Chebychev's problem for the twelfth cyclotomic polynomial

Erdős Centennial, Budapest July 1-5 2013

Cécile Dartyge
Institut Élie Cartan
Université de Lorraine
BP 239
54506 Vandœuvre Cedex
France

1. Introduction

Let $f \in \mathbb{Z}[x]$ be an irreducible polynomial with no fixed divisor. Are there infinitely many integers n such that $f(n)$ is a prime number?
If $\deg f = 1$: Dirichlet's Theorem.
For $\deg f \geqslant 2$?
1978 : Iwaniec proved that there exists infinitely many n such that

$$n^2 + 1 = p \text{ or } n^2 + 1 = p_1 p_2.$$

For $n \in \mathbb{N}$, let $P^+(n)$denote the greatest prime factor of n.

Chebychev (1895): $$\lim_{x \to +\infty} \frac{1}{x} P^+\Big(\prod_{n \leqslant x} (n^2 + 1)\Big) = +\infty.$$

Nagell (1921): $f \in \mathbb{Z}[X]$ irreducible, $\deg f \geqslant 2$, $\vartheta \in [0, 1[$:

$$P^+\Big(\prod_{n \leqslant x} f(n)\Big) \gg_{f,\vartheta} x(\log x)^{\vartheta}.$$

Let $f \in \mathbb{Z}[X]$ irreducible with $\deg f \geqslant 2$,
Erdős (1952): there exists $A > 0$ such that

$$P^+\Big(\prod_{n \leqslant x} f(n)\Big) \gg_f x(\log x)^{A \log\log\log x}.$$

Erdős and Schinzel (1990): there exists $c > 0$ such that

$$P^+\Big(\prod_{n \leqslant x} f(n)\Big) \gg_f x \exp\exp(c(\log\log x)^{2/3}).$$

Tenenbaum (1990): for $\alpha \in]0, 2 - \log 4[$, $(2 - \log 4 = 0.61..)$

$$P^+\Big(\prod_{n \leqslant x} f(n)\Big) > x \exp((\log x)^{\alpha}) \qquad (x > x_0(f, \alpha)).$$

$$P^+\Big(\prod_{n\leqslant x}(n^2+1)\Big) \gg x^{1.1} \quad \text{Hooley (1967)}$$

$$\gg x^{1.2..} \quad \text{Deshouillers and Iwaniec (1982).}$$

Hooley (1978): if the hypothesis (R^*) holds then

$$P^+\Big(\prod_{n\leqslant x}(n^3+2)\Big) \gg x^{31/30}.$$

The hypothesis (R^*) is (with the notations $\mathrm{e}(t) = \exp(2i\pi t)$ and $r\overline{r} \equiv 1 \pmod s$):

$$\sum_{\substack{\zeta_1<r<\zeta_2\\(r,s)=1}} \mathrm{e}\Big(\frac{h\overline{r}+kr}{s}\Big) \ll s^{\varepsilon}(1+\zeta_2-\zeta_1)^{1/2}(h,s)^{1/2}.$$

Heath-Brown (2001): there exists a positive proportion of integers n such that $P^+(n^3+2) > n^{1+10^{-303}}$. In particular we have

$$P^+\Big(\prod_{n\leqslant x}(n^3+2)\Big) \gg x^{1+10^{-303}}.$$

Let $\Phi_{12}(n) = n^4 - n^2 + 1$.

Theorem 1(CD 2013). *There exists $c > 0$ such that for X large enough we have:*

$$P^+\Big(\prod_{X<n\leqslant 2X}\Phi_{12}(n)\Big) \geqslant X^{1+c},$$

the value $c = 10^{-47016}$ is admissible.

2. How to detect polynomial values with a large prime factor?

Lemma 2. *Let* $\mathcal{A} = \{n \in]X, 2X] : \prod_{\substack{p \leqslant 4X \\ p^k \| \Phi_{12}(n)}} p^k \geqslant X\}$. *We suppose that there exists* $\alpha > 0$ *such that* $|\mathcal{A}| \geqslant \alpha X$ *for* X *large enough. Then we have:*

$$(1) \qquad P^+\Big(\prod_{X<n\leqslant 2X} \Phi_{12}(n)\Big) \geqslant X^{1+\frac{\alpha}{3-\alpha}}.$$

The ideas of the proof are from Erdős. We evaluate in two different ways $V(X) = \sum_{X<n\leqslant 2X} \log(\Phi_{12}(n))$. First we have

$$V(X) = 4X \log X + O(X).$$

On the other hand we have:

$$V(X)=\sum_{X<n\leqslant 2X}\ \sum_{\substack{k\geqslant 1, p\ll X^4\\ p^k\|\Phi_{12}(n)}} k\log p$$

$$= X(\log X+O(1))+\sum_{X<n\leqslant 2X}\ \sum_{\substack{p>4X\\ p|\Phi_{12}(n)}} \log p$$

$$= X(\log X+O(1))+\sum_{X<n\leqslant 2X} \log^{(2)}(\Phi_{12}(n)),$$

say. Let P_X denote the greatest prime factor of the product in (1).
We have:

$$\log^{(2)}(\Phi_{12}(n))\leqslant\begin{cases}2\log(P_X) & \text{if } n\in\mathcal{A}\\ 3\log(P_X) & \text{if } n\notin\mathcal{A}.\end{cases}$$

3. Exponential sums

Let $f \in \mathbb{Z}[X]$. We want to estimate the cardinality of the sets

$$\mathcal{A}_d(f) = \{n \in]X, 2X] : d | f(n)\}.$$

To detect this congruence we can use exponential sums. We have to find upper bounds of sums of type:

$$\sum_{D<d\leqslant 2D} \sum_{\substack{0\leqslant v<d \\ f(v)\equiv 0 \pmod d}} \mathrm{e}\Big(\frac{hv}{d}\Big). \tag{2}$$

For $f(n) = n^2+1$, Hooley used the Gauss-Legendre correspondence

$$\{0 \leqslant v < d : v^2+1 \equiv 0 \pmod d\} \leftrightarrow \{d = r^2+s^2 : (r,s) = 1 \text{ and } |r| < s\}.$$

(2) "becomes" $\sum_{s\ll D^{1/2}} \sum_{\substack{|r|<s \\ (r,s)=1}} \mathrm{e}\Big(\frac{h\overline{r}}{s}\Big) \ll D^{3/4+\varepsilon}$ by Weil.

For $f(n) = n^3 + 2$, Hooley proved the correspondence:

$\{0 \leqslant v < d : v^3 + 2 \equiv 0 \pmod{d}\} \leftrightarrow \{\text{some representations } d = \varphi(a,b,c)\}$,

with $\varphi(a,b,c) = a^3 + 2b^3 + 4c^3 - 6abc = N_{\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}}(a + b\sqrt[3]{2} + c\sqrt[3]{4})$.
This leads to sums of type:

$$\sum_{b,c \ll D^{1/3}} \sum_{a \ll D^{1/3}} \mathrm{e}\Big(\frac{hc^2\,\overline{(b^2 - ac)}}{b^3 - 2c^3}\Big).$$

Theorem 3 (Heath-Brown 2001). *Let $q = q_0 \cdots q_k$ be a square-free integer. Let $f, g \in \mathbb{Z}[x]$ satisfying some conditions. Then we have for $(w,q) = 1$:*

$$\sum_{\substack{A<n<A+B \\ (q,g(n))=1}} \mathrm{e}\Big(\frac{wf(n)\overline{g(n)}}{q}\Big) \ll q^{\varepsilon}\Big(\frac{B}{q_0^{1/2^{(k+1)}}} + B^{1-\frac{1}{2^k}} q_0^{\frac{1}{2^{k+1}}} + \sum_{j=1}^{k} B^{1-\frac{1}{2^j}} q_j^{\frac{1}{2^j}}\Big).$$

Another important ingredient of Heath-Brown's method was to use the ideals of $\mathbb{Z}[\sqrt[3]{2}]$.

4. The polynomial Φ_{12}

Let $\zeta_{12} = e^{i\pi/6}$.The integer ring $\mathbb{Z}[\zeta_{12}]$ is principal and we have:

$$N(n-\zeta_{12}) = \Phi_{12}(n), \qquad \prod_{\substack{p\leqslant 4X\\ p^k\|\Phi_{12}(n)}} p^k = \prod_{\substack{N(\mathcal{P})\leqslant 4X\\ \mathcal{P}^k\|(n-\zeta_{12})}} N(\mathcal{P})^k,$$

where $N(I)$ is the norm of the ideal I. We are then interested by

$$\mathcal{A}_{(\alpha)} = \{n \in]X, 2X] : (\alpha)|(n-\zeta_{12})\}.$$

For $\alpha \in \mathbb{Z}[\zeta_{12}]$, $\alpha = a + b\zeta_{12} + c\zeta_{12}^2 + d\zeta_{12}^3$, let m_α denote the matrix of the multiplication by α in the basis $1, \zeta_{12}, \zeta_{12}^2, \zeta_{12}^3$. Let $B_{ij}, 1 \leqslant i, j \leqslant 4$ be the cofactors of this matrix.

Lemma 4. *If* $(B_{14}, N(\alpha)) = 1$ *then for* $n \in \mathbb{Z}$ *we have*

$$(\alpha) | (n - \zeta_{12}) \Leftrightarrow n \equiv B_{13}\overline{B}_{14} \pmod{N(\alpha)}.$$

Proof. We use the fact that for $\ell = 0, 1, 2, 3$, $\zeta_{12}^{\ell}\alpha \in (\alpha)$. This gives the congruence system:

$$\begin{pmatrix} b & c & d \\ a & b+d & c \\ -d & a+c & b+d \\ -c & b & a+c \end{pmatrix} \begin{pmatrix} \zeta_{12} \\ \zeta_{12}^2 \\ \zeta_{12}^3 \end{pmatrix} = \begin{pmatrix} -a \\ d \\ c \\ b+d \end{pmatrix} \operatorname{mod}(\alpha).$$

We apply Cramer formula and use the fact that $m_{\alpha^{-1}} = (m_\alpha)^{-1}$: this gives $B_{14}\zeta_{12} \equiv B_{13} \pmod{(\alpha)}$. □

With this Lemma and standard manipulations on exponential sums, we obtain sums of type:

$$\sum_{(\alpha)\in\mathcal{J}} \mathrm{e}\Big(\frac{-hB_{13}\overline{B_{14}}}{N(\alpha)}\Big),$$ where $\mathcal{J}$ is a set of ideals of $\mathbb{Z}[\zeta_{12}]$.

If we apply again Cramer formula and use some facts from resultant theory we obtain

Lemma 5. *Let* $q = (b^2 + c^2)(b^2 + db + d^2)(-3c^2 + (b + 2d)^2)$*.If* $(q, B_{14}) = 1$ *then*

$$e\Big(\frac{-hB_{13}\overline{B_{14}}}{N(\alpha)}\Big) = \mathrm{e}\Big(\frac{-hU\overline{B}_{14}}{q} + hR(a,b,c,d)\Big),$$

where $U \in \mathbb{Z}[a,b,c,d]$ *is a polynomial of degree five and* R *is a rational fraction.*

5. Joint distribution of some values of binary forms

Let $P =]B, B+M] \times]C, C+M] \times]D, D+M]$, $f_1, f_2 \in \mathbb{Z}[x, y]$ two binary, primitive and irreducible forms with degree $\geqslant 2$. We define also for $i = 1, 2$:

$$\varrho_{f_i}(m) = |\{0 \leqslant r, s < m : m | f_i(r, s) \text{ and } (r, s, m) = 1\}|.$$

We suppose that there exists $\vartheta > 0$ such that

$$M \geqslant \max(|A|, |B|, |C|)^{\vartheta}.$$

We consider

$$\mathcal{A}(m_1, m_2, m_3, \mathbf{u}) = \{(b, c, d) \in P : m_1 | f_1(b, c),\ m_2 | f_2(b, d), \\ (b, c, d) \equiv \mathbf{u} \pmod{m_3}, (m_1, b, c) = 1 = (m_2, b, d)\}.$$

We are interested by

$$E = \sum_{\substack{m_1<Q_1\\ m_2<Q_2}}^{*} \left| |\mathcal{A}(m_1, m_2, m_3, \mathbf{u})| - \frac{M^3 \varrho^*_{f_1}(m_1)\varrho^*_{f_2}(m_2)}{m_1^2 m_2^2 m_3^3} \right|,$$

where the star in the $\sum$ indicates that some coprimality conditions are required.

Theorem 6. *With the above notations, we have:*

$$E \ll (\log M)^7 \Big(Q_1 Q_2 + \frac{(Q_1Q_2)^{1/2} M^{3/2}}{m_3^{3/4}} + \frac{(Q_1Q_2)^{1/3} M^2}{m_3^2} \Big)$$
$$+ M^{1+\varepsilon}(Q_1 + Q_2) + M^{2+\varepsilon} + \frac{M^{2+\varepsilon}}{m_3^2}(\sqrt{Q_1} + \sqrt{Q_2}).$$