Recall that if $f \in \mathbb{Z}_p[x]$ is an irreducible polynomial of degree $n$, then $\mathbb{Z}_p[x]/(f(x)) =: L$ gives a field with $p^n$ elements. This will still be the easiest way to construct them, but thinking a priori in terms of splitting fields gives a much more powerful result:

**I.H.1. Theorem.** Given $n \in \mathbb{N}$ and $p$ prime, (i) there exists a field $L$ with $|L| = p^n$, and (ii) this is unique up to isomorphism.

**Proof.** (i) Let $f := x^{p^n} - x$ and $L$ be a SFE/$\mathbb{Z}_p$. Since $f' = -1$, $\gcd(f, f') = 1$ and $f$ has $p^n$ distinct roots in $L$ by I.E.3. Since the Frobenius map $\phi$ is a homomorphism, the set $R_f = \{ \alpha \in L \mid \phi^n(\alpha) = \alpha \}$ of these roots is actually a subfield of $L$. As it contains all the roots, $R_f / \mathbb{Z}_p$ is itself a SFE for $f$, whence $R_f = L$.

(ii) Let $K$ be another such field. Then $|K^*| = p^n - 1$, and so for every $k \in K^*$, we have $k^{p^n-1} = 1$ hence $k^{p^n} = k$. Thus $f$ has $p^n$ distinct roots in $K$, and is a splitting field for $f$ over $\mathbb{Z}_p$. So $K \cong L$. □

It is worth pausing to remember here that, since a finite field is a vector space over its prime subfield (which is some $\mathbb{Z}_p$), it must have order a power of $p$. The standard notation is to write $\mathbb{F}_q$, or “GF($q$)” for “Galois”, for the finite field of order $q = p^n$. Note that instead of the “huge” polynomial $x^q - x$ in the above proof, we can take any irreducible $f \in \mathbb{Z}_p[x]$ of degree $n$; and by virtue of having degree $n$ over $\mathbb{Z}_p$, $L := \mathbb{Z}_p[x]/(f(x))$ must be isomorphic to $\mathbb{F}_q$ by I.H.1(ii).

So in a way we have classified (and suggested how to construct) all finite fields, though we have yet to elucidate their structure.

**I.H.2. Corollary.** All extensions of finite fields are Galois.

**Proof.** Given $|L| < \infty$, with char($L$) = $p$ and prime subfield $\mathbb{Z}_p$, the extension $L/\mathbb{Z}_p$ is separable because $\mathbb{Z}_p$ is perfect. It is normal (by I.G.4) because the subgroup $\langle \phi \rangle \leq \text{Aut}(L)$ generated by Frobenius is $\mathbb{Z}_p$ (cf. I.E.9-I.E.10). Finally, top-to-intermediate subextensions in a Galois extension are always Galois (see the proof of I.G.22(i)). □
Now recall that for $|L| = p^n < \infty$, $L^*$ is cyclic ($\cong \mathbb{Z}_{p^n - 1}$), with
generator $a$. If $L/K$ is an extension, it follows at once that $K^*$ ($\leq L^*$) and
(the quotient group) $L^*/K^*$ are cyclic, and that $L = K(\alpha)$. (That
is, any extension of finite fields is simple.) We can use this to prove

I.H.3. Theorem. Aut$(L/\mathbb{Z}_p) = \langle \phi \rangle \cong \mathbb{Z}_n$.

Proof. Clearly $L = \mathbb{Z}_p(\alpha)$, and every $\phi^k \in$ Aut$(L/\mathbb{Z}_p)$. If $\phi^k =$
id$_L$, then $\phi^k(\alpha) = \alpha \implies \phi^k(\alpha^d) = \alpha^d$ (\forall $d$) $\implies$ every $\ell \in L$ is a
root of $f = x^p - x \implies |L| \leq p^k \implies k \geq n$. We also know that $\phi^n = \text{id}_L$; and so $1, \phi, \ldots, \phi^{n-1}$ are distinct. But since $L/\mathbb{Z}_p$ is Galois,
there are exactly $|L: \mathbb{Z}_p| = n$ automorphisms. \qed

I.H.4. Corollary. Given an extension $L/K$, with $|L| < \infty$, we have
Aut$(L/K) = \langle \phi^{[L:K]} \rangle \cong \mathbb{Z}_{[L:K]}$. (In particular, any extension of finite
fields has cyclic Galois group.)

Proof. Aut$(L/K)$ is a subgroup of the cyclic group Aut$(L/\mathbb{Z}_p) =$
$\langle \phi \rangle \cong \mathbb{Z}_{[L:Z_p]}$, and $|\text{Aut}(L/K)| = [L:K]$ by the Galois correspondence (cf. I.G.6). \qed

I.H.5. Corollary. Every intermediate field in $\mathbb{F}_{p^n}/\mathbb{Z}_p$ has order $p^m$
for some $m|n$; and there is exactly one intermediate field of each of these
orders.

Proof. Given $K \subseteq \mathbb{F}_{p^n}$, applying the Tower Law gives $m =$
$[K: \mathbb{Z}_p][\mathbb{F}_{p^n}: \mathbb{Z}_p] = n$, and $|K| = p^m$.
The Galois correspondence gives $\text{Aut}(\mathbb{F}_{p^n}/K) = n/m$. There is
only one subgroup of Aut$(\mathbb{F}_{p^n}/\mathbb{Z}_p) \cong \mathbb{Z}_n$ of this order; since it is
unique, so is $K$. \qed

Since we get explicit constructions of larger finite fields from irre-
ducible polynomials over smaller ones,\footnote{These explicit realizations are used, among other places, in the construction of
error-correcting codes and in cryptography, since it is easy for computers to work
modulo a polynomial.} it seems interesting to try
to count these irreducible polynomials (especially over $\mathbb{Z}_p$). That
there must exist irreducible polynomials of every degree over every finite field is clear: just take the extension $\mathbb{F}_{q^d}/\mathbb{F}_q$ guaranteed by I.H.5 ($q = p^m$, $n = md$), which is cyclic with generator $\alpha$, whence $m_\alpha \in \mathbb{F}_q[x]$ is irreducible of degree $d$. So at least we know we are not counting the empty set.

We shall begin with some properties of the Möbius function

$$\mu : \mathbb{Z}_{>0} \to \{-1, 0, 1\},$$

which is defined by:

- $\mu(1) = 1$;
- $\mu(a) = 0 \iff a$ is not squarefree; and otherwise
- $\mu(p_1 \cdots p_n) = (-1)^n$ (where $p_1, \ldots, p_n$ are distinct).

Clearly, $\mu$ is multiplicative in the sense that

- $\mu(a_1a_2) = \mu(a_1)\mu(a_2)$ if $\gcd(a_1, a_2) = 1$.

Moreover, for any $b \in \mathbb{Z}_{>1}$ it satisfies

- $\sum_{d | b} \mu(d) = 0$,

since writing $b = p_1^{r_1} \cdots p_s^{r_s}$ with $p_1, \ldots, p_s$ distinct, we have

$$\sum_{d | b} \mu(d) = \sum_{d | p_1 \cdots p_s} \mu(d) = \sum_{i=1}^{s} \binom{s}{i} (-1)^i = (1 - 1)^s = 0.$$

The following result is very useful in number theory and combinatorics; here it is the key to the counting formula I.H.7 that follows.

**I.H.6. Lemma** (Möbius inversion formula). Given a ring $R$ and a function $f : \mathbb{Z}_{>0} \to R$, set $g(n) := \sum_{d | n} f(d)$; then we may recover $f$ by $f(n) = \sum_{d | n} \mu\left(\frac{n}{d}\right) g(d)$.

**Proof.** First observe that for $e \leq n$ dividing $n$,

$$\sum_{d | n \text{ such that } e | d} \mu\left(\frac{n}{d}\right) = \sum_{a | \frac{n}{e}} \mu(a) = \begin{cases} 1, & e = n \\ 0, & e < n. \end{cases}$$

since $e \mid d \mid n \implies \frac{n}{d} \mid \frac{n}{e}$. It follows that

$$\sum_{d | n} \mu\left(\frac{n}{d}\right) g(d) = \sum_{d | n} \mu\left(\frac{n}{d}\right) \sum_{d \mid e} f(e) = \sum_{e | n} f(e) \sum_{d | n \text{ such that } e \mid d} \mu\left(\frac{e}{d}\right) = f(n),$$

$$0 \implies e \mid d \mid n \implies \frac{n}{d} \mid \frac{n}{e}.$$
as desired. □

I.H.7. THEOREM (Gauss). The number $N(d, q)$ of monic irreducible polynomials of degree $d$ in $\mathbb{F}_q[x]$, where $q = p^m$, is given by

$$N(d, q) = \frac{1}{d} \sum_{e|d} \mu\left(\frac{d}{e}\right) q^e.$$ 

PROOF. Write $K = \mathbb{F}_q$ and let $L/K$ be an extension of degree $d$; then (by the proof of I.H.1, since $|L| = q^d$) it is also a SFE for $f = x^{q^d} - x \in K[x]$, with $L \cong \mathbb{F}_{p^{md}}$. Clearly $f$ has no multiple roots (because $R_f = L$ or $f' = -1$, take your pick), and thus no repeated factors in $K[x]$. I claim that the monic irreducible factors of $f$ in $K[x]$ are precisely the monic irreducible polynomials in $K[x]$ of degrees dividing $d$. If this is true, then the degree of $f$ equals the sum of degrees of these polynomials: $q^d = \sum_{\delta|d} N(\delta, q) \delta$. Möbius inversion gives

$$N(d, q) = \frac{1}{d} \sum_{e|d} \mu\left(\frac{d}{e}\right) q^e.$$ 

To prove the claim, let $g \mid f$ be a monic irreducible factor in $K[x]$, with $\deg(g) =: \delta$, and $\alpha \in L$ a root of $g$; then $[K(\alpha):K] = \delta$ hence $\delta \mid d$. Conversely, if $g \in K[x]$ is a monic irreducible polynomial of degree $\delta \mid d$, the field $K' := K[x]/(g(x))$ has order $|K'| = q^{[K':K]} = q^\delta$, hence is $\cong \mathbb{F}_{p^\delta}$. So I.H.5 gives an embedding $\iota: K' \hookrightarrow L$, and writing $\iota(\bar{x}) =: \alpha \in L$, we have $m_\alpha = g \in K[x]$. Since $\alpha \in L$, the proof of I.H.1 gives $f(\alpha) = 0$; and so $m_\alpha$ (hence $g$) divides $f$. □

We know that $N(d, q)$ is always positive from the existence argument (for irreducible polynomials) above; if so moved, you could try to check this from the formula too. To conclude here are a few light computations.

I.H.8. COROLLARY. The number of irreducible monic polynomials of degree $d$ in $\mathbb{Z}_p[x]$ is $N(d, p) = \frac{1}{d} \sum_{e|d} \mu\left(\frac{d}{e}\right) p^e$. In particular, there are $\frac{1}{2} p(p-1)$ irreducible quadratics, and $\frac{1}{3} p(p-1)(p+1)$ irreducible cubics.

I.H.9. EXAMPLE. How many irreducible monic polynomials of degree 8 are there over $\mathbb{Z}_2$? Since $\mu$ is 0 on all divisors of 8 except 1 and 2, we get $\frac{1}{8} (2^8 - 2^4) = 30$. So you have that many options
for constructing $\mathbb{F}_{2^8}$, which is used in AES (Advanced Encryption Standard).

I.H.10. Example. What can we say about the polynomial $g = x^p - x - 1 \in \mathbb{Z}_p[x]$? It has no roots in $\mathbb{Z}_p$, since $g(a) = -1$ ($\forall a \in \mathbb{Z}_p$). Let $L/\mathbb{Z}_p$ be a splitting field, and $\alpha \in L$ a root. Then for $b \in \mathbb{Z}_p$, we have

$$(\alpha + b)^p - (\alpha + b) - 1 = \alpha^p + b - \alpha - b - 1 = 0,$$

making $\alpha, \alpha + 1, \ldots, \alpha + p - 1$ all roots, and $L = \mathbb{Z}_p(\alpha)$.

Now suppose $g$ factors in $\mathbb{Z}_p[x]$, viz. $g = g_1g_2$. Then there is a subset $S \subset \mathbb{Z}_p$ such that $g_1 = \prod_{b \in S}(x - \alpha - b)$, and the coefficient of $x^{|S|-1}$ in $g_1$, which must belong to $\mathbb{Z}_p$, is $\sum_{b \in S}(\alpha + b) = -|S|\alpha + \{\text{element of } \mathbb{Z}_p\}$. This yields a contradiction unless $|S| = 0$ or $p$, in which case $g_1$ or $g_2$ has degree 0.

So $g$ is irreducible, and we conclude that $[L:\mathbb{Z}_p] = \deg(g) = p$, so that $\mathbb{Z}_p[x]/(g(x))$ gives an explicit construction of $\mathbb{F}_{p^p}$. We should add here that since $g$ is separable, $L/\mathbb{Z}_p$ is Galois, and $\text{Gal}_{\mathbb{Z}_p}(g) \cong \mathbb{Z}_p$ (the only group of order $p$ acting transitively on the roots).

Incidentally, the same argument applies to $x^p - x - a$ for each $a \in \mathbb{Z}_p^*$. But we have only scratched the surface of the irreducible polynomials of degree $p$ over $\mathbb{Z}_p$ — there are $N(p,p) = p^{p-1} - 1$ of them, out of $p^p(p - 1)$ total polynomials of that degree.