PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 3, *Number* 1, *March* 2018, *pages* 1-6

Peter Stevenhagen

Primitivity properties of points on elliptic curves

Written by Mattia Cafferata

1 Artin Conjecture

Let $a \in \mathbb{Q}^*$ be a primitive element, i.e. such that $a \neq b^k$ for every integer $k > 1$ and for every $b \in \mathbb{Q}^*$.
Let consider P_a the set the set of prime numbers for which a is a primitive root, $P_a := \{p \text{ prime } : \mathbb{F}_p^* = \langle a \bmod p \rangle\}$, and define $\delta(a)$ as his natural density. One can try to answer to these questions: is the set P_a infinite? When is $\delta(a)$ positive?
Artin, in 1927, made the following conjecture:

Conjecture 1 ***(Artin, 1927)***
Let a be a square-free primitive element of $\mathbb{Q}^*$, *then* P_a *is infinite and*

$$\delta(a) = \prod_{q \text{ prime}} \left(1 - \frac{1}{q(q-1)}\right). \tag{1}$$

Artin formulated the conjecture starting from this heuristic argument: he observed that, for almost all p, a prime q divides $\left[\mathbb{F}_p^* : \langle a \bmod p \rangle\right]$ if and only if $p \equiv 1 \pmod q$ and $a \equiv b^q \pmod p$ for some b. The last two conditions, together, are equivalent to ask that the prime p splits completely in the field $L_q := \mathbb{Q}(\zeta_q, a^{1/q})$ and so we have that

$$\mathbb{F}_p^* = \langle a \bmod p \rangle \iff \text{for no prime } q, p \text{ splits completely in } L_q.$$

Knowing that the density of primes which split completely in L_q is $\left[L_q : \mathbb{Q}\right]^{-1} = (q(q-1))^{-1}$ one can expect (1) to be valid.
It's interesting to observe that the right-hand side of (1) does not depend from a and so it's reasonable to think that the formula need a correction to hold for any primitive element in $\mathbb{Q}$. The fact is that the events "p does not split completely in L_q" are not not necessarily independent as p and q range through all primes.
A more general form of the conjecture was given by Lehmer and Artin himself in 1953 and later in 1967 Hooley proved the following theorem:

Theorem 1 *Let $a \in \mathbb{Q}^*$ a primitive element; then, under GRH, we have*

$$\delta(a) = \sum_{k=1}^{\infty} \frac{\mu(k)}{[L_k : \mathbb{Q}]} \tag{2}$$

where μ is the Möbius function.

The the Möbius function solves the entanglement problem, i.e. the fact that the field L_q are not linearly disjoint over $\mathbb{Q}$ (e.g. $L_2 \subset L_3$). This is essentially the reason why the densities of prime numbers which do not split completely in L_q can't be considered independent from each other.

2 Lang-Trotter Conjecture

Artin's problem is pertinent to many generalizations and variations. A natural generalization appears in the context of elliptic curves and was formulated by S. Lang and H. Trotter in 1976.
Let $\mathbb{E}(\mathbb{Q})$ be an elliptic curve defined over $\mathbb{Q}$ and let $A \in \mathbb{E}(\mathbb{Q})$ be a

primitive point, i.e. such that $A \neq kB$ for every integer $k > 1$ and for every $B \in \mathbb{E}(\mathbb{Q})$. For a prime p of good reduction for $\mathbb{E}(\mathbb{Q})$, let $\mathbb{E}(\mathbb{F}_p)$ be the reduction of $\mathbb{E}(\mathbb{Q})$ modulo p.

Conjecture 2 ***(Lang, Trotter, 1976)***
For every elliptic curve $\mathbb{E}(\mathbb{Q})$ and every primitive $A \in \mathbb{E}(\mathbb{Q})$ the set $\{p \text{ prime } : \mathbb{E}(\mathbb{F}_p) = \langle A \mod p\rangle\}$ has natural density $\delta_E(A) \geq 0$.

An important remark to do is that, in contrast with the classical situation, when we require that $\mathbb{E}(\mathbb{F}_p) = \langle A \mod p\rangle$ we are making the implicit assumption that $\mathbb{E}(\mathbb{F}_p)$ is cyclic.
In general, $\mathbb{E}(\mathbb{F}_p)$ is the product of two cyclic groups, therefore it is natural to consider, at first, the question of finding the density of primes p for which $\mathbb{E}(\mathbb{F}_p)$ is cyclic. Again we can use an heuristic approach: denoting with $\mathbb{E}[m](\mathbb{F}_p)$ the set of m-torsion points and with Z_q the q-division field it can be showed that

$$\begin{aligned} \mathbb{E}(\mathbb{F}_p) \text{ is cyclic } &\iff \text{ for no prime } q, \quad \mathbb{E}[q](\mathbb{F}_p) \neq q^2 \\ &\iff p \text{ does not split completely in any field } Z_q. \end{aligned}$$

This leads to a conjecture similar to the one in (2), which was conditionally proofed by Serre

Theorem 2 ***(Serre, 1993)***
Let $\mathbb{E}(\mathbb{Q})$ be an elliptic curve as above and δ_E be the density of the set $\{p \text{ prime} : \mathbb{E}(\mathbb{F}_p) \text{ is cyclic}\}$. Then, under GRH,

$$\delta_E = \sum_{k=1}^{\infty} \frac{\mu(k)}{[Z_k : \mathbb{Q}]} \tag{3}$$

An unconditional proof was given by M.R Murty in 1988, but only for elliptic curves with complex multiplication.

3 Primitivity on elliptic curves

Very little is known about the density $\delta_E(A)$ and the results obtained so far require at least to assume *GRH* and additional hypothesis on the elliptic curve.
To better understand the difference between the classical and the elliptic curve case we can analyse the problem from another point of view. We begin with the classical case.
Consider V_q the 2-dimensional vector space over $\mathbb{F}_q$ defined by

$$V_q = \langle \zeta_q, a^{1/q} \rangle / \langle a \rangle.$$

We can define an action of $G_q = \mathrm{Gal}(L_q/\mathbb{Q})$ over V_q identifying the elements of G_q with the matrices

$$\left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in \mathbb{F}_q^*, b \in \mathbb{F}_q \right\} \subset \mathrm{Aut}(V_q).$$

So, if we denote with $\phi_p \in G$ the Frobenius map we get that, for almost all p

$$\begin{aligned} q \text{ divides } \left[\mathbb{F}_p^* : \langle a \bmod p \rangle\right] &\iff \phi_p \text{ acts trivially on } \mathbb{V}_q \\ &\iff \mathbb{V}_q^{\langle \phi_p \rangle} = \mathbb{V}_q \end{aligned}$$

In the elliptic case, instead, we consider the 3-dimensional space V_p defined as

$$V_q = \langle \mathbb{E}[q], q^{-1}A \rangle / \langle A \rangle.$$

Analogously to the previous case we define an action $G_q = \mathrm{Gal}(Z_q/\mathbb{Q})$ over V_q identifying the elements of G_q with the matrices

$$\left\{ \left(\begin{array}{cc|c} \multicolumn{2}{c|}{\multirow{2}{*}{B}} & a \\ & & b \\ \hline 0 & 0 & 1 \end{array} \right) : a, b \in \mathbb{F}_q, B \in GL_2(\mathbb{F}_q) \right\} \subset \mathrm{Aut}(V_q).$$

In this case it can be proved that for almost all p

$$q \text{ divides } \left[\mathbb{E}(\mathbb{F}_p) : \langle A \bmod p \rangle\right] \iff \dim(\mathbb{V}_q^{\langle \phi_p \rangle}) \geq 2.$$

We note that, in the second situation, the condition $\mathbb{V}_q^{\langle \phi_p \rangle} = \mathbb{V}_q$ is sufficient, but non more necessary to expect non primitivity.
For a generic point of an elliptic curve we can say what follows:

Theorem 3 *Let $\mathbb{E}(\mathbb{Q})$ be an elliptic curve and A any point of $\mathbb{E}(\mathbb{Q})$; then q divides $\left[\mathbb{E}(\mathbb{F}_p) = \langle A \mod p\rangle\}\right]$ for almost all primes p if and only if one of the following holds:*

1. $\mathbb{E}[q](\mathbb{Q}) = q^2$;

2. *q divides $|\mathbb{E}(\mathbb{Q})^{tor}|$ and $A = qB \in \mathbb{E}(\mathbb{Q})$;*

3. *exists $\varphi_{|\mathbb{Q}} : \mathbb{E}(\mathbb{Q}) \longrightarrow \mathbb{E}'(\mathbb{Q})$ of degree q such that condition (2) holds for $\mathbb{E}'(\mathbb{Q})$ and $\varphi(A)$.*

Finally we remember a result by G. Meleleo who showed, in his Ph.D. thesis that is possible to have a never-primitivity situation;

Theorem 4 ***(Meleleo,2015)***
There exists elliptic curves $\mathbb{E}(\mathbb{Q})$ with $\delta_E > 0$ and primitive points $A \in \mathbb{E}(\mathbb{Q})$ such that $\mathbb{E}(\mathbb{F}_p) \neq \langle A \mod p\rangle$ for almost all primes p.

References

[1] C. Hooley, *On Artin's conjecture*, J. Reine Angew. Math.,1967

[2] S. Lang, H. Trotter, *Primitive points on elliptic curves*, Bull. Amer. Math. Soc., 1977.

[3] G. Meleleo, *Questions related to primitive points on elliptic curves and statistics for biquadratic curves over finite fields*, Ph.D. Thesis, 2015.

[4] P. Moree, *Artin's Primitive Root Conjecture - A Survey*, 2012.

[5] M. R. Murty, *Artin's conjecture for primitive roots*, Math. Intelligencer 10, 1988.

Mattia Cafferata
Dep. of Mathematical, Phisical and Computer Sciences
university of Parma
parco Area delle scienze 53/a
43124 Parma, italy.
email: mattia.cafferata@unife.it