Given r and a finite field F_k, we are interested in the question: how does $\Phi_r(x)$ factor over F_k ($\Phi_r(x)$ is the r-th cyclotomic polynomial)? In the following discussion, let $r = p^e s$, where $p = \mathrm{char}(F_k), p \nmid s$.

Lemma 1. $\forall a \in F_{k^n}, (x-a)(x-a^k)\dots\left(x-a^{k^{n-1}}\right) \in F_k[x]$.

This is obviously true if $a = 0$. Now suppose $a \neq 0$.

Note that the coefficient of x^{n-m} of $(x-a)(x-a^k)\dots(x-a^{k^{n-1}})$ is $(-1)^m S_m$, where

$$S_m = \sum_{b_{n-1}+b_{n-2}+\cdots+b_1+b_0=m, b_i\in\{0,1\}} a^{b_{n-1}k^{n-1}+b_{n-2}k^{n-2}+\cdots+b_1k+b_0}.$$

Lemma 1 is equivalent to the fact that $S_m \in F_k, m = 0,1,\dots,n$, which is further equivalent to $S_m^k = S_m, m = 0,1,\dots,n$.

By the property of finite fields, we have

$$S_m^k = \left(\sum_{b_{n-1}+b_{n-2}+\cdots+b_1+b_0=m, b_i\in\{0,1\}} a^{b_{n-1}k^{n-1}+b_{n-2}k^{n-2}+\cdots+b_1k+b_0}\right)^k$$

$$= \sum_{b_{n-1}+b_{n-2}+\cdots+b_1+b_0=m, b_i\in\{0,1\}} \left(a^{b_{n-1}k^{n-1}+b_{n-2}k^{n-2}+\cdots+b_1k+b_0}\right)^k$$

$$= \sum_{b_{n-1}+b_{n-2}+\cdots+b_1+b_0=m, b_i\in\{0,1\}} a^{k(b_{n-1}k^{n-1}+b_{n-2}k^{n-2}+\cdots+b_1k+b_0)}$$

$$= \sum_{b_{n-1}+b_{n-2}+\cdots+b_1+b_0=m, b_i\in\{0,1\}} a^{b_{n-1}k^{n}+b_{n-2}k^{n-1}+\cdots+b_1k^2+b_0k}$$

$$= \sum_{b_{n-1}+b_{n-2}+\cdots+b_1+b_0=m, b_i\in\{0,1\}} a^{b_{n-1}\cdot 1+b_{n-2}k^{n-1}+\cdots+b_1k^2+b_0k} \left(\text{By } a^{k^n-1} = 1\right) = S_m,$$

which is what we wanted.

By Lemma 1, we can see that for any $a \in F_{k^n}$, $(x-a)(x-a^k)\dots\left(x-a^{k^{n-1}}\right)$ is a polynomial acting as a bridge between F_{k^n} and F_k. For convenience, we write

$$P_a(x) \coloneqq (x-a)(x-a^k)\dots\left(x-a^{k^{n-1}}\right), \forall a \in F_{k^n}.$$

Now we first consider the case $e = 0$. Write $n = \mathrm{ord}_s(k)$, then $k^n \equiv 1 \pmod{s}$. Since that the multiplicative group of F_{k^n} is cyclic with $k^n - 1$ elements, $x^s - 1$ factors completely into linear polynomials:

$$x^s - 1 = \prod_{i=1}^{s} (x - a^i),$$

where a is some element in F_{k^n}. By the definition of cyclotomic polynomials, over F_{k^n}, $\Phi_s(x)$ also factors completely into linear polynomials:

$$\Phi_s(x) = \prod_{\substack{1 \le i \le s \\ \gcd(i,s)=1}} (x - a^i).$$

Actually, we would rather say "$\bar{i} \in \mathbb{Z}_s^\times$" than say "$\gcd(i,s) = 1$", where $\mathbb{Z}_s^\times$ is the multiplicative group of integers modulo s. Note that

$$< \bar{k} >= \left\{e, \bar{k}, \bar{k}^2, \dots, \bar{k}^{n-1}\right\} = \left\{\bar{1}, \bar{k}, \overline{k^2}, \dots, \overline{k^{n-1}}\right\},$$

then,

$$\mathbb{Z}_s^\times / < \bar{k} >= \left\{\left\{\bar{i}, \overline{ik}, \overline{ik^2}, \dots, \overline{ik^{n-1}}\right\} : \bar{i} \in \mathbb{Z}_s^\times\right\} \triangleq \left\{[\bar{i}] : \bar{i} \in \mathbb{Z}_s^\times\right\},$$

where

$$\bigcup_{[\bar{i}] \in \mathbb{Z}_s^\times / <\bar{k}>} \left\{\bar{i}, \overline{ik}, \overline{ik^2}, \dots, \overline{ik^{n-1}}\right\} = \mathbb{Z}_s^\times.$$

(Here $\cup$ represents disjoint union, similarly hereinafter.) As a result,

$$\bigcup_{[\bar{i}] \in \mathbb{Z}_s^\times / <\bar{k}>} \left\{a^i, a^{ik}, \dots, a^{ik^{n-1}}\right\} = \left\{a^i : \bar{i} \in \mathbb{Z}_s^\times\right\},$$

(both sides should be interpreted as multisets,) which gives

Theorem 1. Suppose $\gcd(k,s) = 1$. Over F_{k^n}, if $\Phi_s(x)$ factors as the form above, where a is some element in F_{k^n}, then over F_k, $\Phi_s(x)$ factors as

$$\Phi_s(x) = \prod_{[\bar{i}] \in \mathbb{Z}_s^\times / <\bar{k}>} P_{a^i}(x).$$

Moreover, P_{a^i} is irreducible over F_k.

This is quite natural because the set of the roots of $\prod_{[\bar{i}] \in \mathbb{Z}_s^\times / <\bar{k}>} P_{a^i}(x)$ is $\cup_{[\bar{i}] \in \mathbb{Z}_s^\times / <\bar{k}>} \left\{a^i, a^{ik}, \dots, a^{ik^{n-1}}\right\}$, and the set of the roots of $\Phi_s(x)$ is $\left\{a^i : \bar{i} \in \mathbb{Z}_s^\times\right\}$, so both sides are the same.

By Lemma 1, $P_{a^i}(x) \in F_k[x]$, so we have factored $\Phi_s(x)$ over F_k.

Now we show that $P_{a^i}(x)$ is irreducible over F_k. Let $Q(x)$ be an irreducible factor of $P_{a^i}(x)$ such that $\deg Q = d' > 0$, then we have $F_{k^{d'}} \cong F_k[y]/Q[y]$, that is to say,

$$Q(x) | x^{k^{d'}-1} - 1.$$

By definition,

$$Q(x) | \gcd\left(\Phi_s(x), x^{k^{d'}-1} - 1\right),$$

or equivalently,

$$Q(x) \mid \gcd\left(\Phi_s(x), \prod_{q|k^{d'}-1} \Phi_q(x)\right).$$

Note that if $s \neq t$, then $\gcd(\Phi_s(x), \Phi_t(x)) = 1$, otherwise $\gcd(\Phi_s(x), \Phi_t(x))^2 \mid x^{\mathrm{lcm}(s,t)} - 1$, which is impossible because $x^{\mathrm{lcm}(s,t)} - 1$ should have no multiple factor. As $\deg Q > 0$, we must have $s|k^{d'} - 1$, but $d' \leq d$, so $d' = d$.

Example. Let $s = 11$ and $k = 3$, then $n = 5$. $\mathbb{Z}_{11}^{\times} = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}\}, < \overline{3} >= \{\overline{1}, \overline{3}, \overline{4}, \overline{5}, \overline{9}\}$, so

$$\mathbb{Z}_{11}^{\times} / < \overline{3} >= \left\{\{\overline{1}, \overline{3}, \overline{4}, \overline{5}, \overline{9}\}, \{\overline{2}, \overline{6}, \overline{7}, \overline{8}, \overline{10}\}\right\} \triangleq \{[\overline{1}], [\overline{2}]\}.$$

Over F_{3^5}, $\Phi_{11}(x)$ factors as

$$(x-a)(x-a^2)(x-a^3)(x-a^4)(x-a^5)(x-a^6)(x-a^7)(x-a^8)(x-a^9)(x-a^{10}),$$

so over F_3, the factorization of $\Phi_{11}(x)$ is

$$\Phi_{11}(x) = P_a(x) P_{a^2}(x),$$

where

$$P_a(x) = (x-a)(x-a^3)(x-a^4)(x-a^5)(x-a^9),$$
$$P_{a^2}(x) = (x-a^2)(x-a^6)(x-a^7)(x-a^8)(x-a^{10}).$$

By Theorem 1, both $P_a(x)$ and $P_{a^2}(x)$ are irreducible over F_3.

Corollary 1. Suppose $\gcd(k, s) = 1$. Over F_k, $\Phi_s(x)$ is the product of $\frac{\varphi(s)}{\mathrm{ord}_s(k)}$ irreducible polynomials of degree $\mathrm{ord}_s(k)$, where φ is the Euler's totient function.

Theorem 2. If $e > 0$, then

$$\Phi_r(x) = (\Phi_s(x))^{(p-1)p^{e-1}}.$$

Proof. By Moebius inversion formula, we have

$$\Phi_s(x) = \prod_{q|s} (x^q - 1)^{\mu\left(\frac{s}{q}\right)}.$$

Since that $r = p^e s$, $\gcd(k, s) = 1$, we have

$$\Phi_r(x) = \prod_{q|p^e s} (x^q - 1)^{\mu\left(\frac{p^e s}{q}\right)} = \prod_{i=0}^{e} \prod_{q|s} \left(x^{p^i q} - 1\right)^{\mu\left(\frac{p^e s}{p^i q}\right)}$$

$$= \prod_{q|s} \prod_{i=0}^{e} \left(x^{p^i q} - 1\right)^{\mu\left(p^{e-i} \frac{s}{q}\right)} = \prod_{q|s} \prod_{i=0}^{e} (x^q - 1)^{p^i \mu(p^{e-i}) \mu\left(\frac{s}{q}\right)}$$

$$= \prod_{q|s} (x^q - 1)^{\mu\left(\frac{s}{q}\right) \sum_{i=0}^{e} p^i \mu(p^{e-i})} = \prod_{q|s} (x^q - 1)^{\mu\left(\frac{s}{q}\right)(p-1)p^{e-1}} = \left(\Phi_s(x)\right)^{(p-1)p^{e-1}}.$$

Corollary 2. Let $r = p^e s$, where $p = \mathrm{char}(F_k), p \nmid s$. Over F_k, $\Phi_r(x)$ is the product of $\frac{\varphi(r)}{\mathrm{ord}_s(k)}$ irreducible polynomials of degree $\mathrm{ord}_s(k)$.

Corollary 3. Over F_k, $\Phi_r(x)$ is irreducible if and only if:

(a) $\gcd(k, r) = 1$, and k is a primitive root modulo r;

(b) k is a power of 2, $r \equiv 2 \pmod 4$, and k is a primitive root modulo $\frac{r}{2}$.

We can see from Corollary 3 that:

(a) If there is no primitive root modulo r (i.e., $r = 8, 12, 15, 16, \ldots$), then $\Phi_r(x)$ is reducible over every finite field, and specially, over every finite field of prime order. This is quite interesting because $\Phi_r(x)$ is irreducible over $\mathbb{Q}$;

(b) If k is a square number, then for every $r > 2$, $\Phi_r(x)$ is reducible over F_k.

The following table gives the number of factors of $\Phi_r(x)$ over F_k for small k and r.

k/r	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	1	1	1	2	1	1	2	4	1	1	1	2	1	2	2	8
3	1	1	2	1	1	2	1	2	6	1	2	2	4	1	2	2
4	1	1	2	2	2	2	2	4	2	2	2	4	2	2	4	8
5	1	1	1	2	4	1	1	2	1	4	2	2	3	1	4	2
7	1	1	2	1	1	2	6	2	2	1	1	2	1	6	2	4
8	1	1	1	2	1	1	6	4	3	1	1	2	3	6	2	8
9	1	1	2	2	2	2	2	4	6	2	2	4	4	2	4	4
11	1	1	1	1	4	1	2	2	1	4	10	2	1	2	4	2
13	1	1	2	2	1	2	3	2	2	1	1	4	12	3	2	2
16	1	1	2	2	4	2	2	4	2	4	2	4	4	2	8	8
17	1	1	1	2	1	1	1	4	3	1	1	2	2	1	2	8
19	1	1	2	1	2	2	1	2	6	2	1	2	1	1	4	2
23	1	1	1	1	1	1	2	2	1	1	10	2	2	2	2	4
25	1	1	2	2	4	2	2	4	2	4	2	4	6	2	8	4
27	1	1	2	1	1	2	3	2	6	1	2	2	12	3	2	2
29	1	1	1	2	2	1	6	2	1	2	1	2	4	6	4	2