28.09.2011

Короткие унитреугольные факторизации М. Всемирнов

$SL_2(\mathbb{Z}[1/p])$: безусловное доказательство

(= число шагов в алгорифме Эвклида над этим кольцом)

$UU^-UU^-U \cup U^-UU^-UU^-$

(сюда Н.А.В., А.С., Сури – с использованием гипотезы Артина)

У нас: $SL_2(\mathbb{Z}[1/p]) = UU^-UU^-U = U^-UU^-UU^-$

$(p^\alpha a, p^\beta b)$ – первая строка

$p^\alpha a - p^\beta b \boxed{p^\gamma c}$ γ может быть >0 и <0 ~ неважно, $\alpha > \beta$ или наоборот

Как избавиться от гипотезы Артина?

Heath-Brown, 1985

Гипотеза Артина: $a \in \mathbb{Z}$, $a \neq \square$

$\Rightarrow \exists$ б. много простых q таких, что a – примитивный корень $\bmod q$.

Н.В. ① $\exists$ не более трех бесквадратных a, для которых нарушается гипотеза Артина

② $\exists$ не более двух простых исключений

~ фан Н.А.В., Андрея и Сури верен для всех p, кроме двух

$(p^\alpha a, p^\beta b) \xrightarrow{(1)} (p^\beta (\underbrace{p^{\alpha-\beta}a + cb}_{q\text{ – простое}}), p^\beta b)$ $\quad q \equiv p^{\alpha-\beta}a \pmod b$

Выберем q: p – первообразный корень

~ $\exists u : p^u \equiv b \pmod q$

$\xrightarrow{(2)} (p^{\alpha+\beta}q, p^{\beta+u}) \longrightarrow (1, *) \longrightarrow (1, 0)$

(1) $(p, b) = 1 \Rightarrow p^{\varphi(b)} \equiv 1 \pmod b$

$p^{2\varphi(b)} \equiv 1 \pmod b$

$q \in$ арифм. прогр. $p^{\alpha-\beta}a + bc$

~ $p^{2\varphi(b)k}q$ – тоже ~ можно в шаге (1) еще и навесить степень p

$(p^\beta q, p^{\beta+u}) \to (p^\delta q, p^{\beta+u}\ell)$? Как нужно подобрать ℓ? – Это возможно, если $p^\delta q \equiv 1 \pmod \ell$

Пусть это будет $(p^\delta q, p^{\beta+u}\ell^\varepsilon)$, ℓ – простое, которое в качестве первообр. корня $\bmod q$ ~ $\ell^\varepsilon \equiv b \pmod q$ // и еще нужно $p^\delta q \equiv 1 \pmod{\ell^\varepsilon}$

→ сначала подбираем l, потом q, потом степень k

Выберем три достаточно больших простых l,
хотя бы для 1 из них вып. тождества Артина ⇝ находим q

Зная q и l, находим ε, потом δ такие, что $p^\delta q \equiv 1 \pmod{l^\varepsilon}$

$$(p^\alpha a,\ p^\beta b) \longrightarrow (p^\alpha a + p^{\beta+\gamma} bc,\ p^\beta b)$$

$$p^\alpha a + p^{\beta+\gamma} bc = p^{\beta+\gamma}(p^{\alpha-\beta-\gamma} a + bc)$$

$\alpha - \beta - \gamma \geq 0$

$\beta + \gamma$ – четно

$$p^{\alpha-\beta-\gamma} a + bc = p^{2\varphi(b)\cdot k} q$$

Итого $p^{\beta+\gamma+2\varphi(b)k}$. Выберем k_0 так, что

$\beta + \gamma + 2\varphi(b) k_0 > 0 = \beta_1$

$$p^{\beta_1} \cdot p^{2\varphi(b)k} q$$

l_1, l_2, l_3 – простые, $l_i \equiv 3 \pmod 4$

$l_i > p^{\beta_1} \Rightarrow p^{\beta_1} \neq 1 \pmod{l_i}$

$$\begin{cases} uq \equiv p^{-\beta_1} \pmod{l_i^{\lambda_i}} & i = 1,2,3 \\ uq \equiv 3 \pmod{16} \end{cases}$$

– такое u если по кто

Лемма $\exists\ \alpha \in (\frac14; \frac12)$, $\delta \in (0, \frac12 - \alpha)$ такие, что

$16 \mid v$, $(\frac{u-1}{2}, v) = 1$

$$\left| \{ q \leq x : q \equiv u \pmod v,\ \frac{q-1}{2} = P_2(\alpha,\delta),\ q \text{ – простое} \} \right| \geq \text{const} \cdot \frac{x}{(\log x)^2}$$

$n = P_2(\alpha,\delta)$ – либо простое,
либо $n = p_1 \cdot p_2$, где $n^\alpha \leq p_1 \leq n^{1/2-\delta}$

У нас $v = 16 l_1^{\lambda_1} l_2^{\lambda_2} l_3^{\lambda_3}$

u – см. выше

$p^{\beta_1} \neq 1 \pmod{l_i}$, $\Rightarrow \frac{u-1}{2}$ нечетно

$\Rightarrow (\frac{u-1}{2}, v) = 1$

Потом надо будет решить сравнение $p^{2\varphi(b)k} \cdot p^{\beta_1} \cdot q \equiv 1 \pmod{l_i^\varepsilon}$

$l_i^{\lambda_i} \parallel p^{2\varphi(b)(l_i-1)} - 1$

Возьмем q из множества из Лемма Н-В.

$$p^{\beta_i} q \equiv 1 \pmod{l_i}$$

Будет ли l_i вычет по mod q?

$$\left(\frac{l_i}{q}\right) = \underbrace{(-1)^{\frac{l_i-1}{2}\frac{q-1}{2}}}_{(-1)} \underbrace{\left(\frac{q}{l_i}\right)}_{\beta_i - \text{четно} \Rightarrow 1} = -1$$

Пусть $l \in \{l_1, l_2, l_3\}$

Если $\frac{q-1}{2} = t$ простое

Каков порядок l по mod q? $1, 2, t, 2t$

l - невычет $\Rightarrow$ это не $t, 1$

$1, 2$ - только для кон. числа q (при $q > l^2$ - не бывает)

$\Rightarrow$ порядок равен $2t = q-1$

Второй случай: $\frac{q-1}{2} = t_1 t_2$ $\quad (t_1 t_2)^{\alpha} \le t_1 \le (t_1 t_2)^{1/2-\delta}$

l невычет $\rightsquigarrow$ порядок l по mod q неизвестен:

$$2, 2t_1, 2t_2, 2t_1 t_2 = q-1$$

$$\left(p^{\beta_i + 2\varphi(l)k} q,\ p^{?} l_i^{\varepsilon}\right)$$

Теперь нужно найти k такое, что

$$p^{\beta_i + 2\varphi(l)k(l_i-1)} q \equiv 1 \pmod{l_i^{\varepsilon}}$$

Но $p^{\beta_i} q \equiv 1 \pmod{l^{\lambda_i}}$ $\rightarrow$ по mod l^{λ_i} - можем

$$(l_i - 1) p^{2\varphi(l)k} = \left(1 + l_i^{\lambda_i} \underbrace{z}_{(z, l_i) = 1}\right)^k$$

и по аналогу Лемма Гензеля - все

$\mathbb{Z}\left[\frac{1}{p}\right]$ $\quad K$ - кон. расширение $\mathbb{Q}$

$\mathcal{O}_K$, π - простой идеал в $\mathcal{O}_K$

$(\mathcal{O}_K)_{(\pi)}$ - длина 5 для SL_2

- по модулю аналога леммы Н.-В.

$p \equiv 3 \pmod 4$

$n = \frac{p+1}{2}$ — матрица $\left(\left(\frac{i-j}{p}\right)\right)_{i,j=0,n-1}$ — Чему равен ее det?

Ответ: $= 1$.

Читать: evil determinant

$p \equiv 1 \pmod 4$

$\rightsquigarrow \det\left(\left(\frac{i-j}{p}\right)\right) =$

размера $n-1$ — тоже 1

p	5	13	17	29	37	41
det	-2	-18	-4	-70	-882	-32

$\mathbb{Q}(\sqrt{p})$

ε

h — число классов

$$a + b\sqrt{p} = \begin{cases} \varepsilon^h \\ \varepsilon^{3h}, \end{cases} \quad \begin{matrix} p \equiv 1 \ (8) \\ p \equiv 5 \ (8) \end{matrix} \quad \rightsquigarrow \det = -a$$

— в аналогичной матрице $(n-1) \times (n-1)$

Гипотеза: $\varepsilon = \alpha + \beta\sqrt{p}$

$p \equiv 1 \ (4) \rightsquigarrow p \nmid \beta$? ответ — что-то такое в