Smooth evaluations of cyclotomic quadratics

Bruno Sterner

Department of Combinatorics & Optimization
University of Waterloo, Waterloo, Canada

Abstract. In this note we find large primes p such that $\Phi_k(p)$ is B-smooth for the cyclotomic polynomials Φ_k, with $k = 3, 4$ and 6, and a sufficiently small smoothness bound B. These primes hence provide the first instantiation of integer factoring challenges that, a priori would be difficult to factor with traditional algorithms but, are actually easy to factor with algorithms not typically used in practice.

Keywords: Smooth integers · cyclotomic polynomials · integer factorisation

1 Introduction

Integer factorisation has been a central theme in modern computational number theory through its significant role in cryptography [RSA78]. As a result there are numerous algorithms to factor integers including: deterministic exponential [Cop97, Har21]; provable subexponential [LP92]; heuristic subexponential [LL93]; and quantum polynomial [Sho94] time algorithms. Throughout this article N will denote a target integer that one would like to factor.

Other algorithms successfully factor an integer depending on certain smoothness properties related to its prime factors. This most notably includes Pollard's $(p-1)$-method [Pol74] which outputs a prime factor p of N at least when $p-1$ is B-smooth[1] for an input smoothness bound B. By B-smooth we mean that every prime factor is at most B. Several generalisations of this exist which require other smoothness properties. The most well-known of these is Williams $(p+1)$-method [Wil82]. Known to a lesser extent are further generalisations [BS89] whose success depends on smoothness evaluations of cyclotomic polynomials Φ_k. For instance, for $k = 3$, one successfully factors a target integer if it has a factor p for which $\Phi_3(p) = p^2 + p + 1$ is B-smooth. In this article, we exclusively restrict to $k \in \{3, 4, 6\}$ where Φ_k are all irreducible quadratics.

The extensive theory on smooth integers (see [Gra08] for a survey) indicates that, for random target integers with large prime factors, one is typically unlikely to factor the integer in this manner. However there are counterexamples where factoring with one of these algorithms is practical. For the $(p\pm1)$-methods, constructing such counterexamples is very elementary, but for the Φ_k generalisations constructing large enough counterexamples is less elementary. This has been explored by several authors [Luc04, CH21] in the case when $k = 4$. The largest integer n with a smooth $\Phi_4(n) = n^2 + 1$ has 73-bits. Among those with a prime n, the largest found has 67-bits. This is small enough so that established and commonly used factoring algorithms, such as the elliptic curve method [Len87], can easily factor such target integers. Even with an optimised implementation similar in nature to [BSC+23] one will struggle to find large enough primes to serve as suitable counterexamples.

E-mail: bsterner@uwaterloo.ca (Bruno Sterner)

[1] Technically the correct condition is actually when $p-1$ is B-powersmooth since size of the prime powers also influences the algorithms performance. However all smooth integers in this work are inherently be powersmooth so we will just use the term smooth integers in this work.

Contributions

In this article we construct such large counterexamples. These primes will be large enough so that state-of-the-art factoring algorithms cannot such factor target integers. To find these primes, we follow a line of work [CMN21, Ste25] and construct irreducible polynomials $P \in \mathbb{Q}[x]$ such that $\Phi_k(P)$ splits into at most quadratic factors (linear factors are not possible since Φ_k is itself irreducible). In this manner we split up the smoothness task and instead of hoping that all of $\Phi_k(p)$ is smooth, we combine a small collection of quadratic evaluations and hope they are all smooth. Additionally the irreducibility of P ensures that if an evaluation of P is an integer then it could potentially be prime.

We outline the strategy to find these primes given such polynomials P. Write $n = \deg(P)$ and $Q_0, \cdots, Q_j$ for the quadratic factors in $\Phi_k(P)$ (fixing $k = 3, 4, 6$ forces $j < n$). Adopting a polynomial version of the sieve of eratothenes (see [CP05, §3.2.6]), one identify integers m in some interval such that $Q_i(m)$ is B-smooth for either all or a large proportion of factors Q_i. If this is only done for a large proportion of factors Q_i, then one brute-forces the remaining factors to ensure they are also smooth. For each integer m that is identified for all factors Q_i, we check whether $p = P(m)$ is firstly an integer; and followed by whether it is prime. Moreover one can check whether $p = P(m)$ is an integer before doing the brute force checks, which eliminates doing unnecessary brute force smoothness checks.

The polynomial degree introduces a tradeoff between the sizes of the resulting primes that can be practically found and the smoothness bound in $\Phi_k(p)$. We illustrate this with three primes that we found in this manner.

Example 1. Let $P(x) = 4x^3 + 6x^2 + 5x + 1$ and $k = 3$ (i.e. with $\Phi_k(x) = x^2 + x + 1$). We note that

$$\Phi_3(P(x)) = (x^2 + x + 1) \cdot (4x^2 + 2x + 1) \cdot (4x^2 + 6x + 3) = Q_0(x) \cdot Q_1(x) \cdot Q_2(x).$$

We sieved the interval $m \in [2^{41}, 2^{42}]$ and identified the integer $m = 2511499194712$ where $p = P(m)$ is a 126-bit prime and $\Phi_3(p) = p^2 + p + 1$ is 51169-smooth. More precisely we sieved for smoothness on the factors Q_0, Q_1 and brute-forced the smoothness check on Q_2 for the identified integers. This prime has the smoothest $\Phi_3(p)$ among the primes derived from this polynomial and interval.

$$\begin{aligned}\Phi_3(p) = 3 \cdot 7^3 \cdot 13 \cdot 37 \cdot 43 \cdot 61 \cdot 109 \cdot 139 \cdot 181^2 \cdot 223 \cdot 373 \cdot 727 \cdot 859 \cdot 1063 \cdot 1117 \cdot 1291 \\ \cdot 1423 \cdot 12073 \cdot 14887 \cdot 19051 \cdot 20011 \cdot 20269 \cdot 20947 \cdot 36943 \cdot 51169.\end{aligned}$$

Example 2. Let $P(x) = (2x^4 + 4x^3 + 3x^2 + x + 15)/15$ and $k = 4$ ($\Phi_k(x) = x^2 + 1$) with

$$\Phi_4(P(x)) = \frac{1}{15^2}\Big[(x^2 + 1) \cdot (x^2 + 6x + 10) \cdot (2x^2 + 2x + 5) \cdot (2x^2 + 10x + 17)\Big].$$

We sieved a shorter interval $[2^{37}, 2^{38}]$ and found a 150-bit prime $p = P(m)$ with $m = 273812471165$ for which $\Phi_4(p) = p^2 + 1$ is 564401-smooth. Finding such a large prime from the degree 3 polynomials would require sieving a much larger interval, say $[2^{47}, 2^{48}]$, and hence require a greater computational effort to find them. We note however that one should be able to finding smoother instances, compared to the one provided, from such a search.

$$\begin{aligned}\Phi_4(p) = 2 \cdot 5^2 \cdot 17 \cdot 29 \cdot 41 \cdot 73 \cdot 113^2 \cdot 149 \cdot 157 \cdot 173 \cdot 293 \cdot 1021 \cdot 1093 \cdot 1721 \cdot 4517 \\ \cdot 4789 \cdot 5189 \cdot 6073 \cdot 12097 \cdot 12953 \cdot 18481 \cdot 50033 \cdot 146989 \cdot 256093 \\ \cdot 288661 \cdot 432241 \cdot 564401.\end{aligned}$$

Example 3. The polynomial $P(x) = (16x^6+48x^5+172x^4+264x^3+379x^2+255x-84)/210$ has 6 quadratic factors in $\Phi_3(P(x))$. Sieving an even shorter interval produces the following 182-bit prime $p = P(m)$ with $m = 1877115093$ and

$$\begin{aligned}\Phi_3(p) = 7 \cdot 19^2 \cdot 43 \cdot 199 \cdot 379 \cdot 457 \cdot 991 \cdot 2539 \cdot 3253 \cdot 4549 \cdot 5527 \cdot 8017 \cdot 8053 \\ \cdot 12553 \cdot 15511 \cdot 18433 \cdot 20641 \cdot 26881 \cdot 64231 \cdot 75967 \cdot 284413 \\ \cdot 361321 \cdot 403369 \cdot 475837 \cdot 824779 \cdot 1058149 \cdot 1334743.\end{aligned}$$

Remark 1. One can have repeated quadratic factors in $\Phi_k(P)$. Take for instance the polynomials $P_\pm(x) = (x^4 \pm x^3 + 1176x^2 \pm 1764x + 329280)/32928$ with $(x^2 + 588)^2 \mid \Phi_3(P_\pm(x))$. Such polynomials could lead to primes with a smaller smoothness bound in $\Phi_k(p)$ (as there are fewer smoothness requirements). However such primes would not guarantee better factoring counterexamples since the induced square factor likely necessitates a larger "powersmooth" input to the factoring algorithm.

Remark 2. Not all polynomials P for which $\Phi_k(P)$ splits completely into quadratics can guarantee integer evaluations. Take for instance $P(x) = (x^6 - 37)/360$ which has 6 quadratic factors in $\Phi_3(P)$. One can easily check that $360 \nmid m^6 - 37$ for each residue classes modulo 360 – so this polynomial cannot give sought after primes.

Technical overview

We highlight the strategy that is employed to obtain these polynomials. We adopt the idea from [Ste25] and work with polynomial rings over rational function fields. One starts with a general description of a polynomial $P(x) = (x^n + a_{n-1}x^{n-1} + \cdots + a_0)/C \in K[x]$ with coefficients in the rational function field $K = \mathbb{Q}(a_0, a_1, \cdots, a_{n-1}, C)$. Then impose dependencies on these coefficients so that $\Phi_k(P)$ has factors. One such dependency is that a quadratic polynomial $(x^2 + ax + b)$ is a factor of $\Phi_k(P)$, where a, b are new variables that are appended to K and now treat the polynomials with coefficients in the field extension $K' = K(a, b)$. Then one computes $\Phi_k(P) \mod (x^2 + ax + b) \in K'[x]$ to get a linear polynomial. If the coefficients of this linear polynomial are 0 then this quadratic is a factor of $\Phi_k(P)$. This gives two dependences on the variables for factorability of $\Phi_k(P)$. We then repeat this strategy with another quadratic factor and introduce more dependences on other variables.

When $\deg(P) \in \{2, 3, 4\}$, one can easily repeat this strategy to obtain complete parameterisations of polynomials for which $\Phi_k(P)$ splits completely into quadratics. For the degree 4 polynomials the strategy to get parameterisations is slightly different and the obtained parameterisation is symmetrically complete (i.e. parameterisations P such that $P(-x) = P(x)$). For the larger degree polynomials, $\deg(P) \geq 5$, the continued repetition of this strategy introduces obstructions to obtaining completely split Φ_k. These obstructions boil down to solving large degree diophantine equations with potentially many variables, which are notoriously challenging to solve.

To obtain the large degree polynomials we start with a parameterisation that features sufficiently many quadratic factors before the obstructions come in. Then one does a search with the remaining variables to see when the non-factored polynomial splits completely into quadratic factors after variable evaluation. To illustrate this for the degree 5 polynomials (see §2.3 for more concrete details), one can obtain a parameterisation in 6 variables of polynomials P such that $\Phi_k(P)$ factors into two quadratics and one sextic. Then one sees which inputs to the 6 variables results in the sextic factoring into 3 quadratic factors. This strategy significantly improves the straightforward and naive strategy to search for these polynomials as one can reduce the variable search space. For example take $P(x) = (x^5 + 2x^4 - 3x^3 - 34x^2 + 74x + 60)/300$ for which $\Phi_4(P)$ has 5 quadratic factors. Searching for it naively requires a variable range $|a_i|, C \leq 300$ but this improved strategy minimises the variable range to be ≤ 3 in absolute value.

As highlighted previously for the degree 4 polynomials, one can impose symmetry to the parameterised polynomials to expedite the searching. For the degree 6 polynomials for instance, one can obtain parameterised polynomials P with $P(-x) = P(x)$ and where $\Phi_k(P)$ factors into 4 quadratic and 1 quartic. This does not give a completely split parameterisation but the factorisation is good enough to find many polynomials after searching. This idea further allows us to find suitable degree 8 polynomials in a reasonable amount of time – which would have been beyond computational scope with the initial approach. We remark that imposing symmetry on the odd degree polynomials is not as fruitful for these applications. The natural symmetry that one could impose, i.e. $P(-x) = -P(x)$, implies that $x \mid P(x)$ and so P is not irreducible.

Remark 3. Parameterisations for $k = 3$ are identical to those with $k = 6$ up to a change of sign (i.e. $\Phi_3(P)$ splits completely into quadratic factors $\Leftrightarrow \Phi_6(-P)$ splits completely). So our focus is on deriving parameterisations and polynomials for $k \in \{3, 4\}$. Moreover for the odd degree polynomials one can set $P'(x) = -P(-x)$ and the positivity of the leading coefficient is preserved. For instance, $P(x) = 4x^3 + 6x^2 + 5x + 1$ suitable for $k = 3$ from Example 1 gives the polynomial $P'(x) = 4x^3 - 6x^2 + 5x - 1$ suitable for $k = 6$.

Roadmap

This work is organised as follows. Firstly we discuss the prime degree search in Section 2 and either obtain parameterisations or present searching strategies to find such polynomials. We follow this in Section 3 with the composite even degree search where we exploit the symmetries highlighted earlier. Finally in Section 4 and showcase our experimental results with these polynomials. This includes more primes that we found as well as some discussion on the practicability of factoring integers with these primes as factors.

Acknowledgements

The author would like to thank Wouter Castryck for bringing this problem and application to our attention which inspired this note. The author was supported by the NSERC Alliance Consortia Quantum Grant "Accelerating the transition to quantum-resistant cryptography" (ALLRP 578463–2022), and the NSERC Discovery Grant program[2].

2 Prime degree polynomials

2.1 Degree 2 polynomials

We start by providing parameterisations for the degree 2 polynomials P. We give details of their derivation for the $k = 4$ setting and the factorisation of $\Phi_4(P)$ is stated in Equation (1). The $k = 3$ parameterisation is derived in an analogous manner and its factorisation is stated in Equation (2).

Start with a polynomial $P(x) = (x^2 + ax + a_1)/C \in \mathbb{Q}(a, a_1, C, b, c)$ and suppose that $\Phi_4(P(x)) = P(x)^2 + 1$ has a quadratic factor $(x^2 + bx + c)$. Then the coefficients of the linear polynomial $P(x)^2 + 1 \mod (x^2 + bx + c)$ are 0; from which we get the following relations:

$$(a - b) \cdot (ab - 2a_1 - b^2 + 2c) = 0, \text{ and}$$
$$a^2c - 2abc - a_1^2 + 2a_1c - C^2 + b^2c - c^2 = 0.$$

We cannot have $a = b$ since the second relation then reduces to $a_1^2 - 2a_1c + C^2 + c^2$ and $\mathsf{Disc}(x^2 - 2xc + C^2 + c^2) = -4C^2$ is always negative. So the first relation gives us

[2] See https://nserc-crsng.canada.ca/en/funding-opportunity/archived-alliance-consortia-quantum-grants-call-proposals-supporting

$a_1 = (ab - b^2 + 2c)/2$ and the second relation now becomes

$$a^2b^2 - 4a^2c - 2ab^3 + 8abc + 4C^2 + b^4 - 4b^2c = 0.$$

By another discriminant calculation, we can replace $c \mapsto (b^2 + c^2)/4$ and this now becomes

$$(ac - 2C - bc) \cdot (ac + 2C - bc) = 0,$$

from which we one of these choices for C and get $a_1 = (2ab - b^2 + c^2)/4$ and $C = (ac - bc)/2$. These expressions for a_1 and C in terms of a, b, c gives the desired reducibility of $\Phi_4(P(x)) = P(x)^2 + 1$. One can get the integral representation of these polynomials (i.e. $a_1, C \in \mathbb{Z}[a, b, c]$) by replacing $b \mapsto 2b$ and $c \mapsto 2c$ (ensuring that $(b^2 + c^2)/4 \in \mathbb{Z}$). With a minor cleaning step by replacing $a \mapsto a + b$, we put all of this and get the $k = 4$ parameterisation as $P(x) \coloneqq (x^2 + (a + b)x + (ab + c^2))/(ac - bc)$ where

$$\Phi_4(P(x)) = \frac{1}{(ac - bc)^2}\Big[(x^2 + 2bx + (b^2 + c^2)) \cdot (x^2 + 2ax + (a^2 + c^2))\Big]. \tag{1}$$

The derivation for the $k = 3$ parameterisation can be done in a very similar manner and is given by $P(x) \coloneqq (x^2 + (a + b + c)x + (ab + ac + c^2))/(bc - ac)$ where

$$\begin{aligned}\Phi_3(P(x)) = \frac{1}{(bc - ac)^2}\Big[&(x^2 + (2b + c)x + (b^2 + bc + c^2)) \\ &\cdot (x^2 + (2a + c)x + (a^2 + ac + c^2))\Big].\end{aligned} \tag{2}$$

2.2 Degree 3 polynomials

Next we discuss the degree 3 parameterisation for $k = 3, 4$. Like previously, we detail the derivation for the $k = 4$ parameterisation, giving its factorisation in Equation (3), and state the $k = 3$ parameterisation, giving its factorisation in Equation (4).

We start in the same manner as we did in §2.1: impose a quadratic factor on $\Phi_4(P)$ for a general cubic P and determine dependencies on the coefficients of this cubic. From this we get a polynomial $P(x) = (x^3 + a_0x^2 + a_1x + a_2)/C \in \mathbb{Q}(a_0, a_1, b, c)[x]$ where $a_2 = a_0(-b^2 + c^2) + b(a_1 + b^2 - 3c^2)$ and $C = c(2a_0b - a_1 - 3b^2 + c^2)$. Now $\Phi_4(P)$ factors into one quadratic and one quartic:

$$\begin{aligned}\Phi_4(P(x)) = \frac{1}{C^2}\Big[&(x^2 + 2bx + b^2 + c^2) \cdot (x^4 + 2(a_0 - b)x^3 + ((a_0 - b)(a_0 - 3b) + 2a_1 - c^2)x^2 \\ &+ 2(-a_0^2b + a_0a_1 + 2a_0b^2 - a_1b - b(b^2 - c^2))x \\ &+ (a_0b - a_1)^2 + a_0^2c^2 + (b^2 + c^2 - 2a_0b)(b^2 + c^2) + 2a_1(b^2 - c^2))\Big].\end{aligned}$$

We repeat this strategy again for this quartic factor: impose a quadratic factor on this quartic and determine more dependencies on the remaining variables. From this we get $a_0 = (ac - 2ad + 2bc - db)/(c - d)$ and $a_1 = [(c - d)(2ab + c^2 - cd + d^2) - (a^2d - b^2c)]/(c - d)$. Making this integral and removing the $(c - d)$ in the denominator amounts knowing when $(ad - bc)/(c - d) \in \mathbb{Z}$. This is trivially the case when $d = c \pm 1$ (as well as some other strict conditions) but there is no known single global constraint on the variables to guarantee this.

As a result we clear this $(c - d)$ from the denominator of these expressions and provide the following complete description of degree 3 polynomials P for $k = 4$. This

parameterisation is given by $P = ((c-d)x^3 + a_0x^2 + a_1x + a_2)/C$ where

$$\begin{aligned} a_0 &= (a+b)(c-d) - (ad-bc), \\ a_1 &= (c-d)(ab + c^2 - cd + d^2) - (a+b)(ad-bc), \\ a_2 &= (ac-bd)(c-d)^2 - (ab+cd)(ad-bc), \text{ and} \\ C &= -cd\Big[(a-b)^2 + (c-d)^2\Big], \end{aligned}$$

giving three irreducible quadratics in $\Phi_4(P(x)) = P(x)^2 + 1$:

$$\begin{aligned} \Phi_4(P) = \frac{1}{C^2}\Big[&(x^2 + 2bx + b^2 + c^2)\cdot(x^2 + 2ax + a^2 + d^2) \\ &\cdot\Big((c-d)^2x^2 - 2(ad-bc)(c-d)x + ((ad-bc)^2 + (c-d)^4)\Big)\Big]. \end{aligned} \tag{3}$$

The parameterisation for $k = 3$ is given by $P = ((c-d)x^3 + a_0x^2 + a_1x + a_2)/C$ where

$$\begin{aligned} a_0 &= (b+c)^2 - (a+d)^2 + a(a+c) - b(b+d), \\ a_1 &= \Big[(c-d)\Big(c^2 + d^2 - a^2 + d(a+b)\Big) + (ac - 2ad + bc)(a+b+c)\Big], \\ a_2 &= \Big[a\Big((b+c)(c(b+c) - d(a+d)) + c(bd - bc - cd)\Big) + d^2(bc + (c-d)(b+c))\Big], \text{ and} \\ C &= cd\Big[(a-b)^2 - (a-b)(c-d) + (c-d)^2\Big], \end{aligned}$$

giving three irreducible quadratics in $\Phi_3(P(x)) = P(x)^2 + P(x) + 1$:

$$\begin{aligned} \Phi_3(P) = \frac{1}{C^2}\Big[&(x^2 + (2a+d)x + a^2 + ad + d^2)\cdot(x^2 + (2b+c)x + b^2 + bc + c^2) \\ &\cdot\Big((d-c)^2x^2 + (d-c)(2ad + d^2 - 2bc - c^2)x \\ &+ (ad-bc)(ad - bc + d^2 - c^2) + (d-c)^2(c^2 - cd + d^2)\Big)\Big]. \end{aligned} \tag{4}$$

Example 4. The polynomial used in Example 1 can be obtained from this $k = 3$ parameterisation in Equation (4). Choosing $a = 1$, $b = 0$, $c = 2$ and $d = 1$ gives the polynomial $P'(x) = (x^3 + 3x^2 + 5x + 2)/2$ and P' takes on integer evaluations only when x is even – giving $P(x) = P'(2x) = 4x^3 + 6x^2 + 5x + 1$. Alternatively one can get P directly by choosing rationals instead of integers, i.e. $a = 1/2$, $b = 0$, $c = 1$ and $d = 1/2$.

2.3 Degree 5 polynomials

Adopting the same strategy as we did in §2.2 to find the degree 3 polynomials, one can obtain computable polynomials of the form $P(x) = ((b-d)x^5 + (b-d)a_0x^4 + (b-d)a_1x^3 + a_2x^2 + a_3x + a_4)/C \in \mathbb{Q}(a_0, a_1, a, b, c, d)[x]$ such that $\Phi_k(P)$ splits into 2 quadratics and 1 sextic.

Continuing this procedure a third time introduces an obstruction to finding explicit variable conditions to reduce the sextic into one further quadratic. For the prior iterations this was easily hurdle through a straightforward discriminant calculation but this time the discriminant calculation induces a diophantine equation which is highly non-trivial to solve. Under certain well-chosen dependencies on the shape of the quadratic factors, solving this diophantine equation becomes manageable. For instance, and somewhat surprisingly,

imposing the third quadratic factor be a repeated factor from one of the previous two iterations allows us to reduce the sextic.

One can still find polynomials $P \in \mathbb{Q}[x]$ with a completely split $\Phi_k(P)$ by taking the parameterised polynomial in $\mathbb{Q}(a_0, a_1, a, b, c, d)[x]$ and doing a search on the variables a_0, a_1, a, b, c, d. We applied this strategy with a narrow searching interval (i.e. $|a_0|, |a_1|, |a|, |b|, |c|, |d| \leq 15$) and record the polynomials with notably small denominators.

For polynomials P with 5 quadratic factors in $\Phi_3(P(x)) = P(x)^2 + P(x) + 1$ we record the following:

$$\begin{aligned}
P(x) &= (256x^5 + 640x^4 + 816x^3 + 584x^2 + 221x + 24)/21;\\
P(x) &= (256x^5 + 640x^4 + 816x^3 + 584x^2 + 221x + 24)/21;\\
P(x) &= (9x^5 - 12x^3 + 21x^2 + 16x - 28)/28;\\
P(x) &= (256x^5 + 144x^3 - 112x^2 + 81x - 63)/63;\\
P(x) &= (256x^5 + 640x^4 + 432x^3 + 8x^2 - 103x - 168)/273.
\end{aligned}$$

For polynomials P with 5 quadratic factors in $\Phi_4(P(x)) = P(x)^2 + 1$ we record the following:

$$\begin{aligned}
P(x) &= (10368x^5 + 22464x^4 + 21816x^3 + 11172x^2 + 3037x + 335)/25;\\
P(x) &= (10368x^5 + 29376x^4 + 35640x^3 + 23172x^2 + 8125x + 1250)/25;\\
P(x) &= (162x^5 + 162x^4 + 27x^3 - 108x^2 + 35x + 50)/50;\\
P(x) &= (162x^5 + 648x^4 + 999x^3 + 837x^2 + 494x + 120)/50;\\
P(x) &= (81x^5 + 54x^4 - 27x^3 - 102x^2 + 74x + 20)/100;\\
P(x) &= (81x^5 + 351x^4 + 567x^3 + 507x^2 + 386x + 156)/100;\\
P(x) &= (19208x^5 + 30184x^4 + 21462x^3 + 10094x^2 + 3515x + 637)/325;\\
P(x) &= (19208x^5 + 65856x^4 + 92806x^3 + 65268x^2 + 23017x + 3270)/325;\\
P(x) &= (82944x^5 + 110592x^4 + 55296x^3 + 16032x^2 + 4145x + 416)/325;\\
P(x) &= (82944x^5 + 304128x^4 + 442368x^3 + 315744x^2 + 110321x + 15345)/325;\\
P(x) &= (8x^5 + 24x^4 + 22x^3 - 126x^2 - 185x + 357)/425;\\
P(x) &= (8x^5 + 16x^4 + 6x^3 + 128x^2 + 77x - 410)/425;\\
P(x) &= (8x^5 + 6x^3 - 252x^2 + 241x - 78)/975;\\
P(x) &= (8x^5 + 6x^3 + 252x^2 + 241x + 78)/975.
\end{aligned}$$

3 Composite even degree polynomials

3.1 Degree 4 polynomials

The same issue arises for obtaining parameterisations of the degree 4 (and larger) polynomials as it did for the degree 5 polynomials. More precisely doing the degree 3 strategy from §2.2 starting from a degree 4 polynomial P, one gets a parameterisation such that $\Phi_k(P)$ splits into 2 quadratics and 1 quartic. Then working out general conditions for the reducibility of the quartic requires the resolution of a non-trivial diophantine equation.

We can however exploit the compositeness of this degree to find a sufficient large parameterisation of polynomials. The idea is to start with the degree 2 parameterisations in §2.1 and replace $x \mapsto x^2 + dx + e$. This gives degree 4 polynomials P such that $\Phi_k(P)$ splits into two quartics. Moreover, by this transformation, such polynomials are symmetric in the sense that $P(x) = P(-d - x)$. Then we apply the same strategy as we did before from this parameterisation. From this we get a symmetrically complete parameterisation of degree 4 polynomials.

It is sufficient to only consider the replacement $x \mapsto x^2$ instead of the more general $x \mapsto x^2 + dx + e$. Firstly, by linear transformations both prior and after the replacement, one can reduce the general expression to either $x \mapsto x^2$ or $x \mapsto x^2 + x$. For a polynomial Q, let $P'(x) = Q(x^2 + x)$, $Q'(x) = Q((x - 1)/4)$ and $\hat{P}(x) = Q'(x^2)$. A straightforward

calculation verifies that $\hat{P}(2x+1) = P'(x)$ – so a $x \mapsto x^2 + x$ replacement is a special case of a $x \mapsto x^2$ replacement. As a result all parameterised polynomials in this section will be even, i.e. $P(x) = P(-x)$.

We now go through the concrete details to derive these symmetrically complete parameterisations for degree 4 polynomials. As we did previously we provide the details for the derivation of the $k = 4$ parameterisation (given in Equation (5)) and the $k = 3$ can be derived analogously (given in Equation (6)).

Start with the parameterisation in Equation (1) and replace $x \mapsto x^2$. This gives the parameterised polynomial $P(x) = (x^4 + (a_0 + a_1)x^2 + (a_0a_1 + a_2^2))/(a_2a_0 - a_2a_1)) \in \mathbb{Q}(a_0, a_1, a_2, a, b, c, d)[x]$. This has 2 quartic factors in $\Phi_4(P)$ but we impose that a quadratic $(x^2 + 2a + (a^2 + b^2))$ is a factor. We proceed similarly and produce dependencies for this factorability. In particular, one obtains $a_0 = a_1 - a^2 - b^2$ and $a_2 = 2ab$. This gives a parameterised polynomial with 2 quadratics and 1 quartic in $\Phi_4(P)$. Repeating the same strategy again and imposing another quadratic factor $(x^2 + 2c + (c^2 + d^2))$ on the other quartic gives the dependencies $a_1 = b^2 - (cd/b)^2$ and $a = -cd/b$.

Putting everything together, letting $C = 2cd(b^2 - d^2)(b^2 + c^2)$, we get the following parameterisation

$$P(x) = \frac{1}{C}\left[b^2x^4 + (b^2 - c^2)(b^2 + d^2)x^2 - \Big(b^2(c - d) - cd(c + d)\Big)\Big(b^2(c + d) + cd(c - d)\Big)\right],$$

such that $\Phi_4(P)$ splits completely into quadratic factors:

$$\begin{aligned}\Phi_4(P) = \frac{1}{C^2}\Big[&(x^2 - 2cx + c^2 + d^2) \cdot (x^2 + 2cx + c^2 + d^2) \\ &\cdot (b^2x^2 - 2bcdx + (b^4 + c^2d^2)) \cdot (b^2x^2 + 2bcdx + (b^4 + c^2d^2))\Big].\end{aligned} \tag{5}$$

Example 5. For instance, $b = 3$, $c = 3$ and $d = 2$ gives $P'(x) = (x^4 + 119)/120$. P' only has integer evaluations when x is odd. This yields the polynomial $P(x) = P'(2x + 1) = (2x^4+4x^3+3x^2+x+15)/15$ used in Example 2. Note that this is consistent with discussion mentioned at the start of the section since $P(x) = Q(x^2+x)$ where $Q(x) = (2x^2+x+15)/15$.

Replicating this to get for the $k = 3$ setting, one gets the following parameterisation

$$\begin{aligned}P(x) = \frac{1}{C}\Big[&c^2x^4 + (c^2 - 2cd + 2d^2)\Big(c(c - 2b + 2d) - 2(b - d)^2\Big)x^2 \\ &+ \Big((c - 2d)(b^2 + bc + c^2) + 2bd^2\Big) \cdot \Big((c - 2d)(b + c - 2d)^2 - b(c^2 + 2cd - 2d^2)\Big)\Big],\end{aligned}$$

where $C = 4d(c - 2d)(c - d)(2b + c - 2d)(b^2 + bc + c^2 - 2bd - cd + d^2)$, such that $\Phi_3(P)$ splits completely into quadratic factors:

$$\begin{aligned}\Phi_3(P(x)) = \frac{1}{C^2}\Big[&(x^2 - (2b + c - 2d)x + (b - d)^2 + bc + (c - d)(c - 3d)) \\ &\cdot (x^2 + (2b + c - 2d)x + (b - d)^2 + bc + (c - d)(c - 3d)) \\ &\cdot (c^2x^2 - c(c - 2d)(2b + c - 2d)x + D) \\ &\cdot (c^2x^2 + c(c - 2d)(2b + c - 2d)x + D)\Big],\end{aligned} \tag{6}$$

where $D = \Big((c - 2d)^2(2b + c - 2d)^2 + 3c^4\Big)/4$.

3.2 Degree 6 polynomials

Repeating this using the degree 3 parmeterisations and replacing $x \mapsto x^2$, gives parameterisations of degree 6 polynomials such that $\Phi_k(P)$ splits into 4 quadratics and 1 quartic. For $k = 4$, the parameterisation is given by $P(x) = ((ab - cd)x^6 + a_0x^4 + a_1x^2 + a_2)/C \in \mathbb{Q}(a, b, c, d)[x]$ where

$$\begin{aligned}
a_0 &= (ab - cd)(a^2 - b^2 + 2c^2 - 2d^2) + ab(a^2 - b^2 - c^2 + d^2),\\
a_1 &= (ab - cd)\Big((a^2 + b^2 + c^2 + d^2)^2 - 4(b^2c^2 + a^2d^2) - 4abcd\Big)\\
&\quad + cd(a^2 - b^2)^2 - ab(c^2 - d^2)^2,\\
a_2 &= ab(c^2 - d^2)(a^2 + b^2) - cd(a^2 - b^2)(c^2 + d^2)^2 + 8abcd(ac + bd)(ad - bc),\\
C &= 2abcd\Big(4(ac - bd)^2 - (a^2 + b^2 + c^2 + d^2)^2\Big).
\end{aligned}$$

For $k = 3$, the parameterisation is given by $P(x) = ((2(ab - cd) + b^2 - d^2)x^6 + a_0x^4 + a_1x^2 + a_2)/C \in \mathbb{Q}(a, b, c, d)[x]$ where

$$\begin{aligned}
a_0 &= (a^2 - b^2)(a^2 - b^2 + 2cd + d^2) - (c^2 - d^2)(2ab + b^2 + c^2 - d^2)\\
&\quad + c^2(c + 2d)^2 - a^2(a + 2b)^2,\\
a_1 &= \Big(2(ab - cd) + b^2 - d^2\Big)\Big(d^2(2c + d)^2 - (a^2 - b^2)^2 + b(2a + b)(a^2 + 2ab + c^2 - d^2)\Big)\\
&\quad - \Big(d(2c + d)(a^2 - b^2 + c^2 - d^2) - 2b(2a + b)(a^2 - b^2)\Big)\Big(a^2 - b^2 + c^2 + 2cd\Big),\\
a_2 &= (a^2 - b^2)\Big[(c^2 + 2cd)\Big(cd(2c + d)(c + 2d) - ab(2a + b)(a + 2b)\Big)\\
&\quad + d(2c + d)\Big((b(2a + b) - d(2c + d))(c^2 - d^2) - bd(2c + d)(2a + b)\Big)\Big]\\
&\quad + b^2(2a + b)^2\Big[d(2c + d)(c^2 - d^2) - c(c + 2d)(2(ab - cd) + b^2 - d^2)\Big]\\
C &= bd(2a + b)(2c + d)\Big((a - c)^2 + (a - c)(b - d) + (b - d)^2\Big)\\
&\quad \Big((a + c)^2 + (a + c)(b + d) + (b + d)^2\Big).
\end{aligned}$$

Repeating this one more time to reduce the final quartic, we encounter a similar challenge as we saw previously – namely the criterion for reducibility requires solving a highly non-trivial diophantine equation. So we go through the variable searching route to find polynomials over $\mathbb{Q}$ that split completely into quadratics and record the polynomials with the notably small denominators.

For polynomials P with 6 quadratic factors in $\Phi_4(P(x)) = P(x)^2 + 1$ we record the following:

$$\begin{aligned}
P(x) &= (162x^6 + 486x^5 + 891x^4 + 972x^3 + 41x^2 - 364x - 688)/850;\\
P(x) &= (324x^6 + 972x^5 + 648x^4 - 324x^3 - 1619x^2 - 1295x + 850)/1700;\\
P(x) &= (8x^6 + 24x^5 - 26x^4 - 92x^3 + 659x^2 + 709x - 1482)/1950;\\
P(x) &= (x^6 + 56x^4 + 1039x^2 + 3584)/7800;\\
P(x) &= (64x^6 + 192x^5 + 1696x^4 + 3072x^3 + 10525x^2 + 9021x + 4005)/9225;\\
P(x) &= (x^6 + 3x^5 + 69x^4 + 133x^3 + 1980x^2 + 1914x + 49000)/18200;\\
P(x) &= (648x^6 + 1944x^5 - 2106x^4 - 7452x^3 + 9179x^2 + 13229x + 1508)/18850;\\
P(x) &= (2x^6 + 6x^5 + 39x^4 + 68x^3 + 3613x^2 + 3580x + 23400)/29250;\\
P(x) &= (x^6 + 14x^4 + 49x^2 + 14336)/31200;\\
P(x) &= (8x^6 + 24x^5 + 70x^4 + 100x^3 + 4427x^2 + 4381x + 85680)/35700.
\end{aligned}$$

For polynomials P with 6 quadratic factors in $\Phi_3(P(x)) = P(x)^2 + P(x) + 1$ we record the following:

$P(x) = (16x^6 + 48x^5 + 172x^4 + 264x^3 + 379x^2 + 255x - 84)/210;$
$P(x) = (10000x^6 + 30000x^5 + 31900x^4 + 13800x^3 + 1759x^2 - 141x - 504)/546;$
$P(x) = (4096x^6 + 4480x^4 + 1225x^2 - 2871)/3255;$
$P(x) = (2304x^6 + 6864x^4 + 9529x^2 - 5831)/4655;$
$P(x) = (x^6 + 3x^5 + 37x^4 + 69x^3 + 907x^2 + 873x + 6300)/5460;$
$P(x) = (2187x^6 + 2106x^4 + 9399x^2 - 1372)/7840;$
$P(x) = (x^6 + 3x^5 + 16x^4 + 27x^3 + 991x^2 + 978x + 2184)/10920;$
$P(x) = (256x^6 - 2288x^4 + 9529x^2 + 3528)/13965;$
$P(x) = (10000x^6 + 30000x^5 + 57100x^4 + 64200x^3 + 48379x^2 + 21279x - 9594)/15678;$
$P(x) = (16x^6 + 48x^5 + 60x^4 + 40x^3 + 15x^2 + 3x + 40320)/24570;$
$P(x) = (144x^6 + 432x^5 + 1788x^4 + 2856x^3 + 4711x^2 + 3355x - 17500)/31850;$
$P(x) = (16x^6 + 48x^5 + 748x^4 + 1416x^3 + 8443x^2 + 7743x + 28080)/38220;$
$P(x) = (16x^6 + 48x^5 + 1180x^4 + 2280x^3 + 21295x^2 + 20163x + 10458)/38430.$

3.3 Degree 8 polynomials

Using the symmetric degree 4 polynomials from §3.1, one can apply the same strategy as mentioned previously to obtain suitable degree 8 polynomials. The resulting parameterisations produces 2 quadratics and 2 quartics in $\Phi_k(P)$. Our searches with these parameterisations produced no polynomials $P \in \mathbb{Q}[x]$ such that $\Phi_3(P)$ splits completely into quadratic. However, we found exactly 12 polynomials $P \in \mathbb{Q}[x]$ with a completely split $\Phi_4(P)$. We list all of these polynomials.

$P(x) = (128x^8 + 512x^7 + 896x^6 + 896x^5 - 101366x^4 - 203628x^3 - 152833x^2 - 50955x + 78480675)/18447975;$
$P(x) = (2560000x^8 + 5120000x^7 + 4480000x^6 + 2240000x^5 - 15884656x^4 - 16444656x^3 - 6201746x^2 - 1035291x + 26845677)/25033554;$
$P(x) = (16384x^8 + 32768x^7 + 28672x^6 + 14336x^5 + 238672x^4 + 235088x^3 + 87934x^2 + 14645x + 79685775)/47222175;$
$P(x) = (1073741824x^8 + 536870912x^7 + 117440512x^6 + 14680064x^5 + 61100032x^4 + 15045632x^3 + 1406944x^2 + 58580x + 79685775)/47222175;$
$P(x) = (20000x^8 + 80000x^7 + 140000x^6 + 140000x^5 - 1985582x^4 - 4111164x^3 - 3100873x^2 - 1035291x + 53691354)/50067108;$
$P(x) = (128x^8 + 512x^7 + 896x^6 + 896x^5 + 29834x^4 + 58772x^3 + 43967x^2 + 14645x + 159371550)/94444350;$
$P(x) = (8748x^8 + 11664x^7 + 6804x^6 + 2268x^5 - 7442901x^4 - 4962186x^3 - 1240557x^2 - 137840x - 2215101200)/3275922650;$
$P(x) = (32x^8 + 128x^7 + 224x^6 + 224x^5 + 1978226x^4 + 3956228x^3 + 2967143x^2 + 989045x + 30298828950)/4337369400;$
$P(x) = (4x^8 + 16x^7 + 28x^6 + 28x^5 - 275663x^4 - 551354x^3 - 413519x^2 - 137840x - 6645303600)/9827767950;$
$P(x) = (32x^8 + 128x^7 + 224x^6 + 224x^5 - 2072942x^4 - 4146108x^3 - 3109609x^2 - 1036539x + 33637897620)/31291942500;$
$P(x) = (128x^8 + 512x^7 + 896x^6 + 896x^5 - 29185846x^4 - 58372588x^3 - 43779553x^2 - 14593195x + 1659928924875)/120652657125;$
$P(x) = (128x^8 + 512x^7 + 896x^6 + 896x^5 + 21678314x^4 + 43355732x^3 + 32516687x^2 + 10838885x + 329267184675)/192951083325;$

4 Experimental results and final remarks

4.1 Factoring in practice

We showcase the practicality of these primes when it comes to factoring sufficiently large integers that have such prime factors. Take the following 1000-bit composite integer

$$N = \texttt{0xfabbb61aee9a690103cb45644699877c761c6b9b395a3ad168bce6e7e594871db5}\\ \texttt{e41f4ca5d15260e7d46a6e1f26bede7c93bc372fbbea584e47a99f3e3539230e641}\\ \texttt{cba316d10434e3c7ecd50443c5261c140d6ac07e1345cc804b28fe31a5266d4bf75}\\ \texttt{8272b76f8e632120aced4089d6f3ec17d0023e9140d42dec9f}.$$

Note briefly that this composite integer is larger than the latest number field sieve records [BGG+20]. However, using an unoptimised SageMath implementation of the Φ_3-method with a first stage smoothness bound $B = 1400000$, one can find the following 182-bit prime factor of N:

$$p = \texttt{0x22cc8bc6f65aba40987e31a4a5e5200c699921e981b9ef}.$$

In particular this prime factor can be found on average in 55 seconds with the SageMath code on an ordinary laptop. This average was taken over a sample of 20 iterations and gives a wide variance in the resulting timings. The successfulness of this factorisation comes from the fact that $p^2 + p + 1$ is 1400000-smooth. In fact this p is the prime that was presented in Example 3.

While larger integers have had similar sized prime factor identified in its factorisation with the elliptic curve method (ECM) [3], the computational effort to find this particular prime factor is far greater with ECM. In particular, using the `ecm.time()` function in SageMath, factoring this N with ECM is estimated to take on the order of 186 days.

4.2 More primes

On top of the primes in Examples 1 – 3 mentioned in Section 1, we found more primes using these polynomials. We report a small sample of these primes in Table 1, which includes one prime with $k = 6$ where $p^2 - p + 1$ is smooth.

While the smoothness bound of the primes found in this work are unusually small compared to random primes of the same size, we note that these bounds are not the smallest. Conducting similar analysis as presented in [MSvW26, §3.1], one make an estimate for the smallest such smoothness bound. For instance, in the 182-bit regime, the smallest smoothness bound for $\Phi_k(p)$ is estimated to be $B \approx 2^{12}$. This is much smaller than the bound on the concrete 182-bit example mentioned in Example 3 and §4.1.

The reason we are not able to find reach such small bounds is due to our carefully construction of the primes. Not all primes will be an evaluation of a polynomial P, especially when $\deg(P)$ is not too small. Hence we tradeoff the size of the smoothness bound with the ability to find such primes.

We finally remark that further progress can be made to find such primes p by adopting a lattice-based approach discussed in [MSvW26] in the context of finding smooth twins (i.e. consecutive smooth integers). The idea is to set up a so-called prime number lattice which consists of $\alpha \log(p_i)$, where the p_i's are primes from a factor base P, in the first row and a diagonal matrix below with weights α_i (depending on p_i) across the diagonals. Then finding the shortest vectors in that lattice will more often than not produce smooth twins. This method proved extremely effective to finding large smooth twins with the smallest possible smoothness bound. In the context of this work, one could replace the set

[3] See https://members.loria.fr/PZimmermann/records/factor.html for the latest ECM records.

Table 1: Primes $p = P(m)$ obtained from polynomials P such that $\Phi_k(p)$ is B-smooth.

m	bits	p	B	k
3438750	128	$(324m^6+972m^5+648m^4-324m^3-1619m^2-1295m+850)/1700$	501157	4
6470538	133	$(16m^6+48m^5+172m^4+264m^3+379m^2+255m-84)/210$	300277	3
28623338	145	$(16m^6+48m^5+172m^4+264m^3+379m^2+255m-84)/210$	849061	3
35352599	184	$(128m^8+4608m^7+72576m^6+653184m^5+3572234m^4+11392308m^3+17376687m^2+1111725m+58214375)/18447975$	49445381	4
1877115093	182	$(16m^6+48m^5+172m^4+264m^3+379m^2+255m-84)/210$	1334743	3
4577979592	161	$(81m^5+54m^4-27m^3-102m^2+74m+20)/100$	743273	4
5119546475	123	$(m^4+2m^3+34m^2+33m+126)/126$	331249	3
6217467721	128	$(2m^4-4m^3+3m^2-m+15)/15$	240017	4
89192098631	139	$(m^4+2m^3+34m^2+33m+126)/126$	212917	3
273812471165	150	$(2m^4+4m^3+3m^2+m+15)/15$	737683	3
500322946851	149	$(m^4+2m^3+34m^2+33m+126)/126$	564401	4
144422787172	114	$4m^3-6m^2+5m-1$	118429	6
2511499194712	126	$4m^3+6m^2+5m+1$	51169	3
3436693717407	130	$18m^3+24m^2+13m+2$	52529	4

of primes $P \subseteq \mathbb{Z}$ by a set of prime ideals $P \subseteq \mathfrak{O}$ in an order of a number field with unique factorisation. For instance, one would work with the Gaussian integers in the $k = 4$ setting and the Eisenstein order in the $k = 3$ setting. We leave this idea as part of future work.

References

[BGG+20] F. Boudot, P. Gaudry, A. Guillevic, N. Heninger, E. Thomé, and P. Zimmermann. Comparing the difficulty of factorization and discrete logarithm: A 240-digit experiment. In *CRYPTO*, volume 12171 of *Lecture Notes in Computer Science*, pages 62–91. Springer, 2020.

[BS89] E. Bach and J. Shallit. Factoring with cyclotomic polynomials. *Math. Comp.*, 52(185):201–219, 1989.

[BSC+23] G. Bruno, M. Corte-Real Santos, C. Costello, J. K. Eriksen, M. Meyer, M. Naehrig, and B. Sterner. Cryptographic smooth neighbors. In *ASIACRYPT*, volume 14444 of *Lecture Notes in Computer Science*, pages 190–221. Springer, 2023.

[CH21] J. B. Conrey and M. A. Holmstrom. Smooth values of quadratic polynomials. *Experimental Mathematics*, 30(4):447–452, 2021.

[CMN21] C. Costello, M. Meyer, and M. Naehrig. Sieving for twin smooth integers with solutions to the Prouhet-Tarry-Escott problem. In *EUROCRYPT*, volume 12696 of *Lecture Notes in Computer Science*, pages 272–301. Springer, 2021.

[Cop97] D. Coppersmith. Small solutions to polynomial equations, and low exponent RSA vulnerabilities. *Journal of cryptology*, 10(4):233–260, 1997.

[CP05] R. Crandall and C. Pomerance. *Prime numbers: a computational perspective*. Springer, 2005.

[Gra08] A. Granville. Smooth numbers: computational number theory and beyond. *Algorithmic number theory: lattices, number fields, curves and cryptography*, 44:267–323, 2008.

[Har21] D. Harvey. An exponent one-fifth algorithm for deterministic integer factorisation. *Math. Comp.*, 90(332):2937–2950, 2021.

[Len87] H. W. Lenstra Jr. Factoring integers with elliptic curves. *Annals of mathematics*, pages 649–673, 1987.

[LL93] A. K. Lenstra and H. W. Lenstra. *The development of the number field sieve*, volume 1554 of *Lecture Notes in Mathematics*. Springer Science & Business Media, 1993.

[LP92] H. W. Lenstra and C. Pomerance. A rigorous time bound for factoring integers. *Journal of the American Mathematical Society*, 5(3):483–516, 1992.

[Luc04] F. Luca. Primitive divisors of lucas sequences and prime factors of $x^2 + 1$ and $x^4 + 1$. *Acta Academiae Paedagogicae Agriensis, Sectio Mathematicae*, 31:19–24, 2004.

[MSvW26] E. Mulder, B. Sterner, and W. van Woerden. Large smooth twins from short lattice vectors, 2026. Appeared at ANTS XVII. URL: https://arxiv.org/abs/2509.17699, arXiv:2509.17699.

[Pol74] J. M. Pollard. Theorems on factorization and primality testing. In *Mathematical proceedings of the Cambridge philosophical society*, volume 76, pages 521–528. Cambridge University Press, 1974.

[RSA78] R. L. Rivest, A. Shamir, and L. M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[Sho94] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134. Ieee, 1994.

[Ste25] B. Sterner. Towards optimally small smoothness bounds for cryptographic-sized smooth twins and their isogeny-based applications. In *SAC*, volume 15516 of *Lecture Notes in Computer Science*, pages 178–202. Springer, 2025.

[Wil82] H. C. Williams. A $p + 1$ method of factoring. *Math. Comp.*, 39(159):225–234, 1982.