Ternary Goldbach for Artin primes

Peter Koymans
Universiteit Leiden

Breukelen 2017

DIAMANT symposium

The ternary Goldbach problem

A very classical problem in analytic number theory is the ternary Goldbach problem, which asks if every odd integer $n > 5$ can be written as the sum of three primes.

Hardy and Littlewood (1923) were the first to seriously attack this problem using their well-known circle method.

They were able to show that every sufficiently large odd integer is the sum of three primes conditional on the veracity of GRH.

Vinogradov (1930s) was able to remove the GRH assumption, and recently Helfgott (2013) completely settled the ternary Goldbach problem.

Artin's conjecture

An integer g is called a primitive root modulo p if it is a generator of the multiplicative group $\mathbb{F}_p^*$.

Throughout this talk we fix an integer g which is neither -1 nor a square.

Then Artin's conjecture ($\sim$1930) states that g is a primitive root modulo infinitely many primes p.

In fact, as part of his conjecture, Artin gave an explicit formula for the natural density of such primes.

Hooley (1967) proved Artin's conjecture under the assumption of GRH, but no unconditional proof has been found yet.

Artin's conjecture and arithmetic progressions

Given g, let Δ be the discriminant of the quadratic field $\mathbb{Q}(\sqrt{g})$ and let $h \geq 1$ be the largest integer such that g is a h-th power.

Theorem 1 (Lenstra (1977))

Let a, f be integers with $\gcd(a, f) = 1$ and let $P_{a,f,g}$ denote the set of primes p such that g is a primitive root modulo p and $p \equiv a \bmod f$. Then, assuming GRH, $P_{a,f,g}$ has a natural density $\delta(a, f, g)$ in the set of prime numbers. Furthermore, $\delta(a, f, g) = 0$ if and only if one of the following holds

- $\gcd(a - 1, f, h) > 1$;
- $\Delta \mid f$ *and* $\left(\frac{\Delta}{a}\right) = 1$;
- $\Delta \mid 3f$, $3 \mid \Delta$, $3 \mid h$ *and* $\left(\frac{-\Delta/3}{a}\right) = -1$.

In this case $P_{a,f,g}$ is a finite set, which one can explicitly compute.

Example: for $g = 27$ we have $\Delta = 12$ and $h = 3$. Taking $f = 12$ one can check that $\delta(a, 12, 27) \neq 0$ if and only if $a = 5$.

Our problem

Let $n > 5$ be an odd integer and let g be an integer not equal to -1 or a square. Can we express n as

$$n = p_1 + p_2 + p_3, \tag{1}$$

where p_1, p_2, p_3 are odd primes having g as a primitive root?

Example: If $g = 27$, then Lenstra's Theorem implies that p can only have g as primitive root if $p \equiv 5 \bmod 12$ or $p = 2$. In this case (1) can only have a solution if $n \equiv 3 \bmod 12$.

Theorem 2 (Frei, Koymans, Sofos (2017))

Assume GRH. Then every sufficiently large integer $n \equiv 3 \bmod 12$ *can be written as the sum of three odd primes* p_1, p_2, p_3 *all having* 27 *as a primitive root.*

General asymptotic results

For general g we have proven the following theorem.

Theorem 3 (Frei, Koymans, Sofos (2017))

Let g be an integer such that g is neither -1 nor a square. Assuming GRH we have for all positive odd integers n and all reals $\beta \in (0,1)$

$$\sum_{\substack{p_1+p_2+p_3=n \\ \forall i:\ \mathbb{F}_{p_i}^* = \langle g \rangle}} \prod_{i=1}^{3} \log p_i = C_g(n) n^2 + O_{g,\beta}(n^2 (\log n)^{-\beta})$$

for some explicit function $C_g(n) \geq 0$.

Trying the circle method directly leads to problems, because no good Siegel–Walfisz type asymptotic formula for the number of primes up to x having g as a primitive root is currently available.

The proof is a combination of Hooley's method with the circle method.

An explicit formula for $C_g(n)$

A large part of the paper is devoted to finding an explicit formula for $C_g(n)$ and in particular establishing when $C_g(n) \neq 0$. Define A_g as

$$A_g := \lim_{x \to +\infty} \frac{\#\{p \leq x : \mathbb{F}_p^* = \langle g \rangle\}}{\#\{p \leq x\}}.$$

Also define

$$\sigma_{g,n}(d) := d \sum_{\substack{b_1, b_2, b_3 \bmod d \\ b_1 + b_2 + b_3 \equiv n \bmod d}} \prod_{i=1}^{3} \frac{\delta(b_i, d, g)}{A_g},$$

where the factors $\delta(b_i, d, g)$ are as in Lenstra's Theorem. Then we have the following explicit expression for $C_g(n)$

$$C_g(n) = A_g^3 \cdot \sigma_{g,n}(|\Delta|) \cdot \prod_{p \nmid \Delta} \sigma_{g,n}(p),$$

where Δ is the discriminant of $\mathbb{Q}(\sqrt{g})$.

More results about $C_g(n)$

In contrast to the usual applications of the circle method, the constant $C_g(n)$ does not factorize completely as an Euler product.

Provided that $C_g(n) \neq 0$, we have the following lower bound for $C_g(n)$

$$C_g(n) \gg \left(\frac{\varphi(h)}{|\Delta|^2 h}\right)^3$$

with an absolute implied constant, where $h \geq 1$ is the largest integer such that g is a h-th power.

Theorem 4 (Frei, Koymans, Sofos (2017))

Let n be an odd positive integer and g an integer not equal to -1 or a square. Then we have the following equivalence

$$C_g(n) > 0 \Leftrightarrow \sigma_{g,n}(|\Delta|)\sigma_{g,n}(3) > 0.$$

When is $C_g(n) > 0$

Our previous theorem gives a nice criterion for $C_g(n) > 0$, but it is in terms of $\sigma_{g,n}(|\Delta|)$ and $\sigma_{g,n}(3)$. We have to make this more explicit.

It is easy to determine when $\sigma_{g,n}(3) > 0$. To decide whether $\sigma_{g,n}(|\Delta|) > 0$ we need to find an equivalent condition that is easier to handle.

Using some elementary estimates one can show that $\sigma_{g,n}(|\Delta|) > 0$ provided that Δ has a prime factor greater than 7. This leaves only finite many possibilities for Δ to check.

Final examples

Let g be an integer neither -1 nor a square. In case $\Delta = 12$ the following table gives us necessary and sufficient congruence conditions for odd n to satisfy $C_g(n) > 0$

$\mathrm{Disc}(\mathbb{Q}(\sqrt{g}))$	Power properties of g	Congruence conditions for n
12	g is not a cube	$n \equiv 3, 5, 7, 9 \bmod 12$
12	g is a cube	$n \equiv 3 \bmod 12.$

If $|\Delta| > 840 = 8 \cdot 3 \cdot 5 \cdot 7$, then we have

$\mathrm{Disc}(\mathbb{Q}(\sqrt{g}))$	Power properties of g	Congruence conditions for n
$3 \nmid \Delta$	g is a cube	$n \equiv 0 \bmod 3$
Otherwise	-	No conditions on n.

The complete table can be found in our paper.

Questions

Thank you for your attention!
Questions?