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 рассматриваются классы 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. Описывается группа обратимых классов эквивалентности 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 многочлены $U(x)$ и $V(x)$ с целыми коэффициентами такие, 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 $P(x)$.

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.

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

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

Если один многочлен из класса эквивалентности обратим, то остальные многочлены этого класса тоже обратимы. Назовём класс эквивалентности, все элементы которого обратимы, обратимым классом эквивалентности.

Обозначим через $H_{p,k}(P(x))$ множество классов эквивалентности по модулю $q = p^k$, где p — простое, и $P(x)$ таких, что все элементы этих классов сравнимы с 1 по модулю p и $P(x)$. Множество $H_{p,k}(P(x))$ является группой относительно операции умножения классов эквивалентности по модулю p^k и $P(x)$. Заметим, что все элементы этой группы являются обратимыми классами эквивалентности.

Основным результатом работы является

Теорема 1. *Пусть $p > 2$ — простое, k — натуральное, $P(x)$ — многочлен с целыми коэффициентами, старший коэффициент которого не делится на p, $\deg P = n$. Тогда*

1) группа $H_{p,k}(P(x))$ изоморфна $(\mathbb{Z}_{p^{k-1}})^n$;

2) каждый элемент группы $H_{p,k}(P(x))$ единственным образом представляется в виде произведения элементов множества $\left\{ [1 + px^s]_{p^k,P} \middle| \, 0 \leqslant s \leqslant n-1 \right\}$ в степенях меньших p^{k-1}.

Во втором параграфе рассматриваются многочлены вида $1 + pS(x)$ и вычисляются их степени по модулю p^k. В третьем параграфе находится порядок группы $H_{p,k}(P(x))$. Наконец, в четвёртом параграфе доказывается теорема 1.

2 Степени элементов вида $1 + pS(x)$

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

Лемма 2. *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] получаем

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

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

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

где последнее равенство верно, так как $\left\lceil\frac{n}{p^i}\right\rceil - \left\lfloor\frac{n}{p^i}\right\rfloor$ равно 0, когда 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 3. *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 $p = 2$. Найдём 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 4. *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

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

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 2 имеем

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

В случае $p > 2$ по лемме 3 справедливо $k-2-\nu_p(i)+i \geqslant k$ для $i > 1$. Поэтому 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 3 справедливо $k - 2 - \nu_p(i) + i \geqslant k$ 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

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

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

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

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

3 Порядок группы $H_{p,k}(P(x))$

Лемма 5. *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 $R(x)$ с целыми коэффициентами*

1) если степень многочлена $R(x)$ не меньше n, то существует многочлен $R_<(x)$ такой, что $\deg R_< < \deg R$ и

$$R(x) \equiv R_<(x) \pmod{p^k, P};$$

2) 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.
1) Пусть степень многочлена $R(x)$ равна $r \geqslant n$. Пусть старший коэффициент многочлена $P(x)$ равен числу a, старший коэффициент многочлена $R(x)$ равен 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 $R(x) \equiv R_<(x) \pmod{p^k, P}$.

2) Из первого пункта следует, что существует многочлен $R_{<n}(x)$ степени меньшей n, сравнимый с $R(x)$ по модулю p^k и $P(x)$. Чтобы получить искомый многочлен $W(x)$ заменим все коэффициенты многочлена $R_{<n}(x)$ на их остатки от деления на p^k. □

Лемма 6. *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) 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.

Докажем, что из 1) следует 2). По определению группы $H_{p,k}(P(x))$ имеем $Q(x) \equiv 1 \pmod{p, P}$, 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 5 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 2) следует 1). 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 $0 \leqslant c_i < p^{k-1}$. Положим $W(x) = 1 + pC(x)$, где $C(x) = c_{n-1}x^{n-1} + \ldots + c_1x + c_0$. Тогда $Q(x) = 1 + pC(x) + P(x)U(x) + p^kV(x)$ для некоторых многочленов с целыми коэффициентами $U(x), V(x)$. Отсюда

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

По определению группы $H_{p,k}(P(x))$, класс эквивалентности, содержащий многочлен $Q(x)$, принадлежит этой группе. □

Лемма 7. *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 если все коэффициенты многочлена $W(x)$ делятся на p, его степень равна $n - 1$ и он сравним с 0 по модулю p^k и $P(x)$, то все коэффициенты $W(x)$ делятся на p^k.*

Доказательство.

По условию, для некоторых многочленов $U(x)$ и $V(x)$ с целыми коэффициентами выполнено равенство

$$W(x) = P(x)U(x) + p^kV(x).$$

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 $P(x)U(x) = d_{m+n}x^{m+n} + \ldots + d_1x + d_0$ при x^{n+t}. Запишем формулу для коэффициента d_{n+t}:

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

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, d_{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 $W(x)$ равен 0. Противоречие с предположением о том, что не все коэффициенты $U(x)$ делятся на p^k.

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, следовательно, все коэффициенты $W(x)$ делятся на p^k. □

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 порядок группы $H_{p,k}(P(x))$ равен $p^{n(k-1)}$.*

Доказательство.

Рассмотрим многочлены вида $W(x) = pc_{n-1}x^{n-1} + \ldots + pc_1x + pc_0 + 1$, где $0 \leqslant c_i < p^{k-1}$. Из леммы 6 следует, что каждому классу эквивалентности из $H_{p,k}(P(x))$ принадлежит хотя бы один многочлен такого вида. При этом если два многочлена $W_1(x)$ и $W_2(x)$ такого вида лежат в одном классе эквивалентности, то их разность $W_1(x) - W_2(x)$ сравнима с 0 по модулю p^k и $P(x)$ и по лемме 7 все коэффициенты их разности $W_1(x) - W_2(x)$ делятся на p^k. Следовательно, $W_1(x) = W_2(x)$. Таким образом, соответствие между классами эквивалентности из $H_{p,k}(P(x))$ и многочленами описанного вида 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. □

4 Доказательство теоремы 1.

Обозначим через M множество $\left\{ [1 + px^s]_{p^k,P} \middle| \, 0 \leqslant s \leqslant n-1 \right\}$.

1) По лемме 8 порядок группы $H_{p,k}(P(x))$ равен $p^{n(k-1)}$. В множестве M ровно n элементов и по леммам 4 и 7 их порядки равны p^{k-1}. Поэтому утверждение 1) теоремы следует из утверждения 2).

2) Докажем утверждение 2) теоремы индукцией по k.

База индукции: $k = 1$. Все многочлены, которые сравнимы с 1 по модулю p и $P(x)$ лежат в одном классе эквивалентности, поэтому группа $H_{p,1}(P(x))$ содержит только один элемент. Все элементы вида $[1 + px^s]_{p,P}$ для целых $0 \leqslant s \leqslant n-1$ одинаковы и совпадают с единственным элементом группы $H_{p,1}(P(x))$.

Шаг индукции. Пусть утверждение доказано для $k = k_0$. По лемме 8 порядок группы $H_{p,k+1}(P(x))$ равен p^{nk}. В M ровно n элементов и по леммам 4 и 7 их порядки равны p^k. Остаётся доказать, что все произведения элементов множества M в степенях не больших p^k попарно несравнимы. Допустим два таких произведения степеней элементов M сравнимы по модулю p^{k+1} и $P(x)$ и $0 \leqslant c_i, d_i < p^k$ — степени элементов $[1 + px^i]_{p^{k+1},P}$ в соответствующих произведениях. Тогда их частное по модулю p^{k+1} и $P(x)$ сравнимо с 1. Значит, существуют такие степени $0 \leqslant a_i < p^k$, что $a_i \equiv c_i - d_i \pmod{p^k}$ и

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

Из предположения индукции следует, что 1 представляется единственным образом в виде произведения элементов $[1 + px^s]_{p^k,P}$ для целых $0 \leqslant s \leqslant n-1$. Порядки этих элементов равны p^{k-1} по леммам 4 и 7, поэтому все числа a_i делятся на p^{k-1}. Пусть $b_i = \frac{a_i}{p^{k-1}}$. Из ограничений на a следует, что $0 \leqslant b_i < p$.

Имеем

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

где второе сравнение выводится из определения b_i, третье выполнено по лемме 4, а последнее верно, так как для любых многочленов $S(x), Q(x)$ выполнено сравнение

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

По лемме 7 числа $b_i p^k$ делятся на p^{k+1} для всех i, следовательно, все $b_i = 0$. Тогда и все a_i равны 0. Следовательно, $c_i = d_i$ для всех i и рассматриваемые произведения степеней элементов M равны. □

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`