тогда: $K[x]/\langle p(x)\rangle = K[x]/\ker\varphi \cong \mathrm{Im}\,\varphi \leq L$

обозначим $I = \langle p(x)\rangle = \ker\varphi$

ун-ся $K[x]/I \Rightarrow$ поле!

Все элементы поля кроме $\forall 4$ в $K[x]/I$

Проверим $\forall 4$:

$$\tilde{f} \neq \tilde{0} \Rightarrow \exists \left(\tilde{f}\right)^{-1} \mid \tilde{f}\left(\tilde{f}\right)^{-1} = \tilde{1}$$

Т.к. $\tilde{f} \neq \tilde{0} \Rightarrow f \notin I \Rightarrow p \nmid f$, т.к.

p-неразложимый $\Rightarrow p \perp f$, $\Rightarrow \exists$ u и $v \in K[x]$)

$$f\cdot u + p\cdot v = 1$$

Отсюда: $\tilde{r} = \widetilde{fu+pv} = \tilde{f}\cdot\tilde{u} + \tilde{p}\cdot\tilde{v} =$

$$= \tilde{f}\cdot\tilde{u} + \tilde{0}\cdot\tilde{v} = \tilde{f}\cdot\tilde{u}$$

$$\Rightarrow \tilde{u} = \left(\tilde{f}\right)^{-1}$$

Следовательно $\Rightarrow \mathrm{Im}\,\varphi$ - подполе в L

$\mathrm{Im}\,\varphi \supset K, \alpha$

$a_0 + 0\cdot x \xrightarrow{\varphi} a_0 \in \mathrm{Im}\,\varphi$

$x \xrightarrow{\varphi} \alpha \in \mathrm{Im}\,\varphi$

$p(\alpha) = 0$

В силу мин. $\mathrm{Im}\,\varphi = L$

$L \simeq K[x]/\langle p(x)\rangle$ - ф-ло доказано.

ВСТАВКА - ЖЁЛТАЯ

два теорема:

Поле F_{p^n} совп с мн-ом кор мн-на $x^{p^n}-x$ над $\mathbb{Z}_p$

Этот мн-н не имеет кр. корней

$$x^{p^n}-x \perp \left(x^{p^n}-x\right)' = -1$$

Поэтому $x^{p^n}-x$ - пр-ие различных нормир. неразл. над $\mathbb{Z}_p$ - мн-ов

Пусть $P_d(x)$ - пр-ие всех неразложимых, нормированных делителей для $x^{p^n}-x$, имеющих ст d

По теор. Кронек. можно утв, что

$$F_{p^d} \leq F_{p^n} \Leftrightarrow \exists \text{ мн-н } P_d(x) \mid x^{p^n}-x \text{ и ст } P_d(x) = d$$

$\Updownarrow$

$d \mid n$

В итоге:

$$x^{p^n}-x = \prod_{d\mid n} P_d(x) \qquad (*)$$

$P_d(x)$ - пр-ие всех нормир. неразл. над $\mathbb{Z}_p$ мн-в ст d, его ст, ст $P_d(x) = d\cdot N_d$

Сравним ст. в (*)

$$p^n = \sum d\cdot N_d$$

применим ф-лу обращ. Мёбиуса для ф-ии $f(d) = d\cdot N_d$ $\Rightarrow$

$$f(n) = \sum_{d\mid n} \mu\left(\frac{n}{d}\right) p^d$$

$\|$

$n\cdot N_n$

$$N_n = \frac{1}{n}\sum_{d\mid n} \mu\left(\frac{n}{d}\right) p^d$$

теорема р-ка

ПРИМЕР: Кол-во неразложимых, нормир. мн-ов ст 3 над $\mathbb{Z}_2$:

$$N_2 = \frac{1}{3}\left(\mu(3)\cdot 2 + \mu(1)\cdot 2^3\right) =$$

$$= \frac{1}{3}\left(-2+2^3\right) = 2 \qquad \left\{ \begin{matrix} x^3+x+1 \\ x^3+x^2+1 \end{matrix} \right\} \text{ дают поле пор. 8.}$$

$N_8 = 30$

ЗАКОН ВЗАИМНОСТИ ГАУССА

Опр: Число $a \in \mathbb{Z}$ наз-ся кв. вычетом по модулю n если разрешимо ур-ие

$$x^2 \equiv a \pmod n$$

(иначе) или a не вычет,

Пример: $n = 7$

x	0	1	2	3	4	5	6
x^2	0	1	4	2	2	4	1

кв. вычеты 0 1 2 4
невычеты 3 5 6

Предложение: $\exists$ p-некот прост. число, тогда число неприв. кв. вычетов по модулю p совп с числом невычетов

доказ-во: Рассмотрим:

$$\varphi : \mathbb{Z}_p^* \to \mathbb{Z}_p^* \quad \text{по пр} \quad \varphi(x) = x^2$$

Тогда φ - гомоморф гр.

$$\varphi(x \cdot y) = (xy)^2 = x^2 y^2 = \varphi(x)\varphi(y)$$

Найдем ядро гомоморф.

$$\operatorname{Ker}\varphi = \{ x \in \mathbb{Z}_p^* \mid x^2 = 1 \} = \{ 1, -1 \mid -1 \neq 1 \text{ т.к. } p\text{-некот} \}$$

в частности 'порядок' $\operatorname{Ker}\varphi = 2$

$\exists$ $C = \operatorname{Im}\varphi = \{ x^2 / x^2 \neq 0 \} \Rightarrow$

$$|C| = |\operatorname{Im}\varphi| = \left| \mathbb{Z}_p^* / \operatorname{Ker}\varphi \right| = \text{число смежных классов}$$

$$= \frac{|\mathbb{Z}_p^*|}{|\operatorname{Ker}\varphi|} \text{ (т. Лагранжа)} = \frac{p-1}{2}$$

порядок $\mathbb{Z}_p^* - |C| = \frac{p-1}{2}$

ч. т. д.

СИМВОЛ ЛЕЖАНДРА

Опр: $\exists$ p - прост, a - целое

Символ Леж $\left(\frac{a}{p}\right)$ а по пр p задается правилом

$$\left(\frac{a}{p}\right) \in \mathbb{Z} \begin{cases} 1, & \text{если } a \text{ - кв выч (по } p) \\ -1, & \text{если } a \text{ - не вычет} \\ 0, & \text{если } (p \mid a) \end{cases}$$

Предложение: формула Эйлера

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p, \text{ где } p \text{ - нечёт.}$$

доказательство: Если $p \mid a$, то. утв очевидно

пусть $p \nmid a$, рассм. утв след отобр

$$\varphi : \mathbb{Z}_p^* \to \mathbb{Z}_p^*$$

$$\varphi(a) = a^{\frac{p-1}{2}}, \quad \varphi \text{ - гомом. гр.}$$

$$\varphi(a_1 a_2) = (a_1 a_2)^{\frac{p-1}{2}} = a_1^{\frac{p-1}{2}} \cdot a_2^{\frac{p-1}{2}} = \varphi(a_1)\varphi(a_2)$$

Если $a \in C$, т.е. a - кв вычет по $\bmod p$ то

$$a \equiv x^2 \pmod p$$

$$a^{\frac{p-1}{2}} = x^{p-1} \pmod p = x^{p-1} \equiv 1 \pmod p$$

по малой Ферма

т.о. ук. ей, что $C \subseteq \operatorname{Ker}\varphi \Rightarrow C \subseteq \operatorname{Ker}\varphi$

Найдем $\operatorname{Im}\varphi$ и его порядок

Если

$$a^{\frac{p-1}{2}} \in \operatorname{Im}\varphi \Rightarrow \left(a^{\frac{p-1}{2}}\right)^2 \equiv 1 \pmod p \Rightarrow$$

$$\Rightarrow a^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$$

Если $\mathbb{Z}_p^* = \langle g \rangle$ $g^{p-1} = 1$ $g^k \neq 1$ $0 < k < p-1$

то $g^{\frac{p-1}{2}} \neq 1$ т.к. $\frac{p-1}{2} < p-1$

След:

$$g^{\frac{p-1}{2}} = -1$$

$$\operatorname{Im}\varphi = \{1, -1\}, \quad |\operatorname{Im}\varphi| = 2$$

$$|\operatorname{Ker}\varphi| = \frac{|\mathbb{Z}_p^*|}{|\operatorname{Im}\varphi|} \Rightarrow = \frac{p-1}{2} \Rightarrow C = \operatorname{Im}\varphi$$

В итоге:

$$a^{\frac{p-1}{2}} \equiv 1 \pmod p \Leftrightarrow a \in C \Leftrightarrow \left(\frac{a}{p}\right) = 1$$

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod p \qquad a \neq 0$$

ч. т. д.

следствие 1) Символ Лежандра мультипл.

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)$$

Д-во:

$$\left(\frac{ab}{p}\right) = (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

2) Если $a = \pm 1 \cdot 2^{k_0} p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}$

где p_i - прост.

$$\left(\frac{a}{p}\right) = \left(\frac{\pm 1}{p}\right)\left(\frac{2}{p}\right)^{k_0} \prod_i \left(\frac{p_i}{p}\right)^{k_i}$$

3) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1 \Leftrightarrow p = 4k+1$

ТЕОРЕМА (Гаусса) для разл. нечётных прост. чисел p и q верно:

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{q}{p}\right)$$

следствие:

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \Leftrightarrow \left\{ p \text{ или } q \underset{4k+1}{\text{имеют вид}} \right\}$$

Пример:

$$\left(\frac{7}{13}\right) = \left(\frac{13}{7}\right) = \left(\frac{6}{7}\right) = \left(\frac{2}{7}\right)\left(\frac{3}{7}\right) = \left(\frac{2}{7}\right)(-1)\left(\frac{1}{3}\right) =$$

$$= -\left(\frac{2}{7}\right)\left(\frac{1}{3}\right) = -1\cdot 1\cdot 1 = (-1)$$

Итак $x^2 \equiv 7 \pmod{13}$ неразрешимо.