Вкратце вывод формулы для числа неприводимых многочленов степени n над F[q] (индексы, в том числе суммирования и произведения, я пишу в []) выглядит так.

Для удобства рассматриваем приведенные (старший коэффициент – нейтральный мультипликативный элемент поля) многочлены. Пусть:

f[i, j] – j-ый неприводимый многочлен i-ой степени

S[i, j] = { f[i, j]^k | k >= 0} (^-операция возведения в степень)

I[n] – число неприводимых многочленов степени n

S – множество всех многочленов

Тогда:

S[1, 1] * S[1, 2] * ... * S[1, I[1]] * S[2, 1] * ... * S[2, I[2]] * ... **=** S

(«прямое произведение» множеств полиномов состоит из полиномов, полученных произведением элементов сомножителей).

Теорема: пусть A, B – множества полиномов, тогда

fi[A * B] = fi[A] * fi[B]

где fi[M] – нумератор множества полиномов M, то есть такой ФСР, коэффициент при i-ой степени которого равен количеству полиномов i-ой степени во множестве M.

Таким образом:

fi[S[1, 1]] * fi[S[1, 2]] * ... * fi[S[1, I[1]]] * fi[S[2, 1]] * ... * fi[S[2, I[2]]] * ... **=** fi[S]

Дальше применяя формулу для всех полиномов данной степени над полем и определения S[i, j] и нумератора, а также соотношения для ФСР сорта:

1 + z + z^2 + z^3 + ... = 1 / (1 – z)

имеем:

П[k >= 1] 1 / ((1 – z^k)^I[k]) **=** 1 / (1 – q*z)

Для обратных величин:

П[k >= 1] (1 – z^k)^I[k] **=** (1 – q*z)

Далее логарифмическая производная от обеих частей (лог. производная от f это выражение f' / f; лог. производная произведения равна сумме лог. производных) и еще пара применений формул для ФСР наподобие той, что уже использована выше (напоминающая сумму геометрической прогрессии), в обеих частях равенства – это позволит получить два ФСР (в одной части нужно будет сперва поменять местами два знака суммирования). Приравняв коэффициенты полученных ФСР и применив формулу обращения Дирихле-Мебиуса, получим необходимое.