My Hildesheimer Problems

Pieter Moree

Abstract

I formulate my Hildesheimer problems together with some background.

0.1 Maximum ternary coefficients

Let $\Phi_n(x) = \sum_{k=0}^{\varphi(n)} a_n(k)x^k$, denote the nth cyclotomic polynomial with φ Euler's (totient) function. Put $A(n) = \max\{|a_n(k)| : 0 \leq k \leq \varphi(n)\}$. Let $p < q < r$ be primes. It is known that $A(pqr) \leq 3p/4$. We define $M(p)$ as the maximum of $A(pqr)$ as r and q range over all the primes with $r > q > p$. Sister Marion Beiter [1] conjectured in 1968 that $M(p) \leq (p+1)/2$. The author and Gallot [5] showed that the conjecture is false for every $p \geq 11$. They showed that for every $\epsilon > 0$ one has $M(p) \geq (2/3-\epsilon)p$ for all p large enough. They formulated the Corrected Sister Beiter Conjecture:

Conjecture 1 (`Gallot and Moree.`) *We have $M(p) \leq 2p/3$ for every $p \geq 2$.*

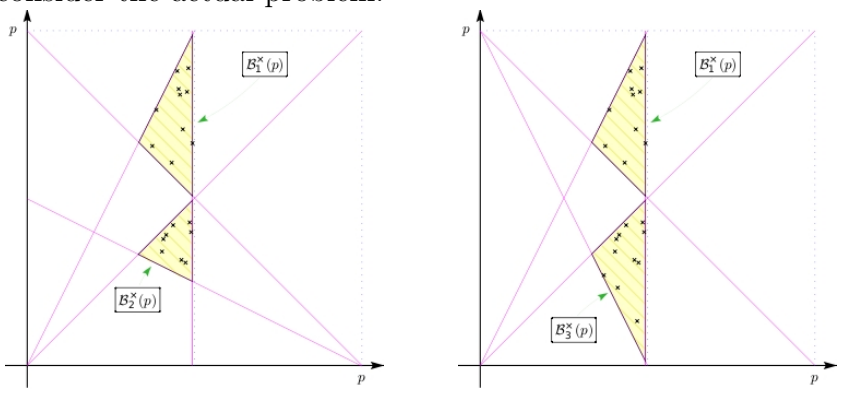
The problem of finding an algorithm that allows one to compute $M(p)$ was solved by the author's intern Dominik Duda [3]. However, his algorithm is not practical. It is thus an open problem to find an efficient algorithm for computing $M(p)$ and it would already be a great advance if one could compute $M(p)$ exactly for all primes $p < 100$.

Gallot and Moree [5] gave a construction showing that $M(p) \geq g_1(p)$, with a certain function $g_1(p)$. Several years later Eugenia Roşu [6] found a construction of the form $M(p) \geq g_2(p)$, with $g_2(p) \geq g_1(p)$. We conjecture that infinitely often $g_2(p) > g_1(p)$. In order to show this we are led to first study a simpler problem, which is the following. Consider two equal squares S_1 and S_2 in $(0,p) \times (0,p)$ having side length pc with $0 < c < 1$ fixed, that do not overlap and have the same projection on the x-axis. It can be shown that for all primes $p \geq p_c$ large enough the set $U_i = \{(x,y) : \ (x,y) \in S_i, \ xy \equiv 1 (\mathrm{mod}\ p)\}$ is non-empty, where we only consider points (x,y) with integer coordinates. The set U_i consists of the points on the modular hyperbola $xy \equiv 1 (\mathrm{mod}\ p)$ (for a comprehensive survey see Shparlinski [7]) that lie in the square S_i. Indeed, asymptotically (as p gets large) both S_1 and S_2 contain pc points from the modular hyperbola. For $p \geq p_c$ we define

$$m_i(p) = \min\{x : (x,y) \in U_i(p)\}.$$

Conjecture 2 (`Moree.`) *For infinitely many primes we have $m_1(p) > m_2(p)$ and for infinitely many primes we have $m_2(p) < m_1(p)$.*

Next we consider the actual problem.



Given a prime p, consider the following triangles.

$$B_1(p) = \{(x,y) \in \mathbb{R}^2 : 1 \le x \le \frac{p-3}{2},\ x+y \ge p,\ y \le 2x\}$$

$$B_2(p) = \{(x,y) \in \mathbb{R}^2 : 1 \le x \le \frac{p-3}{2},\ x+2y+1 \ge p,\ x > y\}$$

$$B_3(p) = \{(x,y) \in \mathbb{R}^2 : 1 \le x \le \frac{p-3}{2},\ 2x+y \ge p,\ x \ge y\}.$$

We leave it as an exercise to show that the intersection of $B_1(p) \cup B_2(p)$ and the modular hyperbola is non-empty for every $p \ge 11$. Note that $B_2(p) \subset B_3(p)$. For $p \ge 11$ we are interested in the quantities

$$\mu_1(p) = \min\{x : (x,y) \in B_1(p) \cup B_2(p),\ xy \equiv 1 (\text{mod } p)\}$$

and

$$\mu_2(p) = \min\{x : x \in B_1(p) \cup B_3(p),\ xy \equiv 1 (\text{mod } p)\}.$$

Note that $\mu_i(p) \le (p-3)/2$. We have $g_1(p) = p - \mu_1(p)$ and $g_2(p) = p - \mu_2(p)$. As we said we have $M(p) \ge g_2(p) \ge g_1(p) > (p+1)/2$, showing that Beiter's conjecture is false for $p \ge 11$.

Definition 1 *If $g_2(p) > g_1(p)$ we say that p is a Roşu prime.*

For $p = 241$ the picture shows the triangles and the modular hyperbola points that are in it. The left most point is in $B_3(p)$, not in $B_1(p) \cup B_2(p)$, making $p = 241$ a Roşu prime. Indeed, the Roşu primes < 400 are: $29, 37, 41, 83, 107, 109, 149, 179, 181, 223, 227, 233, 241, 269, 281, 317, 367, 379, 383, 389$.

For more on counting modular hyperbola points in triangles, see Cobeli et al. [2]. This involves using estimates for Kloosterman sums.

Conjecture 3 `(Moree.)` *There are infinitely many Roşu primes.*

0.2 Quinary non-flat cyclotomic polynomials

The cyclotomic polynomial $\Phi_n(x)$ is said to be flat if $A(n) = 1$. Let p, q, r, s, t be distinct primes. It is easy to see that $\Phi_p(X)$ and $\Phi_{pq}(X)$ are flat. Gallot and the author [4] showed that $(X-1)\Phi_{pqr}(X)$ is always flat. It can be shown that $\Phi_{pqr}(X)$ is flat if, e.g, $q \equiv -1 (\text{mod } p)$ and $r \equiv 1 (\text{mod } pq)$. Likewsie $\Phi_{pqrs}(X)$ is known to be flat if $q \equiv -1 (\text{mod } p)$, $r \equiv \pm 1 (\text{mod } pq)$, $s \equiv 1 (\text{mod } pqr)$.

Conjecture 4 *Quinary non-flat polynomials do not exist, in other words we have* $A(pqrst) > 1$.

I do not know the originator of this conjecture.

References

[1] Sister M. Beiter, Magnitude of the coefficients of the cyclotomic polynomial $F_{pqr}(x)$, *Amer. Math. Monthly* **75** (1968), 370–372.

[2] C. Cobeli, Y. Gallot, P. Moree and A. Zaharescu, Sister Beiter and Kloosterman: A tale of cyclotomic coefficients and modular inverses, *Indag. Math. (N.S.)* **24** (2013), 915–929.

[3] D. Duda, The maximal coefficient of ternary cyclotomic polynomials with one free prime, *Int. J. Number Theory* **10** (2014), 1067–1080.

[4] Y. Gallot and P. Moree, Neighboring ternary cyclotomic coefficients differ by at most one, *J. Ramanujan Math. Soc.* **24** (2009), 235–248.

[5] Y. Gallot and P. Moree, Ternary cyclotomic polynomials having a large coefficient, *J. Reine Angew. Math.* **632** (2009), 105–125.

[6] P. Moree and E. Roşu, Non-Beiter ternary cyclotomic polynomials with an optimally large set of coefficients, *Int. J. Number Theory* **8** (2012), 1883–1902.

[7] I.E. Shparlinski, Modular hyperbolas, *Jpn. J. Math.* **7** (2012), 235–294.