Words and primitive roots

École d'Eté de Calcul Formele et Théorie de Nombres

Monastir - TUNISIA

Francesco Pappalardi

Agost 27, 2007

Introduction: Gauß Conjecture

$$\frac{1}{p} = 0.\overline{a_1 a_2 \cdots a_k} \qquad p \neq 2, 5$$

Where:

- ✎ $k = k_p$ is the period length
- ✎ $k_p \mid p - 1$
- ✎ (Gauß conjecture) $k_p = p - 1$ for infinitely many primes p
- ✎ $k_p = \text{ord}_p(10) = \min\{N \in \mathbb{N} : \; 10^N \equiv 1 \bmod p\}$
- ✎ $k_p = p - 1$ if and only if $\langle 10 \bmod p \rangle = \mathbb{F}_p^*$
- ✎ if $a \in \mathbb{Q}$ and $\langle a \bmod p \rangle = \mathbb{F}_p^*$, we say a primitive root modulo p
- ✎ Today we have the Artin Conjecture for primitive roots.

Artin Conjecture

Let $a \in \mathbb{Q}^*, a \neq -1,\ a \neq b^2$ with $b \in \mathbb{Q}$.

$$P_a := \{p : \ \langle a \bmod p \rangle = \mathbb{F}_p^*\}$$

Weak Form Conjecture(WF)

$$\# P_a = \infty$$

Strong Form Conjecture(SF) $\exists A_a \in \mathbb{R}^>$ such that

$$\# P_a(x) \sim A_a \frac{x}{\log x}$$

NOTATION: if $A \subset \mathbb{R}$, then we set $A(x) := A \cap [1, x]$

We will outline 3 approaches to Artin Conjecture

Three approaches to Artin Conjecture

- ☞ Schinzel's Hypothesis H (SHH) $\rightsquigarrow$ Complete solution of WF
- ☞ Generalized Riemann Hypothesis (GRH) $\rightsquigarrow$ Complete solution of SF
- ☞ Heath–Brown, Gupta Murty (HGM) $\rightsquigarrow$ Unconditional "almost solution" of WF

Schinzel's Hypothesis H (SHH) approach

Conjecture 1 (Hypthesis H (A. Schinzel – 1957) SHH)
Let $f_1, \dots, f_s \in \mathbb{Z}[X]$

- *irreducible*
- *positive leading coefficients*
- $\gcd(f_1(n) \cdots f_s(n), n \in \mathbb{N}) = 1$

(*i.e.* $\forall l$ *prime* $\exists n \in \mathbb{N}$ *s.t.* $l \nmid f_1(n) \dots f_s(n)$)

Then

$\exists \infty$–*many* $n \in \mathbb{N}$ *s.t.* $f_1(n), \dots, f_s(n)$ *are all prime*

SHH$\Rightarrow$ WF

Let $a = 2$ for simplicity

Set $f_1(x) = 8x + 3,\ f_2(x) = 4x + 1$

Note that $f_1(0)f_2(0) = 3$ and $f_1(1)f_2(1) = 11 \cdot 5$ so we can apply SHH

SHH $\Rightarrow \exists\infty$–many p prime s.t. $p \equiv 3 \bmod 8$ and $p = 2q + 1$ with q prime.

Now

- ✎ $\mathrm{ord}_p(2) \mid p - 1 = 2q$
- ✎ $\mathrm{ord}_p(2) \neq 2$ if $p > 3$
- ✎ $\mathrm{ord}_p(2) \neq q$ since $-1 = \left(\frac{2}{p}\right) \equiv 2^{(p-1)/2} \bmod p$ because $p \equiv 3 \bmod 8$
- ✎ Hence $\mathrm{ord}_p(2) = 2q = p - 1$ for ∞–many p

Generalized Riemann Hypothesis (GRH) approach

(Dedekind Criterion) If $m \in \mathbb{N}$ is squarefree and $p \geq 3$. Then

$$m \mid [\mathbb{F}_p^* : \langle 2 \bmod p\rangle] \qquad \Leftrightarrow \qquad p \text{ splits completely in } \mathbb{Q}[\zeta_m, 2^{1/m}]$$

Theorem 1 (C. Hooley - 1967) *Assume that GRH holds of* $\mathbb{Q}[\zeta_m, 2^{1/m}]$. *Then*

$$\#\{p \leq x : \ p \textit{ splits completely in } \mathbb{Q}[\zeta_m, 2^{1/m}]\} = \frac{1}{\varphi(m)m}\,\mathrm{li}(x) + O(\sqrt{x}\log mx)$$

$$\#\{p \le x : \ p \text{ splits completely in } \mathbb{Q}[\zeta_m, 2^{1/m}]\} = \frac{1}{\varphi(m)m}\,\mathrm{li}(x) + O(\sqrt{x}\log mx)$$

So

$$\begin{aligned}
\#P_2(x) &= \#\{p \le x : \ \forall l, l \nmid [\mathbb{F}_p^* : \langle 2 \bmod p\rangle]\} \\
&= \sum_{m=1}^{\infty} \mu(m)\#\{p \le x : \ m \mid [\mathbb{F}_p^* : \langle 2 \bmod p\rangle]\} && \text{(inclusion exclusion)} \\
&= \sum_{m=1}^{\infty} \mu(m)\#\{p \le x : \ p \text{ splits completely in } \mathbb{Q}[\zeta_m, 2^{1/m}]\} && \text{(Dedekind)} \\
&\sim \sum_{m=1}^{\infty} \frac{1}{\varphi(m)m}\frac{x}{\log x} && \text{(Hooley's GRH)}
\end{aligned}$$

After classical estimates to handle various error terms.

Note that $\displaystyle\sum_{m=1}^{\infty} \frac{1}{\varphi(m)m} = \prod_{l \text{ prime}} \left(1 - \frac{1}{l(l-1)}\right) =: A$ Artin's Constant

General statement of Hooley's Theorem (1967)

Theorem 2 *Let $a \in \mathbb{Q}^* \setminus \{\pm 1\}$. Write $a = b^h$ with $b \in \mathbb{Q}$ not a power, $b = b_1 b_2^2$ with b_1 squarefree. Assume that the Generalised Riemann Hypothesis holds for $\mathbb{Q}[\zeta_m, a^{1/m}]$ for all $m \in \mathbb{N}$.*

$$\# P_a(x) \sim A_a \frac{x}{\log x}$$

where

$$A_a = \left(1 + \frac{1}{2}\left(1 - \left(\frac{-1}{b_1}\right)\right) \prod_{l \mid b_1} \frac{\gcd(l,h)}{\gcd(l,h) - l - l^2}\right) \prod_{l \ \mathit{prime}} \left(1 - \frac{\gcd(l,h)}{l(l-1)}\right)$$

Note that $A_a = q_a \cdot A$ with $q_a \in \mathbb{Q}$. So

GRH ⇒ SF Artin Conjecture

Heath–Brown, Gupta Murty (HGM)

We say that $n = P_2(\alpha, \delta)$ if either n is prime or $n = p_1 p_2$ with $n^\alpha \le p_1 \le n^{1/2-\delta}$.

Lemma 1 *Let $k = 2, 4, 8$ and let $u, v \in \mathbb{Z}$ be such that*

✎ $\gcd(u, v) = 1, \qquad k \mid u - 1, \qquad 16 \mid v$ & $\gcd(\frac{u-1}{k}, v) = 1.$

Then $\exists \alpha \in \left(\frac{1}{4}, \frac{1}{2}\right)$ and $\delta \in (0, \frac{1}{2} - \alpha)$ s.t. if

$$S_2 = \left\{ p : \ p \equiv u \bmod v \ \textit{and} \ \frac{p-1}{k} = P_2(\alpha, \delta) \right\}$$

we have that

$$\boxed{\#S_2(x) \gg \frac{x}{\log^2 x}}$$

Note that $k = 4$, $u = 197$ and $v = 240$ satisfy the conditions of the statement.

From the lemma we deduce that

Theorem 3 (Heath Brown, Gupta Murty (1986))

One out of $2, 3, 5$ is a primitive root for infinitely many primes.

Note that this is a quasi resolution of Artin Conjecture WF.

Proof. Take $k = 4$, $u = 197$ and $v = 240$ in the lemma and note that if $p \in \mathcal{S}_2$, $p \equiv 197 \bmod 240$, then

$$\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = \left(\frac{5}{p}\right) = -1$$

If $p \in S_2$, $p - 1 = 4P_2(\alpha, \delta)$.

If $(p-1)/4$ is prime, automatically $2, 3$ and 5 are all primitive root modulo p. Otherwise $p - 1 = 4p_1p_2$ and

$$\mathrm{ord}_p(2), \mathrm{ord}_p(3), \mathrm{ord}_p(5) \in \{4p_1, 4p_2, 4p_1p_2\}$$

By elementary methods:

$$\#\{p \in S_2(x): \text{ either of } \operatorname{ord}_p(2), \operatorname{ord}_p(3), \operatorname{ord}_p(5) \ = 4p_1\} = O\left(x^{1-2\delta}\right) = o\left(\frac{x}{\log^2 x}\right)$$

and

$$\#\{p \in S_2(x): \operatorname{ord}_p(2) = \operatorname{ord}_p(3) = \operatorname{ord}_p(5) = 4p_2\} = O\left(x^{4(1-\alpha)/3}\right) = o\left(\frac{x}{\log^2 x}\right)$$

Therefore

$$\#\{p \in S_2(x): \text{ one of 2, 3 or 5 ia primitive root mod } p\} \gg \frac{x}{\log^2 x}$$

In general

Theorem 4 (Heath Brown) *Given $a, b, c \in \mathbb{Z}$ multiplicatively independent such that none of $a, b, c, -3ab, -3ac, -3bc, abc$ is a perfect square. Then WF of Artin Conjecture holds for at least one of a, b or c*

Many generalizations and analogies in many directions

Some authors: Cangelmi, Chinen, Cojucaru, Goldstein, Gupta, Lapistö, Lenstra, Li Hailong, Manickam, Matthews, Murata, K. Murty, R. Murty, Odoni, Roskam, Saari, Schinzel, Shparlinski, Stephen, Stevenhagen, Susa, Thangadurai, Vaugan, Von Zur Gathen, Wiertelak, Wóicik, Zang Wenpeng and surely many others.

SHH ***GRH*** ***HGM***

Some chosen generalization/analogies

1. r-rank Artin Conjecture
2. Fixed index Artin Conjecture
3. Simultaneous primitive roots
4. Schinzel-Wójcik problem
5. Words and Primitive roots.

❶ r-rank Artin Conjecture

Let $\Gamma \subset \mathbb{Q}^*$ be a subgroup of finite rank $r \geq 1$.

Let Γ_p be the reduction of Γ modulo p. it makes sense for all but finitely many primes.

$$C_\Gamma = \{p : \ \Gamma_p = \mathbb{F}_p^*\}$$

Theorem 5 (Cangelmi & P, 1999) *Assume the GRH for* $\mathbb{Q}[\zeta_m, \Gamma^{1/m}]$*. Then*

$$\#C_\Gamma(x) \sim d_\Gamma \frac{x}{\log x}$$

where $d_\Gamma = q_\Gamma \cdot \prod_{l prime} \left(1 - \frac{1}{l^r(l-1)}\right)$ *and* $q_\Gamma \in \mathbb{Q}$ $\qquad$ $(q_\Gamma = 0 \Leftrightarrow \Gamma \subset (\mathbb{Q}^*)^2)$.

Note: Problem can also be dealt with SHH or HGM. Maybe not so interesting

❷ Fixed index Artin Conjecture

Let

$$M_{a,m} = \{p : [\mathbb{F}_p^* : \langle a \bmod p\rangle] = m\}$$

Question: When is

$$\#M_{a,m} = \infty?$$

Note:

✎ Work by H. Lenstra, L. Murata, S. Wagstaff and others

✎ if $a \equiv 1 \bmod 4$, m odd and $a \mid m$ then $M_{a,m} = \emptyset$ since $\left(\frac{a}{p}\right) = \left(\frac{p}{a}\right) = \left(\frac{1}{a}\right) = 1$ so $[\mathbb{F}_p^* : \langle a \bmod p\rangle]$ is even and cannot be $= m$

❷ Fixed index Artin Conjecture. 2

Theorem 6 (Murata 1991) *Let* $a, m \in \mathbb{Z}$, *a square free. Assume GRH for* $\mathbb{Q}[\zeta_{k_1}, a^{1/k_2}]$ $\forall k_1, k_2 \in \mathbb{N}$. *Then*

$$\#M_{a,m}(x) \sim B_{a,m} \frac{x}{\log x}$$

where $B_{a,m} = q_{a,m} A$ *with* $q_{a,m} \in \mathbb{Q}$

Note: This problem has not been dealt with SHH or HGM.

❸ Simultaneous primitive roots

Let $a_1, \ldots, a_r \in \mathbb{Q}^* \setminus \{\pm 1\}$ and set

$$P_{a_1,\ldots,a_r} = \{p : \ \forall i = 1, \ldots, r, \ \mathrm{ord}_p(a_i) = p - 1\}$$

Question: When is

$$\#P_{a_1,\ldots,a_r} = \infty?$$

Theorem 7 (Matthews, 1976) *Assume GRH for* $\mathbb{Q}[\zeta_{k_0}, a_1^{1/k_1}, \cdots, a^{1/k_r}]$ $\forall k_0, k_1, k_2, \ldots, k_r \in \mathbb{N}$.

Then $\#P_{a_1,\ldots,a_r} < \infty$ *if and only if one of the following two conditions are satisfied:*

(I) $a_{i_1} \cdots a_{i_{2s+1}} \in (\mathbb{Q}^*)^2$ *for some* $1 \le i_1 < \cdots < i_{2s+1} \le r$*;*

(II) $a_{i_1} \cdots a_{i_{2s}} \in -3(\mathbb{Q}^*)^2$ *for some* $1 \le i_1 < \cdots < i_{2s} \le r$ *and* $\forall l \equiv 1 \bmod 3, \ \exists i$ *s.t.* $x^3 \equiv a_i \bmod l$ *has solution.*

❸ Simultaneous primitive roots, 2

In all other cases $\#P_{a_1,\dots,a_r}(x) \sim A_{a_1,\dots,a_r}\dfrac{x}{\log x}$ where

$$A_{a_1,\dots,a_r} = q_{a_1,\dots,a_r} \prod_{l \text{ prime}} \left(1 - \frac{1}{l-1}\left[1 - \left(1 - \frac{1}{l}\right)^r\right]\right) \text{ with } q_{a_1,\dots,a_r} \in \mathbb{Q}^*$$

Theorem 8 (RP, 2006) *Assume SHH. Then*
$\#P_{a_1,\dots,a_r} < \infty$ *if and only if one of the following two conditions are satisfied:*

(I) $a_{i_1}\cdots a_{i_{2s+1}} \in (\mathbb{Q}^*)^2$ *for some* $1 \le i_1 < \cdots < i_{2s+1} \le r$*;*

(II) $a_{i_1}\cdots a_{i_{2s}} \in -3(\mathbb{Q}^*)^2$ *for some* $1 \le i_1 < \cdots < i_{2s} \le r$ *and*
$\forall l \equiv 1 \bmod 3$, $\exists i$ *s.t.* $x^3 \equiv a_i \bmod l$ *has solution.*

Note: This problem has not been dealt with HGM.

❹ Schinzel-Wójcik problem

Let $a_1, \ldots, a_r \in \mathbb{Q}^* \setminus \{\pm 1\}$ and set

$$Q_{a_1,\ldots,a_r} = \{p : \ \mathrm{ord}_p(a_1) = \ldots = \mathrm{ord}_p(a_1)\}$$

PROBLEM (Schinzel-Wójcik) Determine when

$$\#Q_{a_1,\ldots,a_r} < \infty$$

- ✎ If $Q_{a_1,\ldots,a_r} \supset P_{a_1,\ldots,a_r}$. Hence if $\#P_{a_1,\ldots,a_r} = \infty \Rightarrow \#Q_{a_1,\ldots,a_r} = \infty$
- ✎ Schinzel & Wójcik (1991). If $r = 2$, then $\#Q_{a_1,a_2} = \infty$
- ✎ Wójcik (1992). Assume SHH. If $-1 \notin \langle a_1, \ldots, a_r \rangle \subset \mathbb{Q}^*$ then $\#Q_{a_1,\ldots,a_r} = \infty$.

❹ Schinzel-Wójcik problem. 2

Proposition 1 *If* $-1 \in \langle a_1, \ldots, a_r \rangle \subset \mathbb{Q}^*$ *&* $\exists v_1, \cdots, v_r \in \mathbb{Z}$ *s.t.* $v_1 + \cdots + v_r$ *is odd and* $a_1^{v_1} \cdots a_r^{v_r} = 1$, *then*

$$\boxed{\#Q_{a_1,\ldots,a_r} \le 1}$$

Proof. Let $p > 2$ and assume $\delta = \mathrm{ord}_p(a_1) = \cdots = \mathrm{ord}_p(a_r)$ and $a_1^{\omega_1} \cdots a_r^{\omega_r} = -1$. Then

$$(-1)^\delta \equiv a_1^{\delta\omega_1} \cdots a_r^{\delta\omega_r} \equiv 1 \bmod p$$

which implies $2 \mid \delta$ and so $a_i^{\delta/2} \equiv -1 \bmod p$.

Finally

$$1 = (a_1^{v_1} \cdots a_r^{v_r})^{\delta/2} \equiv (-1)^{v_1+\cdots+v_r} \bmod p$$

contradicts $v_1 + \cdots + v_r$odd. □

❹ Schinzel-Wójcik problem. 3

Theorem 9 (FP, 2007) *Assume SHH.* $\#Q_{a_1,\dots,a_r}=\infty$ *if and only either of the following two conditions is satisfied:*

- ☞ $-1 \notin \langle a_1,\dots,a_r\rangle \subset \mathbb{Q}^*$
- ☞ $-1 \in \langle a_1,\dots,a_r\rangle \subset \mathbb{Q}^*$ *and* $\forall v_1,\cdots,v_r\in\mathbb{Z}$ *s.t.* $a_1^{v_1}\cdots a_r^{v_r}=1$ *one has* $2\mid v_1+\cdots+v_r$.

Theorem 10 (Susa & FP, 2005) *Assume GRH for* $\mathbb{Q}[\zeta_{k_0},a_1^{1/k_1},\cdots,a^{1/k_r}]$ $\forall k_0,k_1,k_2,\dots,k_r\in\mathbb{N}$. *Then* $\exists C_{a_1,\dots,a_r}$ *such that*

$$\#Q_{a_1,\dots,a_r}(x)\sim C_{a_1,\cdots,a_r}\frac{x}{\log x}$$

❹ Schinzel-Wójcik problem. 4

In particular if $l_1, \ldots, l_r$ are primes

$$C_{l_1,\cdots,l_r} = q'_{l_1,\ldots,l_r} \prod_l \left(1 - \frac{l(l^r - (l-1)^r - 1))}{(l-1)(l^{r+1} - 1)}\right)$$

where $q'_{l_1,\ldots,l_r} \in \mathbb{Q}^*$.

Note: This problem has not been dealt with HGM.

❺ Words and Primitive roots, 1

Let $\omega = \omega_0\omega_1\cdots\omega_n$ be a word of length $n+1$ on some alphabet.

We say that ω is transposition invariant if $\forall d \mid n+1$, the matrix

$$\begin{pmatrix} \omega_0 & \cdots & \omega_{d-1} \\ \omega_d & \cdots & \omega_{2d-1} \\ \vdots & \ddots & \vdots \\ \omega_{nd-1} & \cdots & \omega_n \end{pmatrix}$$

when transposed gives rise to the same word.

Example. $(v_0 vv \cdots vvv_n)$ is always (trivially) transposition invariant.

❺ Words and Primitive roots, 2

Theorem 11 (A. Lepistö & K. Saari,2006) *Given any alphabet with more then 2 letters, $\exists$ only trivially transposition invariant words of length n if and only if $n = p$ is prime and $\exists d \mid p+1$ which is a primitive root modulo p.*

Therefore we consider the set of primes

$$F = \{p : \ \exists d \mid p+1, \mathrm{ord}_p\, d = p-1\}$$

Note: If $p \equiv 7 \bmod 8$, then $p \notin F$.

Indeed for such primes p, $\left(\frac{2}{p}\right) = 1$ and $\forall$ odd prime $l \mid p+1$,

$$\left(\frac{l}{p}\right) = (-1)^{(l-1)/2}\left(\frac{p}{l}\right) = (-1)^{(l-1)/2}\left(\frac{-1}{l}\right) = 1.$$

So all divisors of $p+1$ are squares modulo p.

❺ Words and Primitive roots, 3

Note: If $\langle 2 \bmod p \rangle = \mathbb{F}_p^*$ then $p \in F$

So on GRH F has positive density ($\geq 0,37$).

Theorem 12 (A. Lepistö, FP & K. Saari,2006)

$$F(x) \gg \frac{x}{\log^2 x}$$

1. The proof is an application of the HGM method.
2. GRH should work for count $F(x)$
3. Empirical data suggests $F(x) \sim 0,63\frac{x}{\log x}$
4. $F(x) \lesssim 0,75\frac{x}{\log x}$ since if $p \equiv 7 \bmod 8$, $p \notin F$
5. Good project for a young mathematician