Cyclotomic Polynomials

(in the parallel worlds of number theory)

by

Alex Samuel **BAMUNOBA**

Thesis presented in partial fulfilment of the
academic requirements for the degree of
Master of Science
at the University of Stellenbosch

Supervisor : Professor Florian **BREUER**
Department of Mathematical Sciences
University of Stellenbosch
November 21, 2011

For-example, if we work over $\mathbf{F}_3[T]$, taking $P_1 = T^2 + 1$, $P_2 = T^2 + 2T + 2$ for our primes, and setting $m = P_1^2 P_2$. Our brute force algorithm using **SAGE** returns the logarithmic height of $\Phi_m(X)$ as 192. Writing this polynomial explicitly would require another 15 pages of the thesis. With the above formula, we can compute this value quickly without worrying about the involved "monster polynomials". We have $n_1 = n_2 = s_1 = 2$, $s_2 = 1$, $r = 3$. So

$$\begin{aligned} h(\Phi_m(X)) &= r^{n_1 s_1 + n_2 s_2 - 1} + r^{n_1(s_1-1)+n_2(s_2-1)-1} - r^{n_1(s_1-1)+n_2 s_2 - 1} - r^{n_1 s_1 + n_2(s_2-1)-1} \\ &= 3^{2(2)+2(1)-1} + 3^{2(2-1)+2(1-1)-1} - 3^{2(2-1)+2(1)-1} - 3^{2(2)+2(1-1)-1} = 192. \end{aligned}$$

By the above results, we are unable to classify Carlitz cyclotomic polynomials according to height depending on order (as in the classical case). The classical result in all order 1 and 2 cyclotomic polynomials being flat is totally lost. However, we can confidently say that the height of $\Phi_m(X)$ over A is a power of r and is unbounded from above. In the next theorem, we explicitly determine the coefficient of $\phi_m(X)$ with the largest size.

Theorem 5.3.10. *Let $m \in A^+$, $\deg(m) = n$, and ϑ_m be the coefficient of maximum size in $\phi_m(X)$, then $\vartheta_m = (\tau^{n-1} + \cdots + \tau^0)(T) + m_1$, where m_1 is the coefficient of T^{n-1} in m.*

Proof. Suppose $\phi_{T^n}(X) = \sum_{i=0}^{n} a_i X^{r^i}$, then by theorem 5.3.5 and lemma 4.3.6, we must have $\vartheta_{T^n} = a_{n-1} = \frac{a_{n-2}^r - a_{n-2}}{T^{r^{n-1}} - T}$. Moreover, $a_n = 1$ since T^n is monic, so $T^{r^n} - T = a_{n-1}^r - a_{n-1}$ and therefore, we obtain $(\tau^n - \tau^0)(T) = (\tau - \tau^0)(a_{n-1})$. Using the left division algorithm, we obtain $a_{n-1} = (\tau^{n-1} + \cdots + \tau^0)(T)$. Next we have $(a_{n-1})(\tau^{n-1} - \tau^0)(T) = (\tau - \tau^0)(a_{n-2})$ and so $a_{n-2} = (\tau - \tau^0)^{-1}(a_{n-1})(\tau^{n-1} - \tau^0)(T)$. In general, one obtains the following recursion formula $a_{n-j} = (\tau - \tau^0)^{-1}(a_{n-j+1})(\tau^{n-j+1} - \tau^0)(T)$ for $n \geq 1$. This formula gives coefficients of $\phi_{T^n}(X)$ in descending order. The term of maximum size in $\phi_{T^n}(X)$ is $(T^{r^{n-1}} + \cdots + T)X^{r^{n-1}}$, similarly $\vartheta_{T^{n-1}} = (T^{r^{n-2}} + \cdots + T)X^{r^{n-2}}$. If we let $\phi_m(X) = \sum_{i=0}^{n} b_i X^{r^i}$, since ϕ is a ring homomorphism, we have $b_{n-1} = (\tau^{n-1} + \cdots + \tau^0)(T) + m_1$, where the m_1 is the coefficient of T^{n-1} in m. This arises from the fact $\phi_{T^{n-1}}(X) = m_1 X^{r^{n-1}} + \cdots + T^{n-1}X$ is the only lower degree Carlitz polynomial linked to m with a term of the form $[\,]X^{r^{n-1}}$. □

It is an obvious non-analogy with the classical cyclotomic polynomials; that none of the Carlitz cyclotomic polynomials (with the exception of $\Phi_{T(T+1)}(X) = X + 1$ in $\mathbf{F}_2[T]$) are flat. In order to get the analogy right, we have to look at these polynomials more closely. We know that $\Phi_P(X)$ has order one and is Eisenstein at the prime P, so we need to consider Eisenstein forms of order one classical cyclotomic polynomials. For details about this consideration and its results, refer to Appendix 8.1.

Definition 5.3.11. *Let $\Phi_m(X)$ be an order one Carlitz cyclotomic polynomial, the prime height of $\Phi_m(X)$ is $\mathcal{A}(m) := h_P(\Phi_m(X))$, where P is the unique prime factor of m.*

Theorem 5.3.12. *For all primes $P \in A^+$, we have $\mathcal{A}(P) = 1$.*

Proof. Suppose $\deg(P) = 1$ (P is of the form $T + \alpha$ where $\alpha \in \mathbf{F}_r$), then $\Phi_P(X) = X^{r-1} + P$, clearly its valuation set is $V_P = \{0, 1\}$, therefore $\mathcal{A}(P) = 1$. Suppose P has degree $n > 1$, then applying lemma 4.3.6, we have $\Phi_P(X) = a_0 + a_1 X^{r-1} + \cdots + a_n X^{r^n-1}$, where the coefficients are given by;

$$a_0 = P, a_1 = \frac{a_0^r - a_0}{T^r - T}, a_2 = \frac{a_1^r - a_1}{T^{r^2} - T}, \ldots, a_{n-1} = \frac{a_{n-2}^r - a_{n-2}}{T^{r^{n-1}} - T}, a_n = 1.$$

Observe that $v_P(a_0) = 1$ and $v_P(a_n) = 0$. Now, $v_P(a_0^r - a_0) = v_P(P^r - P) = 1$ since P does not divide $(P^{r-1} - 1)$ and $v_P(T^r - T) = 0$ since $\deg(P) > 1$, hence $v_P(a_1) = 1$. Similarly, $v_P(a_2) = v(a_1^r - a_1) - v_P(T^{r^2} - T) = 1$. This can be done until a_{n-1} is reached, because if $\deg(P) = n$, then P divides $T^{r^n} - T$ but not $T^{r^m} - T$ for $m < n$. Therefore, we have $v_P(a_n) = v_P(a_n^{r^n} - a_{n-1}) - v_P(T^{r^n} - T) = 0$, because at this point, at-least one of the factors of $T^{r^n} - T$ is P. Therefore, the valuation set of $\Phi_P(X)$ is $V_P = \{0, 1\}$ hence $\mathcal{A}(P) = 1$. □

We now attempt to investigate what happens to the prime height for higher powers of P.

Lemma 5.3.13. *Let $\eta_\alpha : k \to k$ be the map $\eta_\alpha(f) = f(T + \alpha)$, where $f \in A$, $\alpha \in \mathbf{F}_r$. Then we have $\Phi_{(T+\alpha)^s}(X) = \eta_\alpha(\Phi_{T^s}(X))$.*

Proof. Now η_α is an $\mathbf{F}_r$-homomorphism, it fixes $\mathbf{F}_r$ and permutes the elements of A. We also have $\eta_0(f) = f$ for all $f \in A$, and $\eta_\alpha(fg) = (f \cdot g)(T + \alpha) = f(T + \alpha)g(T + \alpha) = \eta_\alpha(f)\eta_\alpha(g)$. By theorem 5.2.9, $\Phi_{(T+\alpha)^s}(X) = \Phi_{T+\alpha}(\phi_{(T+\alpha)^{s-1}}(X)) = \phi_{(T+\alpha)^{s-1}}(X)^{r-1} + T + \alpha$. Similarly, $\Phi_{T^s}(X) = \Phi_T(\phi_{T^{s-1}}(X)) = \phi_{T^{s-1}}(X)^{r-1} + T$. Left to know the action of η_α on $\phi_{T^{s-1}}(X)$. But since η is both an $\mathbf{F}_r$-homomorphism and an A-ring homomorphism, we then have $\eta(\Phi_{T^s}(X)) = \eta(\phi_{T^{s-1}}(X)^{r-1} + T) = \phi_{(T+\alpha)^{s-1}}(X)^{r-1} + T + \alpha = \Phi_{(T+\alpha)^s}(X)$. □

Theorem 5.3.14. *$\Phi_{\eta_\alpha(m)}(X) = \eta_\alpha(\Phi_m(X))$ for any $m \in A^+$.*

Proof. Let $\phi_m(X) = \sum_{j=0}^n a_j X^{r^j}$ and $\phi_{\eta_\alpha(m)}(X) = \sum_{j=0}^n b_j X^{r^j}$. Without loss of generality, assume m is monic. Since η_α is a ring homomorphism, we have $\eta_\alpha(a_0) = \eta_\alpha(m) = b_0$ and $\eta_\alpha(a_n) = \eta_\alpha(1) = 1 = b_n$. This is true since m and $\eta_\alpha(m)$ are both monic. For $1 \leq j < n$,

$$\eta_\alpha(a_j) = \eta_\alpha\left(\frac{a_{j-1}^r - a_{j-1}}{T^{r^j} - T}\right) = \frac{(\eta_\alpha(a_{j-1}))^r - \eta_\alpha(a_{j-1})}{(T+\alpha)^{r^j} - (T+\alpha)} = \frac{(\eta_\alpha(a_{j-1}))^r - \eta_\alpha(a_{j-1})}{T^{r^j} - T} = b_j$$

and so $\eta_\alpha(\phi_m(X)) = \sum_{j=0}^n \eta_\alpha(a_j) X^{r^j} = \sum_{j=0}^n b_j X^{r^j} = \phi_{\eta_\alpha(m)}(X)$. Now we obtain,

$$\begin{aligned}\eta_\alpha(\Phi_m(X)) &= \prod_{d|m} \eta_\alpha(\phi_d(X)^{\mu(\frac{m}{d})}) = \prod_{d|m} \eta_\alpha(\phi_d(X))^{\mu(\frac{m}{d})} = \prod_{d|m} (\phi_{\eta_\alpha(d)}(X))^{\mu(\frac{m}{d})} \\ &= \prod_{\eta_\alpha(d)|\eta_\alpha(m)} (\phi_{\eta_\alpha(d)}(X))^{\mu(\frac{\eta_\alpha(m)}{\eta_\alpha(d)})} = \Phi_{\eta_\alpha(m)}(X).\end{aligned}$$

□

Example 5.3.15. *Let $m_1 = T^3 + T + 1 \in \mathbf{F}_2[T]$, we have $\Phi_{m_1}(X) = X^7 + (T^4 + T^2 + T)X^3 + (T^4 + T^3 + T^2 + 1)X + T^3 + T + 1$. There is another prime in $\mathbf{F}_2[T]$ of degree 3 given by $m_2 =$*

T^3+T^2+1. *A straight forward computation shows that,* $m_2=\eta_1(m_1)$ *and;*

$$\eta_1(\Phi_{m_1}(X))=X^7+(T^4+T^2+T+1)X^3+(T^4+T^3+T)X+T^3+T^2+1=\Phi_{m_2}(X).$$

Theorem 5.3.16. *Let* $P\in A^+$ *be prime of degree* n, $s\in\mathbf{N}_{\geq 2}$, *then* $\mathcal{A}(P^s)=(r^n-1)(s-1)$.

Before we prove this theorem, we need the following lemma.

Lemma 5.3.17. *Let* $s\in\mathbf{N}$ *and* P *be a prime of degree* n *in* A. *The coefficients of* X^{r^j} *for* $0\leq j<n$ *in* $\phi_{P^s}(X)$ *have maximum valuation with respect to* P. *Moreover* $\mathcal{A}(\phi_{P^s}(X))=s$.

Proof. $\mathcal{A}(\phi_P(X))=\mathcal{A}(\Phi_1(X)\Phi_P(X))=0+1=1$ by theorem 5.3.12. Assume $s\geq 2$, and $\phi_{P^s}(X)=\sum_{j=0}^{ns}a_jX^{r^j}$. We know recursively; $a_j=\frac{a_{j-1}^r-a_{j-1}}{T^{r^j}-T}$ for $1\leq j\leq ns$ and $a_0=P^s$. It is obvious $v_P(a_0)=s$ and $v_P(a_{ns})=0$. Left to show is; $0<v_P(a_j)\leq s$ for $0\leq j<ns$. Now, we have $v_P(a_j)=v_P(a_{j-1})+v_P(a_{j-1}^{r-1}-1)-v_P(T^{r^j}-T)$ for $1\leq j\leq ns$. Since P divides a_j, we must have $v_P(a_{j-1}^{r-1}-1)=0$ and so $v_P(a_j)-v_P(a_{j-1})=-v_P(T^{r^j}-T)$. From the theory of finite fields, $v_P(T^{r^j}-T)=0$ for $j\not\equiv 0(\text{mod } n)$ and $v_P(T^{r^{tn}}-T)=1$ for any $t\in\mathbf{Z}^+$. We obtain a telescoping sum that adds up to $v_P(a_j)=s-\sum_{t=1}^{j}v_P(T^{r^t}-T)=s-\lfloor\frac{j}{n}\rfloor$. □

This lemma shows that the coefficients of $\phi_{P^s}(X)$ with the highest valuation with respect to P are the coefficients of X^{r^j} with $j=1,\dots 2n-1$ (where in this case $v_P(a_j)=s$ for $j=1,2,\dots,n-1$ and $s-1$ for $j=n,n+1,\dots,2n-1$) i.e. the upper bound to the prime height of $\phi_{P^s}(X)$ is s. Now, since $\Phi_{P^s}(X)$ is Eisenstein for the prime P, so we have $v_P(\Phi_{P^s}(0))=1$ i.e. the prime height of $\Phi_{P^s}(X)$ is always ≥ 1. This argument, coupled by an induction process on s, we observe that the next suitable candidate for maximum valuation with respect to P is the coefficient of X^{r^n-1}. This comes from the fact v_P is non archimedean. Others may exist, but this is sufficient. We now prove theorem 5.3.16.

Proof. We proceed by induction on powers s of P. Trivially, we have $\Phi_1(X)=X$ and $\Phi_P(X)=X^{r^n-1}+a_1X^{r(r^{n-1}-1)}+\cdots+a_{r(r^{n-1}-1)}X^{r-1}+P$, where by applying theorem 5.3.12, we obtain $\mathcal{A}(P)=1$. In particular $v_P(a_{r(r^{n-1}-1)})=1$. Since both $\phi_P(X)$ and $\Phi_P(X)$ have each prime height 1, and $r^n-1>r^{n-1}$ for all r and $n\in\mathbf{N}$, then it is clear $(\phi_P(X))^{r^n-1}$ contains the term with the highest valuation with respect to P. So

$$\begin{aligned}\Phi_{P^2}(X)&=\Phi_P(\phi_P(X))\\&=(\phi_P(X))^{r^n-1}+\cdots+P\\&=X^{r^n-1}\left(\prod_{t=1}^{1}\Phi_P(X)^{r^n-1}\right)+\cdots+P.\end{aligned}$$

So the coefficient of X^{r^n-1} in $\Phi_{P^2}(X)$ is $\prod_{t=1}^{1}\Phi_P(0)^{r^n-1}=P^{r^n-1}$, so for $s=2$ we observe that $\mathcal{A}(P^2)=r^n-1=(r^n-1)(2-1)$, formula true for $s=2$. Suppose it is true for $s=n'$,

i.e. $\mathcal{A}(P^{n'}) = (r^{n'}-1)(s-1)$. We now compute $\Phi_{P^{n'+1}}(X)$. Now using theorem 5.2.9 and arguing using lemma 5.3.17 (to see position of maximum valuation), we obtain

$$\begin{aligned}\Phi_{P^{n'+1}}(X) &= \Phi_P(\phi_{P^{n'}}(X)) \\ &= \phi_{P^{n'}}(X)^{r^n-1} + \cdots + P \\ &= X^{r^n-1}\left(\prod_{t=1}^{n'} \Phi_{P^t}(X)^{r^n-1}\right) + \cdots + P,\end{aligned}$$

with the position having maximum valuation (with respect to P) at X^{r^n-1}. To obtain the coefficient of X^{r^n-1}, consider the constant terms of $\Phi_{P^t}(X)$. So the coefficient of X^{r^n-1} in $\Phi_{P^{n'+1}}(X)$ is $\prod_{t=1}^{n'} \Phi_{P^t}(0)^{r^n-1} = P^{n'(r^n-1)}$ and so $\mathcal{A}(P^{n'+1}) = (r^n-1)(n'+1-1)$. □

So we obtain $\mathcal{A}(P^s) \propto s-1$. This parallels the classical results where $\mathcal{A}(p^s) \propto s$.

Example 5.3.18. *Suppose $A = \mathbf{F}_3[T]$, and $P = T \in A$. Computations using **SAGE** yield, $\Phi_{T^4}(x) = x^{54} + (2T^9 + 2T^3 + 2T)x^{36} + (2T^6 + 2T^4 + 2T^2)x^{30} + 2T^3x^{28} + (T^{18} + 2T^{12} + 2T^{10} + T^6 + 2T^4 + T^2)x^{18} + (2T^{15} + 2T^{13} + 2T^{11} + 2T^9 + T^7 + T^5 + 2T^3)x^{12} + (2T^{12} + 2T^6 + 2T^4)x^{10} + (T^{12} + 2T^{10} + 2T^6 + T^4)x^6 + (2T^9 + 2T^7 + 2T^5)x^4 + T^6x^2 + T$. The coefficient with highest valuation with respect to the prime T is T^6 and so $\mathcal{A}(P^4) = 6 = (3^1-1)(4-1)$.*

Proposition 5.3.19. *Let $P \in \mathbf{F}_2[T]$ be a non-linear prime, $\alpha \in \mathbf{F}_2$, then $\mathcal{H}_P((T+\alpha)P) = 1$.*

Proof. It is suffices to show that all the coefficients of $\Phi_{(T+\alpha)P}(X)$ are $\not\equiv 0 \pmod{P}$. It is suffices to work with $\Phi_T(X)$, so from proposition 5.3.20, we have the following equation $\Phi_T(X)\Phi_{TQ}(X) = \phi_Q(X) + T \equiv X^{2^n} + T \pmod{Q}$, where $Q = \eta_\alpha(P)$ (by lemma 4.3.6 and theorem 5.2.9). Since P is a non linear polynomial, so is Q, we must have $n \geq 2$ and that $\Phi_{TQ}(X) \equiv X^{2^n-1} + a_1X^{2^n-2} + \cdots + a_{2^n-2}X + 1 \pmod{Q}$ with all the terms a_i being non-zero (via long division) and having degree $\leq n$, therefore $\mathcal{A}(TQ) = 0$. □

Let us investigate the case $P = T$. By theorem 5.3.16, $\mathcal{A}(T^2) = r-1$. This can also be deduced from the following calculation,

$$\begin{aligned}\Phi_{T^2}(X) &= (X^r + TX)^{r-1} + T \\ &= T + \sum_{i=0}^{r-1} \binom{r-1}{i} X^{(r-1)(i+1)} T^{r-1-i} \\ &= T + \sum_{i=0}^{r-1} a_i X^{(r-1)(i+1)} T^{r-1-i}.\end{aligned}$$

The highest possible term in T is T^{r-1}, hence $\mathcal{A}(T^2) = r-1$.

We now discuss the constant and the middle coefficient of $\Phi_m(X)$. We also give a short proof to a special case of Dirichlet's theorem on primes in an arithmetic progression.

Proposition 5.3.20. *Let $s \in \mathbf{N}$, $m \in A^+$ and P be a prime in A, then*

$$\Phi_m(0) = \begin{cases} 1, & m \neq P^s \\ P, & m = P^s. \end{cases}$$

Proof. We shall proceed in 3 steps. Let $\phi_m(X) = \sum_{i=0}^{|m|} c_m(i)X^i$ and $\Phi_m(X) = \sum_{i=0}^{\phi(m)} a_m(i)X^i$.

1. Let $m = P^s$, then by theorem 5.2.10, $\Phi_{P^s}(X)\phi_{P^{s-1}}(X) = \phi_{P^s}(X)$. We get the constant term of $\Phi_{P^s}(X)$ by solving $a_{P^s}(0)c_{P^{s-1}}(1) = c_{P^s}(1)$, therefore $a_{P^s}(0)P^{s-1} = P^s$.

2. Suppose $m \neq P^s$, we shall proceed by induction on the order of $\Phi_m(X)$ with the help of proposition 5.2.1. Suppose $\Phi_m(X)$ is binary, set $m = PQ$, where P, Q are distinct primes. Then $c_{PQ}(1) = \prod_{d|PQ} a_d(0)$ and $PQ = 1 \cdot P \cdot Q \cdot a_{PQ}(0)$ hence $a_{PQ}(0) = 1$. In general, for $s_1, s_2 \in \mathbf{N}$, if $m = P^{s_1}Q^{s_2}$, by part 1, we get $a_{P^{s_1}Q^{s_2}}(0) = 1$.

3. Suppose the statement is true for orders $s < n$, and $\mathrm{ord}_A(m) = n$. We shall first consider the case for m, square free of order n. We have $c_m(1) = \prod_{d|m} a_d(0)$, therefore by the induction hypothesis we get,

$$m = c_m(1) = a_m(0) \prod_{d|m, d\neq m} a_d(0) = a_m(0) \left(\prod_{Q|m, \text{ a prime}} a_Q(0) \right) \cdot 1 = a_m(0) \cdot m \cdot 1,$$

   implying $a_m(0) = 1$. With this construction, if m not square free, then by parts 1, 2, and the first part of 3 we have have $a_m(0) = 1$ which completes the proof.

In fact the same results hold for the classical case. □

Corollary 5.3.21. *Let $a \in A$ and $P \nmid m$, then P divides $\Phi_m(a)$ if and only if $P \equiv 1 (\mathrm{mod}\ m)$.*

Proof. Let P be a prime factor of $\Phi_m(a)$, such that P doe not divide m. Then we have $P \nmid a$ for otherwise we would have $\Phi_m(a) \equiv 0 \pmod{P}$, and on the other hand we would have $\Phi_m(a) \equiv 1 \pmod{P}$ (when m is product of more than one primes different from P) or $\Phi_m(a) \equiv P_0 \pmod{P}$ (when m is a power of P_0) which is different from zero modulo P unless when P divides m. Either way we have a contradiction. Let f be the Carlitz order of a modulo P, that is to say $\phi_f(a) \equiv 0 (\mathrm{mod}\ P)$ for some $0 \neq f \in A/PA$ of least degree. Therefore, f divides m since $\phi_m(a) = 0$. There are two cases we need to consider,

1. If $f = m$, then m divides $P - 1$ since $\phi_{P-1}(a) = \phi_P(a) - \phi_1(a) = a - a \equiv 0 \pmod{P}$.

2. If $0 \leq \deg(f) < \deg(m)$, since $0 \equiv \phi_f(a) = \prod_{d|f} \Phi_d(a) \pmod{P}$, there exists a divisor d of f so that P divides $\Phi_d(a)$. But $d \mid f \mid m$ and $\deg(d) < \deg(m)$, so $\phi_m(X)$ has a repeated root modulo P by proposition 5.2.2 and so P divides m.

($\Leftarrow$) Suppose $P \equiv 1 (\mathrm{mod}\ m)$, then P does not divide m, and there is an element $a (\mathrm{mod}\ P)$ of order m. So $\phi_m(a) = \prod_{d|m} \Phi_d(a) \equiv 0 \pmod{P}$ and the order of a imply that P divides $\Phi_m(a)$. So $P \nmid m$, then P divides $\Phi_m(a)$ for some $a \in A$ if and only if $P \equiv 1 (\mathrm{mod}\ m)$. □

For example, over $\mathbf{F}_2[T]$, if we take $a = 1$, $b = T^2 + T$ and $m = T^2 + T$. We have already seen that $\Phi_m(X) = X + 1$, so $\Phi_m(a) = 0$ and $\Phi_m(b) = T^2 + T + 1$. Now $P = T^2 + T + 1$ divides $\Phi_m(T^2 + T + 1)$ but does not divide m, moreover $P \equiv 1 \pmod{m}$. Similarly, take $c = T^6 + T^5 + T^4 + T^3$, then $P_1 = T^2 + T + 1$ and $P_2 = T^4 + T + 1$ are all congruent to 1 modulo m and both divide $\Phi_m(c)$. Another good example is to consider $m = T^2 + T \in \mathbf{F}_3[T]$. Here $\Phi_m(X) = X^4 + (T + 2)X^2 + 1$; now setting $a = T + 2$, we obtain $\Phi_m(a) = T^4 + 2T + 1 = (T + 1)(T^3 + 2T^2 + T + 1)$. Observe that the prime $Q_1 = T + 1$ divides m (so by the corollary is not considered), but $Q_2 = T^3 + 2T^2 + T + 1$ divides $\Phi_m(a)$ and does not divide m. Moreover, $Q_2 \equiv 1 \pmod{m}$, which agrees with corollary 5.3.21.

Proposition 5.3.22 (Special case of Dirichlet's theorem)**.** *For each $m \in A$ with $\deg(m) > 1$, there are infinitely many primes P with the property that $P \equiv 1 \pmod{m}$.*

Proof. Suppose there are only finitely many primes $P_1, \ldots, P_s$ of the form $P_i \equiv 1 \pmod{m}$ for $i = 1, \ldots, s$. Let $M = mP_1 \cdots P_s$ and $N \in A$, then

$$\Phi_m(NM) \equiv \begin{cases} 1 \pmod{m}, & \text{if } m \neq P^s, \\ P \pmod{m}, & \text{if } m = P^s \end{cases}.$$

where P is a prime in A. In particular, $\Phi_m(NM)$ is not divisible by P_i and none of its factors (with the exception of P) divides m. This is because, $\Phi_m(NM) \equiv 1 \pmod{P_i}$, otherwise, we would have $\Phi_m(NM) \equiv 0 \pmod{P_i}$ which contradicts $P_i \equiv 1 \pmod{m}$. As $\deg(N) \to \infty$, we have $\deg(\Phi_m(NM)) \to \infty$. So for sufficiently large degree of N, we have $\Phi_m(NM) \neq 1$ (by degree comparisons); so there is a prime P_0 that divides $\Phi_m(NM)$. By corollary 5.3.21, $P_0 \equiv 1 \pmod{m}$ and from the above argument, we must have $P_0 \neq P_i$ for $1 \leq i \leq s$. We have just obtained a new prime $P_0 \equiv 1 \pmod{m}$, a contradiction. □

In the next section, we discuss the analogue of classical cyclotomic extensions.

5.4 Cyclotomic function fields

Like its classical counter-part, the m^{th} Carlitz cyclotomic extension field K_m is obtained by adjoining λ_m, a generator of Λ_m to k, so $K_m = k(\lambda_m)$. We have already seen that K_m/k is Galois with Galois group $\mathrm{Gal}(K_m/k)$. If $\sigma \in \mathrm{Gal}(K_m/k)$, then $\sigma(\lambda_m) = \phi_a(\lambda_m)$ where $(a, m) = 1$ and is determined modulo m i.e. $a \in (A/mA)^*$. This also gives rise to a monomorphism $\theta : \mathrm{Gal}(K_m/k) \hookrightarrow (A/mA)^*$. Irreducibility of $\Phi_m(X)$ (by Proposition 5.2.6), implies that θ is in fact an epimorphism from $\mathrm{Gal}(K_m/k)$ to $(A/mA)^*$, therefore we have established the isomorphism $\mathrm{Gal}(K_m/k) \cong (A/mA)^*$. This implies K_m/k is an abelian extension of k with degree $\varphi(m)$, where $\varphi(m)$ is the Euler totient function. We shall denote the integral closure of A in K_m by $\mathcal{O}_m = A[\lambda_m]$. Our goal is to imitate deductions of classical theory, however

before we do this, we need to study the group of units in $\mathcal{O}_m$. We begin with the following proposition which also suggests that it suffices to consider only monic polynomials.

Proposition 5.4.1. *Let $0 \neq m_1, m_2 \in A$, then $K_{m_2} = K_{m_1}$ if and only if $m_2 = \alpha m_1$ where $\alpha \in A^*$.*

Proof. ($\Leftarrow$) $m_2 = \alpha m_1$ with $\alpha \in A^*$, then $\phi_{m_2}(X) = \alpha\phi_{m_1}(X)$, $\Lambda_{m_2} = \Lambda_{m_1} \Rightarrow K_{m_2} = K_{m_1}$. ($\Rightarrow$) Conversely, suppose $K_{m_2} = K_{m_1}$, we compute the largest torsion sub-module of K_{m_1}. If $\Lambda_m \subseteq K_{m_1}$, then $K_m \subseteq K_{m_1}$, so $\varphi(m) \leq \varphi(m_1)$, for any degree of $m \in A$. So there exists Λ_m such that $\Lambda_m \subseteq \Lambda_{m_1}$, which implies m divides m_1 and $K_m = K_{m_1}$. Let us write $m_1 = ms$, so $\varphi(m_1) = \varphi(m)\varphi(s)\frac{|d|}{\varphi(d)} \geq \varphi(m)\varphi(s)$, where $d = (m, s)$. Since $K_m = K_{m_1}$, and so we have $\varphi(m) = \varphi(m_1)$ therefore $\varphi(s) = 1$. This shows $s \in A^*$, so m_1 is a scalar multiple of m, and so $\Lambda_m = \Lambda_{m_1}$. Therefore, $K_{m_2} = K_{m_1}$, and $\Lambda_{m_2} = \Lambda_{m_1}$. So $m_2 = \alpha m_1$ for some $\alpha \in A^*$. □

Proposition 5.4.2. *Let λ_m be a Λ_m-generator and suppose, $a \in A$ is co-prime to m. Then $\frac{\phi_a(\lambda_m)}{\lambda_m}$ is a unit in $\mathcal{O}_m$. Moreover, if m is of order ≥ 2, then λ_m is itself a unit.*

Proof. ([18], Proposition 12.6) Clearly, since $\phi_m(X) \in A[X]$, is monic and $\phi_m(\lambda_m) = 0$, λ_m is integral over A. Replacing m by a, and substituting $X = \lambda_m$, we see that $\frac{\phi_a(\lambda_m)}{\lambda_m} \in \mathcal{O}_m$ (deduced from 5.2.1). We are required to show that, the reciprocal of this element is in $\mathcal{O}_m$.

Let $b \in A$ be such that $ba = 1 (\text{mod } m)$. Then, there exists $f \in A$ such that $ba = 1 + fm$ and we have $\phi_b\phi_a = \phi_{ba} = 1 + \phi_f\phi_m$. Applying this to λ_m yields $\phi_b(\phi_a(\lambda_m)) = \lambda_m$. Therefore,

$$\frac{\lambda_m}{\phi_a(\lambda_m)} = \frac{\phi_b(\phi_a(\lambda_m))}{\phi_a(\lambda_m)} \in \mathcal{O}_m.$$

To prove the second assertion, we have to show that the norm of λ_m is a non-zero constant. Without loss of generality, we assume m is monic. Suppose $m = m_1m_2$ where m_1 and m_2 are monic and relatively prime. We take λ_m as a generator of Λ_m. Set $\lambda_{m_1} = \phi_{m_2}(\lambda_m)$, and $\lambda_{m_2} = \phi_{m_1}(\lambda_m)$. Then, λ_{m_i} is a primitive m_i^{th}-torsion point for $i = 1, 2$. For all $a \in A, \phi_a(X)$ is divisible by $\Phi_1(X) = X$, i.e. $X^{-1}\phi_a(X) \in A[X]$. Consider the factorization,

$$\lambda_{m_1} = \lambda_m \frac{\phi_{m_2}(\lambda_m)}{\lambda_m}.$$

This shows that, λ_m divides λ_{m_1}, and similarly λ_m divides λ_{m_2} in $\mathcal{O}_m$. Taking norms from K_m to k shows that the norm of λ_m divides a power of $\mathcal{N}_{K_m/k}(\lambda_{m_i})$ for $i = 1, 2$, that is to say $\mathcal{N}_{K_m/k}(\lambda_m)$ divides $\mathcal{N}_{K_m/k}(\lambda_{m_i})$ for $i = 1, 2$.

To finish the proof, we have to do induction on the number of distinct primes dividing m. Now suppose $m = P^e$, a prime power, then both proposition 5.3.20 and corollary 5.4.4 imply, the norm of λ_{P^e} is P, (generator of Λ_{P^e}). Suppose m is a product of two prime powers $P_1^{e_1}$ and $P_2^{e_2}$. Then, from what we have proven, it follows that the norm of λ_m divides a power of P_1 and a power of P_2. This implies the norm of λ_m is a non-zero constant (in the sense that it belongs to A) and so λ_m is a unit.

If m is divisible by $t > 2$ distinct primes, set

$$m_1 = P_1^{e_1} \text{ and } m_2 = \prod_{i=2}^{t} P_i^{e_i},$$

then, by induction, λ_{m_2} is a unit and its norm is a non-zero constant. By what we have proven above, it follows that the norm of λ_m is still a non-zero constant. Therefore, λ_m is a unit. □

If $m = P^e$, then λ is analogous to $\zeta - 1$ in the classical case. Otherwise, $\lambda \in \mathcal{O}_m^*$.

In chapter 1, we intentionally left out details on ramification at a prime power, but now we discuss it in rather a generalised fashion. With little strength and the analogies given, one can construct the proofs for the classical case. We begin by considering the case when $m = P^e$ i.e. a power of an irreducible polynomial P of degree n. Since $\Lambda_m \cong A/P^eA$, an element $\lambda_m \in \Lambda_m$ is a Λ_m-generator if and only if $\phi_{P^e}(\lambda) = 0$ and $\phi_{P^{e-1}}(\lambda_m) \neq 0$. Therefore, the generators of Λ_{P^e} are precisely the roots of,

$$\begin{aligned}\Phi_{P^e}(X) = \frac{\phi_{P^e}(X)}{\phi_{P^{e-1}}(X)} &= \frac{\phi_P(\phi_{P^{e-1}}(X))}{\phi_{P^{e-1}}(X)} \\ &= [P,n]\phi_{P^{e-1}}(X)^{r^n-1} + \cdots + [P,1]\phi_{P^{e-1}}(X)^{r-1} + P.\end{aligned}$$

and $\deg(\Phi_{P^e}(X)) = |P|^{e-1}(r^n - 1) = |P|^{e-1}(|P| - 1) = \varphi(P^e)$ as it should be. We can now investigate ramification in K_m. We shall achieve this via the theorem below.

Proposition 5.4.3. *Let $e \in \mathbf{Z}^+$ and $P \in A$ be a prime of degree n. Then, K_{P^e} is un-ramified at every prime ideal Q with $QA \neq PA$. The prime ideal PA is totally ramified with ramification index $\varphi(P^e)$ and consequently, $[K_{P^e} : k] = \varphi(P^e)$, $\mathrm{Gal}(K_{P^e}/k) \cong (A/P^eA)^*$. Finally, $\lambda\mathcal{O}_{P^e}$, (where λ is any generator of Λ_{P^e}) is the prime ideal lying above PA.*

Proof. ([18], Proposition 12.7). □

As a corollary, we restate proposition 5.2.5 and provide another proof to this fact.

Corollary 5.4.4. *Let $e \in \mathbf{N}$, P be a prime. Let λ be a generator of Λ_{P^e} and $g(X) \in k[X]$ its irreducible polynomial (over A). Then $g(X)$ is an Eisenstein polynomial at prime P.*

Proof. ([18], Corollary 12.6) We have,

$$g(X) = \prod_{(a,P)=1} (X - \phi_a(\lambda)),$$

where the product is over all generators of Λ_{P^e}. Except for the leading coefficient, which is 1, the coefficients of g are the elementary symmetric functions of the generators of Λ_{P^e}. Proposition 5.4.3 shows these are all in the ideal $\langle\lambda\rangle$. Therefore, all the coefficients of $g(X)$, except the leading coefficient, are in $\langle\lambda\rangle \bigcap A = PA$. Since the constant term is P, it follows that $g(X)$ is an Eisenstein polynomial at the prime P. □

Having dealt with the case $m = P^e$, we now pass on to the general case. Consider a non-constant polynomial $m \in A$ with the prime decomposition $m = \alpha P_1^{e_1} \cdots P_t^{e_t}$, $\alpha \in A^*$.

Theorem 5.4.5. *$K_m = \bigvee_{i=1}^t K_{P^{e_i}}$ and $P_i A$ with $1 \leq i \leq t$ are the only primes in A ramified in $\mathcal{O}_m$.*

Proof. This proof is divided into 2 parts.

1. Define m_i, to be m divided by $P_i^{e_i}$ and let λ_m be a generator of Λ_m as an A-module. It is clear from our previous discussion that $\phi_{m_i}(\lambda_m)$ is a generator of $\Lambda_{P_i^{e_i}}$.

   ($\Rightarrow$) Define $\lambda_{P_i^{e_i}} := \phi_{m_i}(\lambda_m)$. Clearly, $K_{P_i^{e_i}} = k(\lambda_{P_i^{e_i}}) \subset k(\lambda_m) = K_m$. Therefore, K_m contains the compositum of the fields $K_{P_i^{e_i}}$, for $1 \leq i \leq t$ i.e. $K_m \supseteq \bigvee_{i=1}^t K_{P^{e_i}}$. ($\Leftarrow$) Since the GCD of the set $\{m_i : 1 \leq i \leq t\}$ is just 1, there exist polynomials $a_i \in A$ such that $1 = \sum_{i=1}^t a_i m_i$. It follows that $1 = \sum_{i=1}^t \phi_{a_i}\phi_{m_i}$. Applying this relation to λ_m we obtain $\lambda_m = \sum_{i=1}^t \phi_{a_i}(\lambda_{P_i^{e_i}})$. This shows λ_m is in the compositum of the fields $K_{P_i^{e_i}}$, therefore $K_m \subseteq \bigvee_{i=1}^t K_{P^{e_i}}$, hence the proof that $K_m = \bigvee_{i=1}^t K_{P^{e_i}}$, the compositum of these fields.

2. If P is a prime element such that $PA \neq P_i A$ for any i, then by proposition 5.4.3, PA is un-ramified in every $K_{P_i^{e_i}}$ and so must be un-ramified in their compositum K_m. On the other hand, $P_i A$ is totally ramified in $K_{P_i^{e_i}}$ by the same proposition. Therefore, all ideals $P_i A$ are ramified in K_m.

□

Corollary 5.4.6. *K_m is ramified only at the primes dividing m and possibly at ∞.*

Using the Carlitz action, $\bar{k}_\infty$ can be turned into an A-module in exactly the same way that we turned k into an A-module; namely, if $a \in A$ and $u \in \bar{k}_\infty$, then we define $\sigma_a(u) = \phi_a(u)$. If $m \in A$ has positive degree, we denote the m-torsion points, $\bar{k}_\infty$ by $\hat{\Lambda}[m]$ or simply by $\hat{\Lambda}_m$. Let ι denote a fixed field isomorphism over k from K_m to $\bar{k}_\infty$. Now since K_m/k is a Galois extension, all the field isomorphisms over k from K_m to $\bar{k}_\infty$ are of the form $\iota \circ \sigma$ with $\sigma \in \mathrm{Gal}(K_m/k)$. The isomorphism ι corresponds to a prime $\wp_\infty$ of K_m lying over ∞. To see this, we let $\mathcal{O}_{\wp_\infty} = \{\omega \in K_m : v_\infty(\iota\omega) \geq 0\}$, it is easy to see that $\mathcal{O}_{\wp_\infty}$ is a discrete valuation ring inside K_m which contains $\mathbf{F}_r$ and has K_m as its quotient field. By definition, $\mathcal{O}_{\wp_\infty} \setminus \mathbf{F}_r^*$ is a prime of K_m denoted by $\wp_\infty$, its maximal ideal. The proof of the fact that $\wp_\infty$ lies above ∞ follows immediately. Suppose λ is a root to $\phi_m(X)$ in $\bar{k}$, since $\phi_m(\lambda) = 0$ implies $\phi_m(\iota\lambda) = \iota(\phi_m(\lambda)) = 0$; ι maps Λ_m to $\hat{\Lambda}_m$. This map is an A-module isomorphism thus, there is $\hat{\lambda}_m \in \hat{\Lambda}_m$ with $v_\infty(\hat{\lambda}) = n - 1 - \frac{1}{r-1}$. Let $\hat{\lambda}_m \in \hat{\Lambda}_m$ be such that $\iota\lambda = \hat{\lambda}_m$.

Let $\mathcal{I} = \{\sigma_\alpha \in \mathrm{Gal}(K_m/k) : \alpha \in \mathbf{F}_r^*\}$ and set K_m^+, equal to the fixed field of $\mathcal{I}$. Then ∞ splits completely in K_m^+ and every prime above ∞ in K_m^+ is totally and tamely ramified in K_m. For the proof of this fact is in ([18], Theorem 12.14).

If $f_m(X) = f_{\min}^{\hat{\lambda}}(X) \in k[X]$, then $K_m^+ = k(\hat{\lambda}) \cong k[X]/(f_m(X))k[X]$. Moreover, for $0 \neq m \in A$, K_m/k is a geometric extension i.e. the constant field of K_m is $\mathbf{F}_r$.

The properties of K_m^+ are so similar to those of $\mathbf{Q}^+$ in the number field case. We call K_m^+, the maximal real sub-field of K_m. The motivation for is that, the prime at infinity of k splits completely in K_m^+ and every prime above it (∞) in K_m^+ totally ramifies in K_m. This is analogous to the behaviour of ∞, the only archimedean prime at infinity of $\mathbf{Q}$. This splits completely in $\mathbf{Q}_n^+$ and every prime above it is totally ramified in $\mathbf{Q}_n$. Also notice that the Galois group of K_m/K_m^+ is isomorphic to $\mathbf{F}_r^*$, the non-zero units of A, whereas the Galois group of $\mathbf{Q}_n/\mathbf{Q}_n^+$ is isomorphic to $\mathbf{Z}^* = \{\pm 1\}$, still the units of $\mathbf{Z}$.

In general, we call a finite extension $\mathcal{F}$ of k real if P_∞ splits completely in $\mathcal{F}$. For example, the theory of quadratic function fields is divided up into the theory of real quadratic function fields, the case where ∞ splits, and complex quadratic function fields, the case where ∞ is either inert or ramifies. It is worth noting; like A and $\mathbf{Z}$, K_m contains many interesting arithmetic properties analogous to the cyclotomic number field.

We now turn our attention to the middle coefficient of $\Phi_m(X)$. By middle coefficient of $\Phi_m(X)$, we refer to the coefficient of $X^{\frac{\varphi(m)}{2}}$. We have the following proposition.

Proposition 5.4.7. *Let $s, l \in \mathbf{N}$, $m \in \mathbf{F}_r[T]$ where $r \equiv 1 \pmod 2$ and $P \in A^+$ be a prime. Let $\Phi_m(X) = \sum_{j=0}^{\varphi(m)} a_m(j)X^j$, then the middle coefficient of $\Phi_m(X)$ is*

$$a_m\left(\frac{\varphi(m)}{2}\right) = \begin{cases} 0, & m = P \text{ or } m = (T+\alpha)^l, \\ a_m^+(\frac{s}{2}), & \text{otherwise, } (s = \text{degree of } f_m(X)), \end{cases}$$

where $a_m^+(\frac{s}{2})$ is the middle coefficient of $f_m(X)$, the minimal polynomial of K_m^+-generators.

Proof. In this proof, we shall consider three cases,

1. Consider $m = T^s, s \in \mathbf{N}$, and $r \neq 2^t$ for all $t \in \mathbf{N}$.
   When $m = T^s$, then $\Phi_m(X) = \Phi_T(\phi_{T^{s-1}}(X)) = (\phi_{T^{s-1}}(X))^{r-1} + T$, a polynomial with zero as its middle coefficient. This follows from the fact that $\varphi(T^s) = r^{s-1}(r-1)$, and the observation that there is no term in $\phi_{T^{s-1}}(X)$ with $X^{\frac{r^{s-1}}{2}(r-1)}$. For if it existed (i.e. was there), then we would have 2 divide r^{s-1}, hence $r \equiv 0 \pmod 2$, which contradicts our assumption. Therefore, we must have $a_m\left(\frac{\varphi(m)}{2}\right) = 0$ and the result follows upon applying the ring homomorphism η_α.

2. Consider $m = P$ with degree n, clearly we know $\Phi_P(X)$ is a polynomial in X^{r-1} and therefore its middle term would correspond to the term in $X^{\frac{r^n-1}{2}} = X^{(r-1)\frac{1+r+\cdots+r^{n-1}}{2}}$. But there is no term in $\Phi_P(X)$ with $X^{\frac{r^n-1}{2}}$ since there exists no $n > 1$ such that $\frac{r^n-1}{2} = r-1$. Using theorem 5.3.14, we can extend this to all primes of degree n.

3. Consider m to be a product of more than one distinct primes. We already know, if λ is a generator of Λ_m, then λ is an algebraic unit (by proposition 5.4.2), and so is $\phi_a(\lambda)$ for any $0 \neq a \in A_m$. Now, let $f_m(X)$ be the minimal polynomial of λ^{r-1}, the generator of K_m^+, the maximal real sub-field of K_m. It is not hard to show using elementary methods that $f_m(X) \in A[X]$ (i.e. has integer coefficients) and that for $\deg(m) > 1$, we have $\deg(f_m(X)) = \frac{\varphi(m)}{r-1}$. Moreover, $\Phi_m(X) = f_m(X^{r-1})$, because (after simplifying the right-hand side) the polynomials on both sides are monic, are of degree $\varphi(m)$, and have λ as a root. Now on comparing this with $\Phi_m(X)$, we have, $f_m(X) = X^s + a_{s-1}X^{s-1} + \cdots + a_1 X \pm 1$ where $s = \frac{\varphi(m)}{r-1}$ and $a_i \in A$. So,

$$\Phi_m(X) = f_m(X^{r-1}) = \left(\sum_{i=1}^{s} a_i X^{i(r-1)}\right) + 1 \quad \text{with } a_s = 1.$$

The middle coefficient of $\Phi_m(X)$ is $a_m^+(\frac{s}{2})$, the coefficient of $X^{\frac{s}{2}}$ in $f_m(X)$. This integer is simply the middle coefficient of $f_m(X)$.

□

Over $\mathbf{F}_2$, the degree of all cyclotomic polynomials is odd and so the above result does not hold. For this reason, we needed $r \equiv 1 \pmod 2$. In the case where $r \equiv 0 \pmod 2$, we either have no middle coefficient or there are two possible coefficients depending one's interpretation. This is similar to the classical situations, $\Phi_1(X) = X - 1$ and $\Phi_2(X) = X + 1$. In fact, over $A = \mathbf{F}_2[T]$, one can show that there is only one root of $\phi_m(X)$ with valuation $\deg(m) - 2$ (with respect to ∞). Implying there is no middle coefficient or there are exactly 1 and $\hat{\lambda}$. (of course considering the middle two coefficients since $\deg(\Phi_m(X))$ is odd)

By using the theory of cyclotomic polynomials and extensions, one can establish another proof of the function field (polynomial) version of the quadratic reciprocity law by Carlitz.

In summary,

[1] At this link: http://mathworld.wolfram.com/CyclotomicPolynomial.html, I came across a compelling recursive formula implemented in Wolfram Mathematica that computes numerically the coefficients of classical cyclotomic polynomials. Unfortunately no proof nor reference to the proof was given, however, A. Grytczuk and B. Tropak have a given a proof, but still cannot find their paper. I hope, a thorough understanding of this formula will give heights of classical cyclotomic polynomials either explicitly or asymptotically.

Number fields ($\mathbf{Q}$)	Rational function field (k)
$a, b, d, n \in \mathbf{Z}$, $\alpha = 1, 2$	$a, b, m, d \in A$, $\alpha \in \mathbf{F}_r^*$
$\#\mu_n = \varphi(n)$	$\#\Lambda_m = \varphi(m)$
$d \mid n \Leftrightarrow \mu_d \subset \mu_n$	$d \mid m \Leftrightarrow \Lambda_d \subset \Lambda_m$
$\zeta_n \in \mu_n, a \in \mathbf{Z}$, then $\zeta_n^a \in \mu_n$	$\lambda \in \Lambda_m, a \in A$, then $\phi_a(\lambda) \in \Lambda_m$
$a \equiv b \pmod{n} \Leftrightarrow \zeta_n^a = \zeta_n^b$	$a \equiv b \pmod{m} \Leftrightarrow \phi_a(\lambda) = \phi_b(\lambda)$
$\mathrm{Gal}(K_n/\mathbf{Q}) \cong (\mathbf{Z}/n\mathbf{Z})^*$	$\mathrm{Gal}(K_m/k) \cong (A/mA)^*$
Proposition 1.2.1	Proposition 5.2.1
Proposition 1.2.2	Proposition 5.2.6
Proposition 1.2.3	Theorem 5.2.9
Corollary 1.2.4	Theorem 5.2.11
Proposition 1.2.6	Proposition 5.2.12
Proposition 1.2.7	Observation 5.2.13
Proposition 1.2.5	Theorem 5.2.15
Theorem 1.3.1	Conjecture 5.3.1
$\Phi_{n \neq \alpha p^s}(0) = 1$ and $\widehat{\Phi_{\alpha p^s}}(0) = p$	Proposition 5.3.20
?[1]	$h(\alpha) = 0$ and $h(m) = \sum_{d_+ \mid m} r^{\deg(d_+)-1} \mu(\frac{m}{d_+})$
$\mathcal{A}(\alpha p^s) = s$	$\mathcal{A}(\alpha P^s) = (r^{\deg(P)} - 1)(s - 1)$
$\vdots$	$\vdots$

Table 5.1. Analogy between the classical and Carlitz cyclotomic polynomials

Chapter 6

Mahler measure

In this chapter, we shall review what Mahler measure is, state some of its elementary properties and calculate explicitly the Mahler heights of $\phi_m(X)$ and $\Phi_m(X)$. In this setting, we replace the usual absolute value in $\mathbf{R}$ with the absolute value coming from the place at ∞.

6.1 Elementary properties of Mahler measure

Definition 6.1.1. *Suppose $f(z) \in \mathbf{C}[z]$, then $f(z)$ factors as $f(z) = \alpha(z-\alpha_1)\cdots(z-\alpha_n)$ over $\mathbf{C}$. The Mahler measure of $f(z)$ with respect to the usual absolute value $|\ |$ is given by*

$$\mathcal{M}(f) = |\alpha| \prod_{i=1}^{n} \max\{1, |\alpha_i|\},$$

or equivalently as a logarithmic Mahler measure,

$$m(f) = \ln(|\alpha|) + \sum_{i=1}^{n} \ln(\max_i\{1, |\alpha_i|\}) = \ln(\mathcal{M}(f)).$$

It is easy to show that Mahler measure as a 'measure' is multiplicative, so it makes sense to talk about the Mahler measure of rational functions. Note, for monic polynomials, we observe that $\mathcal{M}(f) \geq 1$. The term Mahler height (or 'measure') was first coined by Waldschmidt [23] to distinguish it from the naive or the classical notion of height, but later Boyd [7] and Durand [9] interpreted the function as a measure rather than the name.

Proposition 6.1.2. *Let $s \in \mathbf{Z}$, $f(z) \in \mathbf{C}[z]$, then $\mathcal{M}(f(z)) = \mathcal{M}(f(-z)) = \mathcal{M}(f(z^s))$.*

6.2 Mahler measure for Carlitz's polynomials

In comparison with the classical Mahler measure, we choose and take our valuations with respect to the place ∞ (this corresponds to $\frac{1}{T}$), and consider the absolute value associated to this valuation. Suppose now $f(z) \in \mathbf{C}_\infty[z]$, then f factors as $f(z) = \alpha(z-\alpha_1)\cdots(z-\alpha_n)$ over $\mathbf{C}_\infty$ where $\alpha \in \mathbf{C}_\infty^*$. We define the Mahler measure of $f(z)$ with respect to $|\ |_\infty$ as

$$\mathcal{M}(f) = |\alpha|_\infty \prod_{i=1}^{n} \max\{1, |\alpha_i|_\infty\}.$$

Through out this section, we take f to be monic and therefore $\mathcal{M}(f) = \prod_{i=1}^{n} \max\{1, |\alpha_i|_\infty\}$.

Since Mahler measure is multiplicative, proposition 5.2.1 shows that to determine Mahler measure of a Carlitz polynomial, it suffices to find Mahler measure of its Carlitz cyclotomic factors. Since all roots of the Carlitz cyclotomic polynomials are conjugate, they must have the same norm and therefore absolute value. So, in principle it is enough to find the norm of any generator of Λ_m as an A-module. We therefore have the following propositions.

Proposition 6.2.1. *Let $a \in A$ be of order ≥ 2, then $\mathcal{M}(\Phi_a) = 1$.*

Proof. Proposition 5.4.2 asserts that, if $a \in A$ is composite, then the generators of Λ_a are units, therefore all the conjugates are units (have absolute value 1) hence $\mathcal{M}(\Phi_a) = 1$. □

This is analogous to the classical result, whereby $\mathcal{M}(g) = 1$ if and only if atleast one of the roots of $g(x)$ lies on (others may lie inside) the unit circle. If this is the case, then classically g is said to be cyclotomic (i.e. 'circle dividing'). Over the function fields, we instead say g is a division polynomial (if its Mahler measure is 1). We now discuss the Mahler measure of the order 1 cyclotomic polynomials, since they are Eisenstein.

Proposition 6.2.2. *Let $P \in A^+$ be a prime polynomial, then $\mathcal{M}(\Phi_P) = |P|$.*

Proof. Proposition 5.4.2 asserts that for every prime $P \in A$, with λ as a generator of the $\phi_P(X)$ torsion points, we have $\frac{\phi_b(\lambda)}{\lambda} \in \mathcal{O}_P^*$ for all $b \in A$ co-prime to P. Since all these P-torsion points are non-zero algebraic functions, moreover non units, their norms in k must be different from 0 and 1 i.e. their absolute values are strictly greater than 1. Thus,

$$\mathcal{M}(\Phi_P) = \prod_{i=1}^{\varphi(P)} \max\{1, |\lambda_i|\} = |P^{\frac{1}{[K_P:k]}}|^{\varphi(P)} = |P^{\frac{1}{\varphi(P)}}|^{\varphi(P)} = |P|.$$

□

Corollary 6.2.3. *Let $s \in \mathbf{N}$ and $P \in A$ be a prime, then $\mathcal{M}(\Phi_{P^s}) = |P|$.*

Proof. Follows from proposition 5.3.20. □

Corollary 6.2.4. *Let $m \in A^+$, then $\mathcal{M}(\phi_m) = |m| = r^{deg(m)}$.*

Proof. Follows from the fact Mahler measure is multiplicative and proposition 6.2.1. □

The height of any element of A is of the form r^n, where $n \in \mathbf{Z}_{\geq 0}$. If for some $f \in A[X]$, $\mathcal{M}(f) = r^n$, then, the product of all the non-zero roots of f is equal to some $m \in A$. Considering all the non zero roots of f, gives we get some form of Carlitz polynomial; so combining propositions 6.2.1, 6.2.2 with corollaries 6.2.3 and 6.2.4, we obtain the theorem below.

Theorem 6.2.5. *If $g(X) \in A^+[X]$, $\alpha \in \mathbf{F}_r^*$, then if $g(X)$ is a product of powers of $X - \alpha$ and Carlitz cyclotomic polynomials, then $\mathcal{M}(g) = r^n$ for some $n \in \mathbf{N}$.*

This is analogous to the forward part of the following classical theorem due to Kronecker,

Theorem 6.2.6 (Kronecker's theorem). *If $f(x) \in \mathbf{Z}[x]$ is monic, then $\mathcal{M}(f) = 1$ if and only if $f(x)$ is a product of cyclotomic factors and x.*

I am still searching the complete analogue to this classical theorem.

6.3 Mahler measure for *classical* Eisenstein forms

In the classical case, we recall that all roots of cyclotomic polynomials are roots of unity and therefore lie on the unit circle and so the Mahler measure of any classical cyclotomic polynomial is 1. In this respect, the Mahler measure gives the average height of the roots of the polynomial away from the unit circle. An interesting case occurs for order 1 cyclotomic polynomials which are well known to have Eisenstein forms. It turns out that these polynomials no longer have $\mathcal{M}(f) = 1$. In fact none of them for $p > 2$ has any root of unity as a zero.

Proposition 6.3.1. *Let p be an odd prime, then*

$$\mathcal{M}(\widehat{\Phi_p}) = 2^{2a[p]} \prod_{j=1}^{a[p]} \cos^2\left(\tfrac{\pi j}{p}\right), \text{ where } a[p] = \lfloor \tfrac{\varphi(p)}{3} \rfloor.$$

Proof. Clearly $\Phi_p(X) = X^{p-1} + \cdots + X + 1$ and its Eisenstein form is $\widehat{\Phi}_p(X) = \Phi_p(X+1)$. Observe that the roots of $\widehat{\Phi}_p(X)$ are $1 + \zeta_p^a$, where $a = 1, \ldots, p-1$ and ζ_p is the p^{th} root of unity. Also when we consider the unit circle, for $p \geq 3$, the roots of $\Phi_p(X)$ occur in conjugate pairs, therefore it suffices to consider those cases where $|1 + \zeta_p^s| \geq 1$ (i.e. all those roots that are mapped onto the major arc of the unit circle centred at $(1,0)$ subtending an angle of 240°). Observe that, when $p \equiv 1, 3 (\text{mod } 4)$, then we have $2\lfloor \frac{\varphi(p)}{3} \rfloor$ roots of $\Phi_p(X)$ on the major arc AB, of the unit circle centred at $(1,0)$ as shown in figure 6.1 i.e those such that $|1 + \zeta^s| \geq 1$,

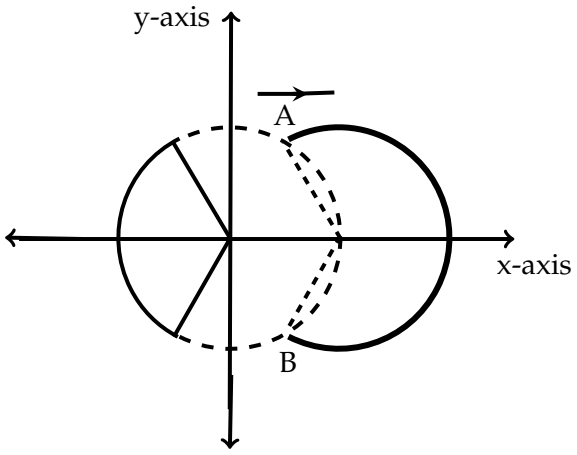

Figure 6.1. Major arc AB of the unit circle shifted to the right by a unit.

therefore $s = 1, \ldots, \lfloor \frac{1}{3}\varphi(p) \rfloor, p-1-\lfloor \frac{1}{3}\varphi(p) \rfloor, \ldots, p-1$. Now since roots of unity always occur in conjugate pairs, it suffices to consider $s = 1, \ldots, \lfloor \frac{1}{3}\varphi(p) \rfloor$.

$$\begin{aligned}\mathcal{M}(\widehat{\Phi_p}) &= \prod_{j=1}^{p-1} \max\{1, |1+\zeta^j|\} = \prod_{j=1}^{a[p]} \left|1+\zeta^j\right| \prod_{j=1}^{a[p]} \left|1+\zeta^{-j}\right| \\ &= \prod_{j=1}^{a[p]} \left|(2+\zeta^j+\zeta^{-j})\right| = \prod_{j=1}^{a[p]} 4\cos^2(\tfrac{\pi j}{p}).\end{aligned}$$

□

Corollary 6.3.2. *Let $s \in \mathbf{N}$, then*

$$\mathcal{M}(\widehat{\Phi_{p^s}}) = \prod_{j=1,(j,p^s)=1}^{a[p^s]} 4\cos^2(\tfrac{\pi j}{p^s}), \text{ where } a[p^s] = \lfloor \tfrac{p^s}{3} \rfloor.$$

Proof. The formula for $a[p^s]$ comes from counting of roots of unity in the first trisection of the unit circle and then the Mahler measure formula in corollary 6.3.2 sieves out the non-primitive p^s roots of unity by taking on only those j's that are co-prime to p^s. The remaining factor is got by taking into account the fact that all the primitive roots of unity for $n \geq 3$ occur in conjugate pairs and the calculation in the proof of proposition 6.3.1. □

Corollary 6.3.3. *Let $s \in \mathbf{N}$, then $\mathcal{M}(\widehat{\Phi_{2p^s}}) = \mathcal{M}(\widehat{\Phi_{p^s}})$.*

Proof. The proof of this corollary follows from the fact that, $\Phi_{2n}(X) = \Phi_n(-X)$ and that $\widehat{\Phi_{2n}}(X) = \Phi_{2n}(X-1)$ (This is just a reflection of Figure 6.1 through the y-axis). □

We illustrate this in the following examples;

1. Consider $s = 2$ and $p = 3$, then $\Phi_9(X) = \Phi_3(X^3) = X^6 + X^3 + 1$ and its Eisenstein form is actually $\widehat{\Phi_9}(X) = \Phi_9(X+1) = X^6 + 6X^5 + 15X^4 + 21X^3 + 18X^2 + 9X + 3$. We calculate its Mahler measure; we have $a[9] = 3$

$$\mathcal{M}(\widehat{\Phi_9}) = 2^4 \cos^2(\tfrac{\pi}{9}) \cos^2(\tfrac{2\pi}{9}) \approx 8.2909.$$

Explicitly, the roots of $\Phi_9(x)$ are $\approx -0.93969 \pm 0.34202i, 0.17365 \pm 0.98481i, 0.76604 \pm 0.64279i$; those of $\widehat{\Phi_9}(x)$ are $0.06031 \pm 0.34202i, 1.17365 \pm 0.98481i, 1.76604 \pm 0.64279i$. The non-effective roots (those that do not contribute anything) in the Mahler measure calculation are $0.06031 - 0.34202i$ and $0.06031 + 0.34202i$. So,

$$\begin{aligned}\mathcal{M}(\widehat{\Phi_9}) &\approx |1.17365 - 0.98481i| \cdot |1.76604 - 0.64279i| \cdot \\ &\quad |1.17365 + 0.98481i| \cdot |1.76604 + 0.64279i| \\ &\approx 8.2909.\end{aligned}$$

2. Consider $s = 2$ and $p = 5$, then $\Phi_{5^2}(X) = \Phi_5(X^5) = X^{20} + X^{15} + X^{10} + X^5 + 1$ and its Eisenstein form is actually $\widehat{\Phi_{25}}(X) = X^{20} + 20X^{19} + \cdots + 50X + 5$. In this case, the Mahler measure is computed as follows. We have $a[25] = 8$ and so,

$$\mathcal{M}(\widehat{\Phi_{25}}) = 2^{12} \cos^2(\tfrac{\pi}{25}) \cos^2(\tfrac{2\pi}{25}) \cos^2(\tfrac{3\pi}{25}) \cos^2(\tfrac{4\pi}{25}) \cos^2(\tfrac{6\pi}{25}) \cos^2(\tfrac{7\pi}{25}) \cos^2(\tfrac{8\pi}{25}) \approx 155.7$$

This can be verified by computing the roots of $\widehat{\Phi_{25}}(X)$ (up to 4 decimal places), then calculating $\mathcal{M}(\widehat{\Phi_{25}})$ using the definition. However, this approach is cumbersome.

We have been unable to provide interesting examples for this since my computer crashed.

Chapter 7

Conclusion

In this thesis, we investigated the analogues of classical cyclotomic polynomials over the rational function field $\mathbf{F}_r(T)$. We used the theory of Carlitz module to define $\phi_a(X)$, $\Phi_a(X)$, mainly followed the discussion in chapter 1 to explore their elementary properties and coefficients. We stated and proved the analogues of propositions 1.2.1,1.2.3,1.2.4,1.2.5 and 1.2.6.

Our attempts to find the full analogue to theorem 1.2.7 (i.e. palindromy of the coefficients of $\Phi_m(X)$) failed because $\text{Char}(k) = p > 0$, $\phi(m)$ is in general NOT a p-power and $\phi_m(X)$ is not reciprocal. Imitating the classical notion of order and the number-function field analogy, we defined order, and height of Carlitz cyclotomic polynomials. Much as these notions yielded no interesting results, we were able to obtain an expression for computing the logarithmic heights of $\Phi_m(X)$ but the classification of the polynomials according to order was lost. We also found that, $h(\Phi_m(X))$ grows exponentially with the degree of m compared to the order of $\Phi_m(X)$ as opposed to the classical case where the size of n does not matter but the order of $\Phi_n(X)$. Motivated by classical results, we defined 'prime height' for order 1 cyclotomic polynomials. This helped us restore the analogy between classical and Carlitz cyclotomic polynomials of order 1. see theorems 5.3.12 and 5.3.16. A quick proof to a special case of Dirichlet's theorem on primes in an arithmetic progression was given. see Theorem 5.3.22.

Again motivated by classical results, we extended the definition of Mahler measure of classical cyclotomic polynomials to Carlitz cyclotomic polynomials and calculated Mahler measures of $\Phi_m(X)$ and $\phi_m(X)$. In this way, we attempted to give the analogue of the classical Kronecker theorem. We used some results from this to again explore more about Mahler measures of classical cyclotomic polynomials. In here, we obtained a formula for computing the Mahler measure of Eisenstein forms of classical cyclotomic polynomials.

We only studied coefficients of order one cyclotomic polynomials, but we hope to further research on coefficients and heights of higher order polynomials. We would also like to

know whether the coefficients of these polynomials are of any arithmetic significance. As a corollary to proposition 5.3.20, each prime in A appears as coefficient in some cyclotomic polynomial. Also since $\phi'_m(X) = m$, A is the set of coefficients of Carlitz polynomials. This evidence together with the polynomial version of the Prime number theorem compelled us to conjecture that, '*the set of all coefficients of cyclotomic polynomials over k is A*'.

In chapter 5, we saw that using the Carlitz action one would generate a Carlitz triangle more less similar to the Pascal's triangle whose arithmetic is worth investigating. Actually it turns out that some classical properties embedded in the Pascal's triangle also have analogues over the function fields. (This is our current micro-project, 2011). We do not yet know whether such nice things exist for Drinfeld modules of arbitrary rank. Another item worth of investigation is the divisibility of $\Phi_m(X)$ over prime moduli, that is to say, finite fields of the form A/PA. Could this also shed more light on how to factor bivariate polynomials over k using Carlitz cyclotomic polynomials? Lastly, studying these polynomials in towers of Galois fields and of course how they factorise in these towers would also be interesting.

Chapter 8

Appendix

8.1 Algorithms

Notation:

$a, m, s \in A^+$ and P is a prime in A.

$\phi_a(X)$ is the Carlitz polynomial corresponding to a.

$\phi_{a_i}(X)$ = part of $\phi_a(X)$ with terms from the 1^{st} up to the i^{th} term.

$\Phi_a(X)$ is the Carlitz cyclotomic polynomial corresponding to a.

Algorithm 1 Computing $\phi_P(X)$ by a recursion formula

Input: P with $n = deg(P) \geq 1$

Output: $\phi_P(X)$

1. $a_0 \longleftarrow P$
2. $\phi_{a_0}(X) \longleftarrow PX$
3. for $i = 1$ to n
4. $\quad a_i \longleftarrow \frac{a_{i-1}^r - a_{i-1}}{T^{r^i} - T}$
5. $\quad \phi_{a_i}(X) \longleftarrow a_i X^{r^i} + \phi_{a_{i-1}}(X)$
6. $\phi_P(X) \longleftarrow \phi_{a_n}(X)$

Return: $\phi_P(X)$

Algorithm 2 Computing $\phi_m(X)$ by repeated polynomial division

Input: $m = P_1^{e_1} \cdots P_t^{e_t}$ where $e_i > 0$ for all $1 \leq i \leq t$

Output: $\phi_m(X)$

1. $a \longleftarrow 1$
2. $\phi_a(X) \longleftarrow X$
3. for $i = 1$ to t
4. $\quad \phi_{aP_i}(X) \longleftarrow \phi_a(\phi_{P_i}(X))$
5. $\quad a \longleftarrow aP_i$
6. $\quad s \longleftarrow \frac{m}{a}$
7. $\phi_m(X) \longleftarrow \phi_a(\phi_s(X))$

Return: $\phi_m(X)$

Algorithm 3 Computing $\Phi_m(X)$ by repeated polynomial division

Input: $m = P_1^{e_1} \cdots P_t^{e_t}$ where $e_i > 0$ for all $1 \leq i \leq t$

Output: $\Phi_m(X)$

1. $a \longleftarrow 1$
2. $\Phi_a(X) \longleftarrow X$
3. for $i = 1$ to t
4. $\quad \Phi_{aP_i}(X) \longleftarrow \frac{\Phi_a(\phi_{P_i}(X))}{\Phi_a(X)}$
5. $\quad a \longleftarrow aP_i$
6. $s \longleftarrow \frac{m}{a}$
7. $\Phi_m(X) \longleftarrow \Phi_a(\phi_s(X))$

Return $\Phi_m(X)$

Appendix B

8.2 Eisenstein forms of order one cyclotomic polynomial

Definition 8.2.1. *Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbf{Z}[x]$. $f(x)$ is said to be an Eisenstein polynomial if there exists prime p such that (i) p divides a_i for $i = 0, 1, \ldots, n-1$ and (ii) p does not divide a_0^2. e.g. $g(x) = x^2 + p^n ax + p$ for any $a \in \mathbf{Z}$ is Eisenstein for the prime p.*

An irreducible polynomial $f(x)$ is said to have an Eisenstein form, if it can be turned into (shifted to) an Eisenstein polynomial of the same degree and leading coefficient by an algebraic transformation. In fact for our cyclotomic polynomials, we shall only use linear transformations. Shortly, we will show that, all prime cyclotomic polynomials have Eisenstein forms. It is these new polynomials that we call the Eisenstein-cyclotomic polynomials (much as their roots are not necessarily roots of unity) or simply 'Eisenstein forms' and denote them with hats e.g. the Eisenstein form corresponding to $\Phi_p(X)$ is $\widehat{\Phi_p}(X)$.

Proposition 8.2.2. *All order one cyclotomic polynomials have 'Eisenstein forms'.*

Proof. We consider 3 cases.
Suppose $n = p > 2$ is a prime, $\widehat{\Phi_p}(X) = \Phi_p(X+1) = X^{-1}\sum_{i=1}^{p}\binom{p}{i}X^i = X^{p-1} + \cdots + p$ is the Eisenstein form required in this case, since p divides $\binom{p}{i}$ for $i = 1, \ldots, p-1$ and p^2 does not divide p. Suppose $n = 2p$, where $p > 2$ is a prime. By proposition 1.2.6, we have $\Phi_{2p}(X) = \Phi_p(-X)$ hence $\Phi_{2p}(X)$ has an Eisenstein form (since -1 is a unit in $\mathbf{Z}$). In fact, $\widehat{\Phi_{2p}}(X) = \Phi_{2p}(X-1) = \Phi_p(-X+1)$, is the required form (the substitution $X-1$ makes every coefficient positive). Lastly, suppose $n = 2^s p^t$ where $s \in \mathbf{N}_{\geq 2}$ and $t \in \mathbf{Z}^+$, then clearly, we have $\Phi_{2^s p^t}(X) = \Phi_{2p}(X^{2^{s-1}p^{t-1}})$. By case 2 above, proposition 5.2.12 is established. □

Definition 8.2.3. *Let $f = \sum_{i=0}^{n} a_i x^i \in \mathbf{Q}[x]$, set $\mathcal{H}_p(f) := \max\{|a_i|_p : \text{for } 0 \leq i \leq n\}$, where $|a|_p$ is the p-adic absolute value of a. We set $\mathcal{H}_\infty := \mathcal{H}$, i.e. the usual absolute value in $\mathbf{R}$.*

For order one cyclotomic polynomials, we set $\widehat{\Phi_{p^s}}(X)$ and $\widehat{\Phi_{2^s p^t}}(X)$ to be the associated Eisenstein forms respectively. $\mathcal{A}(n) := \mathrm{Log}_p(\mathcal{H}_p(\widehat{\Phi_n}(X)))$, where p is the unique odd prime dividing n is called the prime height of $\Phi_n(X)$. In other words, $\mathcal{A}(p)$ is like a 'measure' of

divisibility of coefficients of $\widehat{\Phi_p}(X)$ with respect to p. In order to calculate $\mathcal{A}(p^t), \mathcal{A}(2p^t)$, we first transform $\Phi_p(X)$ into $\widehat{\Phi_p}(X)$. We denote the height of $\widehat{\Phi_n}(x)$ by $\widehat{\mathcal{H}}(n)$ or $\mathcal{H}(\widehat{\Phi_n}(x))$.

Theorem 8.2.4 (Legendre, 1808). *Let p be a prime and let $n = a_0p^t + a_1p^{t-1} + \cdots + a_{t-1}p + a_t$ be the base p expansion of n. The exact power m of p dividing $n!$ is given by*

$$v_p(n!) = \frac{n - (a_0 + a_1 + \cdots + a_t)}{p-1}. \tag{8.1}$$

Lemma 8.2.5. *Let $t \in \mathbf{Z}^+$, then $0 \leq v_p(\binom{p^t}{x}) \leq t$. If $x \not\equiv 0 \pmod{p}$, then $v_p(\binom{p^t}{x}) = t$.*

Proof. Let $g(x) = \binom{p^t}{x} = \frac{p^t!}{(p^t-x)!x!}$, where $x \in \mathbf{N}$. Now, since $g(x) \in \mathbf{Z}$, we have $v_p(g(x)) \geq 0$. Also $v_p(g(x)) = v_p(p^t!) - v_p((p^t - x)!) - v_p(x!)$. By symmetry of the binomial coefficients, it is enough to consider valuations for $x \leq \lfloor \frac{p^t}{2} \rfloor$. Clearly, $v_p(g(0)) = 0$ and $v_p(g(1)) = t$. This follows from considering the following facts (obtained using theorem 8.2.4)

1. $g(0) = 1$,
2. $v_p(p^t!) = \frac{p^{t+1}-1}{p-1}$,
3. if $x = ap^s$ where $0 \leq a \leq p-1$, then $v_p(x!) = a\frac{p^{s+1}-1}{p-1}$,
4. if $x = ap^s, 0 \leq a \leq p-1, 1 \leq s \leq t-1$, then $v_p((p^t - x)!) = \frac{p^{t+1}-1}{p-1} - a\frac{p^{s+1}-1}{p-1} - (t-s)$.

Claim: If $x \equiv 0 \pmod{p}$, then $v_p(g(x)) \leq t-1$, otherwise $v_p(g(x)) = t$.

1. When $x \equiv 0 \pmod{p}$, in particular for $x = ap^s$ with $s \leq t-1$ and $1 \leq a \leq p-1$, we then have $v_p(x!) = v_p(ap^s!) = a\frac{p^{s+1}-1}{p-1}$. Therefore, $0 \leq v_p(g(x)) \leq t-1$.
2. Otherwise, take $x = ap^s + \alpha$, where $1 \leq \alpha, a \leq p-1$. In this case, $v_p(x!) = a\frac{p^{s+1}-1}{p-1}$, since all the first α factors in the factorial expansion of $x!$ have (each) valuation 0. By a similar reasoning to $(p^t - x)!$, we get $v_p((p^t - x)!) = \frac{p^{t+1}-1}{p-1} - a\frac{p^{s+1}-1}{p-1} - t$. Therefore, $v_p((p^t - x)!x!) = \frac{p^{t+1}-1}{p-1} - t$, and we get $v_p(g(x)) = v_p(p^t!) - v_p((p^t - x)!x!) = t$.

This completes the proof. □

Theorem 8.2.6 (Result 1). *We have $\widehat{\mathcal{H}}(2) = 2$. For $s \in \mathbf{N}$, we have $\widehat{\mathcal{H}}(2^s) = \binom{2^{s-1}}{2^{s-2}}$ and*

$$\widehat{\mathcal{H}}(p^s) = \begin{cases} \binom{p}{\frac{p-1}{2}}, & \text{if } p > 2 \text{ and } s = 1, \\ \sum_{i=\frac{p-1}{2}}^{p-1} \binom{p^{s-1}i}{\frac{\phi(p^s)}{2}}, & \text{if } p > 2 \text{ and } s > 1\,. \end{cases}$$

Proof. This is based on the fact that the maximum coefficient in a binomial expansion is the coefficient of the middle term. We shall do this in 3 steps as follows,

1. When $p = 2$, we have $\Phi_2(X+1) = X+2$, thus $\hat{\mathcal{H}}(2) = 2$. For $s > 1$, we get $\Phi_{2^s}(X+1) = (X+1)^{2^{s-1}} + 1$, whose maximum absolute coefficient is $\hat{\mathcal{H}}(2^s) = \binom{2^{s-1}}{2^{s-2}}$.
2. when $p > 2$, $s = 1$, we have $\Phi_p(X+1) = \sum_{i=1}^{p} \binom{p}{i} X^{i-1}$. The maximum coefficient (in absolute values) is the coefficient of $X^{\frac{p-1}{2}}$ or $X^{\frac{p-3}{2}}$, so $\hat{\mathcal{H}}(p) = \binom{p}{\frac{p-1}{2}} = \binom{p}{\frac{p+1}{2}}$.
3. When p is odd and $s > 1$, then $\Phi_{p^s}(X+1) = \Phi_p((X+1)^{p^{s-1}}) = \sum_{i=0}^{p-1} (X+1)^{p^{s-1}i}$. Even heuristics show that $\hat{\mathcal{H}}(p^s)$ is the middle term in $\Phi_{p^s}(X+1)$. Therefore, we have $\hat{\mathcal{H}}(p^s) X^{\frac{\phi(p^s)}{2}} = \sum_{i=0}^{p-1} \sum_{j=0}^{p^{s-1}i} \chi_0(j) \binom{p^{s-1}i}{j} X^j$, where $\chi_0(j) = 1$ if $j = \frac{\phi(p^s)}{2}$, and 0 otherwise. With the help of this sieve, the coefficients of $X^{\frac{\phi(p^k)}{2}}$ are of the form $\binom{p^{s-1}i}{\frac{\phi(p^s)}{2}}$. This restricts us to values of $i \geq \frac{p-1}{2}$, therefore $\widehat{\mathcal{H}}(p^s) = \sum_{i=\frac{p-1}{2}}^{p-1} \binom{p^{s-1}i}{\frac{\phi(p^s)}{2}}$.

□

Corollary 8.2.7. *Let $s \in \mathbf{Z}^+$, then $\mathcal{A}(p^s) = s$ and $\mathcal{A}(2p^s) = s$.*

Proof. By lemma 8.2.5 + $\Phi_{p^s}(X+1) = \sum_{i=0}^{p-1} (X+1)^{p^{s-1}i}$ is Eisenstein, it suffices to consider, the valuation of coefficient of X in $\Phi_{p^s}(X+1)$, so $\mathcal{A}(p^s) = v_p\left(\sum_{i=1}^{p-1} \binom{p^{(s-1)}i}{1}\right) = v_p(p^{s-1}\sum_{i=1}^{p-1} i) = s$. The second formula follows from proposition 1.2.6 + $\mathcal{A}(p^s) = s$. □

Theorem 8.2.8 (Result 2)**.**

$$\widehat{\mathcal{H}}(2p^s) = \begin{cases} \binom{p}{\frac{p-1}{2}}, & \text{if } p > 2 \text{ and } s = 1, \\ \sum_{i=\frac{p-1}{2}}^{p-1} \binom{p^{s-1}i}{\frac{\phi(p^s)}{2}}, & \text{if } p > 2 \text{ and } s > 1\,. \end{cases}$$

Proof. We do this in 2 steps, since it is trivial for $p = 2$ and $s \geq 1$.

1. For $p > 2$ and $s = 1$, $\Phi_{2p}(X-1) = \sum_{i=1}^{p} \binom{p}{i} (-X)^{i-1}$. Therefore, $\hat{\mathcal{H}}(2p) = \binom{p}{\frac{p-1}{2}}$.
2. For $p > 2$ and $s > 1$, then $\Phi_{2p^s}(X-1) = \Phi_{p^s}(-X+1) = \sum_{i=0}^{p-1} (-X+1)^{p^{s-1}i}$. Similar arguments as in theorem 8.2.6 give the desired result.

□

Example 8.2.9. *Take $p = 3$, and $s = 4$, then $\Phi_{3^4}(X) = \Phi_3(X^{27}) = X^{54} + X^{27} + 1$. Its Eisenstein form is $\widehat{\Phi_{3^4}}(X) = \Phi_{3^4}(X+1) = X^{54} + 54X^{53} + 1431X^{52} + 24804X^{51} + \cdots + 333801X^4 + 27729X^3 + 1782X^2 + 81X + 3$. The set of 3-adic valuations of all the coefficients in ascending powers of X is $[1, 4, 4, 3, 4, \ldots, 2, 3, 3, 0]$, so $\mathcal{A}(3^4) = 4$. Moreover, $\widehat{\mathcal{H}}(3^4) = 1946939425648113$ and by theorem 8.2.8, we have*

$$\widehat{\mathcal{H}}(3^4) = \binom{3^3}{3^3} + \binom{2 \cdot 3^3}{3^3} = 1 + 1946939425648112 = 1946939425648113.$$

Bibliography

[1] E. Artin and J. Tate. *Class field theory*. AMS Chelsea Publishing, Providence, RI, 2009. Reprinted with corrections from the 1967 original.

[2] G. Bachmann. Flat Cyclotomic Polynomials of Order Three. *Bull. London Math. Soc.*, 38(1):53–60, 2006.

[3] S. Bae. The arithmetic of Carlitz polynomials. *J. Korean Math. Soc.*, 35:341–360, 1998.

[4] S. Bae and S. Hahn. On the Carlitz module. *J. Chungcheong Math. Soc.*, 4:85–90, 1991.

[5] P. Bateman, C. Pomerance, and R. Vaughan. On the size of the coefficients of the cyclotomic polynomial. In *Topics in classical number theory, Vol. I, II (Budapest, 1981)*, pages 171–202. North-Holland, Amsterdam, 1984.

[6] M. Beiter. Coefficients of the cyclotomic polynomial $F_{3qr}(x)$. *Fibonacci Quart.*, 16(4):302–306, 1978.

[7] D. Boyd. Speculations concerning the range of Mahler's measure. *Canad. Math. Bull.*, 24:453–469, 1981.

[8] L. Carlitz. On polynomials in a Galois field. *Bull. Amer. Math. Soc.*, 38:734–744, 1932.

[9] A. Durand. On Mahler's measure of a polynomial. *Proc. Amer. Math. Soc.*, 83:75–76, 1981.

[10] D. Goss. *Basic Structures of Function Field Arithmetic*. Springer, 1996.

[11] D. Hayes. Explicit class field theory for rational function fields. *Trans. Amer. Math. Soc.*, 189:77–91, 1974.

[12] K. Ireland and M. Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[13] N. Kaplan. Flat cyclotomic polynomials of order four and higher. *Integers*, 10:357–363, 2010.

[14] T. Lam and K. Leung. On the cyclotomic polynomial $\phi_{pq}(x)$. *Amer. Math. Monthly*, 103(1):562–564, 1996.

[15] S. Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[16] J. Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999.

[17] V. Prasolov. *Polynomials*. Springer-Verlag Berlin Heidelberg, 2004.

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

[19] G. Salvador. *Topics in the Theory of Algebraic Function Fields*. Birkhauser, Boston, 2006.

[20] W. Stein et al. SAGE Mathematical Software Version 4.2.6, 2011.

[21] J. Suzuki. On the coefficients of cyclotomic polynomials. *Proc. Japan Acad. Soc.*, A63:279–280, 1987.

[22] D. Thakur. *Function field arithmetic*. World Scientific Publishing Co. Inc., River Edge, NJ, 2004.

[23] M. Waldschmidt. Nombres transcendants et groupes algébriques. *Astérique Sociétié Mathématique de France, Paris*, pages 69–70, 1979.

[24] L. Washington. *Introduction to Cyclotomic Fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1982.