USING PARTIAL SMOOTHNESS OF $p - 1$
FOR FACTORING POLYNOMIALS MODULO $p$

BARTOSZ ŻRALEK

Abstract. Let an arbitrarily small positive constant $\delta$ less than 1 and a polynomial $f$ with integer coefficients be fixed. We prove unconditionally that $f$ modulo $p$ can be completely factored in deterministic polynomial time if $p - 1$ has a $(\ln p)^{O(1)}$-smooth divisor exceeding $p^\delta$. We also address the issue of factoring $f$ modulo $p$ over finite extensions of the prime field $\mathbb{F}_p$ and show that $p - 1$ can be replaced by $p^k - 1$ ($k \in \mathbb{N}$) for explicit classes of primes $p$.

1. Introduction

The existence of a deterministic, polynomial-time method to factor univariate polynomials over a prime field $\mathbb{F}_p$ is a major unsolved problem in computational number theory. The first result in this regard is due to Berlekamp [4], who gave an algorithm with running time bound $p(d \ln p)^{O(1)}$, $d$ being the degree of the polynomial $f$ to be factored. A better, and so far best, time bound $p^{1/2}(d \ln p)^{O(1)}$ is achieved by an algorithm of Shoup [21]. Both bounds can be seen as polynomial only if $p$ is fixed. They are in striking contrast to the complexity $(d \ln p)^{O(1)}$ of practical methods, such as the Cantor-Zassenhaus algorithm [6] (actually dating back to Legendre), which, however, rely on randomness. This considerable gap should not be a surprise if we think of the difficulty of computing deterministically a quadratic nonresidue in $\mathbb{F}_p$—a problem essentially equivalent to the very special case $d = 2$. Nevertheless, Rónyai [19] showed under the assumption of the Generalized Riemann Hypothesis that $f$ can be factored deterministically in time $(d \ln p)^{O(1)}$ and thus solved conditionally the matter for fixed $d$. Evdokimov [7] later improved the complexity of the algorithm to $(d \ln d \ln p)^{O(1)}$.

In this article we continue a line of investigation suggested by von zur Gathen (see [10]); it takes advantage of the multiplicative structure of $p - 1$ to factor $f$. The author of that paper devised a deterministic algorithm running in time $P^+(p - 1)(d \ln p)^{O(1)}$, where $P^+(p - 1)$ is the largest prime factor of $p - 1$ (cf. Rónyai [18]). Shoup [22] refined the technique and obtained the bound $P^+(p - 1)^{1/2}(d \ln p)^{O(1)}$.

Analogue results were obtained for $p$ replaced by the value $\Phi_k(p)$ of the $k$-th cyclotomic polynomial at $p$ [1]. All of them were proved to hold, if the Extended Riemann Hypothesis is true. Here we start out with a fixed irreducible polynomial $f \in \mathbb{Z}[X]$ and consider the problem of factoring $f$ unconditionally modulo varying primes $p$. 

Received by the editor March 17, 2008 and, in revised form, July 2, 2009.

2010 Mathematics Subject Classification. Primary 11Y16; Secondary 11Y05.

Key words and phrases. Prime finite fields, factorization, polynomials, roots, derandomization.
Such a task may seem much less ambitious, yet it has a satisfactory solution (i.e. a deterministic, polynomial-time algorithm) only when \( f \) is quadratic (Schoof [20]) or cyclotomic (Pila [14]). Fix moreover an arbitrarily small positive constant \( \delta < 1 \).

We prove that \( f \) modulo \( p \) can be completely factored in deterministic polynomial time if \( p - 1 \) has a \((\ln p)^{O(1)}\)-smooth divisor exceeding \( p^\delta \).

**Theorem 1.1.** Let \( f \) be an irreducible polynomial of degree \( d \) in \( \mathbb{Z}[X] \). Let \( \theta \) be a complex root of \( f \), and let \( h \) be the class number of \( \mathbb{Q}(\theta) \). Finally, let \( p \) be prime, and let \( B \geq (\ln p)^2 \). Assume that the \( B \)-smooth part \( S \) of \( p - 1 \) is no less than \( p^\delta \). Then the complete factorization of \( f \) modulo \( p \) over \( \mathbb{F}_p \) can be found deterministically in time \( O_{c,\theta}(B^{\frac{1}{2}} \ln B(\ln p)^{ch+3}) \), where \( c \) is any constant greater than \( \frac{\delta}{8} \).

One can ask about factoring \( f \) modulo \( p \) over a given model \( E \) of an extension \( \mathbb{F}_{p^k} \) of \( \mathbb{F}_p \). The standard, deterministic polynomial-time reduction to factoring some completely splitting polynomial over \( \mathbb{F}_p \) (see Theorem 7.8.1 of [2]) does not suit our purposes. It is so because the above time bound depends severely on \( f \). Still, once we have the factorization of \( f \) modulo \( p \) in \( \mathbb{F}_p[X] \), we can refine it deterministically in time \((dk \ln p)^{O(1)}\) to the factorization in \( E[X] \). Here is how.

Without losing any generality, suppose that \( f \) modulo \( p \) is irreducible in \( \mathbb{F}_p[X] \), of degree \( n \), \( 1 \leq n \leq d \). Let \( m \) be the greatest common divisor of \( k \) and \( n \). Find the subfields \( F \) of \( E \) and \( F' \) of \( \mathbb{F}_p[Y]/(f(Y)) \) with \( p^m \) elements. Observe that the factorizations of \( f \) modulo \( p \) in \( F \) and in \( E \) coincide. Furthermore, \( f \) factors in \( F' \) into a product of \( m \) irreducible polynomials as \( f = a \prod_{0 \leq j \leq m-1} f_j \), where \( a \) is the leading coefficient of \( f \) modulo \( p \) and \( f_j \) is obtained by applying \( j \) times the Frobenius automorphism to the coefficients of \( \prod_{0 \leq i \leq \frac{m}{k} - 1}(X - Y^{nm}) \). After expanding the product, we find the images of the \( f_j \) under an isomorphism \( F'[X] \to F[X] \), which is effectively computable with Lenstra’s algorithm [12].

We generalize Theorem 1.1 one more way, replacing \( p - 1 \) by \( p^k - 1 \) \((k \in \mathbb{N})\) for explicit classes of primes \( p \). Of particular interest is the case \( k = 2 \).

**Theorem 1.2.** Let \( f \) be an irreducible polynomial of degree \( d \) in \( \mathbb{Z}[X] \), and let \( \theta \) be one of its complex roots. Additionally, let \( P \) be a monic polynomial of degree \( k \) in \( \mathbb{Z}[Y] \), irreducible in \( \mathbb{Q}(\theta)[Y] \) and having \( \alpha \) as a complex root. Also, let \( h \) be the class number of \( \mathbb{Q}(\theta, \alpha) \). Lastly, let \( p \) be prime, and let \( B \geq (\ln p)^2 \).

Suppose that the \( B \)-smooth part of \( p^k - 1 \) is no less than \( p^\delta \) and that \( P \) modulo \( p \) is irreducible in \( \mathbb{F}_p[Y] \). Then, for every \( m \mid k \), the complete factorization of \( f \) modulo \( p \) over \( \mathbb{F}_{p^m} \) can be computed deterministically in time \( O_{c,\theta,\alpha}(B^{\frac{1}{2}} \ln B(\ln p)^{ch+3}) + (k \ln p)^{O(1)} \), where \( c \) is any constant greater than \( \frac{\delta}{8} \).

# 2. Notation

In all that follows, \( f \) is a fixed, irreducible polynomial of degree \( d \) in \( \mathbb{Z}[X] \) and of discriminant \( \Delta_f \). The number field \( K \) is the extension of \( \mathbb{Q} \) by a complex root \( \theta \) of \( f \). In practice, we think of \( K \) as \( \mathbb{Q}[X]/(f) \). The class number of \( K \) is \( h \), its ring of integers: \( \mathcal{O}_K \). A fixed, integral basis \( \omega = (\omega_1, \ldots, \omega_d) \) of \( \mathcal{O}_K \), as well as a fixed, finite set \( \mathcal{U} \) of generators of the group of units \( \mathcal{O}_K^\times \), is given. Methods of computing \( \omega, \mathcal{U}, h \) are covered for instance in [16] (Sections 4.6, 5.4 and 5.7, 6.5, respectively); we have included the time necessary for these computations in the big-\( O \) constant in Theorem 1.1. The only ideals we are concerned with are nonzero ideals of \( \mathcal{O}_K \). The norm \( N(I) \) of an ideal \( I \) is the cardinality of \( \mathcal{O}_K/I \). We let \( \psi_K(x,y) \), respectively
\( \psi_K'(x, y) \), be the number of ideals, respectively principal ideals, with norm at most \( x \) that split as a product of prime ideals with norm at most \( y \). Define \( \psi_K'(x, y) \) as the number of principal ideals with norm at most \( x \) that can be written as a product of principal ideals with norm at most \( y \). The letter \( p \) denotes an odd prime number.

For \( g \in \mathbb{Z}[X] \), by \( R_g \) we mean the quotient ring \( \mathbb{F}_p[X]/(g) \) and by \( R_g^\ast \) we mean its multiplicative group. If \( B \) is a subset of the ring \( R \), then the symbol \( \langle B \rangle \) stands for the multiplicative semigroup of \( R \) generated by \( B \).

3. Ideas behind the proof of Theorem 1.1

We seek to compute (deterministically) the complete factorization of \( f \) modulo \( p \). This is done recursively: any reducible factor \( g \) of \( f \) modulo \( p \) has to be split further. Very basic techniques allow us to reduce the problem to the case when \( f \) is monic, \( p \nmid \Delta_f \), and \( g \) is a product of distinct irreducible polynomials of degree, say, \( e \). Suppose that we have some way constructed a “small” subset \( F \) of \( R_g \setminus \{0\} \), which generates a relatively “large” multiplicative semigroup \( \langle F \rangle \). If \( F \) contains a zero divisor of \( R_g \), then a nontrivial factor of \( g \) is trivially found with Euclid’s algorithm. If, on the other hand, there are no zero divisors of \( R_g \) in \( F \), then \( \langle F \rangle \) is actually a subgroup of \( R_g^\ast \). To meet this event, we have made \( \langle F \rangle \) so large that even its image under the homomorphism raising elements to the power of \( p^{e-1} \) is noncyclic. The image is generated by \( F^{p^{e-1}} \), a “small” set consisting of elements of \( B \)-smooth orders in \( R_g^\ast \). This information is sufficient to split \( g \) efficiently (Theorem 4.6) with an extension to noncyclic groups of the Pohlig-Hellman algorithm [15] for computing discrete logarithms.

Now let us informally return to the question of finding a suitable set \( F \). Assuming that \( f \) is monic and \( p \nmid \Delta_f \), we can in particular identify the ring \( \mathcal{O}_K/(p) \) (Lemma 4.1). Consider the diagram

\[
\mathcal{O}_K \xrightarrow{\pi} R_f \xrightarrow{\rho} R_g,
\]

where \( \pi \) and \( \rho \) are projections. The idea is to construct a “large” multiplicative semigroup generated by a relatively “small” subset \( B \) of the algebraically rich ring \( \mathcal{O}_K \) and to take \( \mathcal{F} = \rho \pi(\mathcal{B}) \setminus \{0\} \). For \( K = \mathbb{Q} \), i.e. \( \mathcal{O}_K = \mathbb{Z} \), a natural way of proceeding is known from the explicit primality proofs of Fürer [9], Fellows-Koblitz [8], and Konyagin-Pomerance [11]. In these algorithms \( B \) can be chosen as the set of some “small” primes. The main obstacle to this approach is that \( \mathcal{O}_K \) is generally not a unique factorization domain (unless \( h = 1 \)). It is still a Dedekind domain, and just as de Bruijn’s function \( \psi (\psi = \psi_\mathbb{Q}) \) counts the smooth integers in \( \mathbb{Z} \), the function \( \psi_K \) counts the smooth ideals in \( \mathcal{O}_K \). The finiteness of the class number \( h \) enables us to bound from below via \( \psi_K \) the number of products of principal ideals with “small” norm (Lemma 4.2). Following a theorem of Fincke and Pohst, these ideals have generators equal up to units of \( \mathcal{O}_K \) to elements with “small” coordinates in the integral basis \( \omega \) (Theorem 4.3). After plugging the lower bound for \( \psi_K \) of Moree and Stewart (Theorem 4.4), whose result [13] generalizes a theorem of Canfield et al. [5] from \( K = \mathbb{Q} \) to arbitrary number fields, it finally turns out that we can pick \( \mathcal{B} = \mathcal{U} \cup \mathcal{A} \), where \( \mathcal{A} \) is a set of elements of \( \mathcal{O}_K \) with small coordinates in \( \omega \) (Lemma 4.5).
4. Proofs of the theorems

**Lemma 4.1.** If \( f \) is monic and \( p \nmid \Delta_f \), then \( \mathcal{O}_K/(p) = R_f \) (within our model of \( K \)).

**Lemma 4.2.** There is an effective, positive constant \( c_2 = c_2(K) \) such that \( \psi_K'(x, y) \geq \frac{1}{h} \psi_K(c_2 x, y^\frac{1}{h}) \) for \( y \geq c_2^{-h} \).

*Proof.* Let \( I_1, \ldots, I_h \) be a set of representatives for the class group of \( K \) whose norms are bounded above by the Minkowski bound \( M_K = \frac{d^h}{h!} \left( \frac{4}{\pi} \right)^{\frac{h}{2}} |\Delta_K|^{\frac{h}{2}} \), where \( s \) is the number of pairs of complex embeddings of \( K \) and \( \Delta_K \) is its discriminant. We will prove that the lemma holds with \( c_2 = M_K^{-1} \).

Let \( J \) be an ideal counted by \( \psi_K(M_K^{-1} x, y^\frac{1}{h}) \). There exists a \( k, 1 \leq k \leq h \), such that \( JI_k \) is principal. Suppose that \( y^\frac{1}{h} \geq M_K^{-1} \), i.e. \( y \geq M_K^{-h} \). Then \( JI_k \) is counted by \( \psi_K(x, y^\frac{1}{h}) \). Moreover, any ideal counted by \( \psi_K(x, y^\frac{1}{h}) \) can be written in at most \( h \) ways as \( JI_k \), where \( J \) is counted by \( \psi_K(M_K^{-1} x, y^\frac{1}{h}) \) and \( 1 \leq k \leq h \). Consequently, \( \frac{1}{h} \psi_K(M_K^{-1} x, y^\frac{1}{h}) \leq \psi_K'(x, y) \).

Assume that the principal ideal \( I \) is a product of prime ideals with norm at most \( y^\frac{1}{h} \). It is easy to show by induction on the number of these prime factors that \( I \) is a product of principal ideals with norm at most \( y \). Just use the fact that every product of \( h \) ideals contains a principal factor. To see why, recall a general observation: in a group with \( h \) elements, the \( h + 1 \) prefixes of a product \( \prod_{i=1}^{h+1} x_i \) cannot all be distinct. Therefore any ideal counted by \( \psi_K(x, y^\frac{1}{h}) \) is also counted by \( \psi_K'(x, y) \); hence \( \psi_K(x, y^\frac{1}{h}) \leq \psi_K'(x, y) \). \( \square \)

**Theorem 4.3** (Fincke and Pohst). There is an effective, positive constant \( c_3 = c_3(K, \omega) \) such that for any \( \eta \in \mathcal{O}_K \setminus \{0\} \) there exists \( \tilde{\eta} \in \mathcal{O}_K \) generating the same ideal as \( \eta \) and whose coordinates \( a_i \) in the basis \( \omega \) satisfy \( |a_i| \leq c_3(N(\tilde{\eta}))^{\frac{1}{h}} \).

*Proof.* Combine the equations (3.5b), Chapter 5, and (4.3f), Chapter 6, of [16]. \( \square \)

**Theorem 4.4** (Moree and Stewart). There is an effective, positive constant \( c_1 = c_1(K) \) such that for \( x, y \geq 1 \) and \( u := \frac{\ln u}{\ln y} \geq 3 \) we have

\[
\psi_K(x, y) \geq x \exp \left[ -u \left( \ln(u \ln u) - 1 + \frac{\ln \ln u - 1}{\ln u} + c_1 \left( \frac{\ln \ln u}{\ln u} \right)^2 \right) \right].
\]

**Lemma 4.5.** Let notation be as above, let \( g \) be of degree \( d' \), and let \( c \) be a constant greater than \( d \). Define \( A = \{a_1 \omega_1 + \ldots + a_d \omega_d : \forall 1 \leq i \leq d \ a_i \in \mathbb{Z}, |a_i| \leq c_0(\ln p)^{\frac{1}{h}} \} \), \( B = \mathcal{U} \cup A \). Then \#(\rho(\mathcal{B})) > p^{d' - \frac{d}{2} - \varepsilon} + 1 \) for any \( \varepsilon > 0 \) and \( p \geq p_0 \), \( p_0 = p_0(c, c_1, c_2, c_3, d, \varepsilon) \).

*Proof.* Denote by \( R \) the set \( \{a_1 \omega_1 + \ldots + a_d \omega_d : \forall 1 \leq i \leq d \ a_i \in \mathbb{Z}, |a_i| \leq \frac{c}{2} \} \) of distinct representatives for \( \mathcal{O}_K/(p) \) (\( p > 2 \)). We have

\[
\#(\rho(\mathcal{B})) = \#(\rho(\mathcal{B})) \geq \#(\rho((\mathcal{B}) \cap R) = \#(\rho(\mathcal{B}) \cap R).
\]

It is thus sufficient to prove that \#(\rho(\mathcal{B}) \cap R) > p^{d' - \frac{d}{2} - \varepsilon} + 1 \). Let \( I \) be an ideal counted by \( \psi_K''((\frac{p}{2c_3})^d, (\ln p)^{ch}) \). We invoke Theorem 4.3 to deduce that \( I = (\eta) = (\alpha_1) \ldots (\alpha_l) \) for some \( \eta \in R \) and \( \alpha_1, \ldots, \alpha_l \in A \). We can also write \( \eta = u \alpha_1 \ldots \alpha_l \) with \( u \in \mathcal{O}_K \). Hence \( \eta \in (\mathcal{B}) \cap R \). Different principal ideals have, of course, different generators, so we get \#(\mathcal{B}) \cap R \geq \psi_K''((\frac{p}{2c_3})^d, (\ln p)^{ch}) \). By Lemma 4.2, the latter
expression for \( p \) large enough is no less than \( \frac{1}{R} \psi_K(c_2(\frac{\alpha}{2\epsilon^3})^d, (\ln p)^c) \). This, from Theorem 1.4, is in turn greater than \( p^{d - \frac{\delta}{2} - \epsilon} + p^{d - 1} \) for any \( \epsilon > 0 \) and sufficiently large \( p \). Therefore \( \#(\mathcal{B}) \cap R > p^{d - \frac{\delta}{2} - \epsilon} + p^{d - 1} \) if \( p \) exceeds some constant \( p_0 \) depending upon \( c, c_1, c_2, c_3, \alpha, d \), and \( \epsilon \). Assume that it does. The preimage under the projection \( \rho \) of any element of \( R_g \) has \( \# \ker \rho = p^{d - d'} \) elements. It follows that \( p^{d - d'} \cdot \#(\mathcal{B}) \cap R > \#(\mathcal{B}) \cap R > p^{d - \frac{\delta}{2} - \epsilon} + p^{d - 1} \). Consequently, \( \#(\mathcal{B}) \cap R > p^{d - \frac{\delta}{2} - \epsilon} + 1 \). \( \square \)

**Theorem 4.6.** Let a subset \( \mathcal{B} \) of \( R^*_g \) together with the complete factorization of the exponent \( E \) of \( \langle \mathcal{B} \rangle \) be given. Then a generator of \( \langle \mathcal{B} \rangle \) or (particularly in the case when \( \langle \mathcal{B} \rangle \) is not cyclic) a nontrivial factor of \( g \) can be found deterministically in time \( O(\#\mathcal{B} \cdot (q^2 \ln q + d' \ln p)(d' \ln p)^3) \), where \( q = P^+(E) \).

**Proof.** We reason following closely the lines of the proof of Corollary 4.3 from [23], the analogue of our theorem for subsets \( \mathcal{B} \) of the group \( \mathbb{Z}^*_n \), where \( n \) is an odd integer, \( n > 1 \). The key fact used therein is that \( \mathbb{Z}^*_n \) is the direct sum of cyclic groups \( \mathbb{Z}^*_{n_s} \), the prime factorization of \( n \) being \( \prod s^{\alpha_s} \). Here, if we assume that \( g \) is squarefree (and this causes no loss of generality), then the situation becomes similar: \( R^*_g \) is the direct sum of the cyclic groups \( R^*_s \), \( s \) running through the irreducible factors of \( g \). We omit the details of the suitable algorithm and its complexity analysis (for the latter, see Remark 4.4 from [23]). \( \square \)

**Proof of Theorem 1.1.** It is enough to treat the case when \( f \) is monic. Indeed, let \( l \) be the leading coefficient of \( f \). Consider the minimal polynomial \( \tilde{f} \) of the integral element \( l \theta \): \( \tilde{f}(Y) = l^{d - 1}f(Y) \). If \( p \nmid l \), factoring \( \tilde{f}(Y) \) modulo \( p \) reduces to factoring \( f(X) \) modulo \( p \) via the change of variable \( Y = lX \). If \( p \mid l \) or, more generally, \( p \) is “small”, even a direct search will do. So assume that \( f \) is monic and that \( p \nmid \Delta_f \). First, compute the distinct-degree factorization of \( f \) modulo \( p \), that is, the products \( t_e, e \in \mathbb{N} \), of all distinct, degree \( e \) irreducible divisors of \( f \) modulo \( p \). Then, for every fixed \( e \), compute recursively the complete factorization of \( t_e \), as described below. Take any reducible factor \( g \) of \( t_e \) that is found. Let \( g \) have degree \( d' \), say \( d' = ke \). With the notation of Lemma 1.5, choose \( c > \frac{d'}{S} \) and \( \epsilon = \frac{\delta}{S} - \frac{d'}{S} \). Suppose further that \( p \geq p_0 \). Set \( \mathcal{F} = \rho_{\sigma}(\mathcal{B}) \setminus \{0\} \). We can assume that \( \mathcal{F} \subset R^*_g \); otherwise the greatest common divisor of \( g \) and some \( b \in \mathcal{F} \) would be a nontrivial factor of \( g \). Let \( \sigma \) be the endomorphism of \( R^*_g \) raising every element to the power of \( \frac{c - 1}{S} \), where \( S \) is the \( B \)-smooth part of \( p - 1 \). Find the complete factorization of \( S \) using the deterministic Pollard-Strassen algorithm [17], and further compute the order of each \( b \in \sigma(\mathcal{F}) \). By Theorem 4.6, showing that \( \langle \sigma(\mathcal{F}) \rangle \) is not cyclic will conclude the proof. The group \( R^*_g \) is isomorphic to the product of \( k \) copies of \( \mathbb{F}^*_p \); hence \( \# \ker \sigma = (\frac{p - 1}{S})^k \). From Lemma 1.6, we infer that \( \#(\mathcal{F}) > p^{d' - \frac{\delta}{S} - \frac{d'}{S}} \). Consequently,

\[
\#(\sigma(\mathcal{F})) \geq \frac{\#(\mathcal{F})}{\# \ker \sigma} \geq S^k \cdot \frac{p^{d' - \frac{\delta}{S} - \frac{d'}{S}}}{(p^e - 1)^k}.
\]

Since \( k \geq 2 \), \( S \geq p^\delta \), \( d' = ke \), and \( c > \frac{d'}{S} \), it follows that \( \#(\sigma(\mathcal{F})) > S \). If \( \langle \sigma(\mathcal{F}) \rangle \) were cyclic, the reverse inequality would also hold, because \( \langle \sigma(\mathcal{F}) \rangle^S = \{1\} \). Therefore, \( \langle \sigma(\mathcal{F}) \rangle \) is not cyclic. \( \square \)
Proof of Theorem 1.2. The ring $\mathbb{F}_p[Y]/(P)$ is isomorphic to $\mathbb{F}_p$. Let $m \mid k$. Using simple linear algebra, construct the subfield $F$ of $\mathbb{F}_p[Y]/(P)$ with $p^m$ elements. By Lenstra’s theorem on constructive uniqueness of finite fields [12], we only have to deal with the problem of factoring $f$ over $F$. This reduces easily to factoring $f$ over the larger field $\mathbb{F}_p[Y]/(P)$. The rest of the proof is similar to the previous one. Choose to work with $K = \mathbb{Q}[X,Y]/(f, P)$. For $f$ monic and $p \mid \mathcal{O}_K : \mathbb{Z}[\theta, \alpha]$, the rings $\mathcal{O}_K/(p)$ and $\mathbb{F}_p[X,Y]/(f, P)$ are equal. We will need this time to consider the diagram

$$
\mathcal{O}_K \rightarrow \mathbb{F}_p[X,Y]/(f, P) \rightarrow \mathbb{F}_p[X,Y]/(g, P)
$$

and to introduce some obvious changes. \hfill \Box

5. Concluding remarks

Let $\gamma$ and $\delta$ be constants, $\gamma \geq 1, 0 < \delta \leq \frac{1}{3}$. Denote by $\mathcal{P}_{\gamma, \delta}(x)$ the set of primes $p \leq x$, such that $p - 1$ has $(\ln x)^{\gamma}$-smooth divisor exceeding $x^{\delta}$. For $p \in \mathcal{P}_{\gamma, \delta}(x)$, the algorithm corresponding to Theorem 1.1 runs in polynomial time, with the possible exception of, say, $p \leq \sqrt{x}$. It was proved in [11] that $\lim_{x \to \infty} \# \mathcal{P}_{\gamma, \delta}(x) - \sqrt{x} = \infty$. More precisely (see the proof of Theorem 5.2 therein):

**Theorem 5.1** (Konyagin and Pomerance). We have $\# \mathcal{P}_{\gamma, \delta}(x) \geq x^{1 - \frac{\gamma}{3} - \epsilon}$ for any $\epsilon > 0$ and $x \geq x_0$, where the constant $x_0 = x_0(\gamma, \delta, \epsilon)$ is effective.

An important theoretical advantage of using the partial (versus full) smoothness of $p - 1$ lies in the fact that there is no proof of the infinitude of primes $p$ for which $p - 1$ is $(\ln p)^{O(1)}$-smooth. Thanks to a theorem of Baker and Harman [3], we “only” know that infinitely many primes $p$ satisfy $P^+(p - 1) \leq p^{0.2961}$.

Acknowledgements

This paper together with [23] contains the results of the author’s doctoral dissertation, written at the Institute of Mathematics of the Polish Academy of Sciences, under the supervision of Dr. Jacek Pomykala. It is a pleasure to thank him for all his help, encouragement, and kindness. The author also thanks the referees for valuable comments.

References


Institute of Mathematics, Warsaw University, 02-097 Warsaw, Poland

*E-mail address*: b.zralek@mimuw.edu.pl