LMS J. Comput. Math. 15 (2012) 44–58 © 2012 Author
doi:10.1112/S1461157012000034

On modular inverses of cyclotomic polynomials and the magnitude of their coefficients

Clément Dunand

Abstract

Let p and r be two primes, and let n and m be two distinct divisors of pr. Consider Φ_n and Φ_m, the nth and mth cyclotomic polynomials. In this paper, we present lower and upper bounds for the coefficients of the inverse of Φ_n modulo Φ_m and discuss an application to torus-based cryptography.

1. *Introduction*

The magnitude of coefficients of polynomials derived from cyclotomic polynomials has attracted attention since the 19th century. If φ denotes the Euler totient function, the nth cyclotomic polynomial Φ_n is a monic polynomial of degree $\varphi(n)$ whose roots are the primitive nth roots of unity. In the following, we denote its coefficients by $(a_i)_{0\leqslant i\leqslant\varphi(n)}$.

Many results dealing with Φ_n have been published so far. On the one hand, we have asymptotic results saying that these coefficients may exhibit exponential behaviour for infinitely many n (see, for instance, Erdös [13] or Bateman [4]). On the other hand, there exist numerous studies for integers n having only a small number of prime factors. Along these lines, Migotti [17] showed in 1883 that if n is composed of at most two primes p and r, the coefficients of Φ_{pr} can only be -1, 0 or 1. Later, around 1965, Beiter [5] and Carlitz [8] found more precise criteria for these coefficients to be 0 or ±1. More recently, in 1996, Lam and Leung [15] presented these coefficients in an explicit way.

The first example of a cyclotomic polynomial with a coefficient of magnitude 2 is Φ_{105}, whose 7th and 41st coefficients are -2. Yet, when n is the product of a small number of primes, we can still find interesting bounds on the coefficients of Φ_n. For n being a product of three distinct primes $p<q<r$, Bang [3] showed in 1895 that $|a_i|\leqslant p-1$. Later, in 1968, Beiter [5] and Bloom [7] gave a better bound for when q or r equals ±1 modulo p, that is, $|a_i|\leqslant(p+1)/2$. The conjecture that this bound could hold for all prime numbers p, q and r has recently been proved false by Gallot and Moree in [14]. Bachman [2] gave a better bound in 2003: for any distinct primes $p<q<r$, $|a_i|\leqslant p-\lceil p/4\rceil$. In 1968, Bloom [7] even gave a bound for a product of four distinct primes: for $n=pqrs$ with $p<q<r<s$, we have $|a_i|\leqslant p(p-1)(pq-1)$.

Moree has recently studied cofactors of cyclotomic polynomials, that is, polynomials of the form $(x^n-1)/\Phi_n(x)$. It appears that their coefficients tend to be small in absolute value. These results can be extended to the Taylor expansion about 0 of $1/\Phi_n$ (see [18]).

This paper deals with modular inverses of cyclotomic polynomials. If Φ_m and Φ_n are coprime (that is, if $\gcd(\Phi_m,\Phi_n)=1$), then Φ_m is invertible modulo Φ_n and, following the example of Φ_n, we may ask whether the coefficients of $\Phi_m^{-1} \bmod \Phi_n$ are of a special form. In particular, we have noticed that the magnitudes of these coefficients take a very special form when n is composed of a few prime factors, and we thoroughly prove lower and upper bounds for them in the case where m and n are two distinct divisors of pr, the product of two primes. For the product of three primes pqr, the peculiar structure of Φ_{pqr} may also yield interesting results, but this is beyond the scope of the present work.

Received 10 November 2009; revised 6 July 2011.

2010 Mathematics subject classification 11S05 (primary).

Our main motivation is the computation of a convenient morphism between the multiplicative group of a finite field $\mathbb{F}_{q^n}$ and products of some of its subgroups. Such calculations typically occur in torus-based cryptographic schemes, as developed by Silverberg and Rubin [**19, 20**]. The bounds presented in Theorem 1 lead to improvements in the running times of algorithms in this field (see [**11, 12**]). Such schemes are discrete log-based cryptosystems and make use of a subgroup of $\mathbb{F}_{q^n}^{\times}$ in which the communication cost is reduced; that is to say, elements can be represented by fewer than the usual n coordinates in $\mathbb{F}_q$.

In Section 2 we explain more precisely the geometric structure of algebraic tori, which is the mathematical context of torus-based cryptography. A cryptographic application of the results presented in this paper will be sketched in Section 4.

In Section 3 we come to the main theorem of this paper. First, we recall a useful result from Apostol [**1**] on the resultant of two cyclotomic polynomials. Then, in the case of two coprime cyclotomic polynomials, we consider the inverse of Φ_m modulo Φ_n. Most of Section 3 is dedicated to an exhaustive study of the case where n and m are divisors of the product of two primes, and we prove the following theorem.

THEOREM 1. *For all distinct prime numbers p and r:*

(i) $\Phi_p^{-1} \bmod \Phi_1 = 1/p$ *and* $\Phi_1^{-1} \bmod \Phi_p = (-1/p)(X^{p-2} + 2X^{p-3} + \ldots + p - 1)$;

(ii) $\Phi_{pr}^{-1} \bmod \Phi_1 = 1$ *and* $\Phi_1^{-1} \bmod \Phi_{pr} = \sum_{i=0}^{\varphi(pr)-1} v_i X^i$ *with* $v_i \in \{-1, 0\}$;

(iii) $\Phi_{pr}^{-1} \bmod \Phi_p = (1/r) \sum_{i=0}^{d} X^i$ *with* $d = r - 1 \bmod p$ *and*
$\Phi_p^{-1} \bmod \Phi_{pr} = (1/r) \sum_{i=0}^{\varphi(pr)-1} v_i X^i$ *with* $|v_i| < r$;

(iv) $\Phi_p^{-1} \bmod \Phi_r = \sum_{i=0}^{\varphi(r)-1} v_i X^i$ *with* $v_i \in \{0, -1, +1\}$.

2. *Geometry of algebraic tori*

Many protocols and cryptosystems make use of the subgroup of order $\Phi_n(q)$ in the multiplicative group $\mathbb{F}_{q^n}^{\times}$. It is interesting to see it as the set of rational points over $\mathbb{F}_q$ of an algebraic torus. We refer to [**9, 20**] for more details.

2.1. *Structure of algebraic tori*

For a given field K, let $\bar{K}$ be a separable closure of K. Let $\mathbb{G}_m$ denote the multiplicative group. This is an affine absolutely connected algebraic group of dimension one. An algebraic torus over K is an algebraic group T that is isomorphic to $\mathbb{G}_m^s$ over $\bar{K}$ for some $s \geqslant 1$. By a *splitting field of T* we shall mean any subfield L of $\bar{K}$ such that T is isomorphic to $\mathbb{G}_m^s$ over L.

From now on we consider finite extensions of finite fields. Let $L = \mathbb{F}_{q^n}$ be a field extension of $K = \mathbb{F}_q$, and let G denote $\mathrm{Gal}(L/K)$. Let $\mathrm{Res}_{L/K}$ denote the functor of Weil restriction of scalars from L to K. Its basic properties are given in [**22, 23**]. What we need, essentially, is that for a given variety V, there are $|G|$ functorial projection L-morphisms $\mathrm{Res}_{L/K} V \to V$ such that their direct sum gives an L-isomorphism

$$\iota : \mathrm{Res}_{L/K} V \xrightarrow{\sim} V^{|G|}.$$

In the case of $V = \mathbb{G}_m$, this isomorphism allows us to represent an L-point of $\mathrm{Res}_{L/K} \mathbb{G}_m$ by $|G|$ coordinates taking values in $\mathbb{G}_m \subset \mathbb{A}^1$. We can define norm and trace maps by computing, respectively, the product and the sum of these coordinates. Let $n = |G|$; then we have the following explicit definition of the norm map:

$$\begin{array}{ccccc} \mathrm{N}_{L/K} : \mathrm{Res}_{L/K} \mathbb{G}_m & \xrightarrow{\iota} & \mathbb{G}_m^n & \longrightarrow & \mathbb{G}_m \\ \alpha & \longmapsto & (\alpha_g)_{g \in G} & \longmapsto & \prod_{g \in G} \alpha_g, \end{array}$$

which happens to be defined over K.

https://doi.org/10.1112/S1461157012000034 Published online by Cambridge University Press

More generally, for any intermediate extension $K \subseteq F \subseteq L$ we can construct partial norms $\mathrm{N}_{L/F,K} : \mathrm{Res}_{L/K}\,\mathbb{G}_m \to \mathrm{Res}_{F/K}\,\mathbb{G}_m$. These norms correspond to the usual ones on $L^\times$, the set of K-rational points of $\mathrm{Res}_{L/K}\,\mathbb{G}_m$.

Definition 1. The torus T_L is defined as the intersection of the kernels of the norm maps $\mathrm{N}_{L/F,K}$ for all subfields $K \subseteq F \subsetneq L$:

$$T_L = \bigcap_{K \subseteq F \subsetneq L} \mathrm{Ker}[\mathrm{Res}_{L/K}\,\mathbb{G}_m \xrightarrow{\mathrm{N}_{L/F,K}} \mathrm{Res}_{F/K}\,\mathbb{G}_m].$$

With the usual norms over fields, we recover the elementary definition of the K-points of T_L:

$$T_L(K) \simeq \{\alpha \in L^\times |\ \mathrm{N}_{L/F}(\alpha) = 1\ \forall\, K \subset F \subsetneq L\}.$$

Moreover, this torus is L-isomorphic to $\mathbb{G}_m^d$ with $d = \varphi(n)$; we refer to [**20**, Proposition 2.6], where Rubin and Silverberg give a detailed proof of this result.

2.2. *Endomorphisms of algebraic tori*

Any algebraic torus T of dimension s is by definition isomorphic to $\mathbb{G}_m^s$ over a splitting field. This means that it is actually a twist over $\mathbb{F}_q$ of $\mathbb{G}_m^s$. So there exists a $\bar{K}$-isomorphism $I : T \to \mathbb{G}_m^s$.

We call $\sigma : \bar{K} \to \bar{K}$ the Frobenius automorphism. Let ${}^\sigma I : T \to \mathbb{G}_m^s$ be the conjugate of I by σ. The composition ${}^\sigma I I^{-1}$ is an endomorphism of $\mathbb{G}_m^s$. Arguments from Galois cohomology [**9**] show that there is a bijective correspondence which associates each twist of $\mathbb{G}_m^s$ with the conjugacy classes of ${}^\sigma I I^{-1}$ inside the endomorphism ring of $\mathbb{G}_m^s$.

An endomorphism of $\mathbb{G}_m^s$ is given by

$$\mathfrak{a} : (g_1, \ldots, g_s) \mapsto \left(\prod_{1 \leqslant j \leqslant s} g_j^{a_{i,j}} \right)_{1 \leqslant i \leqslant s}.$$

Such a map in characterized by the matrix of the exponents $(a_{i,j})_{1 \leqslant i,j \leqslant s}$. This is an s-dimensional square matrix with integer coefficients, which actually corresponds to an endomorphism of the $\mathbb{Z}$-module of characters of $\mathbb{G}_m^s$. The morphism $\mathfrak{a}$ is invertible if and only if the matrix $(a_{i,j})_{1 \leqslant i,j \leqslant s}$ is invertible. So the automorphism group of $\mathbb{G}_m^s$ is equal to $\mathrm{GL}_s(\mathbb{Z})$.

In the case of the Weil restriction $\mathrm{Res}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\,\mathbb{G}_m$, we obtain ${}^\sigma I I^{-1} = \omega$, where ω denotes the following permutation of the coordinates:

$$\omega(g_1, g_2, \ldots, g_n) = (g_n, g_1, \ldots, g_{n-1}).$$

Let us compute the ring of $\mathbb{F}_q$-endomorphisms of this torus. With every endomorphism ε of $\mathbb{G}_m^n$ we associate an endomorphism of $\mathrm{Res}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\,\mathbb{G}_m$, and the following diagram commutes.

$$\begin{array}{ccc} \mathrm{Res}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\,\mathbb{G}_m & \xrightarrow{I^{-1}\varepsilon I} & \mathrm{Res}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\,\mathbb{G}_m \\ {\scriptstyle I}\downarrow{\scriptstyle \sim} & & {\scriptstyle I}\downarrow{\scriptstyle \sim} \\ \mathbb{G}_m^n & \xrightarrow{\quad\varepsilon\quad} & \mathbb{G}_m^n \end{array}$$

The endomorphism $I^{-1}\varepsilon I$ is defined over $\mathbb{F}_q$ if and only if it is invariant under the action of σ, that is, ${}^\sigma I^{-1} {}^\sigma\varepsilon\, {}^\sigma I = I^{-1}\varepsilon I$. So ε yields an $\mathbb{F}_q$-endomorphism of $\mathrm{Res}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\,\mathbb{G}_m$ if and only if $\omega\varepsilon = \varepsilon\omega$.

https://doi.org/10.1112/S1461157012000034 Published online by Cambridge University Press

2.3. *Decomposition of* $\mathbb{G}_m^n$

Subsection 2.2 shows that there is a functorial correspondence between the category of algebraic tori over finite fields and the category of $\mathbb{Z}$-modules with an automorphism. For instance, the torus $\mathrm{Res}_{\mathbb{F}_{q^d}/\mathbb{F}_q} \mathbb{G}_m$ corresponds to $\mathbb{Z}[X]/(X^q - 1)$, with the automorphism ω given by multiplication by X.

The identity $X^n - 1 = \prod_{d|n} \Phi_d(X)$ gives rise to the isomorphism $\mathbb{Q}[X]/(X^n - 1) \simeq \prod_{d|n} \mathbb{Q}[X]/\Phi_d(X)$. However, we do not necessarily have an isomorphism between $\mathbb{Z}[X]/(X^n - 1)$ and $\prod_{d|n} \mathbb{Z}[X]/\Phi_d(X)$. Still, we can write $(\mathbb{Z}[1/n])[X]/(X^n - 1) \simeq \prod_{d|n} (\mathbb{Z}[1/n])[X]/\Phi_d(X)$. Consequently, there exist two isogenies between the two algebraic groups $\mathrm{Res}_{\mathbb{F}_{q^n}/\mathbb{F}_q} \mathbb{G}_m$ and $\prod_{d|n} T_{\mathbb{F}_{q^d}}$ such that their composition is multiplication by a power of n.

Section 4 sketches how torus-based cryptography makes use of this decomposition up to isogeny. We will explain how the results in Section 3 on the coefficients of some specific polynomials allow us to compute these isogenies more efficiently.

3. *Inversion of* Φ_m *mod* Φ_n

We will describe in Section 4 how the arithmetic of cyclotomic polynomials can be used to compute parts of these isogenies. Notably, the expression for the resultant of cyclotomic polynomials turns out to be of great interest. Its computation goes back to Apostol [1], who gave the following formulae.

THEOREM 2 (Apostol [1]). *Let* $m > 1$*; then*

$$\mathrm{Res}(\Phi_1, \Phi_m) = \begin{cases} p & \text{if } m = p^a \text{ for } p \text{ prime and } a \geqslant 1, \\ 1 & \text{otherwise.} \end{cases}$$

Moreover, if $m > n > 1$*, then*

$$\mathrm{Res}(\Phi_m, \Phi_n) = \prod_{\substack{d|n \\ p \in \mathcal{P} \text{ such that } m/(m,d) = p^a}} p^{\mu(n/d)\varphi(m)/\varphi(p^a)} \tag{1}$$

where μ *is the Möbius function and* φ *the Euler totient function. This product is taken over all divisors* d *of* n *such that* $m/(m, d)$ *is a prime power* p^a*.*

COROLLARY 1 (Apostol [1]). *For all integers* $m > n \geqslant 1$*,*

$$\mathrm{Res}(\Phi_m, \Phi_n) \neq 1 \iff m = np^\alpha \text{ with } p \text{ prime and } \alpha \geqslant 1.$$

As a result, we can show the following condition for coprimality.

COROLLARY 2. *For any integer* q *and integers* $m > n \geqslant 1$*,* $\Phi_m(q)$ *and* $\Phi_n(q)$ *are coprime if* m *does not divide* n*.*

Proof. If m does not divide n, we know from Lemma 1 that $\mathrm{Res}(\Phi_m, \Phi_n) = 1$, which is true in $\mathbb{Z}$, and also in $\mathbb{Z}/\ell\mathbb{Z}$ for any $\ell \in \mathbb{Z}$, since 1 is unchanged. Now suppose that $\Phi_m(q)$ and $\Phi_n(q)$ have a common factor, say ℓ. Then Φ_m and Φ_n have a common root, q, in $\mathbb{Z}/\ell\mathbb{Z}$ and therefore their resultant is zero, which is false. □

It will be shown in Section 4 that knowledge of $\Phi_m(q)^{-1} \bmod \Phi_n(q)$ can be useful in cryptography, particularly information on the magnitude of its coefficients as a polynomial in q. The main theorem of this paper is dedicated to this question.

https://doi.org/10.1112/S1461157012000034 Published online by Cambridge University Press

Consider m and n such that the cyclotomic polynomials Φ_m and Φ_n are coprime. Then Φ_m is invertible modulo Φ_n, and we want to compute ${\Phi_m}^{-1}$ modulo Φ_n; more precisely, we would like to know the magnitude of its coefficients.

Since Φ_m and Φ_n are coprime, we have the Bézout relation

$$\Phi_m U + \Phi_n V = 1. \tag{2}$$

Our goal is to study $U = {\Phi_m}^{-1} \bmod \Phi_n$.

In this section we shall prove the four assertions of Theorem 1 in turn. Recall that $\Phi_n(1) = p$ if $n = p^\alpha$ is a prime power; otherwise $\Phi_n(1) = 1$ for $n > 1$.

3.1. *The $m = p$ and $n = 1$ case and its converse*

The cyclotomic polynomials Φ_p and Φ_1 are both easy to write down, and it is not difficult to obtain explicit expressions for their inverses.

PROPOSITION 1. *For any prime number p:*
- $\Phi_p^{-1} \bmod \Phi_1 = 1/p$;
- $\Phi_1^{-1} \bmod \Phi_p = -(X^{p-2} + 2X^{p-3} + \ldots + p - 1)/p$.

Proof. We simply check that the Bézout relation between Φ_p and Φ_1 is valid:

$$\begin{aligned} &-\Phi_1(X)(X^{p-2} + 2X^{p-3} + \ldots + p - 1) + \Phi_p(X) \\ &= (X-1)\sum_{k=0}^{p-2}(k+1-p)X^k + \Phi_p(X), \\ &= \sum_{k=1}^{p-1}(k-p)X^k - \sum_{k=0}^{p-2}(k+1-p)X^k + \sum_{k=0}^{p-1} X^k = p. \end{aligned}$$

□

3.2. *The $m = pr$ and $n = 1$ case and its converse*

The explicit expression of Φ_{pr} is less convenient than that of Φ_p, but we nonetheless have useful information, thanks to Lam and Leung [**15**].

PROPOSITION 2. *For all distinct prime numbers p and r:*
- $\Phi_{pr}^{-1} \bmod \Phi_1 = 1$;
- $\Phi_1^{-1} \bmod \Phi_{pr} = \sum_{i=0}^{(p-1)(r-1)-1} v_i X^i$ *with* $v_i \in \{-1, 0\}$.

Proof. We first look for U in the Bézout relation $\Phi_{pr}U + \Phi_1 V = 1$, and we know that it has degree zero. So a simple evaluation of this relation at 1 gives $U(1) = 1$, because $\Phi_{pr}(1) = 1$. Therefore ${\Phi_{pr}}^{-1} \bmod \Phi_1 = 1$.

Note that a similar technique would allow us to compute Φ_n^{-1} modulo Φ_1 for any n, since it is simply $\Phi_n(1)^{-1}$, which we know explicitly.

Now V is characterized by $(X-1)V(X) = 1 - \Phi_{pr}(X)$. Let $V(X) = \sum_{i=0}^{d} v_i X^i$ and $\Phi_{pr}(X) = \sum_{i=0}^{d+1} a_i X^i$ with $d = (p-1)(r-1) - 1$. Then we can write the equation as a linear system,

$$\begin{bmatrix} -1 & 0 & \ldots & 0 \\ 1 & -1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \ldots & 1 & -1 \end{bmatrix} \begin{bmatrix} v_0 \\ v_1 \\ \vdots \\ v_d \end{bmatrix} = \begin{bmatrix} 1 - a_0 \\ -a_1 \\ \vdots \\ -a_d \end{bmatrix} \Leftrightarrow \begin{bmatrix} v_0 \\ v_1 \\ \vdots \\ v_d \end{bmatrix} = \begin{bmatrix} 1 & 0 & \ddots & 0 \\ 1 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 1 & \ldots & 1 & 1 \end{bmatrix} \begin{bmatrix} a_0 - 1 \\ a_1 \\ \vdots \\ a_d \end{bmatrix}.$$

https://doi.org/10.1112/S1461157012000034 Published online by Cambridge University Press

We know from [15] that $a_0 = 1$ and $a_i \in \{0, \pm 1\}$ for all i. Moreover, the signs ($+1$ or -1) are alternating. So each v_i is necessarily 0 or ± 1. Furthermore, $a_0 = +1$, so the next non-zero coefficient equals -1. Thus, the alternating sum that defines each v_i starts with a -1, and consequently $v_i \in \{-1, 0\}$ for all i. □

3.3. *The $m = pr$ and $n = p$ case*

This time we will need the explicit expression for Φ_{pr}.

PROPOSITION 3. *For all distinct prime numbers p and r,*

$$\Phi_{pr}^{-1} \bmod \Phi_p = \frac{1}{r} \sum_{i=0}^{d} X^i \quad \textit{with } d = r - 1 \bmod p.$$

Proof. Let us directly show that $(1/r)(\sum_{i=0}^{d} X^i)\Phi_{pr} \equiv 1 \bmod \Phi_p$. For this purpose, we need to use the expression of Φ_{pr} given in [15]. Let s and t be two positive integers such that $(p-1)(r-1) = \varphi(pr) = sp + tr$. Then

$$\Phi_{pr}(X) = \left(\sum_{i=0}^{s} X^{ip}\right)\left(\sum_{j=0}^{t} X^{jr}\right) - \left(\sum_{i=s+1}^{r-1} X^{ip}\right)\left(\sum_{j=t+1}^{p-1} X^{jr}\right) X^{-pr}.$$

Thus,

$$\begin{aligned}\Phi_{pr}(X) \sum_{i=0}^{d} X^i \bmod \Phi_p &= \left((s+1)\sum_{j=0}^{t} X^{jr} - (r-1-s)\sum_{j=t+1}^{p-1} X^{jr}\right)\sum_{i=0}^{d} X^i, \\ &= \left((s+1)\sum_{j=0}^{p-1} X^{jr} - r\sum_{j=t+1}^{p-1} X^{jr}\right)\sum_{i=0}^{d} X^i.\end{aligned}$$

But $\Phi_p(X^r) = \sum_{j=0}^{p-1} X^{jr}$ and, since r is coprime with p, we have

$$\begin{aligned}\Phi_{pr}(X) \sum_{i=0}^{d} X^i \bmod \Phi_p &= -r \sum_{j=t+1}^{p-1} X^{jr} \sum_{i=0}^{d} X^i \\ &= r\frac{X^{(t+1)r} - 1}{X^r - 1}\,\frac{X^{d+1} - 1}{X - 1}.\end{aligned}$$

An explicit computation shows that $(t+1)r = 1 + pr - p(s+1)$. So $X^{(t+1)r} \equiv X \bmod \Phi_p$. Also, $d + 1 \equiv r \bmod p$ and hence $X^{d+1} \equiv X^r \bmod \Phi_p$, which leads to the result. Only r remains in the computed product. □

3.4. *The $m = p$ and $n = pr$ case*

PROPOSITION 4. *For all distinct prime numbers p and r,*

$$\Phi_p^{-1} \bmod \Phi_{pr} = \frac{1}{r} \sum_i v_i X^i \quad \textit{with } |v_i| < r.$$

Proof. We are looking for V in the Bézout relation $\Phi_{pr}U + \Phi_p V = 1$ To that end, we first compute $rV(X)$. We have

$$rV(X) = \frac{r - rU(X)\Phi_{pr}(X)}{\Phi_p(X)} = (-rU(X)\Phi_{pr}(X)) \div \Phi_p(X).$$

Here, the operator $\div$ evaluates the quotient in the Euclidean division of the left-hand side by the right-hand side. Note that removing the constant coefficient r only alters the remainder in this division.

https://doi.org/10.1112/S1461157012000034 Published online by Cambridge University Press

It is well known that $\Phi_{pr}(X) = \Phi_r(X^p)/\Phi_r(X)$; we will now rewrite $\Phi_r(X^p)$ using the following equality:

$$(X^p-1)\sum_{j=0}^{r-2}(r-1-j)X^{pj} = \sum_{j=0}^{r-2}(r-1-j)X^{p(j+1)} - \sum_{j=0}^{r-2}(r-1-j)X^{pj} = \Phi_r(X^p) - r.$$

We recall from Proposition 3 that $rU(X) = \sum_{i=0}^{d-1} X^i = (X^d-1)/(X-1)$ with $d \in [0, p[$ such that $r \equiv d \bmod p$. Moreover, $X^r - 1 = (X-1)\Phi_r(X)$, which finally leads to

$$rV(X) = \left(-(X-1)(X^d-1)\sum_{j=0}^{r-2}(r-1-j)X^{pj}\right) \div (X^r-1).$$

In the simple case where $r < p$, we have $d = r$. Thus, after simplifying by (X^r-1), we obtain $rV(X) = -(X-1)\sum_{j=0}^{r-2}(r-1-j)X^{pj}$ as the quotient of the division. Since the powers of the monomials in the sum increase by p, multiplying by $(X-1)$ leads to no collision. So the coefficients of rV do not exceed r in absolute value.

Let us now come to the case where $r > p$. First, we compute the Euclidean division of $\sum_{j=0}^{r-2}(r-1-j)X^{pj}$ by X^r-1. Let Q denote the quotient and R the remainder. For all $0 \leqslant j < r-2$, we can check that

$$X^{pj} = X^{pj \bmod r} + (X^r-1)\sum_{\substack{0\leqslant k<pj\\ k\equiv pj \bmod r}} X^k$$

by recognizing a geometric sum in the right-hand side. Hence

$$Q(X) = \sum_{j=0}^{r-2}(r-1-j)\sum_{\substack{0\leqslant k<pj\\ k\equiv pj \bmod r}} X^k \quad \text{and} \quad R(X) = \sum_{j=0}^{r-1}((-1-j/p) \bmod r)X^j. \tag{3}$$

We eventually find that

$$rV(X) = -(X-1)(X^d-1)Q(X) - ((X-1)(X^d-1)R(X)) \div (X^r-1).$$

Since $(X-1)(X^d-1)R(X)$ has degree less than $2r$, its quotient by (X^r-1) has degree less than r; therefore it is equal to the quotient by X^r. So it simply comes from the monomials of highest degree in $(X-1)(X^d-1)R(X)$. More precisely, let Q' denote this quotient; then it comes from the monomials of degree at least r in $(X^{d+1} - X^d - X)R(X)$. Write $a = 1/p \bmod r$, that is, the representative of the class of $1/p$ modulo r (in what follows, a quantity mod r will always mean its representative modulo r). We then have the first and last coefficients of Q':

$$Q'(X) = (a-1)X^d + \ldots - (r-1).$$

Indeed, the leading coefficient of R is $R_{r-1} = a-1$. The constant coefficient of Q' is the sum of coefficients of R, that is,

$$R_{r-d-1} - R_{r-d} - R_{r-1} = (da+a-1) \bmod r - (da-1) \bmod r - (a-1).$$

Now we need the value $(da+a-1) \bmod r$ in order to compute the difference from $(da-1) \bmod r$. If we let $d = r - ep$ with $e = \lfloor r/p \rfloor$, then $(da-1) \bmod r = -(e+1) \bmod r = r-e-1$. Let us now compare it with a. We know that $p(a \bmod r) = 1 + kr$ with $k \geqslant 1$ an integer.

- If $k = 1$, then $a = (r+1)/p = e+1$ by definition of the floor function.
- If $k \geqslant 2$, then $p(a) \geqslant r+p$ and thus $a \geqslant e+1$.

So, in any case, $(da-1) \bmod r + a \geqslant r$ and therefore

$$R_{r-d-1} - R_{r-d} - R_{r-1} = 1 - a + a - r = 1 - r.$$

Moreover, for all $1 \leqslant k < d$, the coefficient of the monomial X^k in Q' is

$$((-1-(r-d-1+k)/p) \bmod r) - ((-1-(r-d+k)/p) \bmod r) \in \{a, a-r\}.$$

https://doi.org/10.1112/S1461157012000034 Published online by Cambridge University Press

Similarly, we can show that the $d+1$ coefficients of lowest degree in $(X-1)(X^d-1)Q(X)$ (except the first one, which is zero) are given by the difference of two consecutive coefficients in $Q(X)$, that is, $-a$ or $r-a$. More precisely, we obtain

$$\begin{aligned}&((X-1)(X^d-1)Q(X) \bmod X^{d+1}) + ((X-1)(X^d-1)R(X)) \div (X^r-1)\\ &\quad = -X^d + (r-1)X - (r-1).\end{aligned}$$

Now we must find a bound for the coefficients of the monomials with degree greater than d in $(X^d-1)(X-1)Q(X)$.

First, note that each monomial of $(X-1)Q(X)$ is the difference of two consecutive monomials of Q, and is therefore an integer in $[a-r, a]$.

Similarly, any monomial of $(X^d-1)(X-1)Q(X)$ is the difference of monomials of $(X-1)Q(X)$ that are d steps away from each other. So none of these coefficients can exceed r in absolute value.

Now, in order to show that we can obtain neither r nor $-r$, we are going to show that two coefficients of $(X-1)Q(X)$ cannot be equal to $a-r$ and a if they are d steps away from each other.

From now on, for the sake of simplicity, values taken modulo r will be written in brackets. We start by rewriting equation (3):

$$Q(X) = \sum_{\substack{k=0\\ [ka]p \geqslant k+1}}^{p(r-2)} (r-1-[ka])X^k = \sum_{\substack{k=0\\ [ka]p \geqslant k+1}}^{p(r-2)} q_k X^k.$$

Next, following the example of the Kronecker delta, we will use δ to denote the Boolean evaluation of the assertion in the subscript; so its value equals $+1$ if the latter is true and 0 otherwise. Then the coefficient of X^k in $(X-1)Q(X)$ is given by

$$\Delta_k = q_{k-1} - q_k = (r-1-[(k-1)a])\delta_{[(k-1)a]p \geqslant k} - (r-1-[ka])\delta_{[ka]p \geqslant k+1}.$$

But $[(k-1)a] = [ka] - a$ if $[ak] \geqslant a$, and $[ka] - a + r$ otherwise; so we have the following cases.

Case 1: $0 \leqslant [ak] < a$.

We have $\Delta_k = (-1-[ka]+a)\delta_{(r-a)p+[ka]p \geqslant k} - (r-1-[ka])\delta_{[ka]p-1 \geqslant k}$.

- If $k > [ka]p + (r-a)p$, then $\Delta_k = 0$.
- If $[ka]p + (r-a)p \geqslant k > [ka]p - 1$, then $0 \leqslant \Delta_k = a - 1 - [ka] < a$.
- If $[ka]p - 1 \geqslant k$, then $\Delta_k = (-1-[ka]+a) - (r-1-[ka]) = a - r$.

Case 2: $a \leqslant [ak] < r$.

We have $\Delta_k = (r-1-[ka]+a)\delta_{[ka]p \geqslant k+ap} - (r-1-[ka])\delta_{[ka]p \geqslant k+1}$.

- If $[ka]p < k+1$, then $\Delta_k = 0$.
- If $k+1 \leqslant [ka]p < k+ap$, then $0 \geqslant \Delta_k = -r+1+[ka] > -r+a$.
- If $k+ap \leqslant [ka]p$, then $\Delta_k = (r-1-[ka]+a) - (r-1-[ka]) = a$.

Now the coefficient of X^k in $(X^d-1)(X-1)Q(X)$ is the difference $\Delta_{k-d} - \Delta_k$. The bounds above show that it is always smaller than r in absolute value, except when one of the terms equals $a-r$ and the other equals a.

Case 1: $\Delta_k = a - r$ and $\Delta_{k-d} = a$.

We have $0 \leqslant [ak] < a$, $[ka]p - 1 \geqslant k$, $a \leqslant [a(k-d)] < r$ and $k - d + ap \leqslant [(k-d)a]p$.

- If $[ak] > [ad]$, then $[a(k-d)] = [ak] - [ad]$ and so $a > [ak] \geqslant a + [ad]$, which is impossible.
- If $[ak] < [ad]$, then $[a(k-d)] = [ak] - [ad] + r$ and so $[ak] - [ad] + r \geqslant a$. Putting $\eta = [ad]$, we finally obtain

$$a + \eta - r \leqslant [ak] < a.$$

https://doi.org/10.1112/S1461157012000034 Published online by Cambridge University Press

Note that if $k' = k + p$, then $[ak'] = [ak] + 1$, which leads to $k \in \{k_1, k_1 + p, \ldots, k_2\}$, with bounds such that $[ak_1] = a - (r - \eta)$ and $[ak_2] = a - 1$. Since $[a(d+1)] = [a + \eta] = [a + \eta - r]$, we have $[k_1] = d + 1$ and thus $k_2 = d + 1 + (r - \eta - 1)p$. The possible values for k are $k = d + 1 + xp$ where $x \in \{0, 1, \ldots, r - \eta - 1\}$, with $0 \leqslant d + 1 < r$ being the first one.

The inequality $k - d + ap \leqslant [(k-d)a]p$ leads to $1 + (a + x)p \leqslant [a + x]p$. On the one hand, this is possible only if $(a + x)$ exceeds r. But, on the other hand, this would also imply $1 + (a + x)p < rp$ and thus $a + x < r$, which is a contradiction.

Case 2: $\Delta_k = a$ and $\Delta_{k-d} = a - r$.

We have $0 \leqslant [a(k-d)] < a$, $[(k-d)a]p - 1 \geqslant k - d$, $a \leqslant [ak] < r$ and $k + ap \leqslant [ka]p$.

- If $[ak] < [ad]$, then $[ak] - [ad] + r < a \leqslant [ak]$, which is impossible.
- If $[ak] > [ad]$, then $[a(k-d)] = [ak] - [ad]$. As before, the inequalities give bounds for $[ak]$:

$$a \leqslant [ak] < a + \eta.$$

This corresponds to η values for k consisting of an arithmetic progression with common difference p and starting at $k_1 = 1$, such that $[ak_1] = a$. So we can write $k = 1 + xp$ with $x \in \{0, \ldots, \eta - 1\}$. Then the inequality $k + ap \leqslant [ka]p$ becomes $1 + (x + a)p \leqslant [a + x]p$, which gives the same contradiction as in the previous case.

Therefore, we have finally shown that no coefficient of $(X^d - 1)(X - 1)Q(X)$ is equal to r or $-r$, which completes the proof. □

3.5. *The case of $m = p$ and $n = r$ where p and r are two distinct primes*

Before giving a proof of the last assertion in Theorem 1, we need to work on the general problem. The idea is to evaluate our Bézout relation at the roots of Φ_n and to interpolate U from the values found at these points. We are going to slightly modify the equation to obtain a more convenient linear system.

Recall that $\Phi_p U + \Phi_r V = 1$; see equation (2). If we multiply both sides by $X - 1$, we obtain $\Phi_p \widetilde{U} + (X^r - 1)V = X - 1$, with $\widetilde{U} = (X - 1)U$.

The roots of $X^r - 1$ are the rth roots of 1, $\{\xi^j : 0 \leqslant j \leqslant r - 1\}$. The evaluation of our Bézout relation at these points gives

$$\Phi_p(\xi^j)\widetilde{U}(\xi^j) = \xi^j - 1 \quad \text{for all } 0 \leqslant j \leqslant r - 1.$$

If we write $\widetilde{U} = \sum_{i=1}^{r} \widetilde{u}_i X^{i-1}$, then the equation can be expressed as

$$\sum_{i=1}^{r} \widetilde{u}_i (\xi^j)^{i-1} = (\xi^j - 1)(\Phi_p(\xi^j))^{-1} \quad \text{for all } 0 \leqslant j \leqslant r - 1.$$

We first work on $\widetilde{U}$ and its coefficients.

LEMMA 1. *For $1 \leqslant i \leqslant r$,*

$$\widetilde{u}_i \in \{0, +1, -1\}.$$

Proof. The coefficients $(\widetilde{u}_i)_{1 \leqslant i \leqslant r}$ are the solutions of a system of linear equations, the matrix version of which is $A\widetilde{U} = W$ where $W = \left[(\xi^j - 1)\Phi_p(\xi^j)^{-1}\right]_{0 \leqslant j \leqslant r-1}$ and

$$A = \begin{bmatrix} 1 & 1 & \ldots & 1 \\ 1 & \xi & \ldots & \xi^{r-1} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \xi^{r-1} & \ldots & (\xi^{r-1})^{r-1} \end{bmatrix} = \mathrm{VdM}(1, \xi, \ldots, \xi^{r-1}).$$

https://doi.org/10.1112/S1461157012000034 Published online by Cambridge University Press

Here VdM denotes the Vandermonde matrix. The matrix A is invertible, since all of the $(\xi^i)_{i\in\{0,\dots,r-1\}}$ are distinct. Thus we can give an explicit resolution of the system: $\widetilde{U} = A^{-1}W$. It is proven in [24] that the inverse of such a Vandermonde matrix (where ξ is a primitive root of unity of order r) is still a Vandermonde matrix, with inverse coefficients. Here $A^{-1} = (1/r)\,\mathrm{VdM}(1, \xi^{-1}, \dots, \xi^{-r+1})$, that is, its explicit coefficients are $A^{-1} = (1/r)[(\xi^{-(i-1)})^{j-1}]_{\substack{1\leqslant i\leqslant r\\ 0\leqslant j\leqslant r-1}}$.

Thus, the solutions of the linear system are given by

$$\widetilde{u}_i = \frac{1}{r}\sum_{j=0}^{r-1}(\xi^{-(i-1)})^j(\xi^j - 1)\Phi_p(\xi^j)^{-1}, \quad 1 \leqslant i \leqslant r.$$

Now, using $\Phi_p(X) = (1-X^p)/(1-X)$, we find that

$$\widetilde{u}_i = \frac{1}{r}\sum_{j=0}^{r-1}(\xi^{1-i})^j(\xi^j - 1)\frac{1-\xi^j}{1-\xi^{jp}}, \quad 1 \leqslant i \leqslant r.$$

We can improve this expression by using the relation

$$\frac{1}{1-\xi^{jp}} = \frac{1}{r}(\xi^{jp(r-2)} + 2\xi^{jp(r-3)} + \dots + (r-1)).$$

Indeed, it is easy to show that

$$(1-\xi^{jp})\sum_{k=0}^{r-2}(r-1-k)\xi^{jpk} = r.$$

So the final expression, for all $1 \leqslant i \leqslant r$, is

$$\widetilde{u}_i = \frac{1}{r^2}\sum_{k=0}^{r-2}(r-k-1)\sum_{j=0}^{r-1}\xi^{j(1-i)}(\xi^j - 1)(1-\xi^j)\xi^{jpk}.$$

After expanding and collecting terms, we will work on the following form for any given i:

$$\begin{aligned}\widetilde{u}_i &= -\frac{1}{r^2}\sum_{k=0}^{r-2}(r-k-1)\sum_{j=0}^{r-1}(\xi^{j(pk+1-i)} - 2\xi^{j(pk+2-i)} + \xi^{j(pk+3-i)})\\ &= -\frac{1}{r^2}\sum_{k=0}^{r-2}(r-k-1)(S_1(k) - 2S_2(k) + S_3(k))\end{aligned}$$

where $S_l(k) = \sum_{j=0}^{r-1}\xi^{j(pk+l-i)}$.

The sums $S_l = \sum_{j=0}^{r-1}(\xi^A)^j$ are actually sums of all the powers of an rth root of 1. So if ξ^A is a prime root of 1, the sum simply equals 0. And if ξ^A is not a prime root of 1, the only possibility is $\xi^A = 1$ (that is, $A \equiv 0 \bmod r$), and in this case the sum equals r. Therefore

$$S_l(k) = \begin{cases} 0 & \text{if } pk + l - i \not\equiv 0 \bmod r,\\ r & \text{if } pk + l - i \equiv 0 \bmod r.\end{cases}$$

With the notation of Section 3.4, $a = p^{-1} \bmod r$, put $k_l = a(i-l) \bmod r$ such that $S_l(k_l) = r$. Then $\sum_{k=0}^{r-2}(r-k-1)S_l(k) = (r-k_l-1)r$. Note that this formula holds even when $k_l = r-1$: in this case the contribution of the sums $S_l(k)$ is zero. Putting the three sums together leaves us with

$$\begin{aligned}\widetilde{u}_i &= -\frac{1}{r}[-k_1 + 2k_2 - k_3],\\ &= \frac{1}{r}[a(i-1) \bmod r - 2(a(i-2) \bmod r) + (a(i-3) \bmod r)].\end{aligned} \tag{4}$$

https://doi.org/10.1112/S1461157012000034 Published online by Cambridge University Press

Writing $A_i = a(i-1) \bmod r$, we can split this expression into

$$\widetilde{u}_i = \frac{1}{r}\Big(\underbrace{[A_i - A_{i-1}]}_{D_i} - \underbrace{[A_{i-1} - A_{i-2}]}_{D_{i-1}}\Big),$$

which leads to the following four cases.

- If $D_i = a$ and $D_{i-1} = a$, then $\widetilde{u}_i = 0$.
- If $D_i = a$ and $D_{i-1} = a - r$, then $\widetilde{u}_i = 1$.
- If $D_i = a - r$ and $D_{i-1} = a$, then $\widetilde{u}_i = -1$.
- If $D_i = a - r$ and $D_{i-1} = a - r$, then $\widetilde{u}_i = 0$.

So $\widetilde{u}_i \in \{-1, 0, +1\}$. □

PROPOSITION 5. *For all distinct prime numbers p and r,*

$$\Phi_p^{-1} \bmod \Phi_r = \sum_{j=1}^{r-1} u_j X^{j-1} \quad \textit{with } u_j \in \{-1, 0, +1\}.$$

Proof. Now we can compute the coefficients of U such that $\widetilde{U} = (X-1)U$. A similar calculation has been performed for the proof of Proposition 2, which leads to the following matrix formulation:

$$\begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_{r-1} \end{bmatrix} = - \begin{bmatrix} 1 & 0 & \dots & 0 \\ 1 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 1 & \dots & 1 & 1 \end{bmatrix} \begin{bmatrix} \widetilde{u}_1 \\ \widetilde{u}_2 \\ \vdots \\ \widetilde{u}_{r-1} \end{bmatrix}.$$

Since u_j is a sum of consecutive coefficients $\widetilde{u}_i$, all we need to prove is that $+1$ and -1 alternate in $(\widetilde{u}_i)_{1 \leqslant i \leqslant r-1}$ (among possible zeros). With the notation above, recall from the proof of Lemma 1 that for all $1 \leqslant i \leqslant r$,

$$\widetilde{u}_i = \begin{cases} 1 & \text{if } D_i = a \text{ and } D_{i-1} = a - r, \\ -1 & \text{if } D_i = a - r \text{ and } D_{i-1} = a, \\ 0 & \text{if } D_i = D_{i-1}. \end{cases} \tag{5}$$

Given $\widetilde{u}_i$ for any $1 \leqslant i \leqslant r-1$, we want to show that the next non-zero coefficient differs from $\widetilde{u}_i$. In other words, letting j be the smallest integer greater than i such that $\widetilde{u}_j \neq 0$, we aim to show that $\widetilde{u}_j \neq \widetilde{u}_i$.

If $\widetilde{u}_i = 0$, this is obvious. Now suppose that $\widetilde{u}_i = 1$. Then we know from equation (5) that $D_i = a$ and $D_{i-1} = a - r$. By the definition of j, we have $\widetilde{u}_{i+1} = \ldots = \widetilde{u}_{j-1} = 0$; hence, thanks to equation (5) again, $D_i = Di + 1 = \ldots = D_{j-1}$. So $D_{j-1} = a$, and thus $\widetilde{u}_j = -1 \neq \widetilde{u}_i$. Note that this still holds if $j = i + 1$, since we would then simply have $D_i = D_{j-1}$. And, of course, the argument works in exactly the same way for $\widetilde{u}_i = -1$.

This completes the proof, since the alternation of $+1$ and -1 in $(\widetilde{u}_i)_{1 \leqslant i \leqslant r}$ shows that $u_j \in \{-1, 0, +1\}$ for all $1 \leqslant j \leqslant r-1$. □

4. *A cryptographic application*

Beyond the simple arithmetic context of our computation, we have found a direct application in torus-based cryptography. In this section we will briefly describe how Theorem 1 has been used in [**12**]. We refer to the latter paper for more details and further references.

Over the past twenty years, practical torus-based cryptosystems have been constructed for different extension degrees such as 2, 3 and 6 (see, for instance, LUC[**21**], XTR[**16**] or CEILEIDH[**19**]). Yet the search for rational parametrizations of algebraic tori has raised several

https://doi.org/10.1112/S1461157012000034 Published online by Cambridge University Press

unsolved questions. Following the ideas of van Dijk and Woodruff [11], we construct a map θ whose kernel is annihilated by a power of n, so that θ is not far from being a bijection:

$$\theta : T_n(\mathbb{F}_q) \times \prod_{\substack{d|n \\ \mu(n/d)=-1}} \mathbb{F}_{q^d}^{\times} \to \prod_{\substack{d|n \\ \mu(n/d)=+1}} \mathbb{F}_{q^d}^{\times}. \tag{6}$$

This kind of parametrization has applications in such cryptosystems as Diffie–Hellman multiple key exchange. In [12] we present a practical implementation of this map, whose efficiency relies on the use of a certain class of normal bases (see [10]) in the representation of field extensions.

We suppose that the dimension n is the product of two distinct primes p and r, and we now give explicit details concerning the computation of θ.

In what follows, we shall use several times the following principle. Given the resultant of two polynomials P and Q, we know that there exist U and V such that

$$U(X)P(X) + V(X)Q(X) = \mathrm{Res}(P, Q).$$

Evaluating this relation at some integer yields a Bézout-like relation showing that $\mathrm{pgcd}(P(q), Q(q))$ divides $\mathrm{Res}(P, Q)$. In particular, if we use Theorem 2, we get a relation between the evaluations of two cyclotomic polynomials:

$$U(q)\Phi_n(q) + V(q)\Phi_m(q) = \mathrm{Res}(\Phi_n, \Phi_m).$$

Let us first consider the simple example of $\mathbb{F}_{q^p}^{\times}$. Let T_1 and T_p denote its subgroups of order $q-1$ and $\Phi_p(q)$, respectively. Then we have the following two norm maps:

$$\begin{array}{rcl} \mathbb{F}_{q^p}^{\times} & \to & T_1 \\ x_p & \mapsto & x_p^{\Phi_p(q)} \end{array} \quad \text{and} \quad \begin{array}{rcl} \mathbb{F}_{q^p}^{\times} & \to & T_p \\ x_p & \mapsto & x_p^{q-1}. \end{array}$$

Furthermore, since $\mathrm{Res}(\Phi_1, \Phi_p) = p$, we can obtain an equation linking $q-1$ and $\Phi_p(q)$,

$$\Phi_p(q)u_1 + (q-1)u_p = p$$

where u_1 and u_p are integers. Thus we also have the following reverse map:

$$\begin{array}{rcl} T_1 \times T_p & \to & \mathbb{F}_{q^p}^{\times} \\ (t_1, t_p) & \mapsto & t_1^{u_1} t_p^{u_p}. \end{array}$$

This map is such that its composition with the product of the two norm maps above results in multiplication by p.

We have a similar construction for $\mathbb{F}_{p^r}^{\times}$, where T_r denotes its subgroup of order $\Phi_r(q)$:

$$\begin{array}{rcl} \mathbb{F}_{q^r}^{\times} & \to & T_1 \times T_r \\ x_r & \mapsto & (x_r^{\Phi_r(q)}, x_r^{q-1}) \\ t_1^{v_1} t_r^{v_r} & \leftarrow\!\shortmid & (t_1, t_r) \end{array}$$

with the relation $\Phi_r(q)v_1 + (q-1)v_r = r$.

Now, in the case of $\mathbb{F}_{q^{pr}}^{\times}$, we consider the four subgroups of order $q-1$, $\Phi_p(q)$, $\Phi_r(q)$ and $\Phi_{pr}(q)$, which we call T_1, T_p, T_r and T_{pr}, respectively. Of course, $T_1 = \mathbb{F}_q^{\times}$, $T_p \subset \mathbb{F}_{q^p}^{\times}$ and $T_r \subset \mathbb{F}_{q^r}^{\times}$.

We have the following map whose components are the four natural norms:

$$\begin{array}{rcl} \mathbb{F}_{q^{pr}}^{\times} & \to & T_1 \times T_p \times T_r \times T_{pr} \\ x_{pr} & \mapsto & (x_{pr}^{U_1(q)}, x_{pr}^{U_p(q)}, x_{pr}^{U_r(q)}, x_{pr}^{U_{pr}(q)}), \end{array}$$

where $U_k(X) = (X^{pr} - 1)/\Phi_k(X)$.

https://doi.org/10.1112/S1461157012000034 Published online by Cambridge University Press

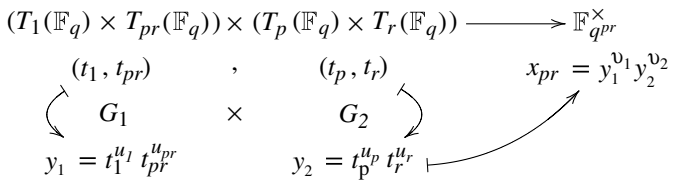

FIGURE 1. *Reconstruction step in the case $n = pr$.*

Now we look for an inverse of this map. Following the previous example, for any Bézout-like relation

$$U_1V_1 + U_pV_p + U_rV_r + U_{pr}V_{pr} = pr,$$

we can construct a map

$$\begin{aligned} T_1 \times T_p \times T_r \times T_{pr} &\to \mathbb{F}_{q^{pr}}^{\times} \\ (t_1, t_p, t_r, t_{pr}) &\mapsto t_1^{V_1(q)} t_p^{V_p(q)} t_r^{V_r(q)} t_{pr}^{V_{pr}(q)} \end{aligned}$$

such that the composition of the two maps yields multiplication by pr on $\mathbb{F}_{q^{pr}}^{\times}$.

In practice, we obtain such a relation in two steps. First we write two Bézout relations, between Φ_{pr} and Φ_1 on the one hand and between Φ_p and Φ_r on the other hand. So the first step consists of two mappings,

$$\begin{aligned} T_1 \times T_{pr} &\xrightarrow{\sim} G_1 \subset \mathbb{F}_{q^{pr}}^{\times} \\ (t_1, t_{pr}) &\mapsto y_1 = t_1^{u_1} t_{pr}^{u_{pr}} \end{aligned} \quad \text{where } \Phi_{pr}(q)u_1 + \Phi_1(q)u_{pr} = 1$$

and

$$\begin{aligned} T_p \times T_r &\xrightarrow{\sim} G_2 \subset \mathbb{F}_{q^{pr}}^{\times} \\ (t_p, t_r) &\mapsto y_2 = t_p^{u_p} t_r^{u_r} \end{aligned} \quad \text{where } \Phi_r(q)u_p + \Phi_p(q)u_r = 1.$$

Then we write a Bézout-like relation linking $\Phi_p\Phi_r$ and $\Phi_1\Phi_{pr}$. Theorem 1 ensures that $(\Phi_p\Phi_r)^{-1}$ yields a factor $1/pr$ both modulo Φ_1 and modulo Φ_{pr}. After recombination, this results in the following relation: there exist polynomials V_1 and V_2 with integer coefficients such that

$$(\Phi_p\Phi_r)V_1 + (\Phi_1\Phi_{pr})V_2 = pr.$$

Thus, we combine the images $y_1 \in G_1$ and $y_2 \in G_2$ to form the element of $\mathbb{F}_{q^{pr}}$,

$$\begin{aligned} G_1 \times G_2 &\to \mathbb{F}_{q^{pr}}^{\times} \\ (y_1, y_2) &\mapsto y_1^{V_1(q)} y_2^{V_2(q)}. \end{aligned}$$

We set $v_1 = V_1(q)$ and $v_2 = V_2(q)$; this process is summarized in Figure 1.

All in all, by composing the different decompositions and recombinations presented here, we manage to provide an explicit way of computing the map θ (see Figure 2).

We note that the computation of this isogeny involves peculiar powers, which are based on evaluations in q of modular inverses of cyclotomic polynomials. The values of their coefficients and the bounds of Theorem 1 proved in Section 3 ensure the low cost of this computation. We make use of a certain class of normal bases [**10**], which allows efficient arithmetic in $\mathbb{F}_{q^n}$. See [**12**] for more details.

https://doi.org/10.1112/S1461157012000034 Published online by Cambridge University Press

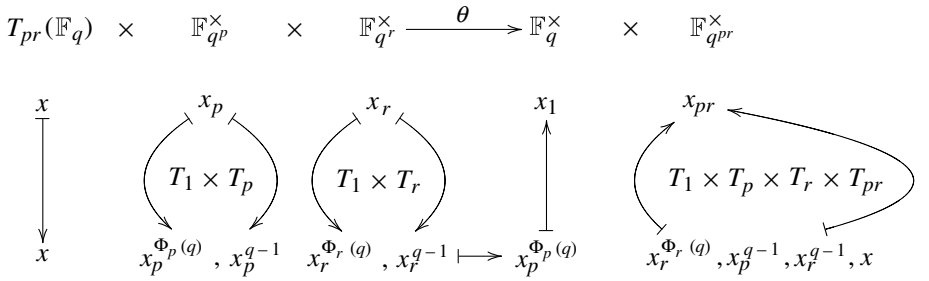

FIGURE 2. *Parametrization of* T_{pr}.

For instance, if we consider the example of $n = 15 = 3 \times 5$, then an explicit computation gives the following values, with the notation of Figure 1:

$$\begin{cases} u_1 = 1 \quad \text{and} \quad u_{15} = -q^7 - q^4 - q^2 - q, \\ u_3 = -q \quad \text{and} \quad u_5 = q^3 + 1, \\ v_1 = 2q^8 - 2q^7 - 3q^6 + 8q^5 - 10q^4 + 6q^3 + 7q^2 - 16q + 9, \\ v_2 = -2q^5 - 6q^4 - 9q^3 - 12q^2 - 10q - 6. \end{cases}$$

Acknowledgements. The author wishes to thank Delphine Boucher, Jean-Marc Couveignes, Reynald Lercier and the anonymous referee for their careful reading and useful suggestions.

References

1. T. M. APOSTOL, 'Resultants of cyclotomic polynomials', *Proc. Amer. Math. Soc.* 24 (1970) 457–462.
2. G. BACHMAN, 'On the coefficients of ternary cyclotomic polynomials', *J. Number Theory* 100 (2003) 104–116.
3. A. S. BANG, 'Om Ligningen $\phi_n(x) = 0$', *Nyt Tidsskrift for Mathematic* 6 (1895) 6–12.
4. P. T. BATEMAN, 'Note on the coefficients of the cyclotomic polynomial', *Bull. Amer. Math. Soc.* 55 (1949) 1180–1181.
5. M. BEITER, 'Magnitude of the coefficients of the cyclotomic polynomial F_{pqr}', *Amer. Math. Monthly* 75 (1968) 370–372.
6. M. BEITER, 'Magnitude of the coefficients of the cyclotomic polynomial F_{pqr}, II', *Duke Math. J.* 38 (1971) 591–594.
7. D. M. BLOOM, 'On the coefficients of the cyclotomic polynomials', *Amer. Math. Monthly* 75 (1968) 372–377.
8. L. CARLITZ, 'The number of terms in the cyclotomic polynomial F_{pqr}', *Amer. Math. Monthly* 73 (1966) 979–981.
9. J.-M. COUVEIGNES, 'Quelques mathématiques de la cryptologie à clés publiques', *Nouvelles méthodes mathématiques pour la cryptographie*, Journée annuelle de la SMF 2007 (Société mathématique de France, Paris, 2007.
10. J.-M. COUVEIGNES and R. LERCIER, 'Elliptic periods for finite fields', *Finite Fields Appl.* 15 (2009) 1–22.
11. M. VAN DIJK and D. WOODRUFF, 'Asymptotically optimal communication for torus-based cryptography', *Crypto 2004*, Lecture Notes in Computer Science 3152Springer, Berlin, 157–178.
12. C. DUNAND and R. LERCIER, 'Elliptic bases and torus-based cryptography', *Ninth international conference on finite fields and applications* (eds G. McGuire *et al.*; American Mathematical Society, Providence, RI, 2009) 137–153.
13. P. ERDÖS, 'On the coefficients of the cyclotomic polynomial', *Bull. Amer. Math. Soc.* 52 (1946) 179–184.
14. Y. GALLOT and P. MOREE, 'Ternary cyclotomic polynomials having a large coefficient', *J. reine angew. Math.* 632 (2009) 105–125.
15. T. Y. LAM and K. H. LEUNG, 'On the cyclotomic polynomial $\Phi_{pq}(X)$', *Amer. Math. Monthly* 103 (1996) 562–564.
16. A. K. LENSTRA and E. R. VERHEUL, 'The XTR public key system', *Advances in cryptology—Crypto 2000*, Lecture Notes in Computer Science 1880 (ed. M. Bellare; Springer, Berlin, 2000) 1–19.
17. A. MIGOTTI, 'Zur Theorie der Kreisteilungsgleichung', *S.-B. der Math.-Naturwiss. Classe der Kaiserlichen Akademie der Wissenschaften, Wien* 87 (1883) 7–14.
18. P. MOREE, 'Inverse cyclotomic polynomials', *J. Number Theory* 129 (2009) 667–680.
19. K. RUBIN and A. SILVERBERG, 'Torus-based cryptography', *Crypto 2003*, Lecture Notes in Computer Science 2729 (Springer, Berlin, 2003) 349–365.

20. K. Rubin and A. Silverberg, 'Algebraic tori in cryptography', *High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams*, Fields Institute Communications 41 (American Mathematical Society, Providence, RI, 2004) 317–326.
21. P. J. Smith and M. J. Lennon, 'LUC: a new public key system', *Proceedings of the IFIP/SEC 1993* (Elsevier Science Publications, 1994).
22. V. E. Voskresenskiĭ, *Algebraic groups and their birational invariants*, Translations of Mathematical Monographs 179 (American Mathematical Society, Providence, RI, 1991).
23. A. Weil, *Adeles and algebraic groups*, Progress in Mathematics 23 (Birkhäuser, Boston, 1982).
24. J. von zur Gathen and J. Gerhard, *Modern computer algebra* (Cambridge University Press, 1999).

Clément Dunand
Institut de recherche mathématique de Rennes
Université de Rennes 1
Campus de Beaulieu
F-35042 Rennes Cedex
France

clement.dunand@wanadoo.fr

https://doi.org/10.1112/S1461157012000034 Published online by Cambridge University Press