Properties of Reductions of Groups of Rational Numbers

On Artin–Gauß Conjeture

Conference

2^{nd} *International Conference of Mathematics and its Applications- ICMA*

University of Basrah College of Science, October 23-24, 2013

Francesco Pappalardi
Dipartimento di Matematica e Fisica
Università Roma Tre

History of Artin Conjecture
Gauß question on lengths of periods

What are the primes p s.t. $1/p$ has length $p-1$?

For example:

$\frac{1}{7} = 0.\overline{142857}$,

$\frac{1}{17} = 0,\overline{0588235294117647}$,

$\frac{1}{19} = 0.\overline{052631578947368421}$,

$\vdots$

$\frac{1}{47} = 0.\overline{0212765957446808510638297872340425531914893617}$

First few primes with this property:

$7, 17, 19, 23, 29, 47, 59, 61, 97, 109, 113, 131, 149, 167, 179, 181, 193, \ldots$

$k_p :=$ length of the period of $1/p$

$k_3 = 1,\ k_{11} = 2,\ k_{13} = 6,$ k_2 and k_5 are not defined

Gauß question on lengths of periods

The period–length of the fraction $1/p$ is the least k s.t.

$$\frac{1}{p} = 0.\overline{a_1 \cdots a_k} = 0.a_1 \cdots a_k \; a_1 \cdots a_k \; \ldots$$

In other words

$$\begin{aligned} \frac{1}{p} &= \Big(\frac{a_1}{10} + \cdots + \frac{a_k}{10^{k+1}}\Big) \times \left(1 + \frac{1}{10^k} + \frac{1}{10^{2k}} + \cdots\right) \\ &= \frac{M}{10^k - 1} \end{aligned}$$

Hence

$$M \times p = 10^k - 1$$

So k_p is the least integer such that $10^k - 1$ is divisible by p!

Algebraic properties of period lengths

- The period length k_p of $1/p$ is the least integer such that $10^k - 1$ is divisible by p
- Fermat Little Theorem says that $10^{p-1} - 1$ is divisible by p
- So $k_p \leq p - 1$
- Indeed it is not hard to show k_p is a divisor of $p - 1$
- Sometimes the period is small:

$$1/111111111111111111 = 0,\overline{000000000000000009}$$

- most of the times $k_p > \sqrt{p}$ not obvious!
- Gauß in particular asked what are the frequencies of periods

Some statistics on period lengths:

Let k_p be the period length of $1/p$. The following table contains

$$\delta_m = \frac{\{p < 2^{31} : k_p = \frac{p-1}{m}\}}{\#\{p \leq 2^{31}\}}$$

for $m = 1, \ldots, 40$.

m	1	2	3	4	5	6	7
δ_m	0.37393	0.28047	0.06649	0.07133	0.01890	0.04986	0.00893
m	8	9	10	11	12	13	14
δ_m	0.01660	0.00739	0.01416	0.00340	0.01268	0.00240	0.00669
m	15	16	17	18	18	20	21
δ_m	0.00335	0.00415	0.00136	0.00553	0.00109	0.00235	0.00158
m	22	23	24	25	26	27	28
δ_m	0.00255	0.00073	0.00294	0.00075	0.00180	0.00081	0.00171
m	29	30	31	32	33	34	35
δ_m	0.00046	0.00251	0.00039	0.00103	0.00060	0.00103	0.00044

Note

$2,94\%$ of primes $p \leq 2^{31}$ have period $k_p = \frac{p-1}{m}$ with $m > 35$

More algebraic properties of period lengths

- Period are also defined with respect to any base $a \in \mathbb{N}$
- The period length of $1/p$ in base a is the least $k_p(a)$ such that $a^k - 1$ is divisile by p (a divisor of $p-1$)
- It is not difficult to see that:
  the period length $k_p(a) = p - 1$ if and only if the set

$$\{a^j : j = 1, \dots, p-1\}$$

  *contains $p-1$ **distinct elements modulo** p*
- *in other words the period length $k_p(a) = p - 1$ if and only if*

  p is not a divisor of $a^s - a^r \quad \forall r, s : 1 \leq r < s \leq p-1$
- we express that condition writing

$$\langle a \bmod p \rangle = \mathbb{F}_p^* \quad \text{or also} \quad \#\langle a \bmod p \rangle = p - 1$$

- If the period length in base a of $1/p$ is $p-1$ (i.e. $k_p(a) = p - 1$), we say that *a is a primitive root modulo p*

Algebraic properties of period lengths
from period lengths to primitive roots

- So *a is a primitive root modulo p* if and only if $\langle a \bmod p\rangle = \mathbb{F}_p^*$
  (i.e. if there are $p-1$ distinct powers of a modulo p)
- It is not hard to check that if p is a divisor of a, then $1/p$ is a finite expansion in base a.
- for example $1/2 = 0.5 \quad 1/5 = 0.2$ in decimal base and $1/10 = 0.1$ in binary base
- the condition *a is a primitive root modulo p* makes sense also when a is a rational number and p does not divide numerator and denominator of a (i.e. $v_p(a) = 0$)
- *a is a primitive root modulo p* iff

$$\forall \textbf{ primes } \ell \textbf{ that divide } p-1, p \textbf{ does not divide } a^{(p-1)/\ell}-1$$

- This is the base for Artin intuition on the

Primitive Roots Conjecture

Artin Conjecture (1927)

Note

Heuristically, the probability that a prime ℓ is such that both

1. ℓ divides $p-1$
2. p divides $a^{(p-1)/\ell}-1$

are satisfied is $1/\ell(\ell-1)$.
Hence the probability that $a^{(p-1)/\ell}-1$ is not divisible by p for all primes ℓ dividing $p-1$ is

$$A=\prod_{\ell\leq 2}\left(1-\frac{1}{\ell(\ell-1)}\right)=0,373955\ldots$$

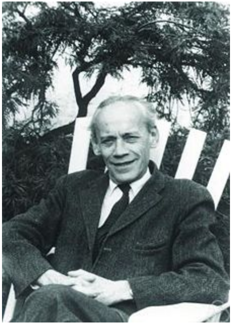
Definition (A is called the ***Artin constant***)

Conjecture

$$lim_{x\to\infty}\frac{\#\{p\leq x:\ p\neq 2,5,\ \langle 10 \bmod p\rangle=\mathbb{F}_p^*\}}{\#\{p\leq x\}}=A$$

What if instead of 10 we consider $a\in\mathbb{Z}\setminus\{-1,0,1\}$?

Artin Conjecture (1927)



Emil Artin (March 3, 1898 - December 20, 1962)

Conjecture (Artin Conjecture – first version)

If $a \in \mathbb{Q} \setminus \left(\{-1, 0, 1\} \cup \{b^2 : b \in \mathbb{Q}\}\right)$, then

$$\#\{p \leq x : \; v_p(a) = 0, \; \langle a \bmod p \rangle = \mathbb{F}_p^*\} \sim A\pi(x)$$

here $\pi(x) = \#\{p \leq x\}$ and $A = \prod_{\ell \leq 2} 1 - \frac{1}{\ell(\ell-1)} = 0,37395\ldots$

Some numerical tests for Artin Conjecture

Let

$$S_a = \{p \leq 2^{29} : \langle a \bmod p \rangle = \mathbb{F}_p^*\}, \quad d_a = \#S_a/\pi(2^{29})$$

Note that $\pi(2^{29}) = 28192750$ and $A = 0,373955\ldots$.

a	S_a	d_a	a	S_a	d_a
-15	10432805	0.37005	2	10543421	0.37397
-14	10543340	0.37397	3	10543631	0.37398
-13	10542796	0.37395	5	11098098	0.39365
-12	12653339	0.44881	6	10543607	0.37398
-11	10639090	0.37736	7	10544579	0.37401
-10	10543135	0.37396	8	6325893	0.22438
-9	10542743	0.37395	10	10542876	0.37395
-8	6325704	0.22437	11	10542933	0.37395
-7	10799148	0.38304	12	10545029	0.37403
-6	10543575	0.37398	13	10611720	0.37639
-5	10542080	0.37392	14	10542946	0.37395
-4	10543032	0.37396	15	10544134	0.37400
-3	12651353	0.44874	17	10582932	0.37537
-2	10542194	0.37393	18	10545385	0.37404

Not always so totally convincing evidence!

Not convincing for $a \in \{-15, -12, -11, -8, -7, -3, 5, 8, 13, 17\}$

Artin Conjecture
Lehmer's correction

Derrick Henry Lehmer (Feb 1905 - May 1991)

Remark (Lehmer's Remark)

The probabilities that, given two primes ℓ_1 and ℓ_2, a prime p is such that

1. ℓ_i divides $p - 1$
2. p divides $a^{(p-1)/\ell_i} - 1$

for $i = 1, 2$ are not always independent!!

So there is the need for a correction factor
(the *entanglement factor*)

Artin Conjecture
after Lehmer's correction

Conjecture (Artin Conjecture – final form)

Let $a \in \mathbb{Q}^* \setminus \{1, -1\}$, then $p - 1 = \#\langle a \mod p\rangle$ for a proportion of primes δ_a where

$$\delta_a = r_a \times t_a,$$

where if $h = \max\{j : a = b^j, b \in \mathbb{Q}\}$, $\partial(a) = \mathrm{disc}(\mathbb{Q}(\sqrt{a}))$,

$$t_a = \prod_{\ell \geq 2} \left(1 - \frac{\gcd(h, \ell)}{\ell(\ell - 1)}\right)$$

and $r_a = 1$ unless if $\partial(a)$ is odd in which case:

$$r_a = 1 - \prod_{\ell | \partial(a)} \frac{-1}{\ell(\ell-1)/\gcd(\ell,h)-1}$$

Note that

- t_a is a rational multiple of the Artin Constant A
- $\delta_a = 0$ iff a is a perfect square
- $\partial(a)$ is easy but technical to define

Artin Conjecture
Effect of the Lehmer entanglement

We were not convinced for
$a \in \{-15, -12, -11, -8, -7, -3, 5, 8, 13, 17\}$

a	δ_a	d_a
-15	0.37001	0.37005
-12	0.44875	0.44881
-11	0.37709	0.37736
-8	0.22437	0.22437
-7	0.38308	0.38304
-3	0.44875	0.44874
5	0.39363	0.39365
8	0.22437	0.22438
13	0.37636	0.37639
17	0.37533	0.37537

For all other values of a in the previous table, $\delta_a = A$

Artin Conjecture
what it is known on Artin Conjecture

Theorem (C. Hooley (1965))

If the Generalized Riemann Hypothesis (GRH) holds for the fields $\mathbb{Q}(a^{1/\ell})$ (ℓ prime) then the modified Artin Conjecture holds for a

What is the GRH?

- It is a complicated conjecture in Number Theory, so important that it often assumed as an Hypothesis
- Stating it is behind the scope of this seminar
- It has many different formulations:
- *all the non trivial zeroes of the Dedekind zeta functions sit on the line $\Re s = 1/2$*
- *primes can be counted very precisely*

Artin Conjecture
The quasi resolution



Theorem (R. Gupta, R. Murty & R. Heath–Brown (1984/86))

$\exists g \in \{2, 3, 5\}$ *s.t.*

$$\#\{p \leq x : \ p > 5, \langle g \bmod p \rangle = \mathbb{F}_p^*\} \gg \frac{\pi(x)}{\log x}$$

The higher rank Artin Quasi–primitive root Conjecture
joint work with Andrea Susa

Notations:

- $\Gamma \subset \mathbb{Q}^*$ finitely generated subgroup
- r rank of Γ
- $m \in \mathbb{N}^+$
- $\sigma_\Gamma = \prod_{p: v_p(x)=0, \exists x \in \Gamma} p$
- $\forall p \nmid \sigma_\Gamma$

  $$\Gamma_p = \{g (\bmod p) : g \in \Gamma\} \subset \mathbb{F}_p^*$$

  is well defined
- $N_\Gamma(x, m) := \#\{p \leq x : p \nmid \sigma_\Gamma, |\Gamma_p| = \frac{p-1}{m}\}$
- Γ_p generalizes the notion of $\langle a \bmod p \rangle$.
- if $\Gamma = \langle a \rangle$ has rank 1 then

$$N_{\langle a \rangle}(x, m) = \#\{p \leq x : \frac{1}{p} \text{ has period of length } \frac{p-1}{m}\}$$

The higher rank Artin Quasi–primitive root Conjecture
joint work with Andrea Susa

Theorem

Let $\Gamma \subset \mathbb{Q}^*$ *has rank* $r \geq 2$*, let* $m \in \mathbb{N}$ *and assume GRH holds for* $\mathbb{Q}(\zeta_k, \Gamma^{1/k})$ *(*$k \in \mathbb{N}$*). Then,* $\forall \epsilon > 0$ *and* $m \leq x^{\frac{r-1}{(r+1)(4r+2)} - \epsilon}$*,*

$$N_\Gamma(x, m) = \left(\rho(\Gamma, m) + O\left(\frac{1}{\varphi(m^{r+1}) \log^r x}\right)\right) \pi(x),$$

where

$$\rho(\Gamma, m) = \sum_{k \geq 1} \frac{\mu(k)}{[\mathbb{Q}(\zeta_{mk}, \Gamma^{1/mk}) : \mathbb{Q}]}.$$

An analogue of the above result holds also in the case when $\Gamma \subset \mathbb{Q}^*$ has infinite rank.

The r–rank Artin Quasi–primitive root Conjecture
joint work with Andrea Susa

Theorem

Let $\Gamma\subset\mathbb{Q}^+=\{q\in\mathbb{Q}; q>0\}$ *with rank* $r\geq 2$ *and* $m\in\mathbb{N}$. *Let* $\Gamma(m):=\Gamma(\mathbb{Q}^*)^m/(\mathbb{Q}^*)^m$,

$$A_{\Gamma,m}=\frac{1}{\varphi(m)|\Gamma(m)|}\times\prod_{\substack{\ell>2\\ \ell\nmid m}}\left(1-\frac{1}{(\ell-1)|\Gamma(\ell)|}\right)\times\prod_{\substack{\ell>2\\ \ell\mid m}}\left(1-\frac{|\Gamma(\ell^{v_\ell(m)})|}{\ell|\Gamma(\ell^{1+v_\ell(m)})|}\right)$$

and

$$B_{\Gamma,k}=\sum_{\substack{\eta\mid\sigma_\Gamma\\ \eta^{2^{v_2(k)-1}}\cdot\mathbb{Q}^{*2^{v_2(k)}}\in\Gamma(2^{v_2(k)})\\ v_2(\partial(\eta))\leq k}}\ \prod_{\substack{\ell\mid\partial(\eta)\\ \ell\nmid k}}\frac{-1}{(\ell-1)|\Gamma(\ell)|-1}.$$

Then

$$\rho(\Gamma,m)=A_{\Gamma,m}\left(B_{\Gamma,m}-\frac{|\Gamma(2^{v_2(m)})|}{(2,m)|\Gamma(2^{1+v_2(m)})|}B_{\Gamma,2m}\right).$$

The Artin Quasi–primitive root Conjecture
vanishing of the density

Theorem

Let $\Gamma \subset \mathbb{Q}^+$ *fin. gen.,* $m \in \mathbb{N}$*. Then*

$$\rho(\Gamma, m) = 0$$

if one of the following holds:

1. $2 \nmid m$ *and for all* $g \in \Gamma, \partial(g) \mid m$*;*
2. $2 \mid m$*,* $3 \nmid m$*,* $\Gamma(3) = \{1\}$ *and* $\exists \eta \mid \sigma_\Gamma$*,*
   - $\eta^{2^{v_2(m/2)}} \cdot \mathbb{Q}^{*2^{v_2(m)}} \in \Gamma(2^{v_2(m)})$
   - $\partial(-3\eta) \mid m$

(if $2 \nmid m$*, (1) is also necessary for* $\rho(\Gamma, m) = 0$*). If* $\Gamma \subset \mathbb{Q}^+$ *and* m *satisfy one of (1) or (2) above, then*

$$\{p : ind_p\Gamma = m\} \quad \text{finite.}$$

Hence, on GRH, if $2 \nmid m$*,*

$$\{p : ind_p\Gamma = m\} \quad \text{finite} \iff \forall g \in \Gamma, \partial(g) \mid m.$$