ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ В КРИПТОГРАФИИ

Лекция 9

КОНЕЧНЫЕ ПОЛЯ И ДИСКРЕТНЫЙ ЛОГАРИФМ

Тема 9. Аудиторная нагрузка: 1 академический час. Расширенный текст включает доказательства и материал для самостоятельной проработки.

Цель лекции: объяснить построение конечного поля через неприводимый многочлен, доказать цикличность его мультипликативной группы и определить дискретный логарифм.

После изучения темы студент сможет проверять неприводимость многочленов малой степени, вычислять в простом расширении поля, находить порядок элемента и отличать неприводимый многочлен от примитивного.

Предварительная подготовка: деление многочленов с остатком, алгоритм Евклида, конечные группы, порядок элемента и теорема Лагранжа. Вычислительная конструкция полей уже рассматривалась в практической работе №8; здесь даётся её теоретическое обоснование.

План лекции

1. Неприводимость многочленов над простым полем.
2. Построение конечных полей и число их элементов.
3. Цикличность мультипликативной группы.
4. Примитивные элементы и таблицы степеней.
5. Дискретный логарифм и метод больших и малых шагов.
6. Применение к обмену ключом и самостоятельные задачи.

1 Неприводимые многочлены

Пусть p — простое число. Кольцо классов вычетов $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ является полем: для каждого ненулевого класса алгоритм Евклида даёт обратный элемент. Через $\mathbb{F}_p[T]$ обозначается кольцо многочленов с коэффициентами из этого поля.

Определение. Многочлен $f \in \mathbb{F}_p[T]$ положительной степени называется неприводимым, если его нельзя представить в виде $f = uv$, где обе степени u и v положительны и меньше степени f. Ненулевые константы являются обратимыми элементами кольца и не считаются неприводимыми многочленами. Любой многочлен первой степени неприводим.

Критерий для степеней два и три. Многочлен степени 2 или 3 над полем неприводим тогда и только тогда, когда он не имеет корней в этом поле.

Доказательство. Если a — корень, то по теореме о делении $f = (T - a)g$, то есть f приводим. Обратно, при разложении степени 2 или 3 на сумму двух положительных степеней хотя бы одно слагаемое равно 1. Значит, имеется линейный множитель и корень. Для степени 4 этот аргумент уже не действует: возможны два множителя степени 2.

Пример 1. Для $f = T^3 + T + 1$ над $\mathbb{F}_2$ имеем $f(0) = 1$ и $f(1) = 1$. Других элементов в поле нет, поэтому многочлен неприводим. Над $\mathbb{F}_3$ многочлен $T^2 + 1$ принимает значения $1,2,2$ при $T = 0,1,2$ и также неприводим.

Пример 2. Многочлен $T^4 + T^2 + 1$ над $\mathbb{F}_2$ не имеет корней, однако

$$T^4 + T^2 + 1 = (T^2 + T + 1)^2.$$

Следовательно, отсутствие корней само по себе не является общим критерием неприводимости. Для степени 4 дополнительно проверяют делимость на неприводимые многочлены степени 2.

Пример 3. Докажем неприводимость $h = T^4 + T + 1$ над $\mathbb{F}_2$. Значения при 0 и 1 ненулевые. Единственный неприводимый нормированный квадратный многочлен над $\mathbb{F}_2$ — $T^2 + T + 1$: для остальных нормированных квадратных многочленов легко найти корень. По модулю этого многочлена $T^2 = T + 1$, $T^3 = 1$ и $T^4 = T$, поэтому остаток h равен 1. Квадратного делителя нет, значит, h неприводим.

Для многочлена степени n достаточно исключить все неприводимые делители степеней не более $\lfloor n/2 \rfloor$. В противном случае в любом нетривиальном разложении найдётся неприводимый множитель такой степени. Это конечная проверка, но при больших n прямой перебор становится затратным.

2 Построение конечного поля

2.1 Классы многочленов и арифметика

Пусть f — нормированный неприводимый многочлен степени n над $\mathbb{F}_p$. Рассмотрим факторкольцо

$$K = \mathbb{F}_p[T]/(f).$$

Два многочлена задают один элемент K, если их разность делится на f. По теореме о делении каждый класс имеет ровно одного представителя степени меньше n. Обозначив класс T через α, получаем запись

$$a = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}, \qquad a_i \in \mathbb{F}_p.$$

Коэффициенты складываются по модулю p, а произведение после обычного перемножения сокращается с помощью равенства $f(\alpha) = 0$. Возможны p независимых значений каждого из n коэффициентов, поэтому $|K| = p^n$.

Теорема. Факторкольцо $\mathbb{F}_p[T]/(f)$ является полем тогда и только тогда, когда f неприводим.

Доказательство достаточности. Пусть a — ненулевой представитель степени меньше n. Неприводимость f означает $\gcd(a, f) = 1$. Расширенный алгоритм Евклида даёт $ua + vf = 1$. После перехода к классам получаем $[u][a] = 1$. Следовательно, у каждого ненулевого элемента есть обратный; остальные свойства поля наследуются от кольца многочленов.

Доказательство необходимости. Если $f = uv$, где $0 < \deg u, \deg v < n$, то классы $[u]$ и $[v]$ ненулевые, но $[u][v] = 0$. В поле такого быть не может: умножение на обратный к $[u]$ привело бы к $[v] = 0$.

Пример 4. В поле $\mathbb{F}_8 = \mathbb{F}_2[T]/(T^3 + T + 1)$ выполняется $\alpha^3 = \alpha + 1$. Поэтому

$$(\alpha^2 + 1)(\alpha + 1) = \alpha^3 + \alpha^2 + \alpha + 1 = \alpha^2.$$

Из тождества $T^3 + T + 1 = (T^2 + T)(T + 1) + 1$ следует

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

Проверка: $(\alpha+1)(\alpha^2+\alpha)=\alpha^3+\alpha=1$. Все сокращения выполняются в характеристике 2, где $a+a=0$.

2.2 Почему число элементов равно степени простого

Теорема. Всякое конечное поле имеет p^n элементов для некоторого простого p и целого $n \geq 1$.

Доказательство. В конечном поле среди $0,1,1+1,\ldots$ обязательно возникнет повторение. Поэтому существует наименьшее положительное p, для которого $p \cdot 1 = 0$. Если $p = ab$ с $1 < a, b < p$, то $(a \cdot 1)(b \cdot 1) = 0$, хотя оба множителя ненулевые. Следовательно, характеристика p проста.

Элементы $0,1,\ldots,(p-1)\cdot 1$ образуют подполе, изоморфное $\mathbb{F}_p$. Исходное поле является конечномерным векторным пространством над ним. Если размерность равна n, то выбор n координат даёт ровно p^n элементов.

Следствие. Поля из 6, 10 или 12 элементов не существуют. Поле из 9 элементов существует, но оно не совпадает с $\mathbb{Z}/9\mathbb{Z}$: в последнем кольце ненулевой класс 3 удовлетворяет $3 \cdot 3 = 0$.

Существование и единственность с точностью до изоморфизма. Для каждого $q = p^n$ существует поле из q элементов. Идея доказательства: в поле разложения $X^q - X$ над $\mathbb{F}_p$ множество его корней замкнуто относительно сложения, вычитания, умножения и обращения ненулевых элементов. Здесь используется $(a+b)^q = a^q + b^q$ в характеристике p. Производная многочлена равна -1, поэтому его q корней различны и образуют поле.

В любом поле из q элементов каждый элемент удовлетворяет $a^q = a$: для $a \neq 0$ это следует из теоремы Лагранжа в группе порядка $q-1$. Значит, такое поле является полем разложения того же многочлена. Теорема о единственности поля разложения даёт изоморфизм. Полное доказательство теоремы о полях разложения выходит за рамки этой лекции.

3 Цикличность мультипликативной группы

Ненулевые элементы поля K образуют абелеву группу $K^\times$ по умножению. Для $|K| = q$ её порядок равен $q-1$. По теореме Лагранжа порядок каждого элемента делит $q-1$, но это ещё не доказывает существование элемента порядка $q-1$.

Лемма о корнях. Ненулевой многочлен степени d над полем имеет не более d различных корней.

Доказательство. Если корень a существует, выносим множитель $X-a$. Остальные корни являются корнями многочлена степени $d-1$. Индукция по степени завершает доказательство; ненулевая константа корней не имеет.

Теорема. Всякая конечная подгруппа мультипликативной группы поля циклична. В частности, $\mathbb{F}_q^\times$ циклична.

Доказательство. Пусть G — такая подгруппа, $N = |G|$, а m — наименьшее общее кратное порядков всех её элементов. Каждый порядок делит N, поэтому $m \mid N$.

Покажем, что в G есть элемент порядка m . Разложим $m = \prod_i \ell_i^{e_i}$ на степени различных простых чисел. Для каждого i выберем элемент a_i, порядок которого содержит

множитель $\ell_i^{e_i}$. Запишем $\operatorname{ord}(a_i) = \ell_i^{e_i} c_i$, где $\gcd(c_i, \ell_i) = 1$. Тогда элемент $b_i = a_i^{c_i}$ имеет порядок $\ell_i^{e_i}$.

Произведение коммутирующих элементов взаимно простых порядков имеет порядок, равный произведению этих порядков. Действительно, если $\operatorname{ord}(u) = r$, $\operatorname{ord}(v) = s$ и $(uv)^k = 1$, то $u^k = v^{-k}$ лежит в пересечении подгрупп $\langle u \rangle$ и $\langle v \rangle$. Порядок элемента этого пересечения делит и r, и s, следовательно, он равен 1. Отсюда $r \mid k$, $s \mid k$ и $rs \mid k$. При этом $(uv)^{rs} = 1$.

Применяя этот факт последовательно к b_i, получаем элемент $b = \prod_i b_i$ порядка m. С другой стороны, все N элементов G являются корнями $X^m - 1$. По лемме о корнях $N \le m$. Вместе с $m \mid N$ это даёт $m = N$. Следовательно, b порождает G. Для тривиальной группы утверждение очевидно.

Почему существенно слово «поле». Группа обратимых классов по модулю 8 состоит из 1,3,5,7. Квадрат каждого элемента равен 1, поэтому элемента порядка 4 нет. Это абелева, но не циклическая группа. Кольцо $\mathbb{Z}/8\mathbb{Z}$ не является полем, и применённая лемма о числе корней в нём не действует: многочлен $X^2 - 1$ имеет четыре корня.

4 Примитивные элементы

Определение. Элемент $g \in \mathbb{F}_q^\times$ называется примитивным, если он имеет порядок $q - 1$. В этом случае все ненулевые элементы имеют вид $g^0, g^1, \ldots, g^{q-2}$, причём повторений нет.

Если простые делители $q - 1$ известны, то примитивность проверяется по критерию

$$g^{(q-1)/\ell} \neq 1 \quad \text{для каждого простого } \ell \mid (q-1).$$

Доказательство критерия. Если порядок d элемента меньше $q - 1$, то целое число $(q-1)/d$ имеет простой делитель ℓ. Поэтому d делит $(q-1)/\ell$ и соответствующая степень равна 1. Обратно, если хотя бы одна из указанных степеней равна 1, порядок не может равняться $q - 1$.

В построенном поле $\mathbb{F}_8$ элемент α отличен от 1. Поскольку $|\mathbb{F}_8^\times| = 7$ — простое число, его порядок равен 7. Последовательное умножение на α даёт таблицу.

k	α^k	k	α^k
0	1	4	$\alpha^2 + \alpha$
1	α	5	$\alpha^2 + \alpha + 1$
2	α^2	6	$\alpha^2 + 1$
3	$\alpha + 1$	7	1

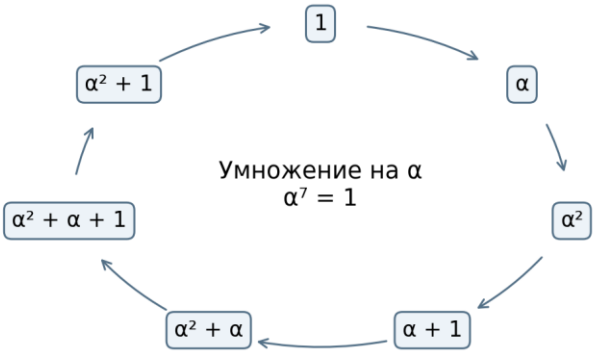


Рисунок 1. Умножение на примитивный элемент проходит через все ненулевые элементы поля.

Неприводимость и примитивность различаются. Многочлен T^2+1 неприводим над $\mathbb{F}_3$, но его корень β в поле из 9 элементов имеет порядок 4: $\beta^2=2$, $\beta^4=1$. Он не порождает группу порядка 8. Элемент $\gamma=\beta+1$ имеет $\gamma^2=2\beta$, $\gamma^4=2\neq 1$ и потому порядок 8. Неприводимый многочлен называют примитивным, если класс T в соответствующем факторполе является примитивным элементом.

Если g примитивен, то g^k также примитивен ровно при $\gcd(k,q-1)=1$. Поэтому в $\mathbb{F}_q$ имеется $\varphi(q-1)$ примитивных элементов. Это следует из формулы $\operatorname{ord}(g^k)=(q-1)/\gcd(q-1,k)$.

5 Дискретный логарифм

5.1 Определение и свойства

Пусть g имеет порядок N и $h\in\langle g\rangle$. Дискретным логарифмом h по основанию g называется класс показателей x по модулю N, удовлетворяющих $g^x=h$. Обычно выбирают представителя $0\le x<N$.

Если основание примитивно в $\mathbb{F}_q$, то $N=q-1$ и логарифм существует для каждого ненулевого элемента. Для нуля он не определён. Если основание не примитивно, элементы вне $\langle g\rangle$ логарифма по этому основанию не имеют. Модуль показателей — порядок основания, а не характеристика поля.

Для $u,v\in\langle g\rangle$ выполняются

$$\log_g(uv)\equiv\log_g u+\log_g v \pmod N,$$

$$\log_g(u^{-1})\equiv-\log_g u \pmod N,\qquad \log_g(u^r)\equiv r\log_g u \pmod N.$$

Эти равенства следуют из законов степеней. Аналогичного правила для логарифма суммы нет. Например, в $\mathbb{F}_8$ имеем $\log_\alpha(\alpha+1)=3$, тогда как $\log_\alpha\alpha+\log_\alpha 1=1$.

Пример 5. По таблице $\log_\alpha(\alpha^2+1)=6$. Произведение $(\alpha+1)(\alpha^2+1)$ можно вычислить через показатели: $\alpha^3\alpha^6=\alpha^9=\alpha^2$. Обратный к $\alpha+1$ равен $\alpha^{-3}=\alpha^4=\alpha^2+\alpha$. Эти результаты совпадают с вычислениями многочленов.

5.2 Метод больших и малых шагов

Прямой перебор последовательно вычисляет $1, g, g^2, \ldots$ и требует до N групповых умножений. Метод больших и малых шагов уменьшает число операций и использует таблицу примерно из $\sqrt{N}$ элементов.

Положим $s = \lceil \sqrt{N} \rceil$. Искомый показатель представим как $x = is + j$, где $0 \le i, j < s$. Из $g^x = h$ следует

$$g^j = h(g^{-s})^i.$$

Сначала запишем малые шаги g^j вместе с показателями j. Затем вычислим большие шаги $h(g^{-s})^i$ и найдём совпадение. Из него получим $x = is + j$ по модулю N. Ответ обязательно проверяется возведением g в найденную степень.

Пример 6. Решим $5^x \equiv 8 \pmod{23}$. Порядок 5 равен 22: $5^{11} \equiv 22 \neq 1$ и $5^2 \equiv 2 \neq 1$. Берём $s = 5$. Малые шаги при $j = 0,1,2,3,4$ равны $1,5,2,10,4$. Поскольку $5^5 \equiv 20$ и $20^{-1} \equiv 15 \pmod{23}$, большие шаги начинаются с 8 и $8 \cdot 15 \equiv 5$.

Совпадение возникает при $i = 1, j = 1$. Поэтому $x = 1 \cdot 5 + 1 = 6$ и $5^6 \equiv 8 \pmod{23}$. Все целые решения имеют вид $x = 6 + 22t$, $t \in \mathbb{Z}$.

Оценка метода составляет $O(\sqrt{N})$ групповых операций и $O(\sqrt{N})$ хранимых элементов при эффективном поиске по таблице. Это оценка числа групповых операций; стоимость арифметики и хранения самих элементов учитывается отдельно. Если h не принадлежит порождённой подгруппе, совпадения, дающего верное решение, не будет.

6 Связь с криптографией

В учебной схеме Диффи — Хеллмана публично известны группа и элемент g. Один участник выбирает показатель a и публикует $A = g^a$, другой выбирает b и публикует $B = g^b$. Они независимо получают один элемент

$$K = B^a = A^b = g^{ab}.$$

В примере по модулю 23 при $g = 5$, $a = 6$, $b = 15$ получаем $A = 8$, $B = 19$, $K = 2$. Дискретный логарифм позволил бы по A восстановить a, после чего вычислить общий элемент. Из этого не следует доказанная эквивалентность задачи дискретного логарифмирования и задачи вычисления общего элемента по двум публичным значениям.

Малые параметры здесь служат только для ручной проверки. Сложность дискретного логарифмирования зависит от порядка подгруппы и свойств выбранного поля; большое число элементов само по себе не является достаточным обоснованием стойкости. Полноценный протокол также должен обеспечивать аутентификацию участников: одно равенство $A^b = B^a$ её не даёт.

7 Закрепление и самостоятельная работа

1. Проверить неприводимость $T^3 + T^2 + 1$ над $\mathbb{F}_2$ и $T^2 + T + 1$ над $\mathbb{F}_3$.
2. В поле $\mathbb{F}_8$ из лекции найти $(\alpha^2 + 1)^{-1}$, $(\alpha + 1)^{10}$ и $\log_\alpha(\alpha^2 + \alpha)$.
3. В поле $\mathbb{F}_9$ с $\beta^2 = 2$ выписать степени $\gamma = \beta + 1$ и все примитивные элементы.
4. По модулю 23 решить $5^x \equiv 10$ и $4^x \equiv 5$. Для второй задачи сначала определить порядок основания.
5. Указать, какие из чисел 16,18,25,27 могут быть числами элементов конечного поля. Объяснить, почему вычеты по модулю 25 не образуют поле.
6. Доказать критерий примитивности и применить его к числу 3 по модулю 7.

Контрольные вопросы

1. Что означает неприводимость многочлена над заданным полем?
2. Для каких степеней отсутствие корней достаточно для неприводимости?
3. Почему неприводимый многочлен позволяет построить поле?
4. Почему порядок конечного поля является степенью простого числа?
5. Чем поле из p^n элементов отличается от кольца вычетов по модулю p^n при $n > 1$?
6. Как в доказательстве цикличности используется ограничение на число корней?
7. Чем примитивный элемент отличается от произвольного ненулевого элемента?
8. Может ли корень неприводимого многочлена быть непримитивным?
9. По какому модулю определяется дискретный логарифм?
10. Почему логарифм нуля не определён?
11. Какова идея метода больших и малых шагов?
12. Как связаны дискретный логарифм и учебный обмен ключом?

Литература

1. Мартынов Л. М. Алгебра и теория чисел для криптографии. 2020. Разделы о конечных полях и циклических группах.
2. Trappe W., Washington L. C. Introduction to Cryptography with Coding Theory. 2nd ed. 2006. §3.11 Finite Fields; глава о дискретных логарифмах.
3. Paar C., Pelzl J. Understanding Cryptography. 2010. §4.3 Galois Fields; §8.2–8.3 Cyclic Groups и The Discrete Logarithm Problem.

Использованы предоставленные учебники. Обозначения, примеры и доказательства адаптированы для настоящего курса; показатели логарифмов выбираются от 0 до $N - 1$.