Семинар 1

17 50 — начало семинара в четверг

1(а) $X \in \mathbb{F}_p^*$

$X_0 \in \mathbb{F}_p^*$, X_0 — невычет

$\frac{X}{X_0}$ $\quad \mathbb{Z}/p\mathbb{Z}/\{0\}$

$x^2 = a$

1 б) $p = 17$

$2, 2, \dots, 16$

$1^2, 2^2, \dots, 8^2$

$1, 4, 9, 16, 8, 2, 15, 13$

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

R R N R N N N R R N N N R N R R

$64 = 17 \cdot 3 + 13$

2(а) RR-3 | RN-4 | NR-4 | NN-4

2(б) $\frac{1}{4}\sum_{i=1}^{p-2}\left(1+\left(\frac{i}{p}\right)\right)\left(1+\left(\frac{i+1}{p}\right)\right)$

кол-во RR в слове W_p

$\frac{1}{4}\sum_{i=1}^{p-2}\left(1-\left(\frac{i}{p}\right)\right)\left(1-\left(\frac{i+1}{p}\right)\right)$ — кол-во NN

$\sum\left(1+\left(\frac{i}{p}\right)+\left(\frac{i+1}{p}\right)+\left(\frac{i(i+1)}{p}\right)\right)$

$p-2+\left(\frac{-1}{p}\right)+1+$

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

$\frac{p-1}{2} = 2k$

$p = 4k+1$

5б

$p = a^2+b^2 = c^2+d^2$?

p — простое

$p = a^2+b^2 = (a+bi)(a-bi)$

✓ простые в $\mathbb{Z}[i]$ — ОТА

(факториальность)

$|a+ib|^2 = p^2$

$|(a+\beta i)(\gamma+\delta i)| = p$

6 $p = a^2+b^2 \Rightarrow -1 = x^2$ в $\mathbb{Z}_p[i]$

$-b^2 = a^2$

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

в $\mathbb{Z}_p[i]$ $\quad p = \frac{1+a^2}{k}$

$-1 = a^2$

$1 + a^2 = 0$

$p = a^2+b^2 \Leftrightarrow$ (p — НЕ простое в $\mathbb{Z}[i]$)

$p = (a+bi)(c+di)$

$p \neq a^2+b^2 \Leftarrow$ (p — простое в $\mathbb{Z}[i]$)

$\forall a, b \in \mathbb{N}$

$\Leftrightarrow \left(\frac{-1}{p}\right) = 1$ $\quad \mathbb{Z}[i]/(p) \simeq \mathbb{Z}[t]/(t^2+1)/(p) \simeq \mathbb{Z}_p[t]/(t^2+1)$

$\Leftarrow \left(\frac{-1}{p}\right) = -1$

5(а)

$x = a^2+b^2$

$y = c^2+d^2$

$xy = (a^2+b^2)(c^2+d^2) = (ac)^2+(ad)^2+(cb)^2+(bd)^2 =$

$= (ac)^2+2abcd+(bd)^2) + ((ad)^2-2abcd+(cb)^2) =$

$= (ac+bd)^2+(ad-cb)^2$

$+2abcd-2abcd$

$p = 17$ **4** $30 = 2 \cdot 3 \cdot 5 = (i+1)(i-1)\cdot(2i+1)(2i-1)\cdot 3$

Ещё один трюк:

$(X, X+1) \mapsto \left(-\frac{X}{X+1}, \frac{1}{X+1}\right)$

$RN = NN$

Трюк:

$RR + RN = \frac{p-1}{2}$ (?)

$NN + NR = \frac{p-1}{2}$ (?)

$NR = NN$ $\quad \frac{x+1}{\| \; x}$

$(x, x+1) \rightsquigarrow \left(\frac{1}{x}, \frac{1}{x}+1\right)$

N R — N N

R N — R N

N N — N R

$x^2+x-a = 0 \bmod p$

$\frac{-1 \pm \sqrt{1+4a}}{2}$

$1+4a = 2$

$a = \frac{2-1}{4}$

$x^2+x-y^2 = 0$ над $\mathbb{F}_p$

$p-1$ реш

① Введение в теорию чисел Семинар 2

№1 а

$1+\dots+1=0$ ($n=pq$), $p,q\neq 1$

$(1+\dots+1)(1+\dots+1)=0$ (p и q)

$p,q<k$: $1\cdot p=0$, $1\cdot q=0$

№1 б

$F_p=\langle 1\rangle$, $F\supset F_p$

$F=\langle e_1,\dots,e_k\rangle$

$\lambda_1 e_1+\dots+\lambda_k e_k$, $\lambda_i\in F_p$

$|F|=|F_p|^k=p^k$

$F_{p^k}\supset F_{p^l}$, $|F_{p^k}|=|F_{p^l}|^m$, $p^k=(p^l)^m$, $k:l$

② №2. $\phi(x)=x^p$:

$\phi(xy)=x^p y^p=\phi(x)\phi(y)$

$\phi(x+y)=\sum_{t=0}^{p}\binom{p}{t}x^t y^{p-t}=x^p+y^p$

В $\mathbb{F}_q$ ($q=p^k$) $\phi^k=id$ по МТФ

$|\mathbb{F}_q^*|=q-1=p^k-1\Rightarrow\forall x: x^q=x$

$\mathbb{F}_q\hookrightarrow\overline{\mathbb{F}_p}\hookleftarrow\mathbb{F}_{p^d}$ ← неподв. при ϕ^d, корни $x^{p^d}-x=0$

⑤ $\mathbb{F}_{p^{HOД(k,d)}}$ (т.к. состоит из корней $x^{\dots}-x=0$)

$x^{p^{nm}}-x=(x^{p^n}-x)(x^{p^{(n-1)m}}+\dots+x^{p^{(n-2)m}}+\dots+x^{p^0})$

$\mathbb{F}_{p^n}\subset\mathbb{F}_{p^{nm}}$

$(x^{p^{mn}-1}-1)=(x^{p^n-1}-1)$

$p^{mn}-1:p^n-1$

③ $a\in R$: $0,a,\dots,0_n a$

$0=(0_i-0_j)a\Rightarrow i=j$

№4

а) $\mathbb{F}_2[X]/(X^2+1)$ ← $(X+1)\cdot(X+1)=0\Rightarrow$ это не поле

$X^2+1=(X+1)^2$ в $\mathbb{F}_2[X]$

X	0	1	2
X^2	0	1	1

X^2+1

б) $\mathbb{F}_3[X]/(X^2+1)$

X^2+1 неприводим в $\mathbb{F}_3[X]$, т.к. нет корней и ст.=2 $\Rightarrow$ это поле

$\mathbb{F}_3[X]=\{\alpha X+\beta\}$ $3\cdot 3=9$

в) $\mathbb{F}_3[X]/(X^2+X+1)=\mathbb{Z}[X]/(3,X^2+X+1)$

X^2+X+1 — неприв., т.к. нет корней

$\{\alpha X+\beta\}$ $2\cdot 2=4$

г) $\mathbb{Z}[i]/(2)=\mathbb{F}_2[X]/(X^2+1)$ — не поле

$\mathbb{Z}[X]/(i$

$(1+i)(1+i)=1+2i-1=2i=0$ в $\mathbb{Z}[i]/(2)$

д) $\mathbb{Z}[\sqrt{-2}]/(5)=\mathbb{Z}[X]/(5,X^2+2)=\mathbb{F}_5[X]/(X^2+2)$

	0	1	2	3	4
	2	3	4		
	1	4	4	1	

неприв. в $\mathbb{F}_5\Rightarrow$ поле из 25 эл.

е) $\mathbb{Z}[e^{\frac{2\pi i}{3}}]/(2)=\mathbb{F}_2[X]/(X^2+X+1)$ — поле из 4 эл.

$e^{\frac{2\pi i}{3}}$

$\alpha=\beta^2=(a+\sqrt{2}b)(a-\sqrt{2}b)$

$\frac{\mathbb{Z}[\sqrt{2}]}{(p)}=\frac{\mathbb{Z}[x]}{(x^2-2,p)}=\frac{\mathbb{F}_p[x]}{(x^2-2)}$

№7 $x^{p^k}-x$ $(x+y)^p=x^p+y^p$

$\mathbb{F}_p\subset\overline{\mathbb{F}_p}$

$x^{p^k}=x$ $y^{p^k}=y$ $(x+y)^{p^k}=x+y$

$\mathbb{F}_{p^k}^1$, $\mathbb{F}_{p^k}^2$ ← α — корень μ_η

$\mathbb{F}_{p^k}^{1*}=\langle\eta\rangle$, $\eta\in\mathbb{F}_p[x]/\mu_\eta(x)$

$\{x^{p^k-1}-1=0\}$

$\mu_\eta(x)$ ⇓ $\deg=k$

⑥ (а)

$-\frac{p-1}{2},\dots,-1,0,1,\dots,\frac{p-1}{2}$

$-\frac{p-1}{2}a,\dots,-a,0,a,\dots,\frac{p-1}{2}a$

$\{-1,1\}$ $a_i+a_j=0$ $(i=j)$

$\{\frac{p-1}{2},-\frac{p-1}{2}\}$ a $(-1)\cdot 1$

$p=8k+1$ $p=8k+7$ $\frac{p-1}{2}$ $\frac{p-1}{2}a$ $(-1)\frac{p-1}{2}$

$[\frac{p}{4}\,|\,\frac{p}{2}]$ $\left(\frac{p-1}{2}\right)!$ $a^{\frac{p-1}{2}}\equiv(-1)^k\left(\frac{p-1}{2}\right)!$

$a^{\frac{p-1}{2}}=(-1)^k$

(Ещё один решение Серр) $[\frac{8k+1}{4}\,|\,\frac{8k+1}{2}]$ $[2k+\frac{1}{4},4k+\frac{1}{2}]$ $2k$

$\mathbb{F}_p\subset\overline{\mathbb{F}_p}\ni\alpha$, $\alpha^8=1$, $\alpha^k\neq 1$, $k<8$

$(\alpha+\alpha^{-1})^2=\alpha^2+\alpha^{-2}+2$ $\alpha^8-1=(\alpha^4-1)(\alpha^4+1)$

$\alpha^4+1=0$ ⇐ $\alpha^2+\alpha^{-2}=0$

$(\alpha+\alpha^{-1})^{p-1}=\begin{cases}1\Rightarrow\alpha+\alpha^{-1}\in\mathbb{F}_p\Rightarrow\left(\frac{2}{p}\right)=1\\-1\Rightarrow\alpha+\alpha^{-1}\in\mathbb{F}_p\Rightarrow\left(\frac{2}{p}\right)=-1\end{cases}$

$\alpha^8=1$

$(\alpha+\alpha^{-1})^n \bmod(\alpha^4+1)$ (см. Серр)

$(\alpha+\alpha^{-1})^p\overset{?}{=}\alpha+\alpha^{-1}$

$\alpha^p+\alpha^{-p}=\alpha+\alpha^{-1}$

$p-1:8$

$p+1:8$

③ $\operatorname{ord}a=p_1$, $(p_1,p_2)=1$ / $\operatorname{ord}ab=p_1p_2$

$\operatorname{ord}b=p_2$

$(p_1,p_2)=d$ $\operatorname{ord}a^d=\frac{p_1}{d}$

$(\frac{p_1}{d},p_2)=1$ / $\operatorname{ord}a^db=HOK(p_1,p_2)$

Пусть m — эл-т с наиб. порядком $\operatorname{ord}m=s$.

$x^s-1=0$

$1,m,m^2,m^3,\dots,m^{s-1}$

① Введение в теорию чисел Семинар 3

$\overline{\chi(-1)}\,\overline{\chi(-1)} = \overline{\chi(1)} = \overline{\chi}(1) = 1$

1(a) $\chi(-1)\overline{G(\chi)} = \chi(-1)\sum \overline{\chi(a)}\eta^{a} =$

$\overline{G(\chi)} = \sum_{a\in\mathbb{F}_p^*} \chi(a)\, e^{\frac{2\pi i}{p}ja} = \sum_{a\in\mathbb{F}_p^*} \overline{\chi(a)}\, e^{-\frac{2\pi i}{p}a} = \langle a \mapsto -a\rangle$

$\overline{\chi(a)} = \overline{\chi}(a)$

$= \sum_{a\in\mathbb{F}_p^*} \overline{\chi}(-a)\, e^{\frac{2\pi i}{p}a} = \overline{\chi}(-1)\cdot \sum_{a\in\mathbb{F}_p^*} \overline{\chi}(a)\, e^{\frac{2\pi i}{p}a}$ $\quad \chi(a)\chi(-1) = \chi(-a)$

② 1(б) $G(\chi)G(\overline{\chi}) = G(\chi)\left[\chi^{-1}(-1)\,\overline{G(\chi)}\right] =$

$= \chi(-1)\, G(\chi)\overline{G(\chi)}$ т.к. $\chi(-1) = \pm 1$

$G(\chi)\overline{G(\chi)} = p$

$e^{\frac{2\pi i}{p}} =: \eta$, $\overline{\eta^{a}} = \eta^{-a}$

$\left(\sum_{a\in\mathbb{F}_p^*} \chi(a)\eta^{a}\right)\left(\sum_{a\in\mathbb{F}_p^*} \overline{\chi(a)}\,\eta^{-a}\right) = (p-1)^2 = p^2 - 2p + 1$

$\overline{\chi(a)} = \chi(a^{-1})$

$= \sum_{b\in\mathbb{F}_p^*} \chi(b)\left(\sum_{a\in\mathbb{F}_p^*} \eta^{a-ab^{-1}}\right) = (p-1)\chi(1) + \sum_{b\neq 0,1} \chi(b)\,(-1) =$

1(а)

③ 1(б) продолжение

$\eta^{(1-b^{-1})} = \zeta$

$\left(\sum_{a\in\mathbb{F}_p^*} \eta^{a-ab^{-1}}\right) = \sum_{a\in\mathbb{F}_p^*} \eta^{a-ab^{-1}} = \sum_{a\in\mathbb{F}_p^*} \eta^{a(1-b^{-1})} =$

(1) $b \neq 1 \Rightarrow \sum_{a\in\mathbb{F}_p^*} \zeta^{a} = -1$

(2) $b = 1 \Rightarrow \sum_{a\in\mathbb{F}_p^*} 1^{a} = p-1$

④ $t \to at$

$\Gamma(x) = \int_0^{+\infty} e^{-t} t^{x} \frac{dt}{t}$ (характер $\mathbb{R}^*$)

$B(x,y) = \int_0^1 t^{x}(1-t)^{y}\, dt$

$\exp: \mathbb{R} \to \mathbb{R}^{>0}$ (аддитивная группа)

$\mathbb{R} \to \mathbb{C}^* \ni a$

$t \to e^{at}$

t^{x-1} – характер

$G = S^1 \quad G^{\vee} = \mathbb{Z}$

⑤ №4 g – образующая $\mathbb{F}_p^*$

$\chi(g) = i$

$g, g^2, \dots, g^{p-1}$

$\chi(g^n) = i^n \quad \chi(g^n)^2 = (-1)^n$

$\chi(g^n) = \pm i, \pm 1 \quad \chi(g^n)^2 = \pm 1$

4(б) $J(\chi,\chi^2) = \sum_{x\in\mathbb{F}_p\setminus\{0,1\}} \chi(x)\chi^2(1-x) =$

$= \pm\underbrace{(b + \dots + i)}_{|b|} \pm \underbrace{(1 + \dots + 1)}_{|a|}$

⑥ $(p-1) - \sum_{b\neq 0,1} \chi(b) = p$ (важно, что $\chi \not\equiv 1$)

$\sum_{b\neq 0,1} \chi(b) = -1$

4(в) $\frac{J(\chi,\chi^2)}{J(\chi,\chi)} = \frac{G(\chi)G(\chi^2)}{G(\chi^3)} \Big/ \frac{G(\chi)^2}{G(\chi^3)}$

$\chi^4 = 1$ $\quad \overline{\chi} = \chi^3$

$\frac{G(\chi^2)^2}{G(\chi^3)G(\chi)} = \frac{((1,4)-(1,2))^2}{G(\chi)G(\overline{\chi})} =$

$\frac{((1,4)-(1,2))^2}{p\cdot(-1)^k} = (-1)^k$ $\quad (-1)^k \cdot p$ $\quad p = 4k+1$

$\prod_{d\mid p-1} \left(\chi^{d} - 1\right) = 0$ (требуется доказать)

(Здесь нужно точнее разобраться, сколько раз пробегается каждый корень)