MATHEMATICS OF COMPUTATION
Volume 79, Number 272, October 2010, Pages 2353–2359
S 0025-5718(2010)02377-4
Article electronically published on May 20, 2010

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

BARTOSZ ŹRAŁEK

ABSTRACT. Let an arbitrarily small positive constant δ 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^{δ}. 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 $p^{\frac{1}{2}}(d\ln p)^{O(1)}$ 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 radomness. 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 $(d^d\ln p)^{O(1)}$ 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

$$P^+(p-1)^{\frac{1}{2}}(d\ln p)^{O(1)}.$$

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 δ, $\delta < 1$. 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^δ.

Theorem 1.1. *Let f be an irreducible polynomial of degree d in $\mathbb{Z}[X]$. Let θ 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^δ. 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 $\frac{d}{\delta}$.*

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 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 $\prod_{0\leq i\leq \frac{n}{m}-1}(X - Y^{p^{im}})$. 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 θ 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 α 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^δ 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 (any model of) $\mathbb{F}_{p^m}$ 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 $\frac{kd}{\delta}$.*

2. Notation

In all that follows, f is a *fixed*, irreducible polynomial of degree d in $\mathbb{Z}[X]$ and of discriminant Δ_f. The number field K is the extension of $\mathbb{Q}$ by a complex root θ 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 $\mathcal{O}_K^*$, 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^* we mean its multiplicative group. If $\mathcal{B}$ is a subset of the ring R, then the symbol $\langle\mathcal{B}\rangle$ stands for the multiplicative semigroup of R generated by $\mathcal{B}$.

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 $\mathcal{F}$ of $R_g \setminus \{0\}$, which generates a relatively "large" multiplicative semigroup $\langle\mathcal{F}\rangle$. If $\mathcal{F}$ 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 $\mathcal{F}$, then $\langle\mathcal{F}\rangle$ is actually a subgroup of R_g^*. To meet this event, we have made $\langle\mathcal{F}\rangle$ so large that even its image under the homomorphism raising elements to the power of $\frac{p^e-1}{S}$ is noncyclic. The image is generated by $\mathcal{F}^{\frac{p^e-1}{S}}$, a "small" set consisting of elements of B-smooth orders in R_g^*. 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 $\mathcal{F}$. Assuming that f is monic and $p \nmid \Delta_f$, we can in particular identify the ring $\mathcal{O}_K/(p)$ with R_f (Lemma 4.1). Consider the diagram

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

where π and ρ are projections. The idea is to construct a "large" multiplicative semigroup generated by a relatively "small" subset $\mathcal{B}$ 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 $\mathcal{B}$ 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 ψ ($\psi = \psi_\mathbb{Q}$) counts the smooth integers in $\mathbb{Z}$, the function ψ_K counts the smooth ideals in $\mathcal{O}_K$. The finiteness of the class number h enables us to bound from below via ψ_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 ω (Theorem 4.3). After plugging the lower bound for ψ_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 ω (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 $M_K = \frac{d!}{d^d}\left(\frac{4}{\pi}\right)^s |\Delta_K|^{\frac{1}{2}}$, where s is the number of pairs of complex embeddings of K and Δ_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 $y^{\frac{1}{h}} \geq M_K$, 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, $\frac{1}{h}\psi_K(M_K^{-1}x, y^{\frac{1}{h}}) \leq \psi'_K(x, y^{\frac{1}{h}})$.

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 $\prod_{i=1}^h x_i$ 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 $\psi'_K(x, y^{\frac{1}{h}}) \leq \psi''_K(x,y)$. □

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 η and whose coordinates a_i in the basis ω satisfy $|a_i| \leq c_3 N((\eta))^{\frac{1}{d}}$.*

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

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 $u := \frac{\ln x}{\ln y} \geq 3$ 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 $\mathcal{A} = \{a_1\omega_1 + \ldots + a_d\omega_d : \forall_{1 \leq i \leq d}\ a_i \in \mathbb{Z},\ |a_i| \leq c_3(\ln p)^{\frac{ch}{d}}\}$, $\mathcal{B} = \mathcal{U} \cup \mathcal{A}$. Then $\#\langle \rho\pi(\mathcal{B})\rangle > p^{d' - \frac{d}{c} - \varepsilon} + 1$ 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 $\{a_1\omega_1 + \ldots + a_d\omega_d : \forall_{1 \leq i \leq d}\ a_i \in \mathbb{Z},\ |a_i| \leq \frac{p}{2}\}$ of distinct representatives for $\mathcal{O}_K/(p)$ $(p > 2)$. We have

$$\#\langle \rho\pi(\mathcal{B})\rangle = \#\rho\pi(\langle \mathcal{B}\rangle) \geq \#\rho\pi(\langle \mathcal{B}\rangle \cap R) = \#\rho(\langle \mathcal{B}\rangle \cap R).$$

It is thus sufficient to prove that $\#\rho(\langle \mathcal{B}\rangle \cap R) > p^{d' - \frac{d}{c} - \varepsilon} + 1$. 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 $I = (\eta) = (\alpha_1) \cdot \ldots \cdot (\alpha_l)$ for some $\eta \in R$ and $\alpha_1, \ldots, \alpha_l \in \mathcal{A}$. We can also write $\eta = u \cdot \alpha_1 \cdot \ldots \cdot \alpha_l$ with $u \in \mathcal{O}_K^*$. Hence $\eta \in \langle \mathcal{B}\rangle \cap R$. Different principal ideals have, of course, different generators, so we get $\#\langle \mathcal{B}\rangle \cap R \geq \psi''_K((\frac{p}{2c_3})^d, (\ln p)^{ch})$. By Lemma 4.2, the latter expression for p large enough is no less than $\frac{1}{h}\psi_K(c_2(\frac{p}{2c_3})^d, (\ln p)^c)$. This, from Theorem 4.4, is in turn greater than $p^{d-\frac{d}{c}-\varepsilon} + p^{d-1}$ for any $\varepsilon > 0$ and sufficiently large p. Therefore $\#\langle\mathcal{B}\rangle \cap R > p^{d-\frac{d}{c}-\varepsilon} + p^{d-1}$ if p exceeds some constant p_0 depending upon c, c_1, c_2, c_3, d, and ε. Assume that it does. The preimage under the projection ρ of any element of R_g has $\#\ker\rho = p^{d-d'}$ elements. It follows that $p^{d-d'} \cdot \#\rho(\langle\mathcal{B}\rangle \cap R) \geq \#\langle\mathcal{B}\rangle \cap R > p^{d-\frac{d}{c}-\varepsilon} + p^{d-1}$. Consequently, $\#\rho(\langle\mathcal{B}\rangle \cap R) > p^{d'-\frac{d}{c}-\varepsilon} + 1$. □

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 $O(\#\mathcal{B} \cdot (q^{\frac{1}{2}} \ln q + d' \ln p)(d' \ln p)^3)$, 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 $\mathbb{Z}^*_{s^{\alpha_s}}$, 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]). □

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 $l\theta$: $\tilde{f}(Y) = l^{d-1} f(\frac{Y}{l})$. 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 4.5 choose $c > \frac{d}{\delta}$ and $\varepsilon = \frac{\delta}{2} - \frac{d}{2c}$. Suppose further that $p \geq p_0$. Set $\mathcal{F} = \rho\pi(\mathcal{B}) \setminus \{0\}$. 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 σ be the endomorphism of R_g^* raising every element to the power of $\frac{p^e-1}{S}$, 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 $\mathbb{F}_{p^e}^*$; hence $\#\ker\sigma = \left(\frac{p^e-1}{S}\right)^k$. From Lemma 4.5 we infer that $\#\langle\mathcal{F}\rangle > p^{d'-\frac{d}{2c}-\frac{\delta}{2}}$. Consequently,

$$\#\langle\sigma(\mathcal{F})\rangle \geq \frac{\#\langle\mathcal{F}\rangle}{\#\ker\sigma} > S^k \cdot \frac{p^{d'-\frac{d}{2c}-\frac{\delta}{2}}}{(p^e-1)^k}.$$

Since $k \geq 2$, $S \geq p^\delta$, $d' = ke$, and $c > \frac{d}{\delta}$, it follows that $\#\langle\sigma(\mathcal{F})\rangle > S$. 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. □

Proof of Theorem 1.2. The ring $\mathbb{F}_p[Y]/(P)$ is isomorphic to $\mathbb{F}_{p^k}$. 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 $p \nmid [\mathcal{O}_K : \mathbb{Z}[\theta,\alpha]]$, 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

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

and to introduce some obvious changes. □

5. Concluding remarks

Let γ and δ 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^δ. 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* $\#\mathcal{P}_{\gamma,\delta}(x) \geq x^{1-\frac{\delta}{\gamma}-\varepsilon}$ *for any* $\varepsilon > 0$ *and* $x \geq x_0$*, where the constant* $x_0 = x_0(\gamma,\delta,\varepsilon)$ *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 Pomykała. It is a pleasure to thank him for all his help, encouragement, and kindness. The author also thanks the referees for valuable comments.

References

1. E. Bach, J. von zur Gathen, H. W. Lenstra, *Factoring polynomials over special finite fields*, Finite Fields and Their Applications, **7** (2001), 5-28. MR1803933 (2001k:11252)
2. E. Bach, J. O. Shallit, *Algorithmic number theory, Volume 1: Efficient algorithms*, MIT Press, 1996. MR1406794 (97e:11157)
3. R. C. Baker, G. Harman, *Shifted primes without large prime factors*, Acta Arithmetica, **83** (1998), 331-361. MR1610553 (99b:11104)
4. E. R. Berlekamp, *Factoring polynomials over finite fields*, Bell Systems Technical Journal, **46** (1967), 1853-1859. MR0219231 (36:2314)
5. E. R. Canfield, P. Erdös, C. Pomerance, *On a problem of Oppenheim concerning "factorisatio numerorum"*, Journal of Number Theory, **17** (1983), 1-28. MR712964 (85j:11012)
6. D. G. Cantor, H. Zassenhaus, *A new algorithm for factoring polynomials over finite fields*, Mathematics of Computation, **36** (1981), 587-592. MR606517 (82e:12020)
7. S. Evdokimov, *Factorization of polynomials over finite fields in subexponential time under GRH*, Lecture Notes in Computer Science, **877** (1994), 209-219. MR1322724 (95m:11145)
8. M. R. Fellows, N. Koblitz, *Self-witnessing polynomial-time complexity and prime factorization*, Designs, Codes and Cryptography, **2** (1992), 231-235. MR1181730 (93e:68032)

9. M. Fürer, *Deterministic and Las Vegas primality testing algorithms*, Lecture Notes in Computer Science, **194** (1985), 199-209. MR819255 (87c:11123)
10. J. von zur Gathen, *Factoring polynomials and primitive elements for special primes*, Theoretical Computer Science, **52** (1987), 77-89. MR918114 (89a:11126)
11. S. Konyagin, C. Pomerance, *On primes recognizable in deterministic polynomial time*, The Mathematics of Paul Erdös (R. L. Graham, J. Nesetril, eds.), Springer-Verlag, 1997, 176-198. MR1425185 (98a:11184)
12. H. W. Lenstra, Jr., *Finding isomorphisms between finite fields*, Mathematics of Computation, **56** (1991), 329-347. MR1052099 (91d:11151)
13. P. Moree, C. L. Stewart, *Some Ramanujan-Nagell equations with many solutions*, Indagationes Mathematicae (N. S.), **1** (1990), 465-472. MR1106093 (92f:11053)
14. J. Pila, *Frobenius maps of abelian varieties and finding roots of unity in finite fields*, Mathematics of Computation, **55** (1990), 745-763. MR1035941 (91a:11071)
15. S. C. Pohlig, M. E. Hellman, *An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance*, IEEE Transactions on Information Theory, **24** (1978), 106-110. MR0484737 (58:4617)
16. M. Pohst, H. Zassenhaus, *Algorithmic algebraic number theory*, Cambridge University Press, 1989. MR1033013 (92b:11074)
17. J. M. Pollard, *Theorems on factorization and primality testing*, Proceedings of the Cambridge Philosophical Society, **76** (1974), 521-528. MR0354514 (50:6992)
18. L. Rónyai, *Factoring polynomials modulo special primes*, Combinatorica, **9** (1989), 199-206. MR1030373 (90k:11161)
19. L. Rónyai, *Factoring polynomials over finite fields*, Journal of Algorithms, **9** (1988), 391-400. MR955147 (89k:11124)
20. R. Schoof, *Elliptic curves over finite fields and the computation of square roots mod p*, Mathematics of Computation, **44** (1985), 483-494. MR777280 (86e:11122)
21. V. Shoup, *On the deterministic complexity of factoring polynomials over finite fields*, Information Processing Letters, **33** (1990), 261-267. MR1049276 (91f:11088)
22. V. Shoup, *Smoothness and factoring polynomials over finite fields*, Information Processing Letters, **39** (1991), 39-42. MR1103697 (92f:11178)
23. B. Źrałek, *A deterministic version of Pollard's p-1 algorithm*, Mathematics of Computation, **79** (2010), 513-533. MR2552238

Institute of Mathematics, Warsaw University, 02-097 Warsaw, Poland
E-mail address: b.zralek@mimuw.edu.pl