Functiones et Approximatio
58.1 (2018), 105–116
doi: 10.7169/facm/1652

EUCLIDEAN PROOFS FOR FUNCTION FIELDS

Thomas Lachmann

Abstract: Schur proved the infinitude of primes in arithmetic progressions of the form $\equiv l \mod m$, such that $l^2 \equiv 1 \mod m$, with non-analytic methods by ideas inspired from the famous proof Euclid gave for the infinitude of primes. Ram Murty showed that Schur's method has its limits given by the assumption Schur made. We will discuss analogous for the primes in the ring $\mathbb{F}_q[T]$.

Keywords: Euclidean proof, function fields, Carlitz module.

1. Euclidean proofs

Definition 1.1. Let $\mathbb{F}_q$ be a finite field with q elements and $F \in \mathbb{F}_q[T][X]$. A prime $p \in \mathbb{F}_q[T]$ is called *prime divisor of* F if there is an element $n \in \mathbb{F}_q[T]$ such that $p \mid F(n)$, which is denoted by $p \mid F$. We write $\mathcal{P}(F)$ for the set of all prime divisors of F.

Lemma 1.2. *Each non-constant polynomial* $F \in \mathbb{F}_q[T][X]$ *has infinitely many prime divisors.*

Proof. We can assume $F(0) = c \neq 0$, otherwise for all $p \in \mathbb{F}_q[T]$ holds $p \mid F(p)$ already. For $n \in \mathbb{F}_q[T]$, with $\deg(n)$ sufficiently large, it is $F(n) \notin \mathbb{F}_q$, hence F has at least one prime divisor. Now assume that F has only finitely many prime divisors $p_1, \ldots, p_n$. Let $Q = p_1 p_2 \ldots p_n$. It is $F(QcX) = cG(X)$ for a polynomial $G \in \mathbb{F}_q[T][X]$ with $G = 1 + b_1 X + b_2 X^2 + \ldots$ and $Q \mid b_i$ for all $i \leqslant \deg(G)$. As we have seen above we know that G has at least one prime divisor p, too. Obviously, every prime divisor of G is also one of F. But then $p \nmid Q$ holds and $p \mid 1$ would be true. Therefore p has to be another prime divisor of F - a contradiction. Hence F has infinitely many prime divisors. ■

The proof of the following generalization is based on an idea of Hornfeck (see [5]).

The author is supported by the Austrian Science Fund (FWF), project Y-901.
2010 Mathematics Subject Classification: primary: 11R02

Lemma 1.3. $|\mathcal{P}(F) \cap \mathcal{P}(G)| = \infty$ *holds for every two non-constant polynomials* $F, G \in \mathbb{F}_q[T][X]$.

Proof. Let a resp. b be roots of F resp. G. With a result of Becker and Maclane (see [3]), in which they show that for a field K of characteristic p with $[K : K^p] = p$ every extension of K is simple, it follows that $\mathbb{F}_q(T)(a, b) = \mathbb{F}_q(T)(c)$ for an element $c \in \overline{\mathbb{F}_q(T)}$, where $\overline{\mathbb{F}_q(T)}$ is the algebraic closure of $\mathbb{F}_q(T)$. Say $H \in \mathbb{F}_q(T)[X]$ is the minimal polynomial of c. Therefore there are $A, B \in \mathbb{F}_q(T)[X]$ such that $A(c) = a$ and $B(c) = b$ exist.

We can also assume that A and B of the kind so that $A(0) = B(0) = 0$ holds. Otherwise replace for example A by

$$A^*(X) = A(X) - \frac{A(0)}{H(0)}H(X)$$

and in the same way for B.

It follows:

$$F(A(c)) = 0 \qquad \text{and} \qquad G(B(c)) = 0$$

Hence H, as the minimal polynomial of c, appears as factor in $F(A(X))$ and $G(B(X))$. We see

$$F(A(X)) = F^*(X)H(X) \qquad \text{and} \qquad G(B(X)) = G^*(X)H(X)$$

holds for suitable $F^*, G^* \in \mathbb{F}_q(T)[X]$. Denote by $a, b, h \in \mathbb{F}_q[T]$ least common denominator of the coefficient of A, B, H. Therefore we have

$$hF(A(abX)),\ hG(B(abX)),\ hH(abX) \in \mathbb{F}_q[T][X]$$

and

$$hF(A(abX)) = F^*(abX)hH(abX) \quad \text{and} \quad hG(B(abX)) = G^*(abX)hH(abX).$$

We see that every prime divisor of $hH(abX)$ is also a prime divisor of $hF(A(abX))$ and $hG(B(abX))$. At last, it follows that F and G have infinitely many common prime divisors, since $hH(abX)$ already possesses infinitely many. ■

Definition 1.4. We denote by $\mathbb{F}_q[T] < \tau >$ the polynomial ring in the variable τ with *twisted multiplication* in respect to τ. The elements in $\mathbb{F}_q[T] < \tau >$ are of the form

$$a_n\tau^n + \ldots + a_1\tau + a_0 \qquad \text{with } \ a_0, \ldots, a_n \in \mathbb{F}_q[T].$$

Here the multiplication of two ring elements out of $\mathbb{F}_q[T] < \tau >$ is well-defined by

$$\tau T := T^q\tau,$$

as one can verify easily.

The $\mathbb{F}_q$−homomorphism

$$C : \mathbb{F}_q[T] \to \mathbb{F}_q[T] < \tau > \qquad \text{with } \; T \mapsto T + \tau$$

is called the *Carlitz module* and for $m \in \mathbb{F}_q[T]$ the image under C is denoted by C_m and is called the *Carlitz module for* m in $\mathbb{F}_q[T]$. Here C_m can be seen as an endomorphism of $\mathbb{F}_q[T]$ via

$$C_m : \mathbb{F}_q[T] \to \mathbb{F}_q[T], \qquad n \mapsto C_m \cdot n,$$

in which the multiplication is well-defined through

$$\tau \cdot n = n^q.$$

We then also write $C_m(n)$ instead of $C_m \cdot n$.

We denote the so-called *Carlitz polynomial for* m *in* $\mathbb{F}_q[T]$ by $C_m(X) = C_m \cdot X \in \mathbb{F}_q[T][X]$. In this case $\tau \cdot X = X^q$ also holds.

Let $m \in \mathbb{F}_q[T]$ be written as $m = \alpha_n T^n + \ldots + \alpha_1 T + \alpha_0$. Then we can calculate the Carlitz module for m in the following way:

$$\begin{aligned} C_m &= C_{\alpha_n T^n} + \ldots + C_{\alpha_1 T} + C_{\alpha_0} \\ &= C_{\alpha_n} C_{T^n} + \ldots + C_{\alpha_1} C_T + C_{\alpha_0} \\ &= \alpha_n (C_T)^n + \ldots + \alpha_1 C_T + \alpha_0 \\ &= \alpha_n (T+\tau)^n + \ldots + \alpha_1 (T+\tau) + \alpha_0 \end{aligned}$$

Therefore the associated Carlitz polynomial is

$$\begin{aligned} C_m(X) &= (\alpha_n (C_T)^n + \ldots + \alpha_1 C_T + \alpha_0) \cdot X \\ &= \alpha_n (C_T)^n \cdot X + \ldots + \alpha_1 C_T \cdot X + \alpha_0 X \\ &= \alpha_n (T+\tau)^n \cdot X + \ldots + \alpha_1 (T+\tau) \cdot X + \alpha_0 X. \end{aligned}$$

To calculate this correctly one has to have the special multiplication with τ within the mapping C_m in mind: $C_T = T + \tau$, $C_{T^2} = C_T C_T = (T+\tau)(T+\tau) = T^2 + (T + T^q)\tau + \tau^2$, etc.

One sees immediately that the linearity of C_m seen as homomorphism transfers to the associated polynomial, since for $f = \alpha_n T^n + \ldots + \alpha_1 T + \alpha_0$ it follows that

$$\tau^k \cdot f = (\tau \cdot f)^k = f^{q^k} = (\alpha_n T^n + \ldots + \alpha_1 T + \alpha_0)^{q^k} = \alpha_n^{q^k} T^{nq^k} + \ldots + \alpha_1^{q^k} T^{q^k} + \alpha_0^{q^k},$$

because of the characteristic p of $\mathbb{F}_q$ for $q = p^n$.

The Carlitz module is a special case of the so-called Drinfeld modules, which are not important for us at this point. For the interested reader the book *Number Theory in Function Fields* from Rosen (see [8]) can be suggested. Many of the following result can be also found there.

Now let $\Lambda[m] := \left\{\lambda \in \overline{\mathbb{F}_q(T)} \mid C_m(\lambda) = 0\right\}$ denote the set for an arbitrary $m \in \mathbb{F}_q[T]$. The extension $\mathbb{F}_q(T)(\Lambda[m])/\mathbb{F}_q(T)$ is Galois and

$$\mathrm{Gal}(\mathbb{F}_q(T)(\Lambda[m])/\mathbb{F}_q(T)) \cong (\mathbb{F}_q[T]/m\mathbb{F}_q[T])^*$$

holds. It does even hold that for every $\sigma \in \mathrm{Gal}(\mathbb{F}_q(T)(\Lambda[m])/\mathbb{F}_q(T))$ and a generator λ_m of this field extension, there exists an $a \in \mathbb{F}_q[T]$ such that $\gcd(a, m) = 1$ and $\sigma(\lambda_m) = C_a(\lambda_m)$. Note that this a is also the image of σ in the above mentioned isomorphism. From now on we always assume that we consider this isomorphism and identify the elements of $(\mathbb{F}_q[T]/m\mathbb{F}_q[T])^*$ with the corresponding automorphisms. Furthermore denote the element σ in the Galois group by σ_a, where a is the image under σ. (See [8, p. 202–207])

Define $|m| := q^{\deg(m)}$ for a polynomial $0 \neq m \in \mathbb{F}_q[T]$ and $|m| := 0$ for $m = 0$. We can assume without loss of generality that m is a monic polynomial, otherwise if $\alpha \neq 1$ is the leading coefficient of m, consider instead $\alpha^{-1}m$ with the inverse α^{-1} of α in $\mathbb{F}_q$. The residue class stays obviously the same for the now monic polynomial.

In the next result we are working with prime ideal. Therefore we need an analogue of the ring of integers in matters of $\mathbb{F}_q(T)$:

Definition 1.5. For the finite field extension $K/\mathbb{F}_q(T)$ define $\mathcal{O}_K := K \cap \mathbb{F}_q(T)$. We call $\mathcal{O}_K$ the *ring of integers* of K in respect to $\mathbb{F}_q(T)$.

This set is in fact a ring, even a Dedekind domain (see [8, p. 241–248]), exactly like its analogue, the ring of integers of a number field. In addition many results are holding for $\mathcal{O}_K$ which are also true for the known ring of integers. We will sometimes say that prime ideals in $\mathcal{O}_K$ are prime ideals of K.

Theorem 1.6. *Let $\mathcal{H}$ be a subgroup of $(\mathbb{F}_q[T]/m\mathbb{F}_q[T])^*$ for an element $0 \neq m \in \mathbb{F}_q[T]$. Then there is a $F \in \mathbb{F}_q[T][X]$ such that all prime divisors of F, with the exception of finitely many, belong to residue classes of $\mathcal{H}$.*

Proof. Let $\mathbb{F}_q(T)(\eta)$ be the fixed field of $\mathcal{H}$, where $\eta = H(\lambda_m)$, with generator λ_m of the Galois extension $\mathbb{F}_q(T)(\Lambda[m])/\mathbb{F}_q(T)$ and suitable $H \in \mathbb{F}_q[T][X]$.

Let $m_1, \dots, m_s$ be coset representatives of $\mathcal{H}$ in $(\mathbb{F}_q[T]/m\mathbb{F}_q[T])^*$. With them we define $\eta_i := H(C_{m_i}(\lambda_m))$ for $i = 1, \dots, s$ and will show that they are pairwise distinct. Assume they are not, then $\sigma_{m_i}(\eta) = \sigma_{m_j}(\eta)$ holds for two distinct coset representatives m_i, m_j of $\mathcal{H}$. This would be equivalent to

$$\begin{aligned}\eta &= \sigma_{m_j}^{-1}\sigma_{m_i}(\eta) = \sigma_{m_j}^{-1}\sigma_{m_i}(H(\lambda_m)) = \\ &= \sigma_{m_j}^{-1}(H(\sigma_{m_i}(\lambda_m))) = \sigma_{m_j^{-1}}(H(C_{m_i}(\lambda_m))) = \\ &= H(C_{m_i}(\sigma_{m_j^{-1}}(\lambda_m))) = H(C_{m_i}(C_{m_j^{-1}}(\lambda_m))) = \\ &= H(C_{m_i m_j^{-1}}(\lambda_m)) = H(\sigma_{m_i m_j^{-1}}(\lambda_m)) = \\ &= \sigma_{m_i m_j^{-1}}(H(\lambda_m)) = \sigma_{m_i m_j^{-1}}(\eta).\end{aligned}$$

Thus $\sigma_{m_i m_j^{-1}}$ fixes $\mathbb{F}_q(T)(\eta)$ and hence $m_i m_j^{-1} \in \mathcal{H}$. This has the consequence that m_i and m_j are in the same coset of $\mathcal{H}$ - a contradiction. It follows that all the η_i are distinct and thus are the different conjugates of η. Now we define the polynomial which will fulfill the conditions of the theorem:

$$F(X) := \prod_{i=1}^{s} (X - \eta_i)$$

As shown above it is $F \in \mathbb{F}_q[T][X]$. Let $p \in \mathbb{F}_q[T]$ be a prime divisor of F, which divides neither m nor the discriminant $D(F)$ of F. By this we only exclude finitely many prime divisors of F. Since p is a prime divisor of F there exists an $a \in \mathbb{F}_q[T]$ such that

$$p \mid F(a) = \prod_{i=1}^{s} (a - \eta_i).$$

Let $\mathscr{P}$ be a prime ideal lying over (p), the ideal generated by p. It is $\mathscr{P} \mid (a - \eta_i)$ for an $i \in \{1, \ldots, s\}$. With Fermat's small theorem (see [8, p. 5]) and the fact that $C_p(X)$ is an Eisenstein polynomial at p (see [8, p. 205]) it follows $C_p(a) \equiv a^{|p|} \equiv a$ mod p and thus also $C_p(a) \equiv a \mod \mathscr{P}$. Together with the linearity of the Carlitz polynomial we get $C_p(H(X)) = H(C_p(X))$. Furthermore following congruence hold:

$$\begin{aligned} H(C_{m_i}(\lambda_m)) = \eta_i \equiv a \equiv C_p(a) \equiv C_p(\eta_i) &= C_p(H(C_{m_i}(\lambda_m))) \\ = H(C_p(C_{m_i}(\lambda_m))) &= H(C_{pm_i}(\lambda_m))) \mod \mathscr{P} \end{aligned}$$

Hence $\mathscr{P} \mid (H(C_{m_i}(\lambda_m)) - H(C_{pm_i}(\lambda_m))$. Since $p \nmid m$ is $\gcd(pm_i, m) = 1$ it has to be $H(C_{pm_i}(\lambda_m)) = \eta_j$ for a $j \in \{1, \ldots, s\}$.

Assume it is $(H(C_{m_i}(\lambda_m)) \neq H(C_{pm_i}(\lambda_m))$. Then $\mathscr{P} \mid D(F)$ and since $D(F) \in \mathbb{F}_q[T]$ it also follows $p \mid D(F)$. This provides a contradiction to $p \nmid D(F)$. Therefore we have $H(C_{m_i}(\lambda_m)) = H(C_{pm_i}(\lambda_m))$ and it follows that η_i is fixated by σ_p, thus also the extension $\mathbb{F}_q(T)(\eta_i)$. Since $\mathbb{F}_q(T)(\eta)$ is Galois, it is $\mathbb{F}_q(T)(\eta_i) = \mathbb{F}_q(T)(\eta)$. In particular σ_p fixes $\mathbb{F}_q(T)(\eta)$. It follows that p belongs to one of the residue classes of $\mathcal{H}$. ■

We see that in $m \in \mathbb{F}_q[T]$ there are infinitely many primes $\equiv 1$ mod m, if we are working with $\mathcal{H} = \{1\}$ in Theorem 1.6. Furthermore we see now that, like already stated right after Lemma 1.3, all non-constant polynomials in $\mathbb{F}_q[T][X]$ possess infinitely many prime divisors of this type.

Like in the work of Murty [7] we can now say what we expect of an *Euclidean proof*: To given $l, m \in \mathbb{F}_q[T]$ we find a polynomial $F \in \mathbb{F}_q[T][X]$ such that all its prime divisors, with finitely many exception, are $\equiv 1, l \mod m$. We call such a polynomial an *Euclidean polynomial* if it actually possesses infinitely many prime divisors of the form $\equiv l \mod m$.

The Polynomial constructed in Theorem 1.6, in the case of $\mathcal{H} = \{1\}$, is the so-called *Carlitz cyclotomic polynomial* $\phi_m(X)$ *of* m which shares many properties of the usual cyclotomic polynomial. Here $\frac{C_m(X)}{X}$ takes the role of $\frac{X^n-1}{X-1}$ regarding the

Carlitz cyclotomic polynomial. $\phi_m(X)$ is the irreducible polynomial of maximum degree which divides $C_m(X)$. Many results holding for the cyclotomic polynomial in $\mathbb{Z}[X]$ are also here true and can be proven almost analogical. One of this results is for example the presentation of $\phi_m(X)$:

$$\phi_m(X) = \prod_{d|m} (C_{\frac{m}{d}}(X))^{\mu(d)},$$

where d is always monic and

$$\mu(d) = \begin{cases} (-1)^r & \text{if } d \text{ is squarefree, } r = |\{p \mid p \text{ prim}, p \mid d\}|; \\ 0 & \text{otherwise,} \end{cases}$$

the Möbius function (see [1]). With this it is easy to calculate the Carlitz cyclotomic polynomial to any given m.

In a converse way to Theorem 1.6 following holds:

Theorem 1.7. *If the conditions are the same as in Theorem 1.6, i.e.* $\mathcal{H} \leqslant (\mathbb{F}_q[T]/m\mathbb{F}_q[T])^*$ *and* F *the to* $\mathcal{H}$ *constructed polynomial. Then every prime belonging to a residue class of* $\mathcal{H}$ *is a prime divisor of* F*.*

Proof. Let p be a prime belonging to one of the residue classes of $\mathcal{H}$. Since $p \in \mathcal{H}$, we have that $\mathbb{F}_q(T)(\eta)$ is fixated by σ_p. In particular it is

$$C_p(\eta) \equiv \eta^{|p|} \equiv \eta \mod p.$$

Hence for every prime ideal $\mathscr{P}$, dividing p, it is $C_p(\eta) \equiv \eta \mod \mathscr{P}$. Since $\mathcal{O}_{\mathbb{F}_q(T)(\eta)}$ is a Dedekind domain $\mathcal{O}_{\mathbb{F}_q(T)(\eta)}/\mathscr{P}$ is a field and it follows that $C_p(X) - X$ has at most $|p|$ solutions in this field. With Fermat's small theorem we have that every element of $\mathbb{F}_q[T]/p\mathbb{F}_q[T]$ is a solution for this polynomial. With $|\mathbb{F}_q[T]/p\mathbb{F}_q[T]| = |p|$ we see that these are exactly all solutions. Thus there is an $a \in \mathbb{F}_q[T]$ such that $\eta \equiv a \mod \mathscr{P}$ holds. Hence $\mathscr{P} \mid F(a)$ and because of $F(a) \in \mathbb{F}_q[T]$ we get $p \mid F(a)$. This shows the assertion. ■

For the Carlitz cyclotomic polynomials we even have a more accurate description of the exceptions in Theroem 1.6:

Corollary 1.8. *All prime divisors of the Carlitz cyclotomic polynomial* $\phi_m(X)$ *are* $\equiv 1 \mod m$ *or are divisors of* m*.*

Proof. We have that ϕ_m is the polynomial from Theorem 1.6 if we choose $\mathcal{H} = \{1\}$. It holds that

$$D(\phi_m) = m^{\phi(m)} \prod_{p|m} p^{-\frac{\phi(m)}{\phi(p)}}.$$

This is a result you can find for example in the PhD-Thesis of Alex Samuel Bamunoba of the year 2014 (see [2, p. 22]). The proof is based on a known idea which can be executed for the discriminant of the normal cyclotomic polynomial.

We saw in theorem 1.6 that all prime divisors of ϕ_m are either $\equiv 1 \mod m$, divisors $D(\phi_m)$ or divisors of m. Since every divisor of $D(\phi_m)$ is also one of m, the assertion follows. ■

With all these tools we can now construct Euclidean polynomial for the arithmetic progression to l modulo m which fulfills the condition $l^2 \equiv 1 \mod m$.

Proposition 1.9. *If $l^2 \equiv 1 \mod m$ then there are infinitely many primes $\equiv l \mod m$, provided there is at least one.*

Proof. The case $l \equiv 1 \mod m$ is a direct consequence of Corollary 1.8. Now assume $l \not\equiv 1 \mod m$, but $l^2 \equiv 1 \mod m$. This means we can apply Theorems 1.6 and 1.7 for $\mathcal{H} = \{1; l\} \leqslant (\mathbb{F}_q[T]/m\mathbb{F}_q[T])^*$. Let $\mathcal{L}$ be the fixed field of $\mathcal{H}$. Define the polynomial $H(X) := (u - X)(u - C_l(X))$ where $u \in \mathbb{F}[T]$ will be chosen later.

Let $m_1, \ldots, m_s$ be the coset representatives of $\mathcal{H}$ in $(\mathbb{F}_q[T]/m\mathbb{F}_q[T])^*$. If we choose u such that all $H(C_{m_i}(\lambda_m))$ pairwise distinct, we get that the $C_{m_i}(\lambda_m)$ are all the conjugates of λ_m and it is $\mathcal{L} = \mathbb{F}_q(T)(H(\lambda_m))$. Note that we only exclude finitely many options for u this way since there are only finitely many equations of the form $H(C_{m_i}(\lambda_m)) = H(C_{m_j}(\lambda_m))$. We apply now Theorem 1.6 on $\mathcal{H}$ with $\eta = H(\lambda_m)$ and get an $F \in \mathbb{F}_q[T][X]$ for which almost all prime divisors are $\equiv 1 \mod m$ or $\equiv l \mod m$. We even can give such an F explicitly by constructing it in the same way as in the proof for Theorem 1.6:

$$F(X)^2 = \prod_{\gcd(a,m)=1} (X - (u - C_a(\lambda_m))(u - C_{la}(\lambda_m)))$$

Note that we squared F since every conjugate appears twice: For every a with $\gcd(a, m) = 1$ is also la co-prime to m. Furthermore we see that if we write $l^2 = km + 1$ for a $k \in \mathbb{F}_q[T]$ then the following holds:

$$C_{l^2a}(\lambda_m) = C_a C_{km+1}(\lambda_m) = C_a(C_{km} + C_1)(\lambda_m) = C_a(\lambda_m)$$

Therefore the factors for a and la are the same, hence $F(X)$ is the product where every of these factors appears exactly once.

One sees that it is $F(0) = \phi_m(u)$. We want now to choose u such that $F(0) = \phi_m(u) \equiv 1 \mod m$ holds. To do this we use a result which can be found, for example, by Sangtae Jeong (see [6, p. 28] or also [2, p. 19]): For the monic polynomial $m \in \mathbb{F}_q[T]$ holds

$$\phi_m(0) = \begin{cases} 0 & \text{if } m = 1 \\ p & \text{if } m = p^e \text{ for } p \text{ prime and } e \geqslant 1 \\ 1 & \text{otherwise.} \end{cases}$$

The case $m = 1$ is already excluded. If $m = p^e$ choose $u = km + 1$ with a $k \in \mathbb{F}_q[T]$ such that it is not one of the above excluded options. Otherwise choose $u = km$ with a $0 \neq k \in \mathbb{F}_q[T]$ and again such that it is not one of the above excluded options. Since ϕ_m is an Eisenstein polynomial at p $m = p^e$

(see [8, p. 205]) it is clear that then $F(0) = \phi_m(u) \equiv 1 \mod m$. With corollary 1.8 we know that every prime divisor of ϕ_m is either a divisor of m or $\equiv 1 \mod m$. It follows that every prime divisor of $\phi_m(u) = F(0)$ has to be $\equiv 1 \mod m$.

Now choose a prime $p \in \mathbb{F}_q[T]$ such that $p \equiv l \mod m$ and such that it does not divide the discriminant $D(F)$ of F. With Theorem 1.7 there exists a $b \in \mathbb{F}_q[T]$ with $p \mid F(b)$. We can even choose b such that $p^2 \nmid F(b)$. Assume that $p^2 \mid F(b)$, then we have

$$F(b+p) \equiv F(b) + pF'(b) \equiv pF'(b) \mod p^2.$$

Since $p \nmid D(F)$ it follows that F has no double roots modulo p and thus $F'(b) \not\equiv 0 \mod p$. So $F(b) \equiv 0$ implies $F(b+p) \not\equiv 0 \mod p^2$. Hence in this case we can exchange b by $b+p$ and get a b with the desired property.

Assume now that there are only finitely many primes $\equiv l \mod m$ and denote them by $p = p_1, p_2, \ldots, p_t$. Further let $q_1, \ldots, q_r$ be the prime divisors of $D(F)$ and set

$$Q := p_2 p_3 \ldots p_t q_1 \ldots q_r.$$

With the chinese remainder theorem for function fields (see [8, p. 3]) there exists a $c \in \mathbb{F}_q[T]$ such that

$$\begin{aligned} c &\equiv b \mod p^2 \\ c &\equiv 0 \mod mQ. \end{aligned}$$

Hence it is also

$$\begin{aligned} F(c) &\equiv F(b) \mod p^2 \\ F(c) &\equiv F(0) \mod mQ. \end{aligned}$$

From theorem 1.6 we see the only prime divisors of F are these which divide m, divide the discriminant $D(F)$ of F or are $\equiv 1, l \mod m$.

Since $F(0) = \phi_m(u)$ is only divisible by primes $\equiv 1 \mod m$ we have that $F(c)$ is only divisible by primes $\equiv 1 \mod m$ and $p_1 = p \equiv l \mod m$. With $p^2 \nmid F(c)$ follows $F(c) \equiv l \mod m$ but at the same time $F(c) \equiv F(0) \equiv 1 \mod m$ holds. This is a contradiction to $l \not\equiv 1 \mod m$. The assertion follows. ■

We were now able to provide a method to prove an analogue to the prime number theorem of Dirichlet without tools of Analysis if we take the assumption of $l^2 \equiv 1 \mod m$.

2. Limits of this method

We want to show that such an *Euclidean polynomial* exists exactly for the arithmetic progressions looked at in the first part of this work. Murty himself was able to show such limits in the case of $\mathbb{Z}$. Keith Conrad was able to prove this result with some other methods than Murty. The following ideas are based on some of Conrad's work (see [4]).

For the function field extension $K/\mathbb{F}_q(T)$ and a polynomial $F \in \mathbb{F}_q[T][X]$ define the sets

$$\begin{aligned}\mathrm{Spl}_1(F) :&= \{p \in \mathbb{F}_q[T] \mid \exists n \in \mathbb{F}_q[T] : p \mid F(n)\}\\ &= \{p \in \mathbb{F}_q[T] \mid F(X) \text{ has a factor of degree modulo } p\}\end{aligned}$$

and

$$\mathrm{Spl}_1(K) := \Big\{p \in \mathbb{F}_q[T] \mid \text{there is a prime ideal } \mathscr{P} \in K \\ \text{with } \mathscr{P} \mid p \text{ and } f(\mathscr{P} \mid p) = 1\Big\}.$$

Additionally define for $m \in \mathbb{F}_q[T]$ the sets

$$S_1(m, F) := \Big\{b \in (\mathbb{F}_q[T]/m\mathbb{F}_q[T])^* \mid p \equiv b \mod m \\ \text{for infinitely many } p \in \mathrm{Spl}_1(F)\Big\},$$

$$S_1(m, K) := \Big\{b \in (\mathbb{F}_q[T]/m\mathbb{F}_q[T])^* \mid p \equiv b \mod m \\ \text{for infinitely many } p \in \mathrm{Spl}_1(K)\Big\}.$$

For irreducible F and a root θ of F the sets $\mathrm{Spl}_1(F)$ and $\mathrm{Spl}_1(\mathbb{F}_q(T)(\theta))$ coincide, with finitely many exceptions (if $\mathcal{O}_{\mathbb{F}_q(T)(\theta)} \neq \mathbb{F}_q[T][\theta]$). Hence it is $S_1(m, F) = S_1(m, \mathbb{F}_q(T)(\theta))$. (See [9, p. 86])

In the following proof we need results for the so-called *Frobenius automorphism* and the *Dirichlet density.* The big part of these results are the same as the ones in the case of number fields. One can find them in the work of Rosen (see [8, S. 115–144]).

Lemma 2.1. *For every function field extension $K/\mathbb{F}_q(T)$ is $S_1(m, K) \leqslant (\mathbb{F}_q[T]/m\mathbb{F}_q[T])^*$. Here $S_1(m, K)$ is the image of the restriction mapping*

$$\mathit{Gal}(K(\lambda_m)/K) \to \mathit{Gal}(\mathbb{F}_q(T)(\lambda_m)/\mathbb{F}_q(T)).$$

Proof. First we classify the congruence classes of which $S_1(m, K)$ is consisting of. We show:

$$S_1(m, K) = \{r \in (\mathbb{F}_q[T]/m\mathbb{F}_q[T])^* \mid r \in \mathrm{Spl}_1(K) \text{ and } r \text{ ramifies not in } K(\lambda_m)\} \tag{2.1}$$

Here the condition on r is to be understood that r is in one of the congruence classes of $(\mathbb{F}_q[T]/m\mathbb{F}_q[T])^*$.

One inclusion is easy to see: Each congruence class in $S_1(m, K)$ contains infinitely many primes of $\mathrm{Spl}_1(K)$ and such a class contains at least one prime which can be chosen as representative which does not ramify in $K(\lambda_m)$. This is because there are only finitely many primes ramifying in $K(\lambda_m)/K$ (see for example [8, S. 87]).

Now for the other inclusion: Let $r \in \mathrm{Spl}_1(K)$ and r not ramifying in $K(\lambda_m)$. We will show that infinitely many $p \in \mathrm{Spl}_1(K)$ such that $p \equiv r \mod m$ exist.

Choose $\mathscr{R} \in K$ with $\mathscr{R} \mid r$ and $f(\mathscr{R} \mid r) = 1$. Since r does not ramify in $K(\lambda_m)$ we have that $\mathscr{R}$ does not ramify in $K(\lambda_m)$, too. Therefore we get the Frobenius element

$$\sigma = \mathrm{Fr}_{\mathscr{R}}(K(\lambda_m)/K) \in \mathrm{Gal}(K(\lambda_m)/K),$$

which, restricted to $\mathbb{F}_q(T)(\lambda_m)$, matches σ_r which again can be identified with the residue class of r in $(\mathbb{F}_q[T]/m\mathbb{F}_q[T])^*$. We denote this in the following way:

$$\sigma \mid_{\mathbb{F}_q(T)(\lambda_m)} \equiv \sigma_r \equiv r \mod m \tag{2.2}$$

With the Chebotarev density theorem (see [8, p. 125]) we have for the extension $K(\lambda_m)/K$ that there are infinitely many $\mathscr{P} \in K$ with the following properties:

- $\mathscr{P}$ is unramified in $K(\lambda_m)$
- $\mathrm{Fr}_{\mathscr{P}}(K(\lambda_m)/K) = \sigma$
- $f_{\mathscr{P}}(K/\mathbb{F}_q(T)) = 1$

The last condition follows from the positive density of the $\mathscr{P}$ with Frobenius σ and the density of 1 of the primes $\mathscr{P} \in K(\lambda_m)$ residue degree 1. Latter is gotten by the definition of the Dirichlet density for primes in K, since the set

$$\{\mathscr{P} \in K \mid \mathscr{P} \text{ prime in } K, f_{\mathscr{P}}(K/\mathbb{F}_q(T)) = k\}$$

for $k > 1$ has a density of 0 (see proof of Proposition 9.13 in [8, p. 123–125]).

Set $p\mathbb{F}_q[T] := \mathscr{P} \cap \mathbb{F}_q[T]$ which lies in $\mathrm{Spl}_1(K)$ by the construction of the $\mathscr{P}$, hence it is also

$$\sigma \mid_{\mathbb{F}_q(T)(\lambda_m)} \equiv p \mod m. \tag{2.3}$$

By comparing (2.2) and (2.3) we get $p \equiv q \mod m$.

By that (2.1) is verified and it is left to show that $S_1(m, K)$ is the image of $\mathrm{Gal}(K(\lambda_m)/K) \to \mathrm{Gal}(\mathbb{F}_q(T)(\lambda_m)/\mathbb{F}_q(T))$. Denote this image by $\mathcal{F}$.

Choose a congruence class of $S_1(m, K)$ and denote it by $[r]$. In (2.2) we saw that $[r]$ identifies with the restriction of the Frobenius $\mathrm{Fr}_{\mathscr{R}}(K(\lambda_m)/K)$ to $\mathbb{F}_q(T)(\lambda_m)$ with $\mathscr{R} \mid r$ and $f(\mathscr{R} \mid r) = 1$. Hence it is $[r] \in \mathcal{F}$ and therefore $S_1(m, K) \subseteq \mathcal{F}$.

Now pick $b \in H$ and $\sigma \mid_{\mathbb{F}_q(T)(\lambda_m)} \equiv b \mod m$ with $\sigma \in \mathrm{Gal}(K(\lambda_m)/K)$. It follows, again with the Chebotarev density theorem, that $\sigma = \mathrm{Fr}_{\mathscr{P}}(K(\lambda_m)/K)$ for infinitely many $\mathscr{P} \in K$ with $f_{\mathscr{P}}(K/\mathbb{F}_q(T)) = 1$. Set again $p\mathbb{F}_q[T] := \mathscr{P} \cap \mathbb{F}_q[T]$ with which $p \in \mathrm{Spl}_1(K)$. Then, as seen above,

$$\sigma \mid_{\mathbb{F}_q(T)(\lambda_m)} \equiv \sigma_p \equiv p \mod m,$$

hence $p \equiv b \mod m$. Since there are infinitely many such p we get $b \in S_1(m, K)$. ■

With this we are now able to prove that there is actually only one Euclidean polynomial for the arithmetic progression l modulo m if we assume $l^2 \equiv 1 \mod m$.

Theorem 2.2. *Let $F \in \mathbb{F}_q[T][X]$ be such that it has infinitely many prime divisors $\equiv l \mod m$ and $|\mathcal{P}(F) \setminus \{p \in \mathbb{F}_q[T] \mid p$ prime,$p \equiv 1 \mod m$ or $p \equiv l \mod m\}| < \infty$. Then $l^2 \equiv 1 \mod m$.*

Proof. Without loss of generality we can assume that F is irreducible. Otherwise for every $p \in \mathbb{F}_q[T]$ with $p \mid F = F_1 F_2$ holds then $p \mid F_1$ or $p \mid F_2$. Therefore F_1 or F_2 would also fulfill the conditions of the theorem. By proceeding further on in this way we can finally reach a irreducible polynomial.

Using theorem 2.1 we get $S_1(m, F) \leqslant (\mathbb{F}_q[T]/m\mathbb{F}_q[T])^*$ with $\{l\} \subseteq S_1(m, F) \subseteq \{1, l\}$, here the field K in theorem 2.1 is the field extension of $\mathbb{F}_q(T)$ together with a root of F. Hence $\{1, l\}$ has to be a subgroup in $(\mathbb{F}_q[T]/m\mathbb{F}_q[T])^*$. This implies $l^2 \equiv 1 \mod m$ immediately. ■

We see that also in the case of $\mathbb{F}_q[T]$ this method of Murty has its limits.

At this point one can suggest some problems in connection to this paper. In number fields there are generalisations of this method, which can be found in the works of Murty and Conrad. They considered a Galois number field extension L/K. There an arithmetic progression is replaced by elements $\sigma \in \mathrm{Gal}(L/K)$ and a prime ideal of L belongs to σ if σ is its Frobenius. They show that in this context an Euclidian polynomial for σ exists iff σ ist of order 2. In the same way one could consider arbitrary Galois function field extensions and try to find an Euclidean proof there.

Another interesting problem would be to ask for an Euclidean proof for polynomial rings in more than one variable. But already Lemma 1.3 could not be proven in the same way since the results of Becker and Maclane show that there are extensions which are not simple in that case. Furthermore one would need a corresponding object to the Carlitz cyclotomic polynomial for polynomial rings in multiple variables.

References

[1] S. Bae, S.-G. Hahn, *On the ring of integers of cyclotomic function fields*, Bull. Korean Math. Soc. **29** (1992), 153–163.

[2] A.S. Bamunoba, *Arithmetic of Carlitz polynomials*, https://scholar.sun.ac.za/handle/10019.1/95850 [17.02.2016].

[3] M.F. Becker, S. Maclane, *The minimum number of generators for inseparable algebraic extensions,* http://projecteuclid.org/download/pdf_1/euclid.bams/1183502442 [17.02.2016].

[4] K. Conrad, *Euclidean proofs of Dirichlet's theorem*, http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/dirichleteuclid.pdf [17.02.2016].

[5] B. Hornfeck, *Primteiler von Polynomen*, J. Reine Angew. Math. **243** (1970), 120.

[6] S. Jeong, *Resultants of cyclotomic polynomials over $\mathbb{F}_q[T]$ and applications*, Commun. Korean Math. Soc. **28** (2013), 25–38.

[7] M.R. Murty, N. Thain, *Prime numbers in certain arithmetic progressions*, Functiones et Approximatio **XXXV** (2006), 249–259.

[8] M. Rosen, *Number Theory in Function Fields*, Springer-Verlag, New York 2002.

[9] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin Heidelberg 2009.

Address: Thomas Lachmann: TU Graz, Institut für Analysis und Zahlentheorie, 8010 Graz, Steyrergasse 30/II, Austria.

E-mail: Lachmann@math.tugraz.at

Received: 27 March 2016; **revised:** 31 January 2017