On Squares in Polynomial Products

Javier Cilleruelo
Departamento de Matemáticas
Universidad Autónoma de Madrid
28049 Madrid, Spain
franciscojavier.cilleruelo@uam.es

Florian Luca
Instituto de Matemáticas
Universidad Nacional Autonoma de México
C.P. 58089, Morelia, Michoacán, México
fluca@matmor.unam.mx

Adolfo Quirós
Departamento de Matemáticas
Universidad Autónoma de Madrid
28049 Madrid, Spain
adolfo.quiros@uam.es

Igor E. Shparlinski
Department of Computing
Macquarie University
Sydney, NSW 2109, Australia
igor@ics.mq.edu.au

Abstract

Let $f(X) \in \mathbb{Z}[X]$ be an irreducible polynomial of degree $D \geq 2$ and let N be a sufficiently large positive integer. We estimate the number of positive integers $n \leq N$ such that the product

$$F(n) = \prod_{k=1}^{n} f(k)$$

is a perfect square. We also consider more general questions and give a lower bound on the number of distinct quadratic fields of the form $\mathbb{Q}(\sqrt{F(n)})$, $n = 1, \ldots, N$.

Keywords quadratic fields, square sieve, character sums

AMS Mathematics Subject Classification 11L40, 11N36, 11R11

1 Introduction

1.1 Motivation

For a nonconstant polynomial $f(X) \in \mathbb{Z}[X]$ and a positive integer n we consider the product

$$F(n) = \prod_{m=1}^{n} f(m).$$

Erdős and Selfridge [6] proved that $F(n)$ is never a perfect power for $n \geq 2$ when $f(X) = X + a$ for some nonnegative integer a. It has been recently shown in [4] that $F(n)$ is a perfect square only for $n = 3$ when $f(X) = X^2 + 1$. The method of [4] can be extended to more general polynomials $f(X) = X^2 + a$ with a positive integer $a \geq 1$. However, the method does not seem apply to polynomials $f(X)$ of degree $D \geq 3$. Here, we pursue an alternative approach which does not give a result of the same strength, but instead can be applied to more general questions.

Accordingly, for a given polynomial $f(X)$, a squarefree integer d, and nonnegative integers M and N, we let $S_d(M, N)$ denote the number of integer solutions (n, s) to the equation

$$F(n) = ds^2, \qquad \text{for } n = M + 1, \ldots, M + N.$$

We obtain an upper bound on $S_d(M,N)$ which is uniform in d. Thus, in particular, our result yields a lower bound on the number of distinct quadratic fields among $\mathbb{Q}(\sqrt{F(n)})$ for $n = M+1, \ldots, M+N$ (see [5, 11, 12, 13], where similar questions are considered for some other sequences).

1.2 Notation

In what follows, we use the symbols 'O', '$\gg$' and '$\ll$' with their usual meanings (that is, $A = O(B)$, $A \ll B$, and $B \gg A$ are all equivalent to the inequality $|A| \le cB$ with some constant $c > 0$). The implied constants in the symbols 'O', '$\ll$' and '$\gg$' may depend on our polynomial $f(X)$.

For a positive number x, we write $\log x$ for the maximum between the natural logarithm of x and 1. Thus, we always have $\log x \ge 1$.

1.3 Our results

Here we prove some unconditional results which hold for irreducible polynomials of arbitrary degree.

Theorem 1. *Let $f(X) \in \mathbb{Z}[X]$ be an irreducible polynomial of degree $D \ge 2$. Then, uniformly for squarefree integers $d \ge 1$ and arbitrary integers $M \ge 0$ and $N \ge 2$, we have*

$$S_d(M,N) \ll N^{11/12}.$$

Corollary 2. *Let $f(X) \in \mathbb{Z}[X]$ be an irreducible polynomial of degree $D \ge 2$. Then there is a positive constant C depending only on the polynomial $f(X)$ such that there are at least $CN^{1/12}$ distinct quadratic fields amongst $\mathbb{Q}(\sqrt{F(n)})$ for $n = M+1, \ldots, M+N$.*

2 Auxiliary Results

2.1 Character Sums

Our proofs rest on some bounds for character sums. For an odd integer m we use (k/m) to denote, as usual, the Jacobi symbol of k modulo m.

The following result is a direct consequence of the Weil bound and the Chinese Remainder Theorem (see [10, Equations (12.21) and (12.21)]).

Lemma 3. *Let $G(X) \in \mathbb{Z}[X]$ be a fixed polynomial of degree $D \geq 2$. For all primes $\ell \neq p$ such that $G(X)$ is not a perfect square modulo ℓ and p and all integers a, we have*

$$\sum_{n=1}^{\ell p} \left(\frac{G(n)}{\ell p}\right) \exp\left(2\pi i \frac{an}{\ell p}\right) \ll D^2 (\ell p)^{1/2}.$$

Using the standard reduction between complete and incomplete sums (see [10, Section 12.2]), we obtain the following result.

Lemma 4. *Let $G(X) \in \mathbb{Z}[X]$ be a fixed polynomial of degree $D \geq 2$. For all primes $\ell \neq p$ such that $G(X)$ is not a perfect square modulo ℓ and p, we have*

$$\sum_{n=M+1}^{M+N} \left(\frac{G(n)}{\ell p}\right) \ll D^2 \left(\frac{N}{\ell p} + 1\right) (\ell p)^{1/2} \log(\ell p).$$

2.2 Prime Divisors of Polynomials

For a real number $z \geq 1$ we let $\mathcal{L}_z$ be the set of primes $\ell \in [z, 2z]$ such that $f(X)$ has no root modulo ℓ; that is, $f(n) \not\equiv 0 \pmod{\ell}$ for all integers n. By the Frobenius Density Theorem, the set $\mathcal{L}_z$ has positive density as a subset of all primes in $[z, 2z]$. In fact, this density is at least $(D-1)/D!$ (see [2, Lemma 3]). Thus, we have the following result.

Lemma 5. *Let $f(X) \in \mathbb{Z}[X]$ be an irreducible polynomial. We have*

$$\#\mathcal{L}_z = \frac{1}{\kappa} \left(\pi(2z) - \pi(z)\right) + O\left(z(\log z)^{-2}\right),$$

where $\kappa \leq D!/(D-1)$ is a positive integer depending on the polynomial $f(X)$.

2.3 Multiplicities Roots of Polynomial Products

We show that products of consecutive shifts of irreducible polynomials always have at least one simple root.

Lemma 6. *Let $f(X) \in \mathbb{Z}[X]$ be an irreducible polynomial. Then for any integers $k > h \geq 0$, the polynomial*

$$\prod_{m=h+1}^{k} f(X+m) \in \mathbb{Z}[X]$$

has at least one root of multiplicity 1.

Proof. Suppose that all roots of the above polynomial are multiple. Since $f(X)$ is irreducible, all roots of each of the $f(X+m)$ for $m = h+1, \ldots, k$ are simple. Thus, every root of $f(X+k)$ must be a root of $\prod_{m=h+1}^{k-1} f(X+m)$. Let α_0 be a root of $f(X)$ such that $\operatorname{Re}\alpha_0 \le \operatorname{Re}\alpha$ for all roots α of $f(X)$ (in general α_0 is not unique; we just pick one of them). Then $\alpha_0 - k$ is a root of $f(X+k)$ and can not be a root of $f(X+i)$ for any positive integer $i < k$ since otherwise, $\alpha = \alpha_0 + i - k$ would be a root of $f(X)$ with a smaller real part than α_0, contradicting the choice of α_0. □

2.4 Character Sums with Polynomial Products

The following estimate of character sums is obtained via an adaptation of the approach in [7] (see also [8, 9]).

Lemma 7. *Let $f(X) \in \mathbb{Z}[X]$ be an irreducible polynomial with $D \ge 2$ and let $z = N^{1/2}$. Then there exists a subset of $\mathcal{R}_z \subseteq [z, 2z]$ with $\#\mathcal{R}_z \gg z/\log z$ and such that for any distinct primes $\ell \ne p$ in $\mathcal{R}_z$ and arbitrary integers $M \ge 0$ and $N \ge 2$ the following bound holds*

$$\sum_{n=M+1}^{M+N} \left(\frac{F(n)}{\ell p}\right) \ll N^{11/12}.$$

Proof. Obviously, for any integer $h \ge 0$ we have

$$\sum_{n=M+1}^{M+N} \left(\frac{F(n)}{\ell p}\right) = \sum_{n=M+1+h}^{M+N+h} \left(\frac{F(n)}{\ell p}\right) + O(h) = \sum_{n=M+1}^{M+N} \left(\frac{F(n+h)}{\ell p}\right) + O(h).$$

Therefore, for any integer $H \ge 1$, we have

$$\sum_{n=M+1}^{M+N} \left(\frac{F(n)}{\ell p}\right) = \frac{1}{H} W + O(H), \qquad (1)$$

where

$$W = \sum_{h=0}^{H-1} \sum_{n=M+1}^{M+N} \left(\frac{F(n+h)}{\ell p}\right).$$

Changing the order of summation and applying the Cauchy inequality, we derive

$$\begin{aligned} |W|^2 &\leq \left(\sum_{n=M+1}^{M+N} \left| \sum_{h=0}^{H-1} \left(\frac{F(n+h)}{\ell p} \right) \right| \right)^2 \\ &\leq N \sum_{n=M+1}^{M+N} \left| \sum_{h=0}^{H-1} \left(\frac{F(n+h)}{\ell p} \right) \right|^2 \\ &= N \sum_{n=M+1}^{M+N} \left| \sum_{h,k=0}^{H-1} \left(\frac{F(n+h)F(n+k)}{\ell p} \right) \right|. \end{aligned}$$

Changing the order of summation again and separating the "diagonal" terms with $h = k$, which contribute at most 1 each, we get

$$|W|^2 \leq HN^2 + 2N \sum_{0 \leq h < k \leq H-1} \left| \sum_{n=M+1}^{M+N} \left(\frac{F(n+h)F(n+k)}{\ell p} \right) \right|. \tag{2}$$

We now notice that for $h < k$ we have

$$\begin{aligned} F(n+h)F(n+k) &= \left(\prod_{m=1}^{n+h} f(m) \right)^2 \prod_{m=n+h+1}^{n+k} f(m) \\ &= \left(\prod_{m=1}^{n+h} f(m) \right)^2 \prod_{m=h+1}^{k} f(n+m). \end{aligned}$$

Therefore,

$$\left| \sum_{n=M+1}^{M+N} \left(\frac{F(n+h)F(n+k)}{\ell p} \right) \right| \leq \left| \sum_{n=M+1}^{M+N} \left(\frac{\prod_{m=h+1}^{k} f(n+m)}{\ell p} \right) \right|. \tag{3}$$

We now assume that $H < z$ and eliminate some primes from $\mathcal{L}_z$ as follows. We recall that, by Lemma 6,

$$F_{h,k}(X) = \prod_{m=h+1}^{k} f(X+m) \in \mathbb{Z}[X]$$

has at least one simple root. Write

$$F_{h,k}(X) = g_{h,k}(X)P_{h,k}(X)^2,$$

where $g_{h,k}(X),\ P_{h,k}(X) \in \mathbb{Z}[X]$ and all the roots of $g_{h,k}(X)$ are simple. Then, for $F_{h,k}(X)$ to be a square modulo p (or ℓ), it is necessary that p (or ℓ) divides the discriminant of $g_{h,k}(X)$. To estimate this discriminant, notice that all roots of $g_{h,k}(X)$ are of the form $\alpha - j$ for some root α of $f(X)$ and some $j \in \{h+1,\dots,k\}$. Thus, writing δ for the diameter of the set of roots of $f(X)$, we get that the discriminant of $g_{h,k}(X)$ does not exceed

$$a_0^{HD^2}(\delta+H)^{HD^2} \le (2a_0H)^{HD^2},$$

assuming that $H \ge \delta$, where a_0 is the leading term of $f(X)$. Hence, using the maximal order $O(\log m/\log\log m)$ of the number of distinct prime divisors of the positive integer m, we get that the number of distinct prime factors of the discriminant of $g_{h,k}(X)$ is $O(H)$; of course, this is also true for $H < \delta$.

Summing up over all pairs (h,k) with $H \ge k > h \ge 0$ we get a total of $O(H^3)$ such possible primes. Thus, by Lemma 5, it follows that if we choose

$$H = \lfloor cz^{1/3} \rfloor \tag{4}$$

with a sufficiently small constant c, then, for a sufficiently large z, there are at least a half of the primes $\ell \in \mathcal{L}_z$ for which $F_{h,k}(X)$ is not a perfect square modulo ℓ for any pair (h,k) with $H \ge k > h \ge 0$. Let $\mathcal{R}_z$ be the subset of $\mathcal{L}_z$ made up of such primes and assume that $p,\ell \in \mathcal{R}_z$. Then the product $F_{h,k}(X)$ is not a a perfect square modulo ℓ and p. Thus, Lemma 4 applies to the sum on the right hand side of (3) and leads to the bound:

$$\begin{aligned}\left|\sum_{n=M+1}^{M+N}\left(\frac{F(n+h)F(n+k)}{\ell p}\right)\right| &\ll (k-h)^2\left(\frac{N}{\ell p}+1\right)(\ell p)^{1/2}\log(\ell p)\\ &\ll H^2\left(\frac{N}{z^2}+1\right)z\log z = H^2\left(\frac{N}{z}+z\right)\log z.\end{aligned}$$

Substituting this bound in (2), we derive

$$|W|^2 \le HN^2 + NH^4\left(\frac{N}{z}+z\right)\log z.$$

We now see from (1) that

$$\sum_{n=M+1}^{M+N} \left(\frac{F(n)}{\ell p} \right) \ll NH^{-1/2} + NHz^{-1/2} + N^{1/2}Hz^{1/2} + H.$$

Recalling how we have chosen H, we get

$$\sum_{n=M+1}^{M+N} \left(\frac{F(n)}{\ell p} \right) \ll Nz^{-1/6} + N^{1/2}z^{5/6} + z^{1/3}.$$

We now take $z = N^{1/2}$ and get that

$$\sum_{n=M+1}^{M+N} \left(\frac{F(n)}{\ell p} \right) \ll N^{11/12},$$

thus concluding the proof. □

3 Proof of Theorem 1

Let again $z > 1$ and take $\mathcal{L}_z$ as in Section 2.2 and $\mathcal{R}_z \subset \mathcal{L}_z$ as in Lemma 7.

We note that if $A \geq 1$ is a perfect square not divisible by primes $\ell \in \mathcal{R}_z$, then

$$\sum_{\ell \in \mathcal{R}_z} \left(\frac{A}{\ell} \right) = \#\mathcal{R}_z.$$

For each n counted in $S_d(M, N)$, we see that $dF(n)$ is a perfect square and that $d \mid F(n)$. Hence, since $F(n) \not\equiv 0 \pmod{\ell}$ for any $\ell \in \mathcal{L}_z$,

$$\gcd \left(dF(n), \prod_{\ell \in \mathcal{R}_z} \ell \right) = 1.$$

Thus, for such positive integers n we have

$$\sum_{\ell \in \mathcal{R}_z} \left(\frac{dF(n)}{\ell} \right) = \#\mathcal{R}_z.$$

Therefore,

$$(\#\mathcal{R}_z)^2 S_d(M, N) \ll \sum_{n=M+1}^{M+N} \left(\sum_{\ell \in \mathcal{R}_z} \left(\frac{dF(n)}{\ell} \right) \right)^2.$$

Thus

$$S_d(M,N) \ll (\#\mathcal{R}_z)^{-2} \sum_{n=M+1}^{M+N} \left(\sum_{\ell \in \mathcal{R}_z} \left(\frac{dF(n)}{\ell} \right) \right)^2. \tag{5}$$

Squaring out, changing the order of summation, and separating the "diagonal term" $N\#\mathcal{R}_z$ corresponding to $\ell = p$, we see that

$$\sum_{n=M+1}^{M+N} \left(\sum_{\ell \in \mathcal{R}_z} \left(\frac{dF(n)}{\ell} \right) \right)^2 \le N\#\mathcal{R}_z + \sum_{\substack{\ell,p \in \mathcal{R}_z \\ \ell \neq p}} \left(\frac{d}{\ell p} \right) \sum_{n=M+1}^{M+N} \left(\frac{F(n)}{\ell p} \right). \tag{6}$$

The estimates (5) and (6) yield

$$\begin{aligned} S_d(M,N) &\ll \frac{1}{(\#\mathcal{R}_z)^2} \left(N\#\mathcal{R}_z + \sum_{\substack{\ell,p \in \mathcal{R}_z \\ \ell \neq p}} \left| \sum_{n=M+1}^{M+N} \left(\frac{F(n)}{\ell p} \right) \right| \right) \\ &\ll \frac{N}{\#\mathcal{R}_z} + \frac{1}{(\#\mathcal{R}_z)^2} \sum_{\substack{\ell,p \in \mathcal{R}_z \\ \ell \neq p}} \left| \sum_{n=M+1}^{M+N} \left(\frac{F(n)}{\ell p} \right) \right|. \end{aligned} \tag{7}$$

Choosing $z = N^{1/2}$, we can use Lemma 7 to get that

$$\sum_{\substack{\ell,p \in \mathcal{R}_z \\ \ell \neq p}} \sum_{n=M+1}^{M+N} \left(\frac{F(n)}{\ell p} \right) \ll \#\mathcal{R}_z{}^2 N^{11/12}.$$

Inserting the last estimate into (7) and recalling that $\#\mathcal{R}_z \gg z/\log z$, we conclude the proof.

4 Commments

Clearly the case of products of linear polynomials is not covered by our method. For example, in the case of $f(X) = X + a$, we immediately conclude from the Erdős–Selfridge result [6] that

$$S_d(M,N) = N - \#\{m \ : \ m^2 \in [M+1+a, M+N+a]\} = N + O(N^{1/2})$$

for all $M \geq -a + 1$ and $N \geq 1$. When $f(X) = aX + b$ is still linear but not monic, then it is easy to see that $S_d(M, N)$ is at least the number of primes congruent to b modulo a in the interval $(f(M + 1), f(M + N))$, which is at least $c \geq N/\log N$ for some constant $c > 0$ depending only on a and b, when N is not very small with respect to M (say, $N > M^{c(a)}$ with some constant $c(a) \in (0, 1)$, see for example [1]; when $a = 1$, we can take any $c(1) > 7/12$).

It is also of interest to study the case when $f(X)$ is not irreducible. In this case, it may happen that $f(X)$ has a root modulo p for all primes p although $f(X)$ might not have any linear factors. An example of such a polynomial is $f(X) = (X^2 - 2)(X^2 - 3)(X^2 - 6)$ (se [3] for more examples of such polynomials). Our method is not applicable to such polynomials so one should use different arguments. Finally, if $f(X)$ has only simple roots and factors completely over $\mathbb{Z}$, then one can again bound $S_d(M, N)$ from below by using primes in arithmetic progressions. For some particular cases, say if $f(X)$ is monic and has an even number of linear factors, then one can do better by noting that

$$F(n) = G(n)^2 H(n),$$

where $G(X)$ is some hypergeometric function and $H(X) \in \mathbb{Z}[X]$ is a monic polynomial and so the question of bounding $S_d(M, N)$ reduces to studying the number of distinct fields among $\{\sqrt{H(n)} \; : \; n = N+1, \ldots, N+M\}$ with a polynomial $H(X)$. This problem was treated in [5] and [13].

Acknowledgements

This work was done during a very pleasant visit of F. L. and I. S. to the Universidad Autónoma de Madrid, Spain. During the preparation of this paper, F. L. was supported in part by Grant SEP-CONACyT 46755, I. S. by ARC Grant DP0556431, J. C. by Project MTM2005-04730 from MEC (Spain) and A. Q. by Project MTM2006-10548 from MEC (Spain). Both J. C. and A. Q. were also supported by the joint Madrid Region-UAM project TENU2 (CCG07-UAM/ESP-1814).

References

[1] A. Balog and K. Ono, 'The Chebotarev density theorem in short intervals and some questions of Serre', *J. Number Theory* **91** (2001), 356–371.

[2] C. Ballot and F. Luca, 'Prime factors of $a^{f(n)} - 1$ with an irreducible polynomial $f(x)$', *New York J. Math.*, **12** (2006), 39–45.

[3] D. Berend and Yu. Bilu, ' Polynomials with roots modulo every integer', *Proc. Amer. Math. Soc.* **124** (1996), 1663–1671.

[4] J. Cilleruelo, 'Squares in $(1^2+1)\cdots(n^2+1)$', *J. Number Theory* (to appear).

[5] P. Cutter, A. Granville and T. J. Tucker, 'The number of fields generated by the square root of values of a given polynomial', *Canad. Math. Bull.*, **46** (2003), 71–79.

[6] P. Erdős, J. L. Selfridge, 'The product of consecutive integers is never a power,' *Illinois J. Math.* **19** (1975), 292–301.

[7] M. Z. Garaev, F. Luca and I. E. Shparlinski, 'Character sums and congruences with $n!$', *Trans. Amer. Math. Soc.*, **356** (2004), 5089–5102.

[8] M. Z. Garaev, F. Luca and I. E. Shparlinski, 'Catalan and Apéry numbers in residue classes', *J. Combin. Theory, Ser. A*, **113** (2006), 851–865.

[9] M. Z. Garaev, F. Luca, I. E. Shparlinski and A. Winterhof, 'On the lower bound of the linear complexity over $\mathbb{F}_p$ of Sidelnikov sequences', *IEEE Trans. on Inform. Theory*, **52** (2006), 3299–3304.

[10] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004.

[11] F. Luca and I. E. Shparlinski, 'Discriminants of complex multiplication fields of elliptic curves over finite fields', *Canad. Math. Bull.* **50** (2007), 409–417.

[12] F. Luca and I. E. Shparlinski, 'Quadratic fields fenerated by the Shanks sequence', *Proc. Edinb. Math. Soc.*, (to appear).

[13] F. Luca and I. E. Shparlinski, Quadratic fields generated by polynomials', *Preprint*, 2007.