Некоторые группы обратимых многочленов с целыми коэффициентами по модулю многочлена и степени простого числа

К. Зюбин
Томск, МАОУ СОШ № 32, 11Б, 2022

Аннотация

В настоящей статье описываются группы обратимых классов эквивалентности по модулю степени простого числа p^k и многочлена с целыми коэффициентами $P(x)$, старший коэффициент и свободный член которого не делятся на p, таких, что все элементы этих классов сравнимы с 1 по модулю p и $P(x)$.

1 Введение

В системе шифрования с открытым ключом MMMC1, предложенной С. К. Росошеком, для создания ключей шифрования используется мультипликативная группа факторкольца $\mathbb{Z}_{2^k}[x]/\langle x^2-1\rangle$, которая исследовалась в работе [2]. Естественно возникает вопрос об изучении мультипликативных групп факторколец $\mathbb{Z}_{p^k}[x]/\langle P(x)\rangle$ для произвольных многочленов $P(x)$ и простых p.

Будем говорить, что многочлены $A(x)$ и $B(x)$ с целыми коэффициентами сравнимы по модулю числа q и многочлена $P(x)$ с целыми коэффициентами, если существуют такие многочлены $U(x)$ и $V(x)$ с целыми коэффициентами, что

$$A(x) - B(x) = P(x)U(x) + qV(x).$$

Будем обозначать это как $A(x) \equiv B(x) \pmod{q, P}$. Формально, $A(x)$ и $B(x)$ сравнимы по модулю числа q и многочлена $P(x)$, если они принадлежат одному классу эквивалентности факторкольца $\mathbb{Z}[x]/\langle q, P\rangle$ кольца многочленов $\mathbb{Z}[x]$ по идеалу, порождённому числом q и многочленом $P(x)$.

Будем говорить, что многочлен $A(x)$ с целыми коэффициентами обратим по модулю числа q и многочлена $P(x)$ с целыми коэффициентами, если существует такой многочлен $B(x)$, что

$$A(x)B(x) \equiv 1 \pmod{q, P}.$$

Рассмотрим классы эквивалентности многочленов по модулю числа q и многочлена $P(x)$. Обозначим класс эквивалентности, содержащий многочлен $A(x)$ через $[A(x)]_{q,P}$. Над классами эквивалентности можно совершать операции сложения и умножения, аналогично сложению и умножению по модулю целого числа.

Если один многочлен из класса эквивалентности обратим, то остальные многочлен этого класса тоже обратимы. Назовём класс эквивалентности, все элементы которого обратимы, обратимым классом эквивалентности. Такие классы эквивалентности образуют группу по умножению, которую мы обозначим через $G_q(P(x))$.

Будем рассматривать такие группы для $q = p^k$, где p — простое. Обозначим через $H_{p,k}(P(x))$ множество обратимых классов эквивалентности по модулю p^k и $P(x)$ таких, что все элементы этих классов сравнимы с 1 по модулю p и $P(x)$. Множество $H_{p,k}(P(x))$ образует подгруппу группы $G_{p^k}(P(x))$.

Будем говорить, что группа G порождается некоторым подмножеством её элементов M, если каждый элемент G можно представить в виде произведения степеней элементов из M.

Основные результаты работы сформулированы в следующих двух теоремах.

Теорема 1. *Пусть p — простое число, k — натуральное число, $P(x)$ — многочлен с целыми коэффициентами, t — наибольшая степень x, при которой коэффициент в многочлене $P(x)$ не делится на p. Тогда существует многочлен с целыми коэффициентами $T(x)$ степени t такой, что его старший коэффициент не делится на p, группы $G_{p^k}(P(x))$ и $G_{p^k}(T(x))$ совпадают, их подгруппы $H_{p^k}(P(x))$ и $H_{p^k}(T(x))$ также совпадают.*

Теорема 2. *Пусть $p > 2$ — простое, $k > 1$ — натуральное, $P(x)$ — многочлен с целыми коэффициентами, старший коэффициент которого не делится на p, $\deg P = n$. Тогда группа $H_{p,k}(P(x))$ изоморфна $(\mathbb{Z}_{p^{k-1}})^n$ и порождается в точности множеством элементов вида $[1+px^s]_{p^k,P}$ для целых $0 \leqslant s \leqslant n-1$.*

2 Вспомогательные утверждения

Обозначим через $\nu_p(n)$ степень, в которой простое число p входит в разложение числа n.

Лемма 3. *Для любых натуральных n, k и простого p справедливо*

$$\nu_p(n) + \nu_p(C_{p^k}^n) = k.$$

Доказательство.
По формуле биномиального коэффициента имеем:

$$\nu_p(C_{p^k}^n) = \nu_p\left(\frac{(p^k)!}{n!(p^k-n)!}\right) = \nu_p((p^k)!) - \nu_p(n!) - \nu_p((p^k-n)!).$$

Далее, по формуле степени вхождения p в факториал [1, Глава 2, §1, b]:

$$\nu_p((p^k)!) - \nu_p(n!) - \nu_p((p^k-n)!) = \sum_{i=1}^{\infty}\left(\left\lfloor\frac{p^k}{p^i}\right\rfloor - \left\lfloor\frac{n}{p^i}\right\rfloor - \left\lfloor\frac{p^k-n}{p^i}\right\rfloor\right) =$$

$$= \sum_{i=1}^{k}\left(p^{k-i} - \left\lfloor\frac{n}{p^i}\right\rfloor - \left\lfloor(p^{k-i} - \frac{n}{p^i})\right\rfloor\right) = \sum_{i=1}^{k}\left(p^{k-i} - \left\lfloor\frac{n}{p^i}\right\rfloor - p^{k-i} - \left\lfloor-\frac{n}{p^i}\right\rfloor\right) =$$

$$= \sum_{i=1}^{k}\left(-\left\lfloor\frac{n}{p^i}\right\rfloor + \left\lceil\frac{n}{p^i}\right\rceil\right) = k - \nu_p(n),$$

где последнее равенство верно, так как $\left\lceil\frac{n}{p^i}\right\rceil - \left\lfloor\frac{n}{p^i}\right\rfloor$ равно 0, если n делится на p^i, и равно 1, когда n не делится на p^i.

Таким образом, $\nu_p(C_{p^k}^n) = k - \nu_p(n)$ и утверждение леммы доказано. □

Лемма 4. *Пусть n — натуральное, p — простое. Тогда неравенство*

$$2 + \nu_p(n) \leqslant n$$

выполнено если и только если либо $p > 2$ и $n > 1$, либо $p = 2$ и $n > 2$.

Доказательство.
Докажем, что неравенство

$$2 + \nu_p(n) > n$$

выполнено тогда и только тогда, когда $n = 1$ или когда $n = 2$ и $p = 2$.

Пусть $n = 1$. Тогда $2 + \nu_p(1) = 2 > 1$.

Пусть $n = 2$ и $p = 2$. Тогда $2 + \nu_2(2) = 3 > 2$.

Пусть теперь $2+\nu_p(n) > n$ и $n = p^t s$, где s не делится на p. Тогда $n = s(1+(p-1))^t \geqslant s + st(p-1)$. Отсюда, по предположению, $s + st(p-1) < 2 + t$ или $t(sp - s - 1) < 2 - s \leqslant 1$. Тогда или $t = 0$, из чего следует, что $s < 2$ и $n = 1$, или $sp - s - 1 = 0$, откуда $s(p-1) = 1$ и $s = 1$ и $p = 2$. Далее, остаётся найти t, для которых $2^t < t + 2$. Заметим, что $2^{t-1} = (1+1)^{t-1} \geqslant 1 + (t-1) = t$. Тогда $t + 2 > 2^t \geqslant 2t$. Отсюда, $2 > t$, $t = 0$ или $t = 1$, поэтому $n = 1$ или $n = 2$. □

Лемма 5. *Пусть p — простое, $k > 1$ – натуральное, $S(x)$ — многочлен с целыми коэффициентами. Тогда*

1) если $p > 2$, то

$$(1 + pS(x))^{p^{k-2}} \equiv 1 + p^{k-1}S(x) \pmod{p^k},$$

а если $p = 2$, то

$$(1 + 2S(x))^{2^{k-2}} \equiv 1 + 2^{k-1}S(x) + 2^{k-1}x^{2s} \pmod{2^k};$$

2) для любого p выполнено

$$(1 + pS(x))^{p^{k-1}} \equiv 1 \pmod{p^k}.$$

Доказательство.
1) Распишем степень $(1+pS(x))^{p^{k-2}}$ по биному Ньютона:

$$(1+pS(x))^{p^{k-2}} = \sum_{i=0}^{p^{k-2}} C_{p^{k-2}}^{i} (pS(x))^i.$$

Оценим степень вхождения p в коэффициент при каждой степени $S(x)$:

$$\nu_p(C_{p^{k-2}}^{i} p^i) = \nu_p(C_{p^{k-2}}^{i}) + \nu_p(p^i) = \nu_p(C_{p^{k-2}}^{i}) + i.$$

Для $i > 0$ по лемме 3 имеем:

$$\nu_p(C_{p^{k-2}}^{i}) + i = k - 2 - \nu_p(i) + i.$$

В случае $p > 2$ по лемме 4 число $k-1-\nu_p(i)+i \geqslant k$ для $i > 1$, следовательно, степень вхождения p в коэффициент для $i > 1$ не меньше k. Для $i = 1$ коэффициент равен $C_{p^{k-2}}^{1} \cdot p^1 = p^{k-1}$. Следовательно,

$$(1+pS(x))^{p^{k-2}} \equiv 1 + p^{k-1} S(x) \pmod{p^k}.$$

В случае $p = 2$ по лемме 4 число $k-1-\nu_p(i)+i \geqslant k$ для $i > 2$, следовательно, степень вхождения p в коэффициент для $i > 2$ не меньше k. Для $i = 1$ и $i = 2$ найдём коэффициенты: $C_{2^{k-2}}^{1} \cdot 2^1 = 2^{k-1}$, $C_{2^{k-2}}^{2} \cdot 2^2 = \frac{2^{k-2}(2^{k-2}-1)}{2} \cdot 2^2 = 2^{k-1}(2^{k-2}-1) \equiv 2^{k-1} \pmod{2^k}$. Имеем,

$$(1+2S(x))^{2^{k-2}} \equiv 1 + 2^{k-1} S(x) + 2^{k-1} S(x)^{2s} \pmod{2^k}.$$

2) Так как $k > 1$, для любого многочлена $P(x)$ выполнено

$$(1 + p^{k-1} P(x))^p \equiv 1 + p p^{k-1} P(x) \equiv 1 \pmod{p^k}.$$

Тогда $(1+pS(x))^{p^{k-1}} \equiv ((1+pS(x))^{p^{k-2}})^p \equiv 1 \pmod{p^k}$. □

Лемма 6. *Пусть p — простое число, k — натуральное и $Q(x)$ — многочлен с целыми коэффициентами, причём все его коэффициенты, кроме свободного члена, делятся на p. Тогда существует такой многочлен с целыми коэффициентами $S(x)$, что*

$$S(x)Q(x) \equiv 1 \pmod{p^k}.$$

Доказательство.
Докажем, что многочлен $S(x) = Q(x)^{p^{k-1}(p-1)-1}$ удовлетворяет требованию теоремы.
Пусть $Q(x) = b + pxR(x)$, где b — целое, не делящееся на p. Рассмотри выражение $Q(x)^{p^{k-1}(p-1)}$ по модулю p^k. Число b не делится на p, поэтому найдётся целое число c такое, что $bc \equiv 1 \pmod{p^k}$. Тогда

$$Q(x)^{p^{k-1}(p-1)} \equiv b^{p^{k-1}(p-1)} (1 + pcxR(x))^{p^{k-1}(p-1)} \pmod{p^k}.$$

По лемме 5 имеем

$$b^{p^{k-1}(p-1)} (1 + pcxR(x))^{p^{k-1}(p-1)} \equiv b^{p^{k-1}(p-1)} \equiv 1 \pmod{p^k},$$

где последнее сравнение верно по теореме Эйлера [1, Глава 3, §6, a]. Таким образом,

$$S(x)Q(x) \equiv Q(x)^{p^{k-1}(p-1)-1} Q(x) \equiv Q(x)^{p^{k-1}(p-1)} \equiv 1 \pmod{p^k}.$$ □

3 Доказательство теоремы 1

Докажем предварительно следующую теорему.

Теорема 7. *Пусть p — простое число, k — натуральное, $P(x)$ — многочлен с целыми коэффициентами, свободный член которого не делится на p, число t — наибольшая степень x, при которой коэффициент многочлена $P(x)$ не делится на p. Тогда существуют такие многочлены $Q(x), T(x)$ с целыми коэффициентами, что*

$$P(x)Q(x) \equiv T(x) \pmod{p^k},$$

при этом все коэффициенты многочлена $Q(x)$, кроме свободного члена, делятся на p, степень многочлена $T(x)$ равна t и его старший коэффициент не делится на p.

Доказательство.

Докажем утверждение теоремы индукцией по k.

База индукции: $k = 1$. Возьмём в качестве многочлена $Q(x)$ константу 1, а в качестве многочлена $T(x)$ — многочлен $P(x)$, из которого мы удалим все мономы, коэффициенты при которых делятся на p. Тогда утверждение теоремы выполняется.

Шаг индукции. Пусть для $k = i$ утверждение теоремы доказано и нашлись $Q_i(x)$ и $T_i(x)$, удовлетворяющие условию. Подберём такие многочлены $\overline{Q}(x), \overline{T}(x) \in \mathbb{Z}[x]$, что

$$P(x)(Q_i(x) + p^i\overline{Q}(x)) \equiv T_i(x) + p^i\overline{T}(x) \pmod{p^{i+1}}$$

и степень многочлена $\overline{T}$ не превосходит степени многочлена T. Искомые многочлены будут равны $Q_{i+1}(x) = Q_i(x) + p^i\overline{Q}(x)$ и $T_{i+1}(x) = T_i(x) + p^i\overline{T}(x)$.

Пусть $P(x)Q_i(x) \equiv T_i(x) + p^i\overline{\overline{T}}(x) \pmod{p^{i+1}}$. Тогда

$$T_i(x) + p^i\overline{T}(x) \equiv P(x)Q_i(x) + p^iP(x)\overline{Q}(x) \equiv T_i(x) + p^i\overline{\overline{T}}(x) + p^iP(x)\overline{Q}(x) \pmod{p^{i+1}}.$$

Отсюда,

$$p^i(\overline{\overline{T}}(x) + P(x)\overline{Q}(x) - \overline{T}(x)) \equiv 0 \pmod{p^{i+1}},$$

что равносильно

$$\overline{\overline{T}}(x) + P(x)\overline{Q}(x) - \overline{T}(x) \equiv 0 \pmod{p}.$$

Поскольку p — простое, то $\mathbb{Z}_p$ — поле и в нём многочлены можно делить с остатком. Разделим многочлен $\overline{\overline{T}}(x)$ на $P(x)$ с остатком по модулю p, пусть многочлены $q(x), r(x) \in \mathbb{Z}[x]$ — это неполное частое и остаток от деления соответственно:

$$\overline{\overline{T}}(x) \equiv P(x)q(x) + r(x) \pmod{p},$$

при этом степень многочлена $r(x)$ меньше, чем t. Положим $\overline{Q}(x) = -q(x)$ и $\overline{T}(x) = r(x)$. Остаётся проверить, что степень многочлена $\overline{T}(x)$ меньше степени многочлена $T_i(x)$, из чего будет следовать, что $\deg T_{i+1} = \deg(T_i + p^i\overline{T}) = \deg T_i$. Действительно, по индукционному предположению степень многочлена $T_i(x)$ равна t. Поэтому степень многочлена $\overline{T}(x)$ меньше, чем t. □

Доказательство теоремы 1.

Утверждение теоремы следует из равенства множеств $I_P = \left\{ P(x)U(x) + p^kV(x) \middle| U(x), V(x) \in \mathbb{Z}[x] \right\}$ и $I_T = \left\{ T(x)U(x) + p^kV(x) \middle| U(x), V(x) \in \mathbb{Z}[x] \right\}$. Докажем, что они совпадают.

По теореме 7 существуют такие многочлены с целыми коэффициентами $Q(x), T(x)$, что $P(x)Q(x) \equiv T(x) \pmod{p^k}$, все коэффициенты многочлена $Q(x)$, кроме свободного члена, делятся на p, степень многочлена $T(x)$ равна t и его старший коэффициент не делится на p.

Докажем, что $I_T \subset I_P$. Имеем, $T(x) \equiv P(x)Q(x) \pmod{p^k}$. Тогда для некоторого многочлена $R(x)$ выполнено $T(x) = P(x)Q(x) + p^kR(x)$. Далее,

$$I_T = \left\{ T(x)U(x) + p^kV(x) \middle| U(x), V(x) \in \mathbb{Z}[x] \right\} =$$

$$= \left\{ P(x)Q(x)U(x) + p^k(R(x)U(x) + V(x)) \middle| U(x), V(x) \in \mathbb{Z}[x] \right\} \subset I_P$$

Остаётся доказать, что $I_P \subset I_T$. По лемме 6 существует многочлен с целыми коэффициентами $S(x)$ такой, что $S(x)Q(x) \equiv 1 \pmod{p^k}$. Отсюда, $P(x) \equiv T(x)S(x) \pmod{p^k}$ и для некоторого многочлена $R(x)$ выполнено $P(x) = T(x)S(x) + p^k R(x)$. Далее,

$$I_P = \left\{ P(x)U(x) + p^k V(x) \middle| U(x), V(x) \in \mathbb{Z}[x] \right\} =$$

$$= \left\{ T(x)S(x)U(x) + p^k(R(x)U(x) + V(x)) \middle| U(x), V(x) \in \mathbb{Z}[x] \right\} \subset I_T. \ \square$$

4 Доказательство теоремы 2.

Докажем предварительно серию лемм.

Лемма 8. *Пусть p – простое, k – натуральное, $P(x)$ — многочлен с целыми коэффициентами, $\deg P = n$, старший коэффициент и свободный член многочлена $P(x)$ не делятся на p. Тогда для любого многочлена с целыми коэффициентами $R(x)$ существует многочлен $W(x) = c_{n-1}x^{n-1} + \ldots + c_0$, где $0 \leqslant c_i < p^k$, такой, что*

$$W(x) \equiv R(x) \pmod{p^k, P}.$$

Доказательство.

Докажем, что для любого многочлена $R(x)$ степени больше n существует многочлен $R_<(x)$ такой, что $\deg R_< < \deg R$ и $R \equiv R_< \pmod{p^k, P}$.

Пусть степень $R(x)$ равна $r \geqslant n$. Пусть старший коэффициент многочлена P равен числу a, старший коэффициент многочлена b. Так как a не делится на p, то существует число c такое, что $ac-1$ делится на p^k. Тогда коэффициент при степени r в многочлене $R(x) - bcx^{r-n}P(x)$ делится на p^k. Пусть он равен dp^k. Положим $R_<(x) = R(x) - bcx^{r-n}P(x) - dp^k x^r$. Тогда $\deg R_< < \deg R$ и $R \equiv R_< \pmod{p^k, P}$.

Пусть $R_{<n}(x) \equiv R(x) \pmod{p^k, P}$ и степень многочлена $R_{<n}(x)$ меньше n. Чтобы получить искомый многочлен $W(x)$ заменим все коэффициенты многочлена $R_{<n}(x)$ на их остатки от деления на p^k. $\square$

Лемма 9. *Пусть p – простое, k – натуральное, $P(x)$ — многочлен с целыми коэффициентами, $\deg P = n$, старший коэффициент и свободный член многочлена $P(x)$ не делятся на p. Тогда для любого многочлена $Q(x)$ равносильны следующие утверждения:*

1) класс эквивалентности $[Q(x)]_{p^k,P}$ принадлежит группе $H_{p,k}(P(x))$;

2) многочлен $Q(x)$ обратим по модулю p^k и $P(x)$, и $Q(x) \equiv 1 \pmod{p, P}$;

3) существует многочлен $W(x) = pc_{n-1}x^{n-1} + \ldots + pc_1x + pc_0 + 1$, где $0 \leqslant c_i < p^{k-1}$, такой, что

$$W(x) \equiv Q(x) \pmod{p^k, P}.$$

Доказательство.

Утверждения 1) и 2) равносильны по определению группы $H_{p,k}(P(x))$.

Докажем, что из 2) следует 3). По предположению, $Q(x) \equiv 1 \pmod{p, P}$, то есть $Q(x) = 1 + P(x)U(x) + pV(x)$ для некоторых многочленов с целыми коэффициентами $U(x), V(x)$. Тогда $Q(x) \equiv 1 + pV(x) \pmod{p^k, P}$. По лемме 8 существует многочлен $W(x) = d_{n-1}x^{n-1} + \ldots + d_0$, где $0 \leqslant d_i < p^k$, который сравним с $1 + pV(x)$ по модулю p^k и $P(x)$. Тогда свободный член многочлена $W(x)$ можно представить в виде $d_0 = 1 + pc_0$, а все остальные коэффициенты многочлена $W(x)$ в виде $d_i = pc_i$. Имеем $Q(x) \equiv W(x) \pmod{p^k, P}$.

Теперь докажем, что из 3) следует 2). По предположению, $Q(x) \equiv W(x) \pmod{p^k, P}$, $W(x) = pc_{n-1}x^{n-1} + \ldots + pc_1x + pc_0 + 1$, где $0 \leqslant c_i < p^{k-1}$. Пусть $W(x) = 1 + pS(x)$, где $S(x) = c_{n-1}x^{n-1} + \ldots + c_1x + c_0$. Тогда $Q(x) = 1 + pS(x) + P(x)U(x) + p^kV(x)$ для некоторых многочленов с целыми коэффициентами $U(x), V(x)$. Отсюда

$$Q(x) = 1 + pS(x) + P(x)U(x) + p^kV(x) = 1 + P(x)U(x) + p(S(x) + p^{k-1}V(x)) \equiv 1 \pmod{p, P}.$$

Все коэффициенты многочлена $1 + pS(x)$, кроме свободного члена, делятся на p. По лемме 6 этот многочлен обратим по модулю p^k. Поэтому $1 + pS(x)$ обратим по модулю p^k и $P(x)$, следовательно, $Q(x)$ обратим. □

Лемма 10. *Пусть p – простое, $k > 1$ – натуральное, $P(x)$ — многочлен с целыми коэффициентами, $\deg P = n$, старший коэффициент и свободный член многочлена $P(x)$ не делятся на p. Тогда для любого класса эквивалентности $[Q(x)]_{p^k,P} \in H_{p,k}(P(x))$ существует единственный многочлен $W = pc_{n-1}x^{n-1} + \ldots + pc_1x + pc_0 + 1$, где $0 \leqslant c_i < p^{k-1}$ такой, что*

$$W(x) \in [Q(x)]_{p^k,P}.$$

Доказательство.

Многочлен, удовлетворяющий требованию, существует по лемме 9.

Докажем единственность такого многочлена от противного.

Пусть $W_1(x) = pc_{n-1}x^{n-1} + \ldots + pc_1x + pc_0 + 1$, $W_2(x) = pd_{n-1}x^{n-1} + \ldots + pd_1x + pd_0 + 1$, где $0 \leqslant c_i, d_i < p^{k-1}$, многочлены W_1 и W_2 не равны и $W_1 \equiv W_2 \pmod{p^k, P}$. Тогда для некоторых многочленов $U(x)$ и $V(x)$ с целыми коэффициентами выполнено равенство

$$W_1 - W_2 = p((c_0 - d_0) + \ldots + (c_{n-1} - d_{n-1})x^{n-1}) = P(x)U(x) + p^kV(x).$$

Докажем от противного, что все коэффициенты многочлена $U(x)$ делятся на p^k. Пусть $P(x) = a_nx^n + \ldots + a_0$, $U(x) = b_mx^m + \ldots + b_0$. Пусть t — наибольшая степень x, при которой коэффициент b_t не делится на p^k. Рассмотрим коэффициент многочлена $P(x)U(x) = e_{m+n}x^{m+n} + \ldots + e_1x + e_0$ при степени x, равной $n + t$. Запишем формулу для коэффициента e_{n+t}:

$$e_{n+t} = \sum_{i=\max(0,\, n+t-m)}^{n} a_ib_{n+t-i} = a_nb_t + \sum_{i=\max(0,\, n+t-m)}^{n-1} a_ib_{n+t-i}.$$

В правой части под знаком суммы коэффициент b_{n+t-i} делится на p^k, так как $n + t - i > t$ при $i < n$ и t — наибольшая степень x, при которой коэффициент b_t не делится на p^k. При этом слагаемое a_nb_t не делится на p^k. Следовательно, e_{n+t} не делится на p^k. Поэтому коэффициент при x^{n+t} многочлена $P(x)U_1(x)+p^kV(x)$ не делится на p^k и не равен 0. Однако коэффициент при x^{n+t} многочлена W_1-W_2 равен 0. Противоречие с предположением о том, что не все коэффициенты $U(x)$ делятся на p.

Таким образом, все коэффициенты $U(x)$ делятся на p^k. Тогда все коэффициенты $P(x)U(x) + p^kV(x)$ делятся на p^k и для каждого i разность c_i-d_i делится на p^k. Из-за ограничений на c_i и d_i, такое возможно только если $c_i = d_i$. Отсюда $W_1 = W_2$. Противоречие с предположением о различности многочленов. □

Лемма 11. *Пусть p – простое, $k > 1$ – натуральное, $P(x)$ — многочлен с целыми коэффициентами, $\deg P = n$, старший коэффициент и свободный член многочлена $P(x)$ не делятся на p. Тогда порядок группы $H_{p,k}(P(x))$ равен $p^{n(k-1)}$.*

Доказательство леммы 11.

Рассмотрим многочлены вида $W(x) = pc_{n-1}x^{n-1} + \ldots + pc_1x + pc_0 + 1$, где $0 \leqslant c_i < p^{k-1}$. По леммам 9, 10 соответствие между многочленами такого вида и классами эквивалентности $H_{p,k}(P(x))$ является взаимно однозначным. Тогда количество классов эквивалентности группы $H_{p,k}(P(x))$ равно количеству различных многочленов описанного в начале доказательства вида, которое, в свою очередь, равно $p^{n(k-1)}$, так как коэффициенты c_i могут быть выбраны независимо друг от друга. □

Доказательство теоремы 2.

Докажем теорему индукцией по k.

База индукции: $k = 2$. Предположим, что $H_{p,2}(P(x))$ не порождается множеством $M = \{[1 + px^s]_{p^2,P} \mid 0 \leqslant s \leqslant n - 1\}$. Тогда некоторые из элементов группы $H_{p,2}(P(x))$ непредставимы в виде произведения степеней элементов множества M. По лемме 11 порядок группы $H_{p,2}(P(x))$ равен p^n. В M ровно n элементов и их порядки равны p по лемме 5. Тогда, по принципу Дирихле, существует

элемент, представимый несколькими способами в виде произведения элементов множества M в степенях не больших p. Следовательно, для некоторых $0 \leqslant c_i, d_i < p$ следующие элементы принадлежат одному классу эквивалентности

$$\prod_{i=0}^{n-1}(1+px^i)^{c_i} \equiv \prod_{i=0}^{n-1}(1+px^i)^{d_i} \pmod{p^2, P}.$$

Поэтому существуют такие степени $0 \leqslant a_i < p$, что $a_i \equiv c_i - d_i \pmod{p}$ и

$$\prod_{i=0}^{n-1}(1+px^i)^{a_i} \equiv 1 \pmod{p^2, P},$$

при этом хотя бы одно $a_i \neq 0$.

Так как для любых многочленов $S(x), Q(x)$ выполнено сравнение

$$(1+pS(x))(1+pQ(x)) \equiv 1 + p(S(x)+Q(x)) \pmod{p^2, P},$$

то

$$\prod_{i=0}^{n-1}(1+px^i)^{a_i} \equiv 1 + \sum_{i=1}^{n-1} a_i p x^i \equiv 1 \pmod{p^2, P}.$$

По лемме 10 последнее сравнение выполняется только при $a_i = 0$ для всех i. Противоречие.

Шаг индукции. Пусть утверждение доказано для $k = k_0$. По индукционному предположению $H_{p,k}(P(x))$ порождается элементами вида $[1+px^s]_{p^k,P}$ для целых $0 \leqslant s \leqslant n-1$.

Предположим, что $H_{p,k+1}(P(x))$ не порождается множеством $M = \left\{ [1+px^s]_{p^{k+1},P} \middle| \, 0 \leqslant s \leqslant n-1 \right\}$. Аналогично рассуждениям в доказательстве базы выводим, что существуют такие степени $0 \leqslant a_i < p^k$, что

$$\prod_{i=0}^{n-1}(1+px^i)^{a_i} \equiv 1 \pmod{p^{k+1}, P},$$

при этом хотя бы одно $a_i \neq 0$. Отсюда,

$$\prod_{i=0}^{n-1}(1+px^i)^{a_i} \equiv 1 \pmod{p^k, P}.$$

Из предположения индукции следует, что все числа a_i делятся на p^{k-1}. Пусть $a_i = b_i p^{k-1}$, $0 \leqslant b_i < p$. По лемме 5 имеем $(1+px^s)^{p^{k-1}} \equiv 1 + p^k x^s \pmod{p^{k+1}, P}$. Тогда

$$\prod_{i=0}^{n-1}(1+px^i)^{a_i} \equiv \prod_{i=0}^{n-1}(1+px^i)^{b_i p^{k-1}} \equiv \prod_{i=0}^{n-1}(1+p^k x^i)^{b_i} \equiv 1 \pmod{p^{k+1}, P}.$$

Аналогично рассуждениям в доказательстве базы выводим, что $b_i = 0$ для всех i. Тогда и все a_i равны 0. Противоречие. □

Список литературы

[1] Виноградов И. М., *Основы теории чисел*, Москва-Ижевск: НИЦ «РХД», 2003, 176 с.

[2] Зюбин К. С., *Описание строения группы обратимых центросимметричных двумерных матриц над* $\mathbb{Z}_{2^k}$, ММКШ, 2021, `https://www.mccme.ru/circles/oim/mmks/works2021/zyubin7.pdf`