The number of irreducible polynomials, Lemma 1

- Apply method of generating functions to find numbers of irreducible polynomials over the field $\mathbb{Z}_p$.

- The number of irreducible polynomials of degree n with coefficient of the highest degree equal to one denoted as *P(n)*.
- **Lemma 1**

  For sequence *P(n)* the following recurrent equation exists

$$p^n = \sum_{m|n} m\,P(m) \qquad (13)$$

Proof of Lemma 1 (1/3)

- Assume $p_{1m}, p_{2m}, \cdots, p_{P(m)m}$ all of the irreducible polynomials with degree equal to m.
- Opening brackets in the product

$$\prod_{m=1}^{\infty} \prod_{k=1}^{P(m)} \left(1 + p_{km} + (p_{km})^2 + \cdots + (p_{km})^l + \cdots\right) \tag{14}$$

we get the sum of all possible products of the irreducible polynomials. Each of the products will be in this sum only once.

- As each polynomial uniquely decomposed into product of the irreducible polynomials, the sum will contain p^n products of degree n.

Proof of Lemma 1 (2/3)

- Each irreducible polynomial of degree m is associated with x^m and product (14) is associated with

$$\prod_{m=1}^{\infty}\prod_{k=1}^{P(m)}\left(1 + x^m + (x^m)^2 + \cdots + (x^m)^l + \cdots\right) = \prod_{m=1}^{\infty}\left(\frac{1}{1-x^m}\right)^{P(m)} \qquad (15)$$

- As there are p^n polynomials of degree n in which coefficient of x^n is equal to 1, it can be seen that after disclosure of x^n brackets in (15) coefficient of x^n will be equal to p^n.
- Hence $$\frac{1}{1-px} = \prod_{m=1}^{\infty}\left(\frac{1}{1-x^m}\right)^{P(m)} \qquad (16)$$
- Logarithm the left and the right side of (16)

Proof of Lemma 1 (3/3)

$$\ln \frac{1}{1-px} = \sum_{m=1}^{\infty} P(m) \ln \frac{1}{1-x^m}$$

- Apply the formula $\ln \frac{1}{1-x} = \sum_{n=1}^{\infty} \frac{1}{n} x^n$ and decompose

the right and the left parts of the last equation

$$\sum_{n=1}^{\infty} \frac{1}{n} p^n x^n = \sum_{m=1}^{\infty} \sum_{k=1}^{\infty} \frac{1}{k} P(m) x^{km} = \sum_{n=1}^{\infty} \left(\sum_{km=n} \frac{1}{k} P(m) \right) x^n$$

- Equate the coefficients of x^n

$$\frac{1}{n} p^n = \sum_{km=n} \frac{1}{k} P(m) = \sum_{m|n} \frac{m}{n} P(m)$$

QED

Mobius function, Lemma 2

- Mobius function is

$$\mu(n) = \begin{cases} 1, & \textit{if } n = 1; \\ (-1)^k, & \textit{if n-multiplication of k prime numbers}; \\ 0, & \textit{if n divides by the square of a prime number}. \end{cases}$$

- **Lemma 2**

$$\sum_{m|n} \mu(m) = \begin{cases} 1, & if\ n = 0; \\ 0, & if\ n > 0. \end{cases} \qquad (17)$$

Proof of Lemma 2

- If n=1 then 1 is the only divider and hence $\mu(1) = 1$.
- If n>1 then $n = p_1^{q_1} \dots p_r^{q_r}$.
- It can be seen that in sum (17) only divisors without multiple multipliers should be considered.
- Hence

$$\sum_{m|n} \mu(m) = \sum_{k=0}^{r} \sum_{1 \le i_1 < \cdots < i_k \le r} \mu\left(p_{i_1} \dots p_{i_k}\right) = \sum_{k=0}^{r} \binom{r}{k} (-1)^k = 0$$

QED

Lemma 3

- **Lemma 3**
  Functions *f(n)* and *h(n)* defined on the set of positive integers satisfy

$$f(n) = \sum_{m|n} h(m), \quad n \in \mathbb{N}$$

  if and only if

$$h(n) = \sum_{m|n} \mu\left(\frac{m}{n}\right) f(m), \quad n \in \mathbb{N}$$

Proof of Lemma 3 (1/2)

- We will show that from (18) follows (19).
- Note that $$\sum_{m|n} \mu\left(\frac{n}{m}\right) = \sum_{m|n} \mu(m) f\left(\frac{n}{m}\right),$$

  as sums from the both parts of the equation only differ by the order of the terms.

- Instead of *f(m)* substitute the right part of equation (18) into the right part of the last equation.
- Changing the order of summation and using *lemma 2* we will get

Proof of Lemma 3 (2/2)

$$\sum_{m|n} \mu(m) f\left(\frac{n}{m}\right) = \sum_{m|n} \mu(m) \sum_{k|\frac{n}{m}} h(k) =$$

$$= \sum_{m|n} \sum_{k|\frac{n}{m}} \mu(m) h(k) = \sum_{km|n} \mu(m) h(k) =$$

$$= \sum_{k|n} \sum_{m|\frac{n}{k}} \mu(m) h(k) = \sum_{k|n} h(k) \sum_{m|\frac{n}{k}} \mu(m) = h(n)$$

- The converse assertion proved similarly.

QED

Theorem 2

Theorem 2

- *P(n)* – number of irreducible polynomial of degree *n*

$$P(n) = \frac{1}{n}\sum_{m|n} \mu\left(\frac{n}{m}\right) p^m$$

Proof

- From lemma 1 follows that equation (18) from lemma 3 exists if $f(n) = p^n$ and $h(n) = nP(n)$ for all natural n.
- Hence assertion of the theorem follows from lemma 3.

QED