Galois Theory and Factoring of Polynomials over Finite Fields. For Jo's $p-1$–th Anniversary

Preda Mihăilescu

Mathematisches Institut Universität Göttingen

Version 1.0 May 26, 2010

Contents

Introduction I

Factoring polynomials over $\mathbb{F}_p$

Let p be a (large) prime and $f \in \mathbb{F}_p[X]$ be a polynomial of degree $n = d \cdot g$ with equal degree factorization.

$$f(X) = \prod_{i=1}^{g} f_i(X), \quad \deg(f_i) = d.$$

The $\mathbb{F}_p$ - algebra defined by f is:

$$\begin{aligned}
\mathbb{A} &= \mathbb{F}_p[X]/(f(X)) = \prod_{i=1}^{g} \mathbb{F}_p[X]/(f_i(X)) \cong \prod_i \mathbb{F}_{p^d}, \\
\mathbb{A} &= \{\ y = (y_1, y_2, \ldots, y_g)\ :\ y_1 \in \mathbb{F}_p[X]/(f_i(X))\ \} \\
&= \left\{ y = \sum_{i=1}^{g} e_i y_i \right\} : \qquad \text{Chinese Remainder Theorem.}
\end{aligned}$$

Introduction II

Berlekamp's strategy

Let the *diagonal Frobenius automorphism* be $\Phi : \mathbb{A} \to \mathbb{A}; y \mapsto y^p$. The Berlekamp subalgebra is

$$\mathbb{B} = \mathbb{A}^{\Phi} = \{y \in \mathbb{A} : y_i \in \mathbb{F}_p\}.$$

and it is an g - dimensional $\mathbb{F}_p$ - space. A base for the Berlekamp algebra $\mathbb{F}_p$ can be computed by linear algebra, and then traditional factoring algorithms proceed by choosing random $b \in \mathbb{B}$ and computing the $\mathrm{GCD}(b^{(p-1)/2} \pm 1, f(X))$, as polynomials in $\mathbb{F}_p[X]$.

Introduction III

A remark

The algebra $\mathbb{A}/\mathbb{F}_p$ is rich in automorphisms: let $\mathcal{A} = \text{ Aut } (\mathbb{A}/\mathbb{F}_p)$. Let

$$\begin{aligned} \varphi_i &\in \mathcal{A} : \varphi(y_1, y_2, \ldots, y_g) = (y_1, y_2, \ldots, y_i^p, \ldots, y_g), \\ \Phi &= \circ_{i=1}^g \varphi_i : \quad \text{the diagonal Frobenius } . \end{aligned}$$

Then $\mathbb{B} = \mathbb{A}^\Phi$ is the fixed algebra of the diagonal Frobenius. But there are more automorphisms, and some can be computed globally!

Introduction IV

Galois lifts

1. Suppose $F \in \mathbb{Z}[X]$ is a lift of f such that $\mathbb{K} = \mathbb{Q}[X]/(F)$ is even a galois extension (non abelian lifts are interesting, so there is some luck in this assumption... but there will be work arounds).
2. Let $G = \text{ Gal }(\mathbb{K}/\mathbb{Q})$. Then there is an embedding $G \hookrightarrow \mathcal{A}$ that can be computed explicitly and quite efficiently using algebra in $\mathbb{C}$.
3. We assume additionally that p is not a *ausserwesentlicher Diskriminantenteiler* of $\mathbb{K}$. Then an old theorem of Kummer yields a one to one correspondence $\wp_i = (p, f_i(\theta))$, with $\theta \in \mathbb{K}, F(\theta) = 0$ and $\wp_i$ the primes above p in $\mathbb{K}$.

Introduction V

A case for factoring

1. Let $D(\wp) \subset G$ be the decomposition group of $\wp$; it is cyclic since p is unramified.
2. We make the further assumption that $d > 1$ and there is some $\sigma \in D(\wp_1)$ which permutes some of the primes $\wp_i, i > 1$.
3. As a consequence, for $y = (y_1, y_2, \ldots, y_g) \in \mathbb{B}$, we have $\sigma(y_1) = y_1$ but $\sigma(y_i) \neq y_j, i \neq j$ for at least one $i > 1$.
4. Then $y(\sigma) = \sigma(y) - y$ is a *factoring element*, in the sense that the $\mathrm{GCD}(y(\sigma), f(X))$ – as polynomials in $\mathbb{F}_p$, is non trivial.
5. Compared to Berlekamp, this happens without additional exponentiations!

Introduction VI

Motivation

1. The interest of this construction is that it works without additional exponentiations in $\mathbb{B}$. When $\log(p) > n^2$, say, this may be of interest.
2. This motivation (...), suggests looking deeper into global galois actions on algebras over $\mathbb{F}_p$.
3. The *mantra* of the talk will be to identify numerous morphisms which can be computed explicitly without use of the Frobenii φ_i, Φ.

Introduction VII

Plan

1. We give an overview of global - rational and p - adic - lifts which can be computed explicitly.
2. We suggest a work around which allows $\mathbb{K}$ to have a non trivial automorphism group, without being necessarily galois. This reduces in general the degree of the working extensions.
3. We give some explicite examples where global galois theory helps improving some classical algorithms over $\mathbb{F}_p$.
4. We present as an application a (not so new) algorithm for primality testing, which combines cyclotomy and elliptic curve approaches using common galois algebras over $\mathbb{F}_p$. The algorithm runs in random cubic time and is asymptotically best in state of the art (if someone would still care ...)

Global lifts and their morphisms I

Completions

Let $\mathbb{F}_p, f, F, \mathbb{K}$ be like before. The following construction is very useful in Iwasawa Theory:

- Let
$$\mathfrak{K} = \mathbb{K} \otimes_{\mathbb{Q}} \mathbb{Q}_p = \prod_{i=1}^{g} \mathbb{K}_{\wp_i} = \mathbb{Q}_p[X]/(F),$$
where $\mathbb{K}_{\wp}$ is the *completion* at the place $\wp$. This is a galois algebra over $\mathbb{Q}_p$
- Then $\mathbb{K}_{\wp} \cong \mathbf{K} = \mathbb{Q}_p[X]/(f_i)$, the unramified extension of degree d of $\mathbb{Q}_p$.
- Let $U(\mathbb{K}) = \mathcal{O}(\mathfrak{K})$. Then
$$\mathbb{A} = U(\mathbb{K})/(pU(\mathbb{K})).$$

Global lifts and their morphisms II

Global and local algebra

Thus $U(\mathbb{K})$ is a global lift that preserves information about the factoring of f, via Hensel lift. Moreover,

$$\mathrm{Aut}\ (\mathfrak{K}/\mathbb{Q}_p) \cong \ \mathrm{Aut}\ (\mathbb{A}/\mathbb{F}_p).$$

In particular, $G \hookrightarrow \ \mathrm{Aut}\ (\mathfrak{K}/\mathbb{Q}_p)$.
The decomposition of $U(\mathbb{K})$ only depends on the primes $\wp_i$ but not on the particular polynomial representation of the algebra. One can thus choose among many isomorphisms representing $\mathfrak{K}$.

Global lifts and their morphisms III

Computing G

1. Let $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$ be the zeroes of F and $\alpha = \alpha_1$. Then $\sigma \in G$ is fixed by the value $\alpha_i = \sigma(\alpha)$.
2. Given $\alpha_i \in \mathbb{C}$, one can compute using essentially discriminants, the polynomials $g_i \in \mathbb{Q}[X]$ with

$$\sigma_i(\alpha) = \alpha_i = g_i(\alpha).$$

3. The required precision can be controlled and $g_i \in \mathbb{Z}_{(p)}[X]$ (the algebraic localization) iff $(\mathrm{disc}(F), p) = 1$.

Global lifts and their morphisms IV

The polynomial action of G

1. For $\beta \in \mathbb{K}$ one can compute with the same methods the polynomial $h \in \mathbb{Q}[X]$ with $\beta = h(\alpha)$.
2. In this case, for arbitrary $\beta = h(\alpha) \in \mathbb{K}$, we have
$$\sigma_i(\beta) = \sigma_i(h(\alpha)) = h(\sigma_i(\alpha)) = h \circ g_i(\alpha).$$
Note thus that polynomial composition is contravariant: $\sigma \circ h = h \circ g$.
3. If $(\mathrm{disc}(F), p) = 1$ all the above computations have good reduction at p.

Global lifts and their morphisms V

Computing isomorphisms of $\mathbb{A}$

- Let $\theta \in \mathbb{K}$ be an other generator of $\mathbb{K}$ as a simple extension and $\theta = h(\alpha)$ have minimal polynomial $T \in \mathbb{Q}[X]$.
- Assume that $(\mathrm{disc}(F), p) = (\mathrm{disc}(T), p) = 1$ and let $t = T \bmod p \in \mathbb{F}_p[X]$. Then the algebra

$$\mathbb{A}' = \mathbb{F}_p[X]/(t(X)) \cong \mathbb{A}.$$

If $a = X + (f(X)) \in \mathbb{A}, b = X + (t(X)) \in \mathbb{A}'$, then the isomorphism $\iota : \mathbb{A}' \hookrightarrow \mathbb{A}$ is given explicitly by $a \rightarrow h(a)$.

Global lifts and their morphisms VI

Non galois extensions

We consider now the case when natural lifts F of f fail to be galois – which is the general case.

- Let like before $\alpha_i \in \mathbb{C}$ be the zeroes of F. We extract an arbitrary subset, say $A = \{\alpha_1, \alpha_2, \ldots, \alpha_j\}$ of these zeroes.
- By building an adequate linear combination

$$\beta = \sum_{i=1}^{j} c_i \alpha_i \in \mathbb{C},$$

  we obtain a simple extension $\mathbb{K} = \mathbb{Q}[\beta] = \mathbb{Q}[X]/(\overline{F}) \supset A$, where $\overline{F}$ is the minimal polynomial of β.
- This minimal polynomial can be computed in $\mathbb{C}$ using, for instance, Newton sums.

Global lifts and their morphisms VII

Using global automorphisms

- Then, assuming that $\mathbb{K}$ contains no further roots of F, $\text{Aut}\ (\mathbb{K}/\mathbb{Q}) \hookrightarrow \Sigma_j$ and the automorphisms $\sigma \in \text{Aut}\ (\mathbb{K}/\mathbb{Q})$ can be computed explicitly, together with isomorphisms sending $\mathbb{K}$ to its conjugate fields.
- Note that the primes above p in $\mathbb{K}$ have also in this case the degree d - but the primes $(p, f_i(\alpha))$ of $\mathbb{Q}[X]/(F)$ split completely in $\mathbb{K}$.

Global lifts and their morphisms VIII

Back to factoring

Consider the following lucky case:

1. Let $f \in \mathbb{F}_p[X]$ be given as above and $F \in \mathbb{Z}[X]$ be some lift. Let a subset $A \subset F^{-1}(0)$ of j elements be given, such that $\mathbb{Q}[A] = \mathbb{Q}[\beta] = \mathbb{Q}[X]/(\overline{F})$.
2. Let $\wp_i = (p, f_i(\alpha)) \subset \mathcal{O}(\mathbb{K})$ be ideals above p (these are not primes, for $j > 1$).
3. Suppose that F, A can be found such that they enjoy the following property:

$$\exists \sigma \in \text{ Aut } (\mathbb{K}/\mathbb{Q}) : \sigma(\wp) = \wp, \sigma(\wp_i) \neq \wp_i,$$

for some i with $\alpha_i \in A$.

Global lifts and their morphisms IX

... factoring

1. Then we have a case for factoring: let $\overline{f} = \overline{F} \bmod p \in \mathbb{F}_p[X]$ and $\overline{\mathbb{A}} = \mathbb{F}_p[X]/(\overline{f}), \overline{\mathbb{B}} = \overline{\mathbb{A}}^{\Phi}$, the Berlekamp algebra of $\overline{\mathbb{A}}$.
2. Like in the galois case, $\sigma(b) - b \in \overline{\mathbb{B}}$ is a factoring element that induces a non trivial factorization not only for $\overline{f}$ but also for f.

Global lifts and their morphisms X

Open theoretical questions

Note that the previous algorithms all require the fact that $\mathbb{K}$ is not abelian: in the abelian case, all automorphisms act like Frobenii. Non abelian extensions can be easily achieved, by choosing adequate lifts F. Here are some open questions.

1. Given the number g of factors of f, what is the average size of j, such that the above construction may succeed? Are there further obstructions?
2. Is there any lower bound on $j(g)$ such that the algorithm is necessarily successful? Is there any work around for the case when $d = 1$?
3. What are further special algorithms, in which the use of global automorphisms can bring advantages?

Global lifts and their morphisms XI

A p - adic question

1. Let $F, G \in \mathbb{Z}[X]$ be two distinct lifts of the same $f \in \mathbb{F}_p[X]$ and $\mathbb{K} = \mathbb{Q}[X]/(F), \mathbb{L} = \mathbb{Q}[X]/(G)$, while the completions are $\mathfrak{K} = \mathbb{Q}_p[X]/(F); \mathfrak{L} = \mathbb{Q}_p[X]/(G)$.
2. The fields $\mathbb{K}$ and $\mathbb{L}$ are unrelated, but since they are unramified at p, the completions $\mathfrak{K} \cong \mathfrak{L}$ and we have seen how to construct the isomorphism κ at ground level.
3. Modulo p, the isomoprhism restricts to an isomorphism of the algebra $\mathbb{A} = \mathbb{F}_p[X]/(f)$. Over the global field $\mathbb{Q}_p$ we have however different factors for F and G, which are identical only in the first approximation.
4. Can κ be lifted p - adically? Can this observation bring more information on the actual factors? (Experiments are going on ...)

Some applications I

Factoring cyclotomic polynomials

- Let q be a prime and $F = \Phi_q(X) \in \mathbb{Z}[X]$ be the $q-$th cyclotomic polynomial. The factors $\Psi_i \in \mathbb{F}_p[X]$ of this polynomial all have degree $d = \mathrm{ord}_q(p)$; there are thus $g = \frac{q-1}{d}$ such factors.
- Let $\chi : (\mathbb{Z}/q \cdot \mathbb{Z})^* \rightarrow \mathbb{C}$ be a primitive character of order g and conductor q and $\tau(\chi)^g \in \mathbb{Z}[\rho_g]$ be its Gauss sum.
- It is a fact that g is in general *small* with respect to q. If both p and q are large, even one Frobenius in $\mathbb{F}_p[X]/(F)$ can be more than afforded.
- Using galois theory, one can reduce the cost of factoring F to essentially computing some Gauss sums of order (dividing) g and conductor q as follows:

Some applications II

Factoring with Gauss sums

1. Let $\mathbb{A} \supset \mathbb{F}_p$ be some galois algebra containing an $g-$th root of unity and $\beta \in \mathbb{A}$ be the image of $\tau(\chi)$.
2. By choice of g, the equation $X^g = \beta$ has a solution in $\mathbb{A}$, which can be computed using usual methods in extensions of degree $\delta \leq g$. From the solutions one can compute the images of *Gauss periods* of conductor q and order g in $\mathbb{F}_p$; let these be $\eta_i \in \mathbb{F}_p; i = 1, 2, \ldots, g$.
3. The irreducible factors $\Psi = \sum_{k=0}^{d-1} c_k X^k \in \mathbb{F}_p[X]$. The Newton sums $S(j) = \sum_{k=1}^{d} \alpha_k^j$ of the zeroes of Ψ are Gauss periods. Therefore, the only computation that depends on q, consists in the retrieval of c_k from the values $S(j)$. For this, $O^{\sim}(q)$ algorithms are known (Ask Alin).

Some applications III

Polynomial cyclic algebras

- The above example indicates that galois theory helps saving operations even in algorithms which are purported to be *best understood*.
- The central idea in the above factoring variant is the use of Lagrange resolvents in algebras $\mathbb{A}$ in which $\mathcal{A}$ contains an abelian subgroup.
- A simple generalization are *polynomial cyclic algebras*:(Joint work with V. Vuletescu)
- The polynomial cyclic algebras describe the algebras generated by polynomials with cyclic global lifts.

Some applications IV

… definition

Definition

Let $\mathbb{K}$ be a finite field of characteristic p and $f \in \mathbb{K}[X]$ be a polynomial of degree n. Assume that there exists a polynomial $C \in \mathbb{K}[X]$, with $m-$th iterate denoted by $C^{(m)}(X), m > 0$, such that

A. $f(C(X)) \equiv 0 \bmod f(X)$.

B. $C^{(n)}(X) - X \equiv 0 \bmod f(X)$ and $(C^{(m)}(X) - X, f(X)) = 1$ for $m < n$.

Then $\mathbb{A} = \mathbb{K}[X]/(f)$ is called a **polynomially cyclic algebra** and C is its **cyclicity polynomial**.

Some applications V

… and properties

- The cyclicity polynomial behaves like we have seen that the polynomials g_σ describing global automorphisms must behave.
- With help of cyclicity polynomials, one may define in an intrinsic way (i.e. without use of global lifts), what Lagrange resolvents are, and verify that their properties are consistent with the usual ones from galois theory.
- Lagrange resolvents help reduce operations in larger algebras (or even fields) $\mathbb{A}$, to more operations in subalgebras of minimal degrees.
- The example of factoring cyclotomic polynomials is the simplest such reduction.

Some applications VI

The discrete logarithm in the SEA algorithm

(Joint work with F. Morain and É. Schost)

- Torsion groups of elliptic curves yield interesting examples, in which the cyclicity polynomials stem from the point multiplication.
- In the Elkies variant of Schoof's point counting algorithm for elliptic curves one encounters the following discrete logarithm problem:
- Let $\mathcal{E} : Y^2 = X^3 + aX + b$ be an elliptic curve defined over $\mathbb{F}_p$ and let ℓ be a prime.
- Let $\psi_\ell(X)[a, b]$ denote the $ell-$th division polynomial, i.e. the polynomial over $\mathbb{Z}$, whose zeroes are all the x coordinates of $\ell-$th division points in $\mathcal{E}[\ell]$.

Some applications VII

Elkies case

- An *eigenfactor* $f(X)|\psi(X)$ of degree $\ell - 1$ over $\mathbb{F}_p$ is known.
- Let $\rho = X + (f(X))$, and $g_k(X)$ be the multiplication polynomials, with $g_k(P_x) = ([k]P)_x$ for $P \in \mathcal{E}[\ell]$. Then

  $$\rho^p = g_\lambda(\rho).$$

  Here λ is an *eigenvalue* of the Frobenius, which should be computed.
- The traditional solution for finding λ, is to compute ρ^p and then use some small step giant step strategy for computing λ.

Some applications VIII

and elliptic Gauss sums

- Using Lagrange resolvents, one considers characters χ of conductor ℓ and order $q|(\ell-1)$ that map to some algebra $\mathbb{A} \supset \mathbb{F}_p$ and computes (essentially)

$$\tau_e(\chi) = \sum_{x \in (\mathbb{Z}/\ell\cdot\mathbb{Z})^*} g_x(\rho)\chi(x).$$

- Analogues of Gauss periods occur in this sum, and these can be computed efficiently in extensions of degree at most q.
- The elliptic Gauss sums verify, like their traditional counterparts

$$(\tau_e(\chi))^p = \chi(\lambda^{-p}) \cdot \tau_e(\chi^p).$$

Some applications IX

Elkies and Atkin cases

1. By exponentiations in small extensions, one recovers the value of $\chi(\lambda)$ for a set of characters which generate the dual $\widehat{(\mathbb{Z}/\ell \cdot \mathbb{Z})^*}$, thus determining $\lambda \in \mathbb{F}_\ell$.
2. In the so called Atkin case of the SEA algorithm, there are no eigenpolynomials. The characteristic polynomial $F(X) = X^2 - tX + p$ of the Frobenius is irreducible over $\mathbb{F}_\ell$, so Frobenius acts on a pair of point P, P^p, spanning $\mathcal{E}[\ell]$, like a matrix $M_\Phi \in \mathrm{GL}(2, \mathbb{F}_\ell)$.
3. In this case, one usually is contempted with the determination of the order of M_Φ.

Some applications X

Atkin case

1. Using Lagrange resolvents and cyclic polynomials, one may construct a map $\mu : \mathbb{A}[X]/(F) \rightarrow A[\xi]$, where $\mathbb{A}$ is an algebra containing the traces of the kernels of the ℓ - isogenies of $\mathcal{E}$ (or alternatively, $\mathbb{A}$ is defined by the *modular equation* Ψ_ℓ, which is a polynomial of degree $\ell + 1$). The variable ξ is an $\ell-$th root of unity.
2. Like in the Elkies case, computations take place in smaller subfields or subalgebras. The value of the trace t can easily be recovered using μ. Thus one can compute in the Atkin case the trace t almost as efficiently as in the Elkies case.
3. The run time is dominated in both cases by one Frobenius in $\mathbb{A}$. This method is described but not implemented yet.

CIDE - primality proving in cubic time I

General primality proving

- Let n be a large integer, which is a pseudoprime. Its primality should be proved efficiently.
- There are essentially two efficient, general approaches to this problem: the cyclotomy approach CPP and the elliptic curve approach ECPP.
- Primes in the order of 20000 decimal digit are state of the art for fans. They are proved using ECPP, which is well maintained by F. Morain (CPP is by noone).

CIDE - primality proving in cubic time II

more ...

- The first is de facto more efficient for some still actual range of integers, but is loaded with a final trial division step, which is asymptotically not polynomial.
- The second has been improved over decades to run in essential quartic time.
- The deterministic algorithm AKS is **beautiful**, but unafordable, mainly for space reasons: an improved variant due to Berrizbeitia solves in part the time problem.

CIDE - primality proving in cubic time III

The cyclotomic approach

- One chooses parameters $s, t = \mathrm{ord}_s(n)$ with s highly decomposed and $t = O\left(\log(n)^{\log\log\log(n)}\right)$. For all pairs (p^k, q) with $p^k | (q-1)$ and $q|s$, one chooses characters $\chi_{p,q} : (\mathbb{Z}/q\cdot\mathbb{Z})^* \to \mathbb{A}_p$ and computes the Jacobi sums

$$J(p,q) = (\tau(\chi_{p,q}))^{p^k}, G(p,q) = \frac{\tau(\chi_{p,q}^{n(p)})}{\tau(\chi_{p,q}^{n(p)})}, \quad n(p) = n \,\mathrm{rem}\, p^k.$$

- If $r(p) = (n - n(p))/p^k$, the central test stage consists in verifying that

$$J(p,q)^{r(p)} \cdot G(p,q) \in < \zeta_{p^k} > \subset \mathbb{A}.$$

CIDE - primality proving in cubic time IV

The cyclotomic approach ...

- If all these tests are passed successfully, one has the proof for the following fact:

$$\forall r \mid n, \ \exists j < t : r \equiv n^j \bmod s. \tag{1}$$

- The possible remaining factors are then eliminated in a *final trial division*. This step is the *crux* of the approach.

CIDE - primality proving in cubic time V

The elliptic curve approach

- One uses modular forms to find an order $\mathcal{O} \subset \mathbb{K}$ of an imaginary quadratic field, in which $n = \nu \cdot \overline{\nu}$ splits. Moreover, a Hilbert polynomial associated to the class group of this order has zeroes in $\mathbb{Z}/(n \cdot \mathbb{Z})$.
- One determines a curve $\mathcal{E} : Y^2 = X^3 + aX + b$ with the property that if n is prime, then $|\mathcal{E}_n| = m(\mathbb{K}) = n \pm \mathbf{Tr}(\nu) + 1$.
- This step is repeated until some m is found with a large factor $q|m$, $q > (p^{1/4} + 1)^2$. One is *not happy* if $m(\mathbb{K})$ is prime.

CIDE - primality proving in cubic time VI

The elliptic curve approach

- When these steps have been completed, it suffices to find by simple trial and error a point $Q \in \mathcal{E}_n$ with $Q \neq \mathcal{O}$ but $[qQ] = \mathcal{O}$. Since q can only be a probable prime, the algorithm proceeds recursively, so we need descent.
- The case when m is pseudoprime is thus unfavorable for ECPP, since it does not allow (in general) descent.

CIDE - primality proving in cubic time VII

Dual elliptic primes

- If $m = m(\mathbb{K})$ is prime, there is a factorization $m = \mu \cdot \overline{\mu}$ and $\mu = \nu \pm 1$. Thus μ, ν are quadratic version of twin primes. We call these *dual elliptic primes*.
- The following property of *dual elliptic primes* allows the combination of the CPP and ECPP approaches in a mixed algorithm CIDE, which runs in cubic time:
- Suppose that m, n were found to be pseudoprimes, in the first stage of ECPP (a long list of conditions, which we spare here...). Then both m and n are square free and their *smallest prime factors* $p|m, q|n$ are *actual dual elliptic primes.*

CIDE - primality proving in cubic time VIII

CIDE - the idea

1. One starts by performing the CPP test for both m, n ... but it can be shown that it suffices now to select $s > (m+n)^{1/4}$.
2. Let $n = \nu \cdot \overline{\nu}, m = (\nu - 1)(\overline{\nu} - 1)$ be the factorizations in $\mathbb{K}$. If they are composite, then the relation (1) together with the property of dual elliptic pseudoprimes, imply that

$$\begin{aligned} p &= \pi\overline{\pi} \equiv (\nu - 1)^j (\overline{\nu} - 1)^j \bmod s \\ q &= \rho\overline{\rho} \equiv \nu^k \overline{\nu}^k \bmod s. \end{aligned}$$

CIDE - primality proving in cubic time IX

CIDE - the idea

1. This reduces, for any product of primes $L|s$ to an equation

$$(\nu - 1)^j - \nu^k \equiv \pm 1 \bmod L\mathcal{O}.$$

   For this reduction, some additional tests on elliptic Gauss sums, defined in the same *working algebras* used for the CPP test, are required. Their number is small.

2. Suppose that one can, by eventually adding a few factors to s, find $L|s$ such that the equation above **has only the trivial solution** $k = j = 1$ modulo $L\mathcal{O}$

CIDE - primality proving in cubic time X

CIDE - Strategy

1. In general L has at most $1-3$ prime facotrs. Note that ν is fixed by the input number n and the order $\mathcal{O}$, so the free parameters are indeed k, j.
2. In this case, it follows that the final trial division step of CPP is superfluous, since we obtained a proof for $j = k = 1$, so the only possible divisors of m, n are their remainders modulo s.
3. If, nevertheless, m, n are composite, then they must both be decomposed and their least prime factors p, q, which are dual elliptic primes and thus very close, verify $|p - q| < (n^{1/4} + 1)$. This explains why one can choose smaller values for s in CIDE.

CIDE - primality proving in cubic time XI

CIDE - Analysis

1. The first step of CIDE consists in finding two dual elliptic pseudoprimes m, n. This corresponds to the first stage of ECPP and takes heuristic cubic time (note that ECPP only has an heuristic run-time, it is not provable).
2. The next step requires finding L, and is fast.
3. The central step consists in two CPP tests and few additional elliptic Gauss sum tests. The number of algebra exponentiations is $O(\log(n)^{1-\varepsilon})$, so this step takes also cubic time.
4. There is no final trial division. The test requires however some precomputed Jacobi sums - alternatively, these can be computed by using LLL.