to \infty$, we get

$$\varprojlim_n K^\times/(K^\times)^{p^n} \simeq H^1(G_K, \mathbb{Z}_p(1)).$$

Thus,

$$K^\times \otimes \mathbb{Q}_p := \left(\varprojlim_n K^\times/(K^\times)^{p^n} \right) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \simeq H^1(G_K, \mathbb{Z}_p(1)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \simeq H^1(G_K, \mathbb{Q}_p(1))$$

where the Kummer map $\mathbb{G}_m(K) = K^\times \to H^1(G_K, \mathbb{Q}_p(1))$ is given by the natural map. $\square$

Corollary 1.2.

$$\mathbb{Q}^\times \otimes \mathbb{Q}_p := \left(\varprojlim_n \mathbb{Q}^\times/(\mathbb{Q}^\times)^{p^n} \right) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \simeq H^1(G_{\mathbb{Q}}, \mathbb{Q}_p(1)) \tag{2}$$

$$\mathbb{Q}_l^\times \otimes \mathbb{Q}_p := \left(\varprojlim_n \mathbb{Q}_l^\times/(\mathbb{Q}_l^\times)^{p^n} \right) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \simeq H^1(G_l, \mathbb{Q}_p(1)) \tag{3}$$

Lemma 1.3. *The l-valuation map $v_l : \mathbb{Q}_l^\times \to \mathbb{Z}$ gives us the following split short exact sequence*

$$0 \longrightarrow \mathbb{Z}_l^\times \xrightarrow{i} \mathbb{Q}_l^\times \xrightarrow{v_l} \mathbb{Z} \longrightarrow 0 \tag{4}$$

where $i : \mathbb{Z}_l^\times \to \mathbb{Q}_l^\times$ is the inclusion.

Proof. Note that $v_l : \mathbb{Q}_l^\times \to \mathbb{Z}$ has a section $s : \mathbb{Z} \to \mathbb{Q}_l^\times, m \mapsto l^m$ such that $v_l \circ s = \mathrm{id}_{\mathbb{Z}}$. So the above short exact sequence splits. $\square$

Lemma 1.4. *We have an isomorphism*

$$\varprojlim_n \mathbb{Q}_l^\times/(\mathbb{Q}_l^\times)^{p^n} \xrightarrow{\simeq} \left(\varprojlim_n \mathbb{Z}_l^\times/(\mathbb{Z}_l^\times)^{p^n}\right) \oplus \mathbb{Z}_p \tag{5}$$

where

- *the map to the first component is induced by a section $s : \mathbb{Q}_l^\times \to \mathbb{Z}_l^\times$ of the inclusion $i : \mathbb{Z}_l^\times \to \mathbb{Q}_l^\times$ with $s \circ i = \mathrm{id}_{\mathbb{Z}_l^\times}$;*
- *the map to the second component is induced by the l-valuation map $v_l : \mathbb{Q}_l^\times \to \mathbb{Z}$.*

Proof. Consider the commutative diagram below with exact rows:

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Z}_l^\times \arrow[r, "i"] \arrow[d, "\times p^n"] & \mathbb{Q}_l^\times \arrow[r, "v_l"] \arrow[d, "\times p^n"] & \mathbb{Z} \arrow[r] \arrow[d, "\times p^n"] & 0 \\
0 \arrow[r] & \mathbb{Z}_l^\times \arrow[r, "i"] & \mathbb{Q}_l^\times \arrow[r, "v_l"] & \mathbb{Z} \arrow[r] & 0
\end{tikzcd}$$

By snake lemma, we have the following short exact sequence

$$0 \longrightarrow \mathbb{Z}_l^\times/(\mathbb{Z}_l^\times)^{p^n} \xrightarrow{i} \mathbb{Q}_l^\times/(\mathbb{Q}_l^\times)^{p^n} \xrightarrow{v_l} \mathbb{Z}/p^n\mathbb{Z} \longrightarrow 0$$

By taking the limit $n \to \infty$, we have

$$0 \longrightarrow \varprojlim_n \mathbb{Z}_l^\times/(\mathbb{Z}_l^\times)^{p^n} \xrightarrow{i} \varprojlim_n \mathbb{Q}_l^\times/(\mathbb{Q}_l^\times)^{p^n} \xrightarrow{v_l} \mathbb{Z}_p \longrightarrow 0$$

The above exact short sequence splits (which basically follows from the splitness of the exact sequence (4)). So we have our desired isomorphism. $\square$

Lemma 1.5. *Let $l \in \mathbb{Z}$ be an odd prime. The reduction modulo l map $\mathrm{mod}_l : \mathbb{Z}_l^\times \to \mathbb{F}_l^\times$ gives us the following split short exact sequence*

$$0 \longrightarrow \mathbb{Z}_l \xrightarrow{\iota} \mathbb{Z}_l^\times \xrightarrow{\mathrm{mod}_l} \mathbb{F}_l^\times \longrightarrow 0$$

where $\iota : \mathbb{Z}_l \to \mathbb{Z}_l^\times$ is given by the following compositions:

$$\mathbb{Z}_l \xrightarrow[\simeq]{\times l} l\mathbb{Z}_l \xrightarrow[\simeq]{\exp} 1 + l\mathbb{Z}_l \xrightarrow{\text{inclusion}} \mathbb{Z}_l^\times$$

Proof. For any $\alpha \in \mathbb{F}_l^\times$, pick the lift $a \in \mathbb{Z}_l^\times$ of $\alpha \in \mathbb{F}_l^\times$ under mod_l with $a \in \mathbb{Z}, 1 \le a \le l-1$. Consider $f(x) = x^{l-1} - 1 \in \mathbb{Z}_l[x]$. Then we have $f(a) \equiv 0 \pmod{l}$ and $f'(a) = (l-1)a^{l-2} \not\equiv 0 \pmod{l}$. By Hensel's lemma, there exists a unique $r \in \mathbb{Z}_l^\times$ such that $f(r) = 0$ and $a \equiv r \pmod{l}$, i.e., $\mathrm{mod}_l(r) = \mathrm{mod}_l(a) = \alpha$. Thus, we define a section $s : \mathbb{F}_l^\times \to \mathbb{Z}_l^\times$ which sends α to r in the above process. We have $\mathrm{mod}_l \circ s = \mathrm{id}_{\mathbb{F}_l^\times}$. So the above short exact sequence splits. $\square$

Remark 1.6. For $l = 2$, the split short exact sequence becomes

$$0 \longrightarrow \mathbb{Z}_2 \xrightarrow{\iota} \mathbb{Z}_2^\times \xrightarrow{\mathrm{mod}_4} (\mathbb{Z}/4\mathbb{Z})^\times \longrightarrow 0$$

where $\iota : \mathbb{Z}_2 \to \mathbb{Z}_2^\times$ is given by the following compositions:

$$\mathbb{Z}_2 \xrightarrow[\simeq]{\times 4} 4\mathbb{Z}_2 \xrightarrow[\simeq]{\exp} 1 + 4\mathbb{Z}_2 \xrightarrow{\text{inclusion}} \mathbb{Z}_2^\times$$

Lemma 1.7. *We have an isomorphism*

$$\varprojlim_n \mathbb{Z}_l^\times/(\mathbb{Z}_l^\times)^{p^n} \xrightarrow{\simeq} \varprojlim_n \mathbb{Z}_l/p^n\mathbb{Z}_l. \tag{6}$$

which is induced by a section $s : \mathbb{Z}_l^\times \to \mathbb{Z}_l$ of $\iota : \mathbb{Z}_l \to \mathbb{Z}_l^\times$ with $s \circ \iota = \mathrm{id}_{\mathbb{Z}_l}$.

Remark 1.8. Such section $s : \mathbb{Z}_l^\times \to \mathbb{Z}_l$ is derived by picking a section $\mathbb{Z}_l^\times \to 1 + l\mathbb{Z}_l$ of the inclusion $1 + l\mathbb{Z}_l \to \mathbb{Z}_l^\times$ and forming the compositions:

$$\mathbb{Z}_l^\times \longrightarrow 1 + l\mathbb{Z}_l \xrightarrow[\simeq]{\log} l\mathbb{Z}_l \xrightarrow[\simeq]{\div l} \mathbb{Z}_l$$

So roughly speaking, such section $s : \mathbb{Z}_l^\times \to \mathbb{Z}_l$ is the "logarithm map".

Proof of lemma. Let's first assume that $l \in \mathbb{Z}$ is an odd prime. Consider the commutative diagram below with exact rows:

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Z}_l \arrow[r, "\iota"] \arrow[d, "\times p^n"] & \mathbb{Z}_l^\times \arrow[r, "\mathrm{mod}_l"] \arrow[d, "\times p^n"] & \mathbb{F}_l^\times \arrow[r] \arrow[d, "\times p^n"] & 0 \\
0 \arrow[r] & \mathbb{Z}_l \arrow[r, "\iota"] & \mathbb{Z}_l^\times \arrow[r, "\mathrm{mod}_l"] & \mathbb{F}_l^\times \arrow[r] & 0
\end{tikzcd}$$

By snake lemma, we have the following short exact sequence

$$0 \longrightarrow \mathbb{Z}_l/p^n\mathbb{Z}_l \xrightarrow{\iota} \mathbb{Z}_l^\times/(\mathbb{Z}_l^\times)^{p^n} \xrightarrow{\mathrm{mod}_l} \mathbb{F}_l^\times/(\mathbb{F}_l^\times)^{p^n} \longrightarrow 0$$

By taking the limit $n \to \infty$,

$$0 \longrightarrow \varprojlim_n \mathbb{Z}_l/p^n\mathbb{Z}_l \xrightarrow{\iota} \varprojlim_n \mathbb{Z}_l^\times/(\mathbb{Z}_l^\times)^{p^n} \xrightarrow{\mathrm{mod}_l} \varprojlim_n \mathbb{F}_l^\times/(\mathbb{F}_l^\times)^{p^n} \longrightarrow 0$$

But note that $\varprojlim_n \mathbb{F}_l^\times/(\mathbb{F}_l^\times)^{p^n} = 0$. So we have our desired isomorphism.

For $l = 2$, the proof is essentially the same except $\mathbb{F}_l^\times$ should be replaced by $(\mathbb{Z}/4\mathbb{Z})^\times$. But we still have $\varprojlim_n (\mathbb{Z}/4\mathbb{Z})^\times/((\mathbb{Z}/4\mathbb{Z})^\times)^{p^n} = 0$. So our result does not change. □

Proposition 1.9.

$$H^1(G_l, \mathbb{Q}_p(1)) \simeq \begin{cases} 0 \oplus \mathbb{Q}_p & l \neq p \\ \mathbb{Q}_p \oplus \mathbb{Q}_p & l = p \end{cases}$$

where

- *the map to the first component comes from the logarithm;*
- *the map to the second component comes from the l-valuation.*

Proof. By Corollary 1.2, Lemma 1.4 and Lemma 1.7, we have

$$H^1(G_l, \mathbb{Q}_p(1)) \simeq \left(\varprojlim_n \mathbb{Q}_l^\times/(\mathbb{Q}_l^\times)^{p^n}\right) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \simeq \left(\left(\varprojlim_n \mathbb{Z}_l/p^n\mathbb{Z}_l\right) \oplus \mathbb{Z}_p\right) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

where the map to the first component ($\varprojlim_n \mathbb{Z}_l/p^n\mathbb{Z}_l$) is induced by the logarithm map (see Remark 1.8) and the map to the second component ($\mathbb{Z}_p$) is induced by the l-valuation.

Note that

$$\varprojlim_n \mathbb{Z}_l/p^n\mathbb{Z}_l \simeq \begin{cases} 0 & l \neq p \\ \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p & l = p \end{cases}$$

So

$$H^1(G_l, \mathbb{Q}_p(1)) \simeq \begin{cases} (0 \oplus \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \simeq 0 \oplus \mathbb{Q}_p & l \neq p \\ (\mathbb{Z}_p \oplus \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \simeq \mathbb{Q}_p \oplus \mathbb{Q}_p & l \neq p \end{cases}$$

□

Lemma 1.10. *We have an isomorphism coming from the prime factorization*

$$\mathbb{Q}^\times \xrightarrow{\simeq} \mathbb{F}_2 \oplus \bigoplus_{q \text{ prime}} \mathbb{Z}$$

Proof. Any nonzero rational number can be written as $\pm 2^a 3^b 5^c \cdots$ uniquely. □

Lemma 1.11. *We have an isomorphism coming from the prime factorization*

$$\varprojlim_n \mathbb{Q}^\times/(\mathbb{Q}^\times)^{p^n} \xrightarrow{\simeq} \bigoplus_{q \text{ prime}} \mathbb{Z}_p \tag{7}$$

Proof. By Lemma 1.10 and the fact of $\varprojlim_n \mathbb{F}_2/p^n\mathbb{F}_2 = 0$, we have

$$\begin{aligned}\varprojlim_n \mathbb{Q}^\times/(\mathbb{Q}^\times)^{p^n} &\xrightarrow{\simeq} \varprojlim_n \left(\mathbb{F}_2/p^n\mathbb{F}_2 \oplus \bigoplus_{q \text{ prime}} \mathbb{Z}/p^n\mathbb{Z}\right)\\ &\simeq \bigoplus_{q \text{ prime}} \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \bigoplus_{q \text{ prime}} \mathbb{Z}_p\end{aligned}$$

□

Proposition 1.12. *$H^1(G_\mathbb{Q}, \mathbb{Q}_p(1))$ is a countably infinite dimensional $\mathbb{Q}_p$-vector space*

$$H^1(G_\mathbb{Q}, \mathbb{Q}_p(1)) \simeq \bigoplus_{q \text{ prime}} \mathbb{Q}_p$$

where the isomorphism comes from the prime factorization.

Proof. By Corollary 1.2 and Lemma 1.11, we have

$$H^1(G_\mathbb{Q}, \mathbb{Q}_p(1)) \simeq \left(\varprojlim_n \mathbb{Q}^\times/(\mathbb{Q}^\times)^{p^n}\right) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \simeq \left(\bigoplus_{q \text{ prime}} \mathbb{Z}_p\right) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \simeq \bigoplus_{q \text{ prime}} \mathbb{Q}_p.$$

□

Definition 1.13. The Selmer scheme $\mathrm{Sel}_\infty(\mathbb{G}_m)$ is defined as the scheme representing the subfunctor of $H^1(G_\mathbb{Q}, \mathbb{Q}_p(1))$ consisting of classes α such that for all primes l, the localization $\mathrm{loc}_l(\alpha)$ is contained in $j_l(\mathbb{G}_m(\mathbb{Z}_l))^{\mathrm{Zar}}$, the Zariski closure of $j_l(\mathbb{G}_m(\mathbb{Z}_l))$.

Definition 1.14. $H^1_f(G_p, \mathbb{Q}_p(1)) := j_p(\mathbb{G}_m(\mathbb{Z}_p))^{\mathrm{Zar}}$.

Lemma 1.15. *The localization map $\mathrm{loc}_l : H^1(G_\mathbb{Q}, \mathbb{Q}_p(1)) \to H^1(G_l, \mathbb{Q}_p(1))$ in the diagram diagram (1) can be identified with*

$$\bigoplus_{q \text{ prime}} \mathbb{Q}_p \to (0 \text{ or } \mathbb{Q}_p) \oplus \mathbb{Q}_p, \quad (\alpha_q)_{q \text{ prime}} \mapsto (0, \alpha_l).$$

Lemma 1.16. *The local Kummer map $j_l : \mathbb{G}_m(\mathbb{Z}_l) \to H^1(G_l, \mathbb{Q}_p(1))$ in the diagram (1) is identified with $\mathbb{Z}_l^\times \to (0 \text{ or } \mathbb{Q}_p) \oplus \mathbb{Q}_p$. Write $j_{l,1} : \mathbb{Z}_l^\times \to (0 \text{ or } \mathbb{Q}_p)$ and $j_{l,2} : \mathbb{Z}_l^\times \to \mathbb{Q}_p$ as the map j_l to the first and the second component respectively. Then*

- *$j_{l,1}$ is the zero map when $l \neq p$ and $j_{l,1}$ is the logarithm map when $l = p$.*
- *$j_{l,2}$ is always the zero map.*

Proof. By Proposition 1.1, j_l is the natural map. Then by Proposition 1.9, $j_{l,1}$ is the logarithm map and $j_{l,2}$ is the l-valuation map.

- When $l \neq p$, the target of $j_{l,1}$ is zero, so $j_{l,1}$ is the zero map.
- Now for any prime l, the l-valuation of elements in $\mathbb{Z}_l^\times$ are all zero. So the map $j_{l,2}$ is always the zero map.

□

Corollary 1.17. • *When $l \neq p$, $j_l(\mathbb{G}_m(\mathbb{Z}_l)) = 0$ and hence $j_l(\mathbb{G}_m(\mathbb{Z}_l))^{\mathrm{Zar}} = 0$.*

- $H^1_f(G_p, \mathbb{Q}_p(1)) := j_p(\mathbb{G}_m(\mathbb{Z}_p))^{\mathrm{Zar}} = \mathbb{Q}_p \oplus 0$ *in* $\mathbb{Q}_p \oplus \mathbb{Q}_p$.

Proof. • When $l \neq p$, j_l is the zero map by Lemma 1.16 and the result follows.

- Note that $j_p(\mathbb{G}_m(\mathbb{Z}_p)) = \log(\mathbb{Z}_p) \oplus 0$ where $\log(\mathbb{Z}_p)$ has infinitely many points in $\mathbb{Q}_p$. Since the Zariski topology for $\mathbb{Q}_p$ is the cofinite topology, we have that the Zariski closure of $\log(\mathbb{Z}_p)$ is the whole $\mathbb{Q}_p$.

□

Proposition 1.18. *The Selmer scheme* $\mathrm{Sel}_\infty(\mathbb{G}_m) = 0$.

Proof. Let $\alpha = (\alpha_q)_{q \text{ prime}} \in \mathrm{Sel}_\infty(\mathbb{G}_m)$. Then for any prime l, $\mathrm{loc}_l(\alpha) = (0, \alpha_l) \in j_l(\mathbb{G}_m(\mathbb{Z}_l))^{\mathrm{Zar}}$. By Corollary 1.17, the second component of $j_l(\mathbb{G}_m(\mathbb{Z}_l))^{\mathrm{Zar}}$ is always zero. So $\alpha_l = 0$. Since it holds for any prime l, we have $\alpha = 0$. This implies $\mathrm{Sel}_\infty(\mathbb{G}_m) = 0$. □

Proposition 1.19. *The Chabauty-Kim diagram*

$$\begin{tikzcd} \mathbb{G}_m(\mathbb{Z}) \arrow[r] \arrow[d, "j"] & \mathbb{G}_m(\mathbb{Z}_p) \arrow[d, "j_p"] \\ \mathrm{Sel}_\infty(\mathbb{G}_m) \arrow[r, "\mathrm{loc}_p"] & H^1_f(G_p, \mathbb{Q}_p(1)) \end{tikzcd}$$

can be identified with

$$\begin{tikzcd} \mathbb{G}_m(\mathbb{Z}) \arrow[r] \arrow[d] & \mathbb{G}_m(\mathbb{Z}_p) \arrow[d, "\log"] \\ 0 \arrow[r, "\mathrm{loc}_p"] & \mathbb{Q}_p \end{tikzcd} \tag{8}$$

Proof. $\mathrm{Sel}_\infty(\mathbb{G}_m) = 0$ follows from Proposition 1.18. $H^1_f(G_p, \mathbb{Q}_p(1)) \simeq \mathbb{Q}_p$ follows from Corollary 1.17. The fact that the map j_p is log follows from Lemma 1.16. □

Proposition 1.20. $\mathbb{G}_m(\mathbb{Z}_p)_\infty \simeq \mathbb{F}_p^\times$ *for odd prime* $p \in \mathbb{Z}$.

Proof. Let $p \in \mathbb{Z}$ be an odd prime. Looking at the diagram (8),

$$\begin{aligned} \mathbb{G}_m(\mathbb{Z}_p)_\infty &:= \{x \in \mathbb{G}_m(\mathbb{Z}_p) \mid j_p(x) \in \mathrm{im}(\mathrm{loc}_p)\} \\ &= \left\{x \in \mathbb{Z}_p^\times \mid \log(x) = 0\right\} \\ &= \left\{x \in \mathbb{Z}_p^\times \mid x \in \mu_{p^n}(\mathbb{Q}_p) \text{ for some } n\right\} \\ &= \left\{p^n\text{-torsion points of } \mathbb{Z}_p^\times \text{ for some } n\right\} \end{aligned}$$

Recall that we have the split short exact sequence by Lemma 1.5:

$$0 \longrightarrow \mathbb{Z}_p \xrightarrow{\iota} \mathbb{Z}_p^\times \xrightarrow{\mathrm{mod}_p} \mathbb{F}_p^\times \longrightarrow 0$$

So $\mathbb{Z}_p^\times \simeq \mathbb{Z}_p \times \mathbb{F}_p^\times$. Then it's easy to see the result. □

Proposition 1.21. $\mathbb{G}_m(\mathbb{Z}) = \{1, -1\}$.

Proof. By choosing $p = 3$, we find $\mathbb{G}_m(\mathbb{Z}) \subseteq \mathbb{G}_m(\mathbb{Z}_3)_\infty = \{1, -1\}$. So the result follows. □