Riduzioni di punti di ordine infinito su gruppi algebrici commutativi

Ormai oltre cinquant'anni fa, Hasse ha dimostrato che l'insieme dei numeri primi p che dividono almeno un intero della forma $2^n + 1$ ammette una densità naturale pari a $\frac{17}{24}$. Questo risultato si può interpretare come un enunciato relativo alle proprietà del punto razionale $\alpha = 2 \in \mathbb{G}_m(\mathbb{Q})$, e questo punto di vista conduce a una domanda molto più generale: dati un gruppo algebrico commutativo A su un campo di numeri K e un punto razionale $\alpha \in A(K)$, si vorrebbe comprendere per "quanti" primi $\mathfrak{p}$ di K la riduzione modulo $\mathfrak{p}$ di α abbia ordine divisibile per un certo primo fissato ℓ.

Cercherò di descrivere un quadro generale nel quale studiare questo problema e di dare una risposta alla domanda precedente nel caso A sia il prodotto di una varietà abeliana e di un toro. La forma di questa risposta è sorprendentemente uniforme rispetto alla scelta del gruppo algebrico A e del punto razionale α, e questo conduce ad enunciati particolarmente precisi nel caso in cui A sia una curva ellittica.

Si tratta di un lavoro in comune con Antonella Perucca (Université du Luxembourg).