Введение

- **Криптология** - наука, изучающей математические методы защиты информации путем ее преобразования
- **Криптология** разделяется на два направления - криптографию и криптоанализ
- ***Криптография*** - наука о математических методах обеспечения конфиденциальности и аутентичности (целостности и подлинности) информации
- **Криптоанализ** - задача исследования методов преодоления криптографической защиты (объединяет математические методы нарушения конфиденциальности и аутентичности информации без знания ключей)

- **Криптография** — прикладная наука, она использует самые последние достижения математики и существенно зависит от уровня развития техники и технологии, от применяемых средств связи и способов передачи информации.

- **Криптография** - совокупность методов преобразования данных, направленных на сокрытие смысла сообщения с помощью шифрования и открытие его расшифровыванием, которые выполняются по специальным криптографическим алгоритмам с помощью ключей отправителя и получателя.

Основы теории чисел

- ✔Основные понятия и теоремы
- ✔Алгоритмы Евклида и Эратосфена
- ✔Каноническое разложение числа
- ✔Непрерывные и подходящие дроби

Определение 1

Если a делится на b нацело, мы будем говорить, что b делит a. При этом a называется кратным числа b, a b – делителем числа a.

Число a можно представить как

$$a = q \cdot b$$

где q – полное частное

Теорема 1

Если a кратно c, c кратно b, то a кратно b.

Доказательство:

$$a = c \cdot a_1$$
$$c = b \cdot c_1$$
$$a = b \cdot a_1 \cdot c_1$$

т.о. a представляется произведением b на целое число $a_1 \cdot c_1$ и тем самым делится на b

Теорема 2

Если в равенстве вида

$$k+l+\ldots+n=p+q+\ldots+s$$

относительно всех членов, кроме какого-либо одного, известно, что они кратны b, то и этот один член кратен b

Теорема 2

Доказательство:

Пусть таким одним членом будет k. Имеем

$$l=b\cdot l_1 \quad n=b\cdot n_1 \quad p=b\cdot p_1 \quad q=b\cdot q_1 \quad s=b\cdot s_1$$

$$k+b\cdot l_1+\ldots+ b\cdot n_1= b\cdot p_1+ b\cdot q_1+\ldots+ b\cdot s_1$$

$$k=b\cdot p_1+b\cdot q_1+\ldots+ b\cdot s_1- (b\cdot l_1+\ldots+ b\cdot n_1)=$$
$$=b\cdot(p_1+ q_1+\ldots+ s_1- l_1-\ldots- n_1)$$

Таким образом, k представляется произведением b на целое число и тем самым делится на b (по определению).

Теорема 3 (о делении с остатком)

Всякое целое a представляется единственным способом с помощью положительного целого b равенством вида

$$a = b \cdot q + r \quad 0 \leq r < b$$

(без доказательства)

Число q называется **неполным частным**, а число r – **остатком от деления** a на b.

Наибольший общий делитель (НОД)

Определение: Наибольший из делителей чисел a и b называется НОД этой пары чисел.

Пример: НОД(14, 21)=7.

Обозначение: НОД≡(a,b).

Наибольший общий делитель (НОД)

Аналогично дается определение НОД системы n-чисел.

$$НОД \equiv (a_1, a_2, \ldots, a_n)$$

Пример: НОД(15, 21,105)=3

Взаимно простые числа

Определение: Если НОД(a,b)=1, то числа a и b называются попарно простыми.

Определение: Если НОД(a_1,a_2,…,a_n)=1, то числа a_1,a_2,…,a_n называются взаимно простыми.

Примеры: Числа 5,11,16,19 взаимно простые, т.к. (5,11,16,19)=1.

Числа 5,13,22 – попарно простые, т.к. (5,13)=1; (13,22)=1; (5,22)=1.

Теорема 4

Если a кратно b, то совокупность общих делителей a и b совпадает с совокупностью делителей одного числа b; в частности, (a,b)=b.

(без доказательства)

Теорема 5

Если

$$a = b \cdot q + c,$$

то совокупность общих делителей чисел a и b совпадает с совокупностью делителей чисел b и c; в частности (a,b)=(b,c).

(без доказательства)

Алгоритм Евклида

Применяется для отыскания НОД.

Пусть a,b – положительные целые и a>b.

Согласно теореме 3(о делении с остатком) находим ряд равенств

Алгоритм Евклида

$$a = b \cdot q_1 + r_2 \quad 0 \le r_2 < b$$

$$b = r_2 \cdot q_2 + r_3 \quad 0 \le r_3 < r_2$$

$$r_2 = r_3 \cdot q_3 + r_4 \quad 0 \le r_4 < r_3 \qquad (1)$$

…

$$r_{n-2} = r_{n-1} \cdot q_{n-1} + r_n \quad 0 \le r_n < r_{n-1}$$

$$r_{n-1} = r_n \cdot q_n$$

Алгоритм Евклида

(1) заканчивается, когда получается некоторое $r_{n+1}=0$. Последнее неизбежно, т.к. ряд $b,r_2,r_3,\ldots$ не может содержать более чем b положительных чисел.

Т.о., НОД равен последнему не равному нулю остатку алгоритма Евклида. Поскольку, согласно теоремам 4 и 5:

$$\mathbf{(a,b)=(b,r_2)=(r_2,r_3)=\ldots=(r_{n-1},r_n)=r_n}$$

Пример

Отыскать НОД(25,9) - ?

$25=9 \cdot 2+7$
$9=7 \cdot 1+2$
$7=2 \cdot 3+1$
$2=1 \cdot 2+0$

НОД(25,9)=1

Простые числа

Пусть $a>1$

Определение: Всякое $a>1$ будем называть **простым**, если у него нет других делителей, кроме 1 и самого себя, иначе – **составным**.

Свойство 1: Наименьший отличный от единицы делитель целого числа, большего единицы, есть число простое.

Теорема 6

Наименьший отличный от единицы делитель составного числа a не превосходит $\sqrt{a}$.

Доказательство:

Пусть q – наименьший делитель числа a отличный от единицы, тогда:

$$a = q \cdot a_1$$

$$a_1 \geq q$$

$$a_1 \cdot a \geq q \cdot a$$

$$a_1 \cdot a \geq q^2 \cdot a_1$$

$$a \geq q^2$$

$$q \leq \sqrt{a}$$

Алгоритм Эратосфена

Используется для построения последовательности простых чисел в ряду целых чисел, не превосходящих данного целого N.
Выписываем ряд чисел

1,2,…, N (2)

Первое простое число в ряду (2) – 2.
Вычеркиваем из ряда (2) все числа кратные 2, кроме самого числа 2.

Алгоритм Эратосфена

Первое, оставшееся после 2, простое число – 3. Вычеркиваем из ряда (2) все числа кратные 3, кроме самого числа 3.
Первое, следующее за 3, невычеркнутое простое число 5. Вычеркиваем из ряда (2) все числа кратные 5, кроме числа 5. И т.д.

Когда указанным способом вычеркнуты все числа, кратные простых, меньше простого p, то все невычеркнутые меньшие p^2 будут простые.

Алгоритм Эратосфена

Выводы:

1) приступая к вычеркиванию кратных простого p, это вычеркивание следует начать с p^2.

2) составление последовательности простых чисел, не превосходящих N, закончено, как только вычеркнуты все составные кратные простых, не превосходящих $\sqrt{N}$.

Пример

- Построить последовательность простых чисел для N=16

- 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16
- $\sqrt{16}=4$
- 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16

- 1,2,3,5,7,11,13

Каноническое разложение

Утверждение 1: Всякое целое a
или взаимно простое с данным простым: $(a,p)=1$
или делится на p : $(a,p)=p$

Утверждение 2: Если произведение нескольких сомножителей делится на данное простое p, то хотя бы один из сомножителей делится на p.

Теорема 7

Всякое целое, большее единицы, разлагается на произведение простых сомножителей и притом единственным способом.

Теорема 7

Доказательство:

Пусть $a>1$, p_1 – наименьший простой делитель a, тогда $a=p_1 \cdot a_1$.
Если $a_1>1$, обозначим через p_2 наименьший простой делитель a_1, тогда $a_1=p_2 \cdot a_2$.
Если $a_2>1$, то аналогично находим $a_2=p_3 \cdot a_3$ и т.д., пока не получим некоторое $a_n=1$, т.е. $a_{n-1}=p_n$.
Перемножив найденные равенства и произведя сокращения, получим

$a=p_1 \cdot p_2 \cdot \ldots \cdot p_n \quad (3)$

Докажем, что разложение (3) числа a – единственное.

Предположим, существует второе разложение a на простые сомножители:

$a=q_1 \cdot q_2 \cdot \ldots \cdot q_m \quad (4)$

Тогда

$p_1 \cdot p_2 \cdot \ldots \cdot p_n = q_1 \cdot q_2 \cdot \ldots \cdot q_m \quad (5)$

Правая часть выражения (5) делится на q_1,следовательно и в левой части этого выражения хотя бы один из сомножителей делится на q_1 (утв. 1.2).
Пусть таким сомножителем будет p_1. Тогда $p_1=q_1$, т.к. p_1 кроме 1 делится только на p_1. Сократив обе части равенства (5) на q_1, получим

$$p_2 \cdot \ldots \cdot p_n = q_2 \cdot \ldots \cdot q_m \quad (6)$$

Повторив прежние рассуждения применительно к равенству (6), получим, что

$q_2=p_2$,
$p_3=q_3$,
…,
пока в одной части, например, в левой не сократятся все сомножители. Но одновременно должны сократиться и все сомножители в правой части, т.к. равенство вида

$$1= q_{n+1} \cdot \ldots \cdot q_m$$

невозможно при $q_{n+1},\ldots, q_m > 1$.

Каноническое разложение числа

В разложении числа a на простые сомножители некоторые из них могут повторяться.

Каноническое разложение числа a:

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$$

где $p_1,\ldots,p_n$ – простые сомножители числа a,

$\alpha_1,\ldots,\alpha_n$ – кратности вхождения соответственно сомножителей $p_1,\ldots,p_n$ в число a.

Непрерывные и подходящие дроби

Пусть α - любое вещественное число. Тогда α очевидно можно представить в виде:

$$\alpha = q_1 + \frac{1}{\alpha_2}$$

где q_1 – наибольшее целое, не превосходящее α;

α_2 – вещественное число, $\alpha_2 > 1$.

Непрерывные и подходящие дроби

Точно так же при нецелых $a_S,\ldots,a_{S-1}$ имеем:

$$\alpha_2 = q_2 + \frac{1}{\alpha_3}, \qquad \alpha_3 > 1$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\alpha_{S-1} = q_{S-1} + \frac{1}{\alpha_S}, \quad \alpha_S > 1$$

Получаем следующее разложение α в непрерывную дробь:

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ldots + \cfrac{1}{q_{S-1} + \cfrac{1}{\alpha_S}}}}$$

Непрерывные и подходящие дроби

Если α - рациональное и может быть представлено рациональной несократимой дробью с положительным знаменателем,

$$\alpha = \frac{a}{b}$$

то указанный процесс будет конечен и может быть выполнен с помощью алгоритма Евклида.

Непрерывные и подходящие дроби

$a = b \cdot q_1 + r_2 \quad 0 \le r_2 < b$

$$\frac{a}{b} = q_1 + \frac{r_2}{b}$$

$b = r_2 \cdot q_2 + r_3 \quad 0 \le r_3 < r_2$

$$\frac{b}{r_2} = q_2 + \frac{r_3}{r_2}$$

...

$r_{n-2} = r_{n-1} \cdot q_{n-1} + r_n \quad 0 \le r_n < r_{n-1}$

$$\frac{r_{n-2}}{r_{n-1}} = q_{n-1} + \frac{r_n}{r_{n-1}}$$

$r_{n-1} = r_n \cdot q_n$

$$\frac{r_{n-1}}{r_n} = q_n$$

Непрерывная и подходящие дроби

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ldots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}}$$

представляет собой непрерывную дробь для рационального числа.

Непрерывные и подходящие дроби

Числа $q_1,q_2,\ldots$, участвующие в разложении числа α в непрерывную дробь, называются неполными частными (в случае рационального α это будут неполные частные последовательных делений алгоритма Евклида).

Дроби

$$\delta_1 = q_1 \qquad \delta_2 = q_1 + \frac{1}{q_2} \qquad \delta_3 = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3}}$$

называются подходящими дробями

Пример

Пусть имеется рациональная дробь 7/8, необходимо построить непрерывную дробь и найти неполные частные и подходящие дроби.

$7 = 8 \cdot 0 + 7 \quad q_1 = 0$
$8 = 7 \cdot 1 + 1 \quad q_2 = 1$
$7 = 1 \cdot 7 + 0 \quad q_3 = 7$

$$\frac{7}{8} = 0 + \frac{1}{1 + \frac{1}{7}}$$

$$\delta_1 = 0$$

$$\delta_2 = 0 + \frac{1}{1}$$

$$\delta_3 = 0 + \frac{1}{1 + \frac{1}{7}}$$

Непрерывные и подходящие дроби

Выберем практический способ построения подходящих дробей. Обозначим через

$$P_0 = 1, \qquad Q_0 = 0, \qquad P_1 = q_1, \qquad Q_1 = 1$$

$$\delta_1 = \frac{q_1}{1} = \frac{P_1}{Q_1}$$

$$\delta_2 = \frac{q_1 + \frac{1}{q_2}}{1} = \frac{q_2 * q_1 + 1}{q_2 * 1 + 0} = \frac{q_2 * P_1 + P_0}{q_2 * Q_1 + Q_0} = \frac{P_2}{Q_2}$$

$$\delta_3 = \frac{\left(q_2 + \frac{1}{q_3}\right) * P_1 + P_0}{\left(q_2 + \frac{1}{q_3}\right) * Q_1 + Q_0} = \frac{q_3 * (q_2 * P_1 + P_0) + P_1}{q_3 * (q_2 * Q_1 + Q_0) + Q_1} = \frac{q_3 * P_2 + P_1}{q_3 * Q_2 + Q_1} = \frac{P_3}{Q_3}$$

$$\delta_4 = \frac{q_4 * P_3 + P_2}{q_4 * Q_3 + Q_2}$$

.. .. ..

Непрерывные и подходящие дроби

По индукции легко доказать, что

$$\delta_n = \frac{P_n}{Q_n}$$

$$P_n = q_n * P_{n-1} + P_{n-2}$$

$$Q_n = q_n * Q_{n-1} + Q_{n-2}$$

Алгоритм нахождения

1. Ищем неполные частные, реализовав алгоритм Евклида ($q_1,q_2,\ldots,q_n$).
2. Обозначаем $P_0=1$ $Q_0=0$ $P_1=q_1$ $Q_1=1$.
3. Находим

$$P_s = q_s * P_{s-1} + P_{s-2}$$
$$Q_s = q_s * Q_{s-1} + Q_{s-2}$$

s=2,3…

4. Рассчитываем

$$\delta_s = \frac{P_s}{Q_s}$$

Функция Эйлера

Функцией Эйлера $\phi(a)$ называется функция, которая для $\forall\ a \in Z_+$, равна количеству чисел в ряду от 1,…,a-1 попарно простых с a, где $a \geq 1$.

$\phi(1)=1$
$\phi(2)=1$
$\phi(3)=2$ (1,2)
$\phi(4)=2$ (1,3)
$\phi(5)=4$ (1,2,3,4)
$\phi(6)=2$ (1,5)

Теорема 8

Пусть число a представлено в виде канонического разложения

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$$

Тогда имеем

$$\varphi(a) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right) \cdot \left(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}\right) \cdot \ldots \cdot \left(p_k^{\alpha_k} - p_k^{\alpha_k - 1}\right)$$

без доказательства

$$\varphi(P) = \left(p^1 - p^0\right) = P - 1$$

Вычеты

Определение: Пусть m – некоторое целое положительное число m>1. Пусть a и b – это числа, которые при делении на m имеют один и тот же остаток:

$$a = m \cdot t_1 + r \qquad 0 \le \mathrm{r} < \mathrm{m}$$

$$b = m \cdot t_2 + r$$

Числа a и b будем называть равноостаточными.

Вычеты

Сравнимость чисел a и b по модулю m записывается:

$$a = b \bmod m$$

a сравнимо с b по модулю m.
Очевидно, что все сравнимые между собой числа можно представить в виде:

$$a = b + m \cdot t,$$

где t – целое число.

Примеры сравнимых чисел

$7 = 10 \bmod 3$

$7 = 3 \cdot 2 + 1$

$10 = 3 \cdot 3 + 1$

$5 = 7 \bmod 2$

$6 = 11 \bmod 5$

Свойства сравнимых чисел

1. $a = b \bmod m$
$b = a \bmod m$

2. Сравнимые числа можно почленно складывать:

$a_1 = b_1 \bmod m$
$a_2 = b_2 \bmod m$

$(a1+a2) = (b1+b2) \bmod m$

3. Слагаемые можно переносить из одной части в другую:

$a = (b + c) \bmod m$
$a - c = b \bmod m$

Свойства сравнимых чисел

4. Сравнения можно почленно перемножать:

$$a_1 = b_1 \bmod m$$
$$a_2 = b_2 \bmod m$$

$$a_1 \cdot a_2 = b_1 \cdot b_2 \bmod m$$

5. Если **a = b mod m**, d – делитель a и b, причем так, что $a=a1 \cdot d$ $b=b1 \cdot d$ и $(d,m)=1$, то левую и правую часть сравнения можно сократить на d.

Свойства сравнимых чисел

6. Сравнения можно почленно перемножать:

Если **a = b mod m**, a,b,m имеют общий делитель d – то на него можно сократить:

a=a1·d, b=b1·d, m=m1·d ⇨ **a1 = b1 mod m1**

7. Все части сравнения можно умножать на одно и тоже целое:

a = b mod m перемножив на **k = k mod m**
получим: **a·k=b·kmodm**

Сравнения и их свойства

- ✔Сравнения
- ✔Классы сравнимых чисел
- ✔Вычеты, системы вычетов
- ✔Теорема Эйлера, Ферма
- ✔Решение линейных сравнений 1 степени

Сравнения

Определение: Если a и b два целых числа и их разность a-b делится на целое положительное число m, то говорят, что a сравнимо с b по модулю m:

$$a \equiv b (\mathrm{mod}\, m)$$

То есть a - b=mk или a=b+mk, k - Z

Если представить b в виде b=mq1+r, то a=mq1+r+mk=m(q1+k)+r, то есть при делении чисел a и b на модуль m получаем один и тот же остаток

$$a = m \cdot t_1 + r \qquad 0 \le \mathrm{r} < \mathrm{m}$$

$$b = m \cdot t_2 + r$$

Вычеты. Приведенная система вычетов

Множество равноостаточных по модулю m чисел – это класс чисел, представленных в виде:

$$a = b + m \cdot t$$

Любое число класса называется **вычетом** по модулю m по отношению ко всем числам того же класса.

Всего по модулю m существует m различных классов равноостаточных
сел
(с остатками 0,1,…,m-1).

Полная система вычетов по модулю m – состоит из представителей классов Чисел сравнимых друг с другом по модулю m.

Приведенная система вычетов по модулю m – состоит из представителей классов чисел взаимнопростых с модулем (по одному вычету из каждого класса)

Пример

- Обычно приведенную систему вычетов выделяют из системы наименьших неотрицательных вычетов: {0, 1, …, m-1}

- Так как среди этих чисел число взаимнопростых с m определяется функцией Эйлера, то число чисел приведенной системы, равно как и число классов, содержащих числа, взаимнопростых с модулем, есть **$\phi(m)$**

- Пример: m=15 **$\phi(15)=8$**
- Полная система наименьших неотрицательных вычетов: {0,1,2,3,4,5,6,7,8,9,10,11,12,13,14}

- Приведенная система вычетов: {1,2,4,7,8,11,13,14}

.

Свойство: Если $(a,m)=1$, x пробегает приведенную систему вычетов по модулю m, то a·x тоже пробегает приведенную систему вычетов по модулю m.

Док-во: Чисел a·x будет столько же, сколько и чисел x, т.е. $\varphi(m)$

Предположим, что для x_1 получим $a\cdot x_1$, не принадлежащее приведенной системе вычетов, т.е. $(a\cdot x_1, m)\neq 1$

Предположим, что существует некоторое число d: d делит $a\cdot x_1$, d делит m. Но

$(a,m)=1 \Rightarrow$ d делит x_1, но и $(x_1,m)=1$

Получаем противоречие.

Теорема Эйлера

При m>1 и (a,m)=1 $a^{\varphi(m)} = 1 \bmod m$

Док-во: Пусть x пробегает приведенную систему вычетов: $x = r, x = r_2, \ldots, x = r_l$, где $l = \varphi(m)$

Найдем значение a·x в указанных точках:

$$\rho_1 = (a \cdot r_1) \bmod m$$
$$\rho_2 = (a \cdot r_2) \bmod m$$
$$\ldots$$
$$\rho_l = (a \cdot r_l) \bmod m$$

Согласно Св. 3.2 $\rho_1, \rho_2, \ldots, \rho_l$ пробегают ту же систему, но расположенную в ином порядке.

Перемножая почленно сравнения

$$a \cdot r_1 = \rho_1 \bmod m, \quad a \cdot r_2 = \rho_2 \bmod m \quad \ldots \quad a \cdot r_l = \rho_l \bmod m$$

получим $a^l \cdot r_1 \cdot r_2 \cdot \ldots \cdot r_l = \rho_1 \cdot \rho_2 \cdot \ldots \cdot \rho_l \bmod m$

Разделив обе части на произведение $r_1 \cdot r_2 \cdot \ldots \cdot r_l = \rho_1 \cdot \rho_2 \cdot \ldots \cdot \rho_l$

$$a^l = 1 \bmod m$$

Теорема Ферма

При p простом и (a,p)=1 $a^{p-1} = 1 \bmod p$

Эта теорема является следствием Т. Эйлера при m=p.

Умножая обе части сравнения $a^{\varphi(m)} = 1 \bmod m$ на a, получим сравнение

$$a^{(p-1)} \cdot a = a \bmod p$$

$$a^{p} = a \bmod p$$

Это сравнение справедливо при всех целых a, т.к. оно верно и при a атном p.

Пример $9^{111} \bmod 5 \qquad (9,5) = 1 \qquad \varphi(5) = 4$

$$9^{111} \bmod 5 = \left(9^4\right)^{27} \cdot 9^3 \bmod 5 = (1)^{27} \cdot 9^3 \bmod 5 = 243 \bmod 5 = 3 \bmod 5$$

Сравнения с одним неизвестным

Пусть $f(x) = a_0 \cdot x^n + a_1 \cdot x^{n-1} + \ldots + a_n \cdot x^0$, где

$a_0, a_1, \ldots, a_n \in Z,\ n \in Z,\ x$ - некоторая переменная величина.

Функция $f(x)$ называется степенным многочленом

Если $a_0 \neq 0$ $Q_n(x)$ Многочлен степени n

Будем рассматривать этот многочлен на множестве целых чисел.

Рассмотрим сравнение вида: $f(x) = 0 \bmod m$ (1)

Решить сравнение – значит найти все значения x, ему удовлетворяющие, т.е. такие значения x, при подстановке которых в левую часть (1), мы получим верное числовое сравнение.

Если сравнению (1) удовлетворяет какое-либо x=x1, то тому же сравнению будут удовлетворять и все числа сравнимые с x1, по модулю m: x=x1modm

Линейные сравнения с одним неизвестным

$a \cdot x + b \equiv 0 \bmod m$

$a \cdot x \equiv b \bmod m$

Количество решений:

(a,m)=1 – одно решение

2. (a,m)=d d>1

2.1) d не делит b (b не кратно d) – решений нет

2.2) d делит b не цело - d решений.

$$b = b_1 \cdot d$$

$$a_1 \cdot d \cdot x = (b_1 \cdot d) \bmod (m_1 \cdot d) \Rightarrow \; a_1 \cdot x = b_1 \bmod m_1$$

$(a_1, m_1) = 1 \Rightarrow$ существует единственное решение сравнения по модулю m1:

$$x = x_1 \bmod m_1 \qquad (1)$$

По модулю m числа (1) образуют не одно решение, а столько решений, сколько чисел (1) найдется в ряде 0,1,…,m-1.

Числа $x_1 + 0 \cdot m_1, \quad x_1 + 1 \cdot m_1, \quad x_1 + 2 \cdot m_1, \quad \ldots, \quad x_1 + (d-1) \cdot m_1$

являются решениями сравнения по модулю m.

1 Способ решения линейного сравнения

- Согласно теории непрерывных дробей

$$\frac{m}{a} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ldots}} \\ + \frac{1}{q_n}$$

$$\frac{P_{n-1}}{Q_{n-1}}, \frac{P_n}{Q_n} = \frac{m}{a}$$

$$m \cdot Q_{n-1} - a \cdot P_{n-1} = (-1)^n$$

$$x = \left((-1)^{n-1} \cdot P_{n-1} \cdot b\right) \bmod m$$

Алгоритм нахождения подходящих дробей

1. Ищем неполные частные, реализовав алгоритм Евклида ($q_1,q_2,\ldots,q_n$).
2. Обозначаем $P_0=1$ $Q_0=0$ $P_1=q_1$ $Q_1=1$.
3. Находим

$$P_s = q_s * P_{s-1} + P_{s-2}$$
$$Q_s = q_s * Q_{s-1} + Q_{s-2}$$

s=2,3…

4. Рассчитываем

$$\delta_s = \frac{P_s}{Q_s}$$

Свойства подходящих дробей

Свойство 1. При S>0 имеем $P_S \cdot Q_{S-1} - Q_S \cdot P_{S-1} = (-1)^S$

Свойство 2. При S>0 имеем $\delta_S - \delta_{S-1} = \dfrac{(-1)^S}{Q_S \cdot Q_{S-1}}$

Доказательство:

$h_S = P_S \cdot Q_{S-1} - Q_S \cdot P_{S-1}$

$S = 1 \qquad h_1 = q_1 \cdot 0 - 1 \cdot 1 = -1$

$S = 2 \qquad h_2 = P_2 \cdot Q_1 - P_1 \cdot Q_2 = q_2(P_1 + P_0) - P_1(q_2 \cdot Q_1 + Q_0) = P_0 \cdot Q_1 - P_1 \cdot Q_0 = 1 \cdot 1 - q_1 \cdot 0 = 1$

$h_S = (-1)^S$

$$\delta_S - \delta_{S-1} = \frac{P_S}{Q_S} - \frac{P_{S-1}}{Q_{S-1}} = \frac{P_S \cdot Q_{S-1} - Q_S \cdot P_{S-1}}{Q_S \cdot Q_{S-1}} = \frac{h_S}{Q_S \cdot Q_{S-1}} = \frac{(-1)^S}{Q_S \cdot Q_{S-1}}$$

Согласно свойствам непрерывных дробей имеем:

$$m \cdot Q_{n-1} - a \cdot P_{n-1} = (-1)^n$$

Вычислим левую и правую часть по модулю m:

$$(m \cdot Q_{n-1}) \bmod m - (a \cdot P_{n-1}) \bmod m = (-1)^n \bmod m$$

$$(a \cdot P_{n-1}) \bmod m = (-1)^{n-1} \bmod m$$

$$\left((-1)^{n-1} \cdot a \cdot P_{n-1}\right) \bmod m = (-1)^{n-1+n-1} \bmod m$$

$$\left((-1)^{n-1} \cdot a \cdot P_{n-1}\right) \bmod m = (-1)^{2n-2} = 1 \bmod m$$

$$\left((-1)^{n-1} \cdot a \cdot P_{n-1} \cdot b\right) \bmod m = b \bmod m$$

$$a \cdot x = b \bmod m \Rightarrow$$

$$x = \left((-1)^{n-1} \cdot P_{n-1} \cdot b\right) \bmod m.$$

Мультипликативные функции

Опр: Всякую функцию $\theta(a)$ определяют на множество целых (+) будем называть мультикативной если:

1)она определена на множестве целых положительных чисел (Z+) а и не равна нулю по меньшей мере при одном таком а;

2) для любых положительных попарно простых а1 и а2 имеем:

$$\theta(a_1 * a_2) = \theta(a_1) * \theta(a_2)$$

Например, $$\theta(a) = a^S$$

Свойства мультипликативных функций

1. Для всякой мультипликативной функции $\theta(a)$ $\theta(1)=1$

2. Если $a=a_1\cdot a_2\cdot\ldots$, где $a_1,a_2,\ldots,a_n$ – взаимно простые, то
$$\theta(a)=\theta(a_1\cdot a_2\cdot\ldots\cdot a_n)=\theta(a_1)\cdot\theta(a_2)\cdot\ldots\cdot\theta(a_n)$$

3. Если $\theta_1(a), \theta_2(a)$ – мультипликативные функции, то $\theta(a)=\theta_1(a)\cdot\theta_2(a)$ - есть также функция мультипликативная.

4. Пусть $\theta(a)$ – мультипликативная функция и $a=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_k^{\alpha_k}$
Тогда, обозначая символом $\sum_{d/a}$ сумму, распространенную на все делители d числа a, будем иметь:

$$\sum_{d/a}\theta(d)=\left(1+\theta(p_1)+\theta(p_1^2)+\ldots+\theta(p_1^{\alpha_1})\right)*\ldots*\left(1+\theta(p_k)+\theta(p_k^2)+\ldots+\theta(p_k^{\alpha_k})\right)$$

Функция Эйлера

Функцией Эйлера $\phi(a)$ называется функция, которая для $\forall\ a \in Z_+$, равна количеству чисел в ряду от 1,…,a-1 попарно простых с a, где $a \geq 1$.

$\phi(1)=1$
$\phi(2)=1$
$\phi(3)=2$ (1,2)
$\phi(4)=2$ (1,3)
$\phi(5)=4$ (1,2,3,4)
$\phi(6)=2$ (1,5)

2 Способ решения линейного сравнения

- Согласно теореме Эйлера $a^{\varphi(m)} = 1 \bmod m$

$$a^{\varphi(m)} \cdot b = b \bmod m$$

$$a \cdot x = b \bmod m \Rightarrow \qquad (\text{св - во } 1)$$

$$a \cdot x = \left(a^{\varphi(m)} \cdot b\right) \bmod m$$

$$x = \left(a^{\varphi(m)^{-1}} \cdot b\right) \bmod m$$

Основы теории чисел

1. Алгоритм быстрого возведения в степень
2. Системы линейных сравнений 1 степени
3. Китайская теорема об остатках
4. Показатели
5. Первообразные корни
6. Индексы

Алгоритм быстрого возведения в степень по модулю

1. Представим b в двоичный системе исчисления: $b = (b_0\, b_1 \ldots b_k)_2$, $b_i \in \{0, 1\}$. Например, $199 = 11000111_2$,

2. Заполним следующую таблицу

b	b_0	b_1	...	b_k
a	a_0	a_1	...	a_k

где $a_0 = a$, $a_{i+1} = \begin{cases} a_i^2 \bmod n, & \text{если } b_{i+1} = 0, \\ a_i^2 \cdot a \bmod n, & \text{если } b_{i+1} = 1 \end{cases}$ для $i \geq 0$.

Результат появится в последней ячейке второй строки.

Пример. Вычислить $2^{199} \mod 1003$:

b	1	1	0	0	0	1	1	1
c	2	8	64	84	35	444	93	247

Ответ: $2^{199} \mod 1003 = 247$.

Решение системы линейных сравнений

$$\begin{cases} a_1 x \equiv b_1 \bmod m_1 \\ a_2 x \equiv b_2 \bmod m_2 \\ \dots \\ a_s x \equiv b_s \bmod m_s \end{cases} \qquad \begin{cases} x_1 \equiv b_1 \bmod m_1 \\ x_2 \equiv b_2 \bmod m_2 \\ \dots \\ x_s \equiv b_s \bmod m_s \end{cases} \quad (*)$$

Если каждое из этих сравнений имеет решение, тогда разрешив каждое линейное сравнение относительно x систему сравнений можно привести к следующему виду (*)

Китайская теорема об остатках

- *Суть теоремы:* целое число можно восстановить по множеству его остатков от деления на числа из некоторого набора попарно взаимно простых чисел.

- *Теорема была доказана приблизительно в*

100 году до н.э.

- Впервые была упомянута в трактате китайского математика С. Цзы.

- В 1247 г. до н.э. китайский математик Джу Шао Квин вывел формулу для вычисления этого числа

Китайская теорема об остатках (КТО)

- Пусть $m_1,\dots m_k$ – попарно взаимно простые натуральные числа.
  Тогда всякая система (*) имеет одно и только одно решение в $Z_{m1,\dots mk}$

$$\begin{cases} x_1 \equiv b_1 \bmod m_1 \\ x_2 \equiv b_2 \bmod m_2 \\ \quad\dots \\ x_s \equiv b_s \bmod m_s \end{cases} \qquad (*)$$

- Пусть m_i , $1 \le I \le k$, – взаимно простые числа и $M = m_1 \cdot m_2 \cdot \dots \cdot m_k$

- Пусть a_i , $0 \le a_i \le m_i$, целые числа.
  Введем обозначение $M_i = M/m_i$

- Пусть y_i число, которое удовлетворяет системе сравнений
  $M_i y_i \equiv 1 \bmod m_i$

- При этих условиях система сравнений
  $x \equiv a_i \bmod m_i$ имеет на интервале [0, M – 1] единственное решение, которое определяется формулой

$$x = a_1 y_1 M_1 + a_2 y_2 M_2 + \dots + a_k y_k M_k$$

Пример КТО

Решить систему сравнений:

$$\begin{cases} x \equiv a_1 \bmod 4, \\ x \equiv a_2 \bmod 5, \\ x \equiv a_3 \bmod 7, \end{cases}$$

где $m_1=4$, $m_2=5$, $m_3=7$.

1) Определим число

$M = m_1 \cdot m_2 \cdot m_3 = 4 \cdot 5 \cdot 7 = 140$

2) Вычислим

$M_1 = M/m_1 = 140/4 = 35,$

$M_2 = M/m_2 = 140/5 = 28,$

$M_3 = M/m_3 = 140/7 = 20.$

3) Вычислим N_1, N_2, *и* N_3 *из следующих сравнений:*

$M_1y_1 = 35y_1 \equiv 1 \bmod 4,$

$M_2y_2 = 28y_2 \equiv 1 \bmod 5,$

$M_3y_3 = 20y_3 \equiv 1 \bmod 7.$

$y_1=3$; $y_2=2$; $y_3=6$

4) $x = (a_1y_1M_1 + a_2y_2M_2 + a_3y_3M_3 = (35 \cdot 3a_1 + 28 \cdot 2a_2 + 20 \cdot 6a_3) \bmod 140.$

Первообразные корни

Пусть (a,m)=1 , тогда на основании т. Эйлера

$$a^{\varphi(m)} = 1 \bmod m$$

Существуют ли другие показатели γ, для которых

$$a^{\gamma} = 1 \bmod m \qquad \gamma : \gamma \le \varphi(m)$$

Опр1: **Показатель** a – по модулю m

Наименьшее из чисел *γ: δ=min* *γ:* $a^{\gamma} = 1 \bmod m$

Опр2: Если *δ=φ(m)* – число a – **Первообразный** корень по модулю m

Пример

Пример: Найти показатель числа 2 по mod 7.

$\varphi(7)=7-1=6$

$2^1 = 2 \bmod 7$

$2^2 = 4 \bmod 7 \Rightarrow \delta = 3 \Rightarrow$ 2 не является первообразным корнем.

$2^3 = 1 \bmod 7$

Пример: Найти показатель числа 3 по mod 7.

$3^1 = 3 \bmod 7$

$3^2 = 2 \bmod 7$

$3^3 = 6 \bmod 7 \Rightarrow \delta = 6 \Rightarrow$ 3 является первообразным корнем

$3^4 = 4 \bmod 7$

$3^5 = 243 \bmod 7 = 5 \bmod 7$

$3^6 = 729 \bmod 7 = 1 \bmod 7$

Пример

Пример: Найти показатель числа 5 по mod 7.

$$a = 5 \bmod 7$$

$5^1 = 5 \bmod 7$

$5^2 = 4 \bmod 7$

$5^3 = 125 \bmod 7 = 6 \bmod 7$

$5^4 = 625 \bmod 7 = 2 \bmod 7$

$5^5 = 3125 \bmod 7 = 3 \bmod 7$

$5^6 = 15625 \bmod 7 = 1 \bmod 7$

$$\Rightarrow \delta = 6 \Rightarrow$$

5 является первообразным корнем по mod 7.

Вывод: По одному и тому же mod могут существовать первообразные корни и сравнимые по одному mod числа, принадлежащие одному показателю

Теорема

Пусть (a,m)=1 и (a_1,m)=1 и a=$a_1$modm, тогда числа a и a_1 принадлежат одному и тому же показателю по mod m

Доказательство (от противного)

Пусть $a \in \delta$ по mod m и $a_1 \in \delta_1$ по mod m

Допустим, что $\delta < \delta_1$

Поскольку $a = a_1 \bmod m$,то левую и правую часть сравнения (согласно свойствам сравнений) можно возвести в степень δ

$$a^{\delta} = a_1^{\delta} \bmod m$$

$$a_1^{\delta} = \underset{\equiv 1 \bmod m}{a^{\delta}} \bmod m$$

Тогда на основании определения a_1 имеет показатель < δ1, а это противоречит исходному допущению, значит допущение δ < δ_1 неверно. Аналогично может быть рассмотрена ситуация δ > δ1.

ч.т.д.

- Следствие из теоремы: вместе с некоторым числом a показателю δ принадлежит весь класс сравнимых по mod m классов вычетов по mod m.

- Теорема (без доказательства)

Если a по модулю m принадлежит показателю δ, то числа

$$l = a^0, a^1, \ldots, a^{\delta-1} \quad (1)$$ по модулю m несравнимы.

В частности, отметим, что если a является первообразным корнем по mod m,

Последовательность чисел (2) $a^0, a^1, \ldots, a^{\varphi(m)-1}$ приведенная

система вычетов и все эти числа не сравнимы между собой по mod m.

Все элементы взаимно просты с mod m.

Если a – первообразный корень, то степени a порождают классы вычетов по mod m и представители этих классов образуют приведенную систему вычетов

Пример

- Найти приведенную систему вычетов по mod 7

1) 1,2,3,4,5,6

2) т.к. 3 – первообразный корень по модулю 7, то $3^0, 3^1, \ldots, 3^5$ Образуют приведенную систему вычетов по модулю 7.

$$3^0 = 1 \bmod 7$$

$$3^1 = 3 \bmod 7$$

$$3^2 = 2 \bmod 7$$

$$3^3 = 6 \bmod 7$$

$$3^4 = 4 \bmod 7$$

$$3^5 = 5 \bmod 7$$

Разыскание первообразных корней по модулям

$$p^{\alpha} \quad \text{и} \quad 2p^{\alpha}$$

Теорема: Пусть $c = \varphi(m)$ $q_1, q_2, \ldots, q_k$ – различные простые делители числа c. Для того, чтобы число q, взаимно простое с m, было первообразным корнем по модулю m, необходимо и достаточно, чтобы это q не удовлетворяло ни одному из сравнений:

$$g^{\frac{c}{q_1}} = 1 \bmod m, \; g^{\frac{c}{q_2}} = 1 \bmod m, \ldots, \; g^{\frac{c}{q_k}} = 1 \bmod m$$

Пример:

Пусть $m = 31, \varphi(m) = 30 = 2 \cdot 3 \cdot 5$

$$\frac{30}{2} = 15 \qquad \frac{30}{3} = 10 \qquad \frac{30}{5} = 6$$

$$g^{15} = 1 \bmod 31 \qquad g^{10} = 1 \bmod 31 \qquad g^{6} = 1 \bmod 31$$

Если g не удовлетворяет ни одному из сравнений, то g – первообразный корень

Индексы

- Если P – простое и g первообразный корень по модулю P, то любой элемент из множества чисел 1, 2, … P-1, имеет однозначные представления в виде $a = g^{\gamma}$ для некоторого целого числа $\gamma \in \{0,1,...,P-1\}$

- Число γ – дискретным логарифмом или индексом числа a по основанию g

$$\gamma = ind_g a \bmod P$$

Свойства индексов

$$g^{\gamma} = g^{\gamma} \bmod P, ind_{\gamma} a = \gamma \bmod (P-1)$$

$$\gamma = \gamma_1 \bmod P, \gamma = ind_{\gamma} a \bmod (P-1)$$

Из этого следует, что индексы данного числа по данному основанию образуют класс вычетов по модулю P=1

Два числа принадлежащие одному и тому же классу вычетов имеют индексы, принадлежащие одному и тому же классу вычетов.

Аналитического аппарата для выделенных индексов нет.
Их находят подбором или по таблице.

Пример

$3=5^y \bmod 7$ $y=\mathrm{ind}_5 3$

- Вычисляется подбором:

y=1	$5^1 \bmod 7 \neq 3$
y=2	$5^2 \bmod 7 = 25 \bmod 7 = 4 \neq 3$
y=3	$5^3 \bmod 7 = 125 \bmod 7 = 4*5 \bmod 7 = 6 \neq 3$
y=4	$5^4 \bmod 7 = 625 \bmod 7 = 6*5 \bmod 7 = 2 \neq 3$
y=5	$5^5 \bmod 7 = 3125 \bmod 7 = 2*5 \bmod 7 = 3$

- $\mathrm{Ind}_5 3=5$

Таблицы индексов

- Составленные таблицы индексов для простых модулей p дают возможность по числу находить его индекс и, наоборот, по индексу – число.

- В качестве основания выбирается один из первообразных корней числа p.

- Первые таблицы индексов для простых модулей до 200 составил в 1837 г. русский математик М.В. Остроградский, немецким математиком К. Якоби эти таблицы были доведены до 1000, сейчас до 10000.

Таблицы индексов

- Таблицы обычно содержат наименьшие неотрицательные вычеты по модулю $\phi(p)=p-1$ (первая таблица) и наименьшие неотрицательные приведенные вычеты чисел (вторая таблица).

- Пример. Построить таблицы для определения индексов по числам и чисел по индексам по модулю $p=7$

- В качестве основания а удобно взять наименьший первообразный корень по модулю 7. $a=3$.
- Запишем две приведенные системы вычетов по модулю 7
- 1) 1, 2, 3, 4, 5, 6;
- 2) 3^0, 3^1, 3^2, 3^3, 3^4, 3^5.
- С помощью сравнения устанавливаем соотношение между

1) и 2)

Таблицы индексов

1) 1, 2, 3, 4, 5, 6;

2) 3^0, 3^1, 3^2, 3^3, 3^4, 3^5.

- Запишем две приведенные системы вычетов по модулю 7

$3^0 \equiv 1 \pmod 7$

$3^1 \equiv 3 \pmod 7$

$3^2 \equiv 2 \pmod 7$

$3^3 \equiv 6 \pmod 7$

$3^4 \equiv 4 \pmod 7$

$3^5 \equiv 5 \pmod 7$

n	1	2	3	4	5	6
$ind_3 n$	0	2	1	4	5	3

$ind_3 n$	0	1	2	3	4	5
n	1	3	2	6	4	5

Применение индексов к решению сравнений

- Решение сравнений первой степени по простому модулю.

$$a^x \equiv b \pmod{p}, \text{ где } (a,p)=1$$

- «Индексируем» левую и правую части

$\text{Ind } a + \text{ind } x \equiv \text{ind } b \pmod{p-1}$

$\text{ind } x \equiv \text{ind } b - \text{ind } a \pmod{p-1}$

Индексы находят из таблиц

$\text{Ind } x \equiv \text{ind } c \pmod{p-1}$

$x \equiv c \pmod{p}$

Применение индексов к решению сравнений

Пример. Решить сравнение $4x \equiv 5 \pmod 7$

Решение: $(4, 7) = 1$, сравнение имеет единственный класс решений.

Индексируем обе части:

$\mathrm{Ind}4 + \mathrm{ind}x \equiv \mathrm{ind}5 \pmod 6$

По таблице индексов находим

$\mathrm{ind}_3 5 = 5 \quad \mathrm{ind}_3 4 = 4$

Тогда $\mathrm{ind}_3 x \equiv 1 \pmod 6$

По обратной таблице находим, что $x \equiv 3 \pmod 7$

Применение индексов к решению сравнений

Задача 6. Решить сравнение $2x^5 \equiv 3 \pmod 7$

Решение. «Индексируем» обе части сравнения:

$$\operatorname{ind} 2 + 5\operatorname{ind} x \equiv \operatorname{ind} 3 \pmod 6 \Leftrightarrow$$

$$\Leftrightarrow 5\operatorname{ind} x \equiv \operatorname{ind} 3 - \operatorname{ind} 2 \pmod 6 \Leftrightarrow$$

$$\Leftrightarrow 5\operatorname{ind} x \equiv 1 - 2 \pmod 6 \Leftrightarrow$$

$$\Leftrightarrow 5\operatorname{ind} x \equiv -1 \pmod 6 \Leftrightarrow$$

$$\Leftrightarrow 5\operatorname{ind} x \equiv 5 \pmod 6, \quad (5,\ 6) = 1 \Leftrightarrow$$

$$\Leftrightarrow \operatorname{ind} x \equiv 1 \pmod 6 \Leftrightarrow$$

$$\Leftrightarrow x \equiv 3 \pmod 7.$$

Основы теории чисел

1. Сравнения второй степени
2. Квадратичные вычеты и невычеты
3. Символ Лежандра
4. Символ Якоби
5. Извлечение квадратного корня из квадратичного вычета

Сравнения второй степени

Из сравнений степени n>1 рассматриваем простейшие – двучленные сравнения:

$x^n \equiv a (\mathrm{mod} p)$; $(a,m)=1$ (1)

Если сравнение (1) имеет решения, то a называется вычетом степени n по модулю m.

Если n=2 вычеты и невычеты называются квадратичными

Если n=3 вычеты и невычеты называются кубическими

Если n=4 вычеты и невычеты называются биквадратными.

Сравнения второй степени

Рассмотрим более подробно двучленные сравнения второй степени:

$$x^2 \equiv a \pmod{p};\ (a,p)=1 \qquad (2)$$

Если a – квадратичный вычет по модулю p, то сравнение (2) Имеет 2 решения.

Действительно, если a - квадратичный вычет, то сравнение (2) имеет, по крайней мере, одно решение $x \equiv x_1 \pmod{p}$, тогда ввиду $(-x_1)^2 = x_1^2$, то же сравнение имеет второе решение $x \equiv -x_1 \pmod{p}$, которое отлично от первого, так как из $x_1 \equiv -x_1 \pmod{p}$ было бы $2x_1 \equiv 0 \pmod{p}$, что невозможно в виду $(2,p) = (x_1,p) = 1$

Вывод: Двумя решениями исчерпываются все решения сравнения (2), так сравнение второй степени более двух решений иметь не может.

Сравнения второй степени

Приведенная система вычетов по модулю p состоит из квадратичных вычетов, сравнимых с числами: $\frac{p-1}{2}$

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

и $\frac{p-1}{2}$ квадратичных невычетов

Действительно, среди вычетов приведенной системы вычетов по модулю p квадратичными вычетами являются те и только те, которые сравнимы с квадратами чисел (приведенной системы вычетов), то есть числами (3)

$$-\frac{p-1}{2}, \ldots, \quad -2, \quad -1, \quad 1, \quad 2, \quad \ldots, \quad \frac{p-1}{2}$$

При этом числа (3) по модулю p не сравнимы

Символ Лежандра

$$\left(\frac{a}{p}\right)$$

Определяется для всех a, не делящихся на p.

Задается равенством $\left(\frac{a}{p}\right)=1$,если a квадратичный вычет по модулю p,

и равенством $\left(\frac{a}{p}\right)=-1$, если a квадратичный невычет по модулю p,

Вычислить символ Лежандра и таким путем определить, является ли a квадратичными вычетом или невычетом по модулю p позволяет критерий Эйлера (теорема):

При a, не делящемся на p, имеем

$$a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right) (\mathrm{mod}\ p)$$

Пример

- 1. Определить является ли 5 квадратичным вычетом по модулю 29

$$a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right)(\mathrm{mod}\ p) = 5^{\frac{29-1}{2}} = \left(\frac{5}{29}\right)(\mathrm{mod}\ 29) = 5^{14} \bmod 29 = 1$$

Следовательно 5 квадратичный вычет по модулю 29 и сравнение $x^2 \equiv 5 (\mathrm{mod}\ 29)$ имеет два решения

- 2. Определить является ли 3 квадратичным вычетом или невычетом по модулю 29

Следовательно 3 квадратичный невычет по модулю 29 и сравнение $x^2 \equiv 3 (\mathrm{mod}\ 29)$ решение не имеет

$$3^{14} = \left(\frac{3}{14}\right)(\mathrm{mod}\ 29) = 28(\mathrm{mod}\ 29) = -1(\mathrm{mod}\ 29)$$

Свойства символа Лежандра

1. Если $a \equiv a_1 \pmod p$, то $\left(\frac{a}{p}\right)=\left(\frac{a_1}{p}\right)$
2. $\left(\frac{1}{p}\right)=1$ Действительно, $1=1^2$, следовательно 1 - квадратичный вычет
3. $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$ Следствие из теоремы при a=-1
4. $\left(\frac{a\cdot b\cdot \ldots \cdot l}{p}\right)=\left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)\cdot\ldots\cdot\left(\frac{l}{p}\right)$ Следствие $\left(\frac{a\cdot b^2}{p}\right)=\left(\frac{a}{p}\right)$
5. $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$,
6. Если p и q простые нечетные, то (закон взаимности квадратичных вычетов)

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

Алгоритм нахождения $\left(\frac{a}{p}\right)$.

- Если $a > p$ или $a < 0$, берем остаток от a при делении на p: $a = pq + r$. Тогда $\left(\frac{a}{p}\right) = \left(\frac{r}{p}\right)$.
- Если $0 < a < p$, то раскладывая a на простые сомножители (и -1) по свойству 4 сводим задачу к нахождению $\left(\frac{p_1^k}{p}\right)$, где p_1 — простое или -1; $k \in \mathbb{N}$.
- если $p_1 = -1$, находим символ Лежандра по свойству 2.
- если k-чётное, то $\left(\frac{p_1^k}{p}\right) = 1$, иначе $\left(\frac{p_1^k}{p}\right) = \left(\frac{p_1}{p}\right)$ (свойство 5).
- если $p_1 = 2$, то $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.
- если p_1 — нечётное простое, то, применяя закон квадратичной взаимности, сводим нахождение $\left(\frac{p_1}{p}\right)$ к нахождению $\left(\frac{p}{p_1}\right)$. Далее повторяем процедуру сначала.

Символ Якоби

- Обобщение символа Лежандра

- Пусть P – нечетное, большее единицы, и $P=p_1p_2\ldots p_r$ – разложение его на простые сомножители. Пусть (a,P)=1, тогда символ Якоби определяется равенством

$$\left(\frac{a}{P}\right)=\left(\frac{a}{p_1}\right)\cdot\left(\frac{a}{p_2}\right)\cdot\ldots\cdot\left(\frac{a}{p_r}\right)$$

Свойства символа Якоби

1. Если $a \equiv a_1 \pmod p$, то $\left(\frac{a}{P}\right) = \left(\frac{a_1}{P}\right), \quad если \quad a \equiv a_1 (\mathrm{mod}\, P)$
2. $\left(\frac{1}{P}\right) = 1$
3. $\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}$
4. $\left(\frac{a \cdot b \cdot \ldots \cdot l}{P}\right) = \left(\frac{a}{P}\right) \cdot \left(\frac{b}{P}\right) \cdot \ldots \cdot \left(\frac{l}{P}\right)$, Следствие $\left(\frac{a \cdot b^2}{P}\right) = \left(\frac{a}{P}\right)$
5. $\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}},$
6. Если P и Q простые нечетные и взаимно простые, то

$$\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}} \left(\frac{P}{Q}\right)$$

Применение

- Рассматривая символ Лежандра как частный случай символа Якоби и пользуясь свойствами можно вычислить символ Лежандра быстрее, чем по критерию Эйлера (теореме)

$$\left(\frac{219}{383}\right)=(-1)^{\frac{219-1}{2}\cdot\frac{383-1}{2}}\left(\frac{383}{219}\right)=-\left(\frac{383}{219}\right)=-\left(\frac{164}{219}\right)=-\left(\frac{41}{219}\right)=$$

$$\left(\frac{219}{41}\right)=-\left(\frac{14}{41}\right)=-\left(\frac{2}{41}\right)\cdot\left(\frac{7}{41}\right)=-\left(\frac{7}{41}\right)=-\left(\frac{41}{7}\right)=-\left(\frac{-1}{7}\right)=1$$

Следовательно, рассмотренное сравнение имеет два решения

Извлечение квадратного корня из квадратичного вычета

Пусть p нечетное простое число, a – целое число, взаимно простое с p

Если сравнение $x^2 \equiv a \pmod p$ разрешимо, то выполнены следующие утверждения

1. если $p \equiv 3 \pmod 4$, то $x \equiv a^{\frac{p+1}{4}} \pmod p$

2. если $p \equiv 5 \pmod 8$, то)

$$\text{если} \quad a^{\frac{p-1}{4}} \equiv 1 \pmod p, \quad \text{то} \quad x \equiv a^{\frac{p+3}{8}} \pmod p$$

$$\text{если} \quad a^{\frac{p-1}{4}} \equiv -1 \pmod p, \quad \text{то} \quad x \equiv 2a(4a)^{\frac{p-5}{8}} \pmod p$$

Алгоритм Тоннели-Шенкса

3. если p≡1 (mod 4, то)

Вход: нечетное простое число $p = 2^n q + 1$, q — нечетное целое и целое число a такое, что $\left(\frac{a}{p}\right) = 1$.

Выход: вычет x такой, что $x^2 \equiv a \pmod{p}$.

Выбирая случайным образом найти квадратичный невычет c и определить

$$z \equiv c^q \pmod{p}, \quad r = n.$$

Определить

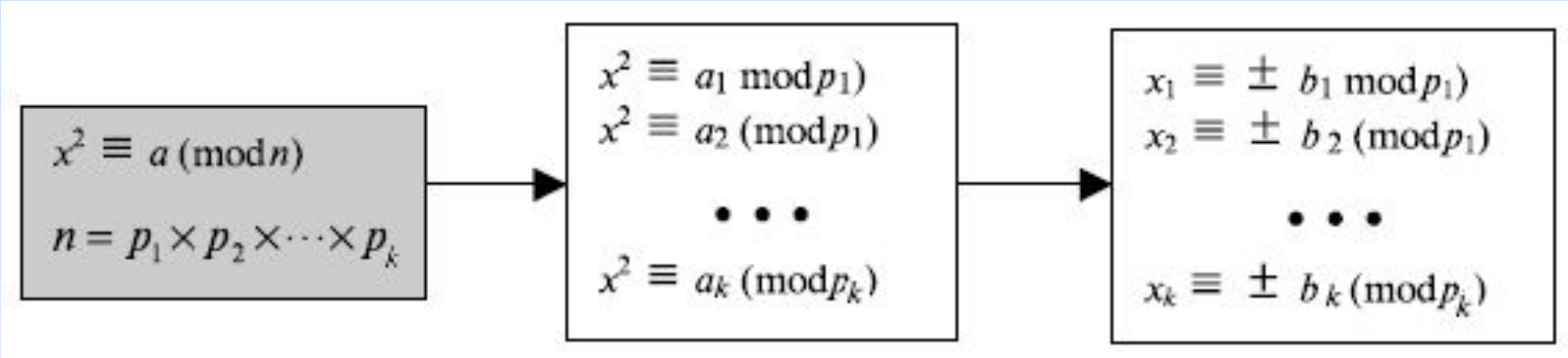
$$t \equiv a^{\frac{q-1}{2}} \pmod{p}, \quad x \equiv at \pmod{p}, \quad b \equiv xt \pmod{p}.$$

* **Если** $x \equiv 1 \pmod{p}$, **то** закончить вычисления,
Иначе вычислить наименьшее m такое, что $b^{2^m} \equiv 1 \pmod{p}$.
Определить $t \equiv z^{2^{r-m-1}} \pmod{p}$,

$$z \equiv t^2 \pmod{p}, \quad x \equiv xt \pmod{p}, \quad b \equiv bz \pmod{p}, \quad r = m$$

и вернуться на шаг *. □

Извлечение квадратного корня по составному модулю



Предположим, что $x^2 \equiv 36 \pmod{77}$ $77 = 7 \times 11$

Мы можем написать $x^2 = 36(mod\ 7) \equiv 1(mod\ 7)$и$x^2 \equiv 36(mod\ 11)$

$x \equiv +1 \pmod{7}$ $x \equiv +5 \pmod{11}$

$x \equiv -1 \pmod{7}$ $x \equiv -5 \pmod{11}$

Теперь мы можем из них составить четыре системы уравнений:

$$\begin{cases} x \equiv +1(\mathrm{mod}\,7) & x \equiv +1(\mathrm{mod}\,7) & x \equiv -1(\mathrm{mod}\,7) & x \equiv -1(\mathrm{mod}\,7) \\ x \equiv +5(\mathrm{mod}\,11) & x \equiv -5(\mathrm{mod}\,11) & x \equiv +5(\mathrm{mod}\,11) & x \equiv -5(\mathrm{mod}\,11) \end{cases}$$

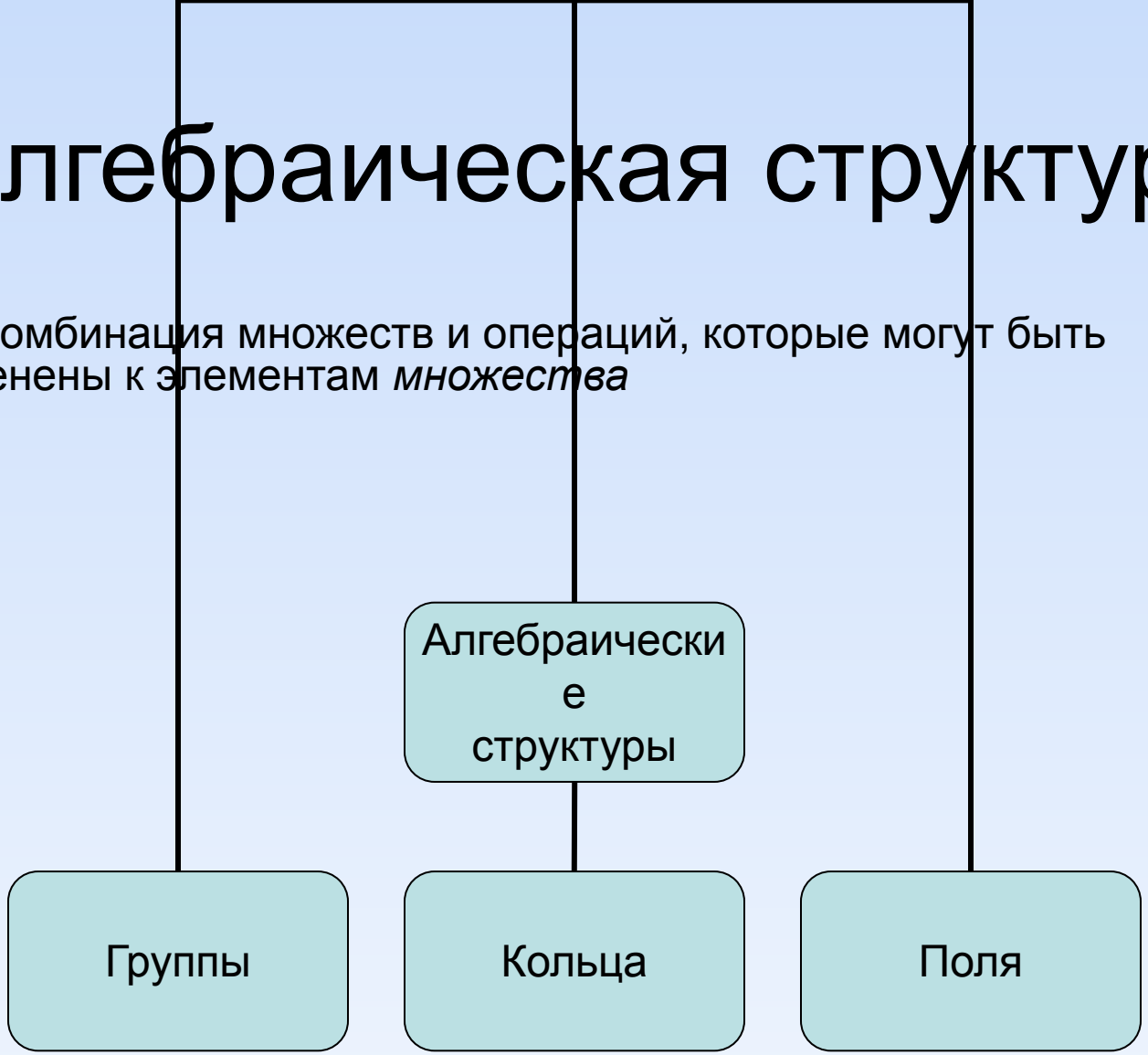
Ответы : $x \pm 6$ ± 27

Алгебраические структуры

1. Бинарная алгебра (БА)
2. Группа. Циклическая группа. Абелева группа
3. Кольцо
4. Поля
5. Поля Галуа

Алгебраическая структура

АС - комбинация множеств и операций, которые могут быть применены к элементам *множества*



Группа

- Группа (G) — набор элементов с *бинарной операцией* "•" обладает четырьмя свойствами:

1. **Замкнутость**. Если a и b — элементы G, то c = a • b — также элемент G.

2. **Ассоциативность**. Если a, b и c — элементы G, то верно
   (a• b) • c = a• (b •c)

3. **Существование нейтрального элемента**. Для всех элементов в G существует элемент e, который называется нейтральным элементом, такой, что
   e • a = a • e = a.

4. **Существование инверсии**. Для каждого a в G существует элемент a', называемый инверсией, такой, что a • a' = a' • a = e.

Абелева группа

Коммутативность. Для всех a и b в G мы имеем a • b = b • a.

Коммутативная (абелева) группа - группа, в которой оператор обладает четырьмя свойствами (замкнутость, ассоциативность, нейтральный элемент и инверсия) для групп плюс дополнительным — коммутативностью.

Группа включает единственный оператор.

Но свойства, присущие каждой операции, позволяют использование пары операций, если они — инверсии друг друга.

Например, если оператор — сложение, то группа поддерживает и сложение, и вычитание, ибо вычитание и сложение — аддитивно инверсные операции (другая операция - умножения и деления).

Группа

1. Замкнутость
2. Ассоциативность
3. Коммутативность
4. Нейтральный элемент
5. Инверсия

Замечание:
Свойство 3
коммутативность только для коммутативной группы

Множество {a, b, c, …}

Операция ●

Пример группы

- Множество целых чисел, входящих в вычет с оператором сложения, G = <Zn, +>, является коммутативной группой.

1. Замкнутость удовлетворяется. Результат сложения двух целых чисел в Zn — другое целое число в Zn.

2. Ассоциативность удовлетворяется. Результат 4 + (3 + 2) тот же самый, что в случае (4 + 3) + 2.

3. *Коммутативность* удовлетворяется. Мы имеем 3 + 5 = 5 + 3.

4. Нейтральный элемент — 0. Мы имеем 3 + 0 = 0 + 3 = 3.

5. Каждый элемент имеет аддитивную *инверсию*. *Инверсия* элемента — его дополнение. Например, *инверсия* 3 — это –3 (n – 3 в Zn), и *инверсия* –3 — это 3. *Инверсия* позволяет нам выполнять вычитание на множестве.

Кольцо

- Кольцо – алгебраическая структура с двумя операциями.
  R={…}, ●, $\perp$
  ● должна удовлетворять всем свойствам (замкнутость, ассоциативность, коммутативность, нейтральный элемент, инверсия)
  $\perp$ замкнутость и ассоциативность и эта распределена с помощью первой операции ●.

  Дистрибутивность означает, что для всех a, b и c элементов из R мы имеем
  $a \perp (b \bullet c) = (a \perp b) \bullet (a \perp c)$ и
  $(a \bullet b) \perp c) = (a \perp c) \bullet (b \perp c)$

  Коммутативное кольцо —*коммутативное* свойство удовлетворено и для второй операции

Кольцо

Дистрибутивность $\perp$ с помощью $\bullet$

1. Замкнутость $\bullet$ 2. Ассоциативность 3. Коммутативность 4. Нейтральный элемент 5. Инверсия	1. Замкнутость $\perp$ 2. Ассоциативность 3. Коммутативность

→ *Замечание: Свойство 3 только для Коммутативного кольца*

Множество {a, b, c, …}

Операции $\bullet$ $\perp$

Умножение дистрибутивно с помощью сложения

- $5\times(3+2) = (5\times3)+(5\times2) = 25$

- Можно выполнить на множестве целых чисел сложение и вычитание и умножение, но не деление. Деление не может применяться в этой структуре, потому что оно приводит к элементу из другого множества. Результат деления 12 на 5 есть 2,4, и он не находится в заданном множестве

Поле

F={…}, ●, ⊥ *коммутативное* кольцо, в котором вторая операция ⊥ удовлетворяет всем пяти свойствам, определенным для первой операции, за исключением того, что нейтральный элемент первой операции (иногда называемый нулевой элемент) не имеет инверсии.

Поле — структура, которая поддерживает две пары операций, используемые в математике: сложение/вычитание и умножение/деление. Есть одно исключение: не разрешено деление на нуль.

Поле

Дистрибутивность $\perp$ с помощью $\bullet$

1. Замкнутость $\bullet$
2. Ассоциативность
3. Коммутативность
4. Нейтральный элемент
5. Инверсия

1. Замкнутость $\perp$
2. Ассоциативность
3. Коммутативность
4. Нейтральный элемент
5. Инверсия

Замечание:
Нейтральный элемент первой операции не имеет инверсии относительно второй операции

Множество {a, b, c, …}

Операции $\bullet$ $\perp$

Поля Галуа

- **Конечное поле** — поле с конечным числом элементов — является очень важной структурой в криптографии.

- Галуа показал что поля, чтобы быть конечными, должны иметь число элементов p^n, где p — простое, а n — положительное целое число.

- Конечные поля обычно называют **полями Галуа** и обозначают как GF(p^n).

- **Поля GF (p)**
- Когда n = 1, мы имеем поле GF (p). Это поле может быть множеством Zp, (0, 1, …p–1) с двумя арифметическими операциями (сложение и умножение).

Поле GF(2)

+	0	1
0	0	1
1	1	0

Сложение

×	0	1
0	0	0
1	0	1

Умножение

a	0	1
-a	1	0

a	0	1
a^{-1}	-	1

Инверсия

Множество	{0, 1}
Операции	+ ×

1.Множество имеет только два элемента (0 и 1).
2. Операция сложения — ИСКЛЮЧАЮЩЕЕ ИЛИ ( ),
3. Операция умножения — AND
4. Сложение и операции вычитания — XOR
5. Умножение и операции деления — AND

Поле $GF(2^n)$

- В криптографии используют 4 операции (сложение, вычитание, умножение и деление), то есть используются поля

- Положительные целые числа в компьютере представляются как n битовые слова, в которых n – 8, 16, 32, 64 и т.д., то есть диапазон целых чисел 0 до 2^n-1

- То есть используется в $GF(2^n)$ - множество 2^n элементов.
  Например, если n = 3, множество равно:
  {000,001,010,100,101,110,111}

  М*одуль* 2^n — не *простое число*. Мы должны определить множество слов по 2 бита и две новых *операции*, которые удовлетворяют свойствам, определенным для поля.

Полиномы

- **Полиномиальное** выражение степени n – 1 имеет форму

$$f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots\ldots + a_1x^1 + a_0x^0$$

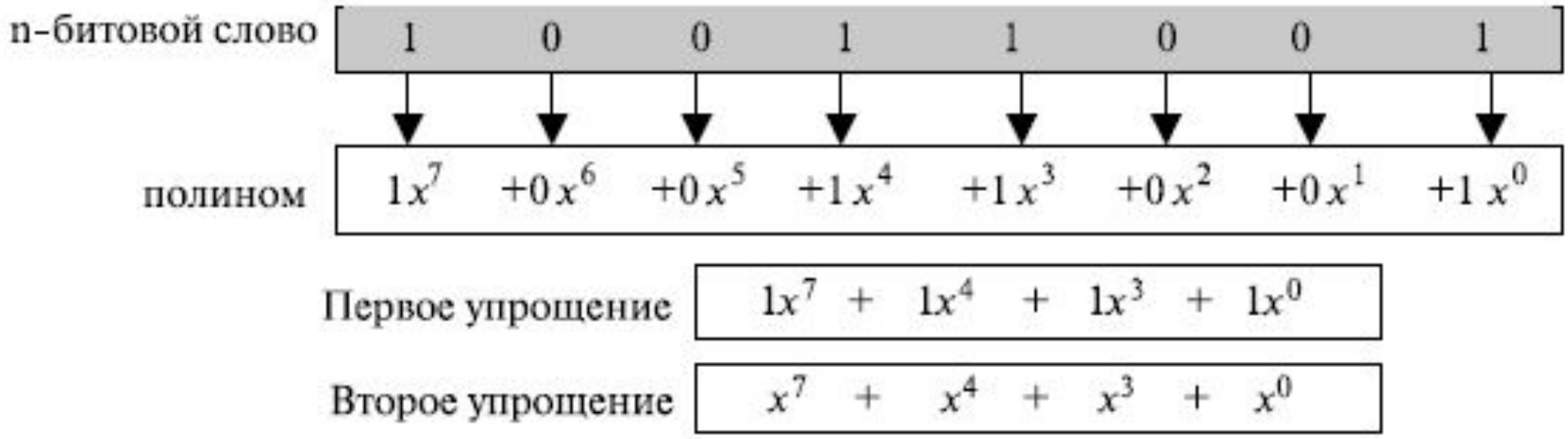
где x^i - i -тый элемент, а a_i - коэффициент i - того элемента.

При представлении n -битовых слов полиномами необходимо следовать некоторым правилам:

- степень x определяет позицию бита в n - битовых слов. Это означает, что крайний левый бит находится в нулевой позиции (связан с x^0), самый правый бит находится в позиции n–l (связан с x^{n-l});
- коэффициенты сомножителей определяют значение битов. Каждый бит принимает только значение 0 или 1, поэтому наши полиномиальные коэффициенты могут иметь значение 0 или 1.

Использование полиномов для предоставления слова из 8 бит (10011001)

Элемент полностью пропущен, если его коэффициент равен 0, и пропущен только коэффициент, если это 1. Также заметим, что элемент x^0 равен 1.



Необходимо найти слово на 8 битов, связанное с полиномом $X^5+ X^2 + X$, n = 8, это означает *полином* степени 7. Расширенный *полином* имеет вид:

$0X^7 + 0X^6 + 1X^5 + 0X^4 + 0X^3 + 1X^2 + 1X^1 + 0X^0$

Полином X5+ X2 + X связан со словом на 8 битов 00100110.

Неприводимые полиномы

- Умножение двух полиномов может создать *полином* со степенью большей, чем n – 1.
- Необходимо делить результат на модуль и сохранять только остаток, как в модульной арифметике.
- Для множеств полиномов в $GF(2^n)$ группа полиномов степени n определена как модуль. То есть никакие полиномы множества не могут делить этот *полином*.
- Простое полиномиальное число не может быть разложено в полиномы со степенью меньшей, чем n. Такие полиномы называются **неприводимые полиномы**.
- Для каждого значения степени часто есть более чем один неразлагаемый *полином*, — при определении $GF(2^n)$, необходимо объявить, какой неприводимый *полином* мы используем как модуль.

Степень	**Неприводимый *полином***
1	$(x+1)x$
2	(x^2+x+1)
3	$(x^3+x^2+1)(x^3+x+1)$
4	$(x^4+x^3+x^2+x+1)(x^4+x^3+1)(x^4+x+1)$
5	$(x^5+x^2+1)(x^5+x^3+x^2+x+1)(x^5+x^4+x^3+x+1)(x^5+x^4+x^3+x^2+1)(x^5+x^4+x^2+x+1)$

Сложение в GF(2^n)

- Операция сложения : складываем коэффициенты соответствующих элементов полинома

$$(x^5 + x^2 + x) \oplus (x^3 + x^2 + 1)$$

$$0x^7+0x^6+1x^5+0x^4+0x^3+1x^2+1x^1+0x^0 \oplus 0x^7+0x^6+0x^5+0x^4+1x^3+1x^2+0x^1+1x^0$$

$$0x^7 + 0x^6 + 1x^5 + 0x^4 + 1x^3 + 0x^2 + 1x^1 + 1x^0 \rightarrow$$

$$x^5 + x^3 + x + 1$$

Результат сложения - сохранены элементы с коэффициентом 1 и удалены элементы с коэффициентом 0. Кроме того, удалены совпадающие элементы обоих полиномов, а несовпадающие сохраняются.

Поскольку сложение в GF(2) означает операцию *ИСКЛЮЧАЮЩЕЕ ИЛИ* (*XOR*), мы можем получить результат *ИСКЛЮЧАЮЩЕГО ИЛИ* для этих двух слов бит за битом. В предыдущем примере x5 + x2 + x есть 00100110, или *полином*, и x3 + x2 + 1 есть 00001101. Результат — 00101011 или, в полиномиальном обозначении, x5 + x3 + x + 1.

Сложение и операции вычитания на полиномах — та же самая операция.

Умножение в $GF(2^n)$

Умножение в полиномах — сумма умножения каждого элемента одного полинома с каждым элементом второго полинома.

1. умножение коэффициента проводится в поле GF(2).
2. умножение x^i на x^j дает результат x^{i+j}.
3. умножение может создать элементы со степенью большей, чем n–1, и это означает, что результат должен быть уменьшен с использованием полинома-модуля.

Пример умножения

- Найдите результат $(x^5 + x^2 + x) \otimes (x^7 + x^4 + x^3 + x^2 + x)$

в GF(2^8) с неразлагаемым полиномом ($x^8 + x^4 + x^3 + x + 1$).

Решение

- Сначала умножаем эти два полинома так, как мы это делали в обычной алгебре (пара элементов с равной степенью удаляется – нулевой полином)

$$P_1 \otimes P_2 = x^5(x^7+x^4+x^3+x^2+x)+x^2(x^7+x^4+x^3+x^2+x)+x(x^7+x^4+x^3+x^2+x) P_1 \otimes P_2 =$$
$$= x^{12}+x^9+x^8+x^7+x^6+x^9+x^6+x^5+x^4+x^3+x^8+x^5+x^4+x^3+x^2 P_1 \otimes P_2 =$$
$$= (x^{l2}+x^7+x^2) \mod (x^8+x^4+x^3+x+1) = x^5+x^3+x^2+x+1$$

Чтобы найти конечный результат, разделим *полином* степени 12 на *полином* степени 8 (модуль) и сохраним только остаток.

$x^{12}+x^7+x^2$	$x^8+x^4+x^3+x+1$
$x^{12}+x^8+x^7+x^5+x^4$	x^4+1
$x^8+x^5+x^4+x^2$	
$x^8+x^4+x^3+x+1$	
$x^5+x^3+x^2+x+1$	Остаток

Процесс деления тот же самый, что и в обычной алгебре, но здесь вычитание то же самое, что и сложение.

Модулярная арифметика

Множество классов вычетов по модулю n образуют кольцо – непустое множество элементов, на котором определены две арифметические операции сложения + и умножения ·, относительно которых выполняются следующие формулы:

1. Ассоциативность по сложению $a+(b+c)=(a+b)+c$
2. Существование нулевого элемента

$a+0=0+a=a$

3. Существование обратного элемента

$a+b=b+a=0$

4. Ассоциативность по умножению $a \cdot (b \cdot c)=(a \cdot b) \cdot c$
5. Дистрибутивность $a \cdot (b + c)=a \cdot b + a \cdot c$

$(b+c) \cdot a = b \cdot a + c \cdot a$

Множество элементов, удовлетворяющих только первым трем свойствам – группа, если в группе <G, +> выполняется свойство коммутативности a+b=b+a, то группа абелева. Группа по сложению кольца Zn – абелева группа.

Модулярная арифметика

- Алгебраические структуры, содержащие абелеву групы по сложению и группу по умножению, связанные законами дистрибутивности – полями
- Конечные поля – поля Галуа
- Пусть G – произвольная группа по умножению
- Опр. Порядком элемента a группы G ($ord_G(a)$) называется наименьшее число k такое, что $a^k = 1$. Порядком группы называется число ее элементов
- Теорема Лагранжа. Порядок любого элемента конечной группы является делителем порядка группы

Пример

- Кольцо Zp при p=29. Ненулевые элементы этого кольца образуют группу по умножению, порядок которого равен p-1=28. По теореме Лагранжа порядок любого элемента a этой группы является делителем 28, т.е. может принимать одно из следующих значений: 1, 2, 4, 7, 14 и 28.

- Элемент a называется примитивным элементом или генератором группы, если его порядок $ord_G(a)$ равен порядку группы. Группа, в которой есть генератор, порождается одним элементом и называется циклической

Линейные рекуррентные последовательности над конечными полями

ЛРП

Пусть к – натуральное число, a_0, a_1, ,,,a_{k-1} – заданные элементы конечного поля F_q. Последовательность S_0, S_1, … элементов поля F_q, удовлетворяющая соотношению

$$S_{n+k}=a_{k-1}S_{n+k-1}+a_{k-2}S_{n+k-2}+\ldots+a_0S_0+a,$$

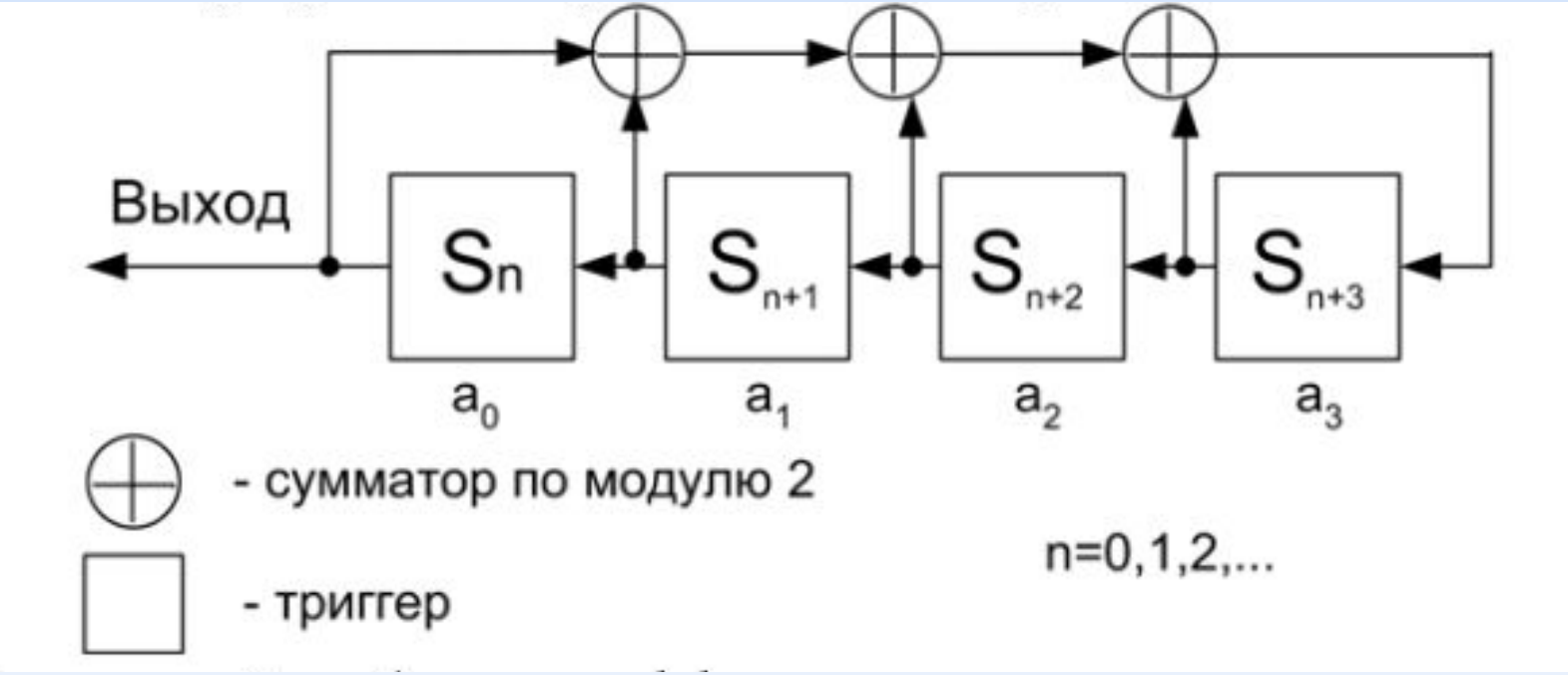
n=1,2,…называется **линейной рекуррентной последовательностью (ЛРП) k-го порядка над полем F_q**

Первые члены S_0, S_1, … S_{k-1} однозначно определяют всю последовательность и называется начальными значениями или линейное рекуррентное соотношение k-го порядка.

Пример: k=4, тогда линейная рекуррентная последовательность 4 порядка над полем имеет вид:

$$S_{n+4}=a_3S_{n+3}+a_2S_{n+2}+ +a_1S_{n+1} +a_0S_0+a$$

Реализация ЛРП на основе регистра сдвига



$$S_{n+4}=a_3S_{n+3}+a_2S_{n+2}+a_1S_{n+1}+a_0S_0$$

$$a_0=a_1=a_2=a_3=1$$

Характеристический многочлен ЛРП

$$S_{n+k}=a_{k-1}S_{n+k-1}+a_{k-2}S_{n+k-2}+\ldots+a_0S_0+a,$$

Многочлен вида $f(x)=x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} -\ldots- a_0$

Пример:

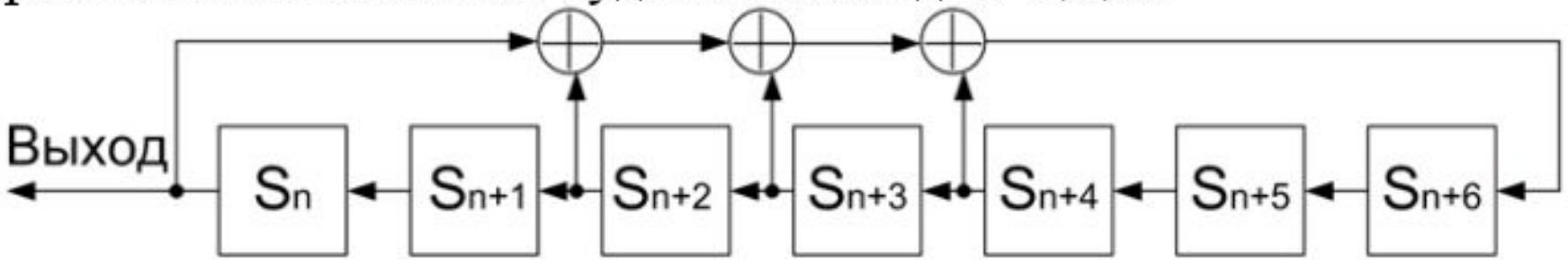
$S_{n+2}=S_{n+1}+S_n$ $f(x) = x^2-x-1$

Пример: Пусть есть рекуррентное соотношение для однородной ЛРП над F_2 вида:

$$S_{n+7} = S_{n+4} + S_{n+3} + S_{n+2} + S_n \quad n = 0,1,...$$

Характеристический многочлен этой ЛРП имеет вид: $f(x) = x^7 - x^4 - x^3 - x^2 - 1 \in F_2[x]$ и является примитивным над F_2 т.е. является нормированным неприводимым над F_2 многочленом порядка $ord(f(x)) = 2^7 - 1 = 127$.

Соответствующий регистр сдвига для заданного рекуррентного соотношения будет иметь вид: ***n=0,1,…***



Математическая основа

ГПСП поточных шифров строятся на основе класса вычетов многочленов по модулю $p(x)$ неприводимого многочлена степени n, которое образует поле Галуа $GF(p^n)$ с конечным числом элементов.

Многочлен, по которому строится LFSR, должен быть примитивным по модулю 2.

Степень многочлена является длиной сдвигового регистра.

Примитивный(базовый) многочлен степени n по модулю 2 – это неприводимый многочлен, который является делителем $x^{2^n-1}+1$

но не является делителем x^d+1 для всех d, являющихся делителями 2^n-1.

Неприводимый многочлен степени n нельзя представить в виде умножения многочленов кроме него самого и единичного.

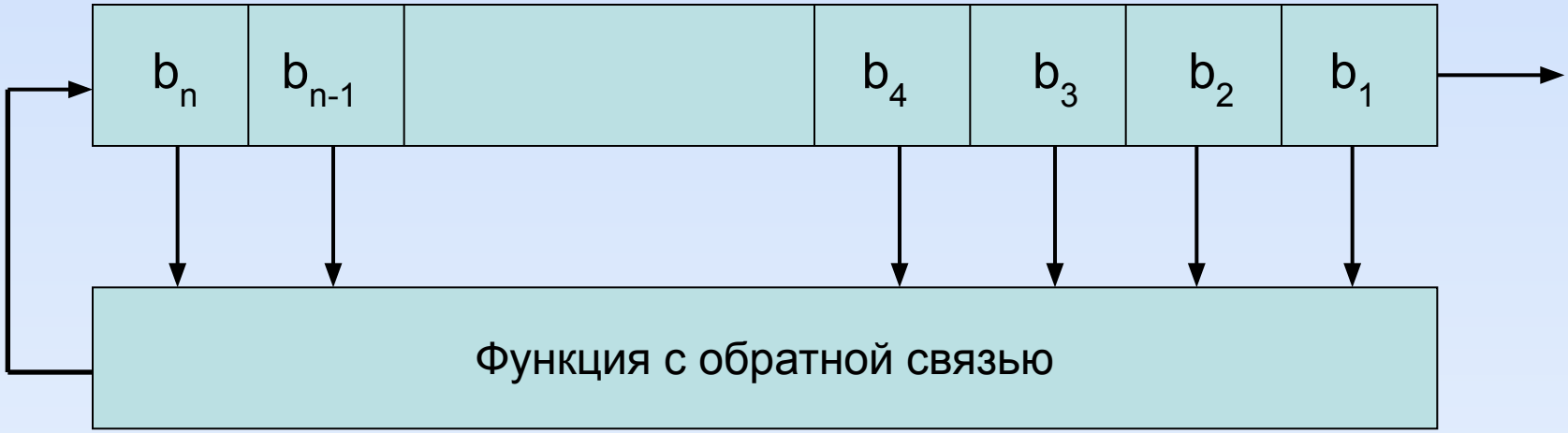
- В общем случае не существует простого способа генерировать примитивные многочлены данной степени по модулю 2. Проще всего выбирать многочлен случайным образом и проверять, не является ли он примитивным.

- (32, 7, 5, 3, 2, 1, 0) означает, что следующий многочлен примитивен по модулю 2:
- $x^{32} + x^7 + x^5 + x^3 + x^2 + x + 1$

- Для LFSR с максимальным периодом первым числом является длина LFSR. Последнее число всегда равно 0, и его можно опустить. Все числа, за исключением 0, задают отводную последовательность, отсчитываемую от правого края сдвигового регистра. То есть, члены многочлена с меньшей степенью соответствуют позициям ближе к правому краю регистра.

- (32, 7, 5, 3, 2, 1, 0) означает, что для взятого 32-битового сдвигового регистра новый бит генерируется с помощью XOR 32, 7, 5, 3, 2 и 1 битов, получающийся LFSR будет иметь максимальную длину, циклически проходя до повторения через 2^{32}-1 значений.

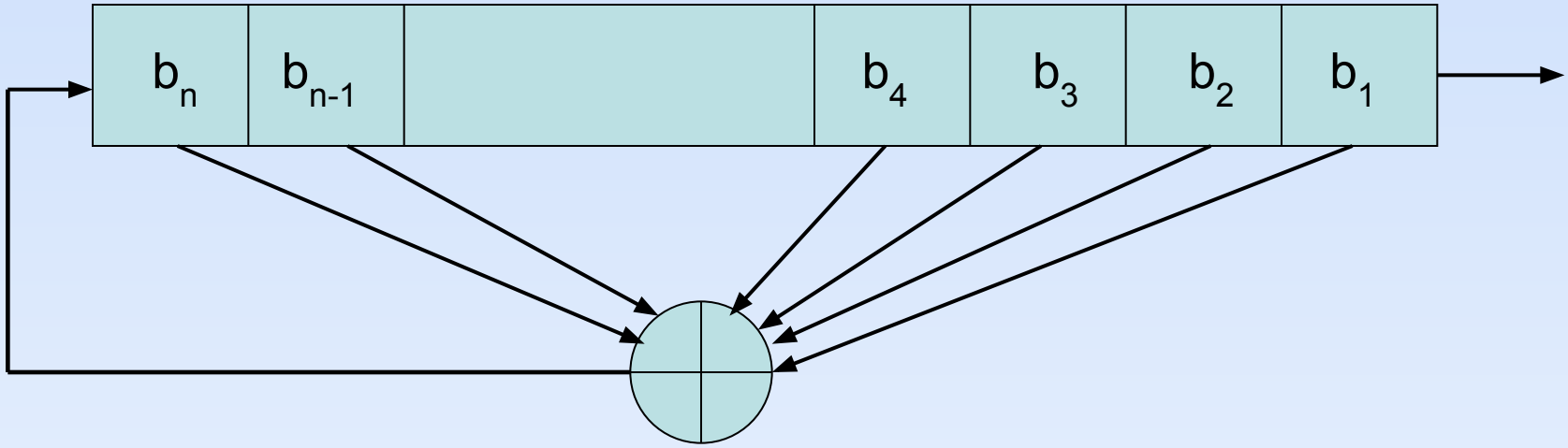
Сдвиговые регистры с обратной связью



- Сдвиговый регистр представляет собой последовательность битов.
- Когда нужно извлечь бит, все биты сдвигового регистра сдвигаются вправо на 1 позицию.
- Новый крайний левый бит является значением функции обратной связи от остальных битов регистра.

Период сдвигового регистра - длина получаемой последовательности до начала ее повторения.

Сдвиговый регистр с линейной обратной связью (РСЛОС или LFSR)



Обратная связь представляет собой просто XOR некоторых битов регистра, перечень этих битов называется ***отводной последовательностью***.

n-битовый LFSR может находиться в одном из 2^n-1 внутренних состояний. Регистр может генерировать псевдослучайную последовательность с периодом 2^n-1 битов.

Только при определенных отводных последовательностях LFSR циклически пройдет через все 2^n-1 внутренних состояний - LFSR ***с максимальным периодом***.

1 1 1 1

0 1 1 1

1 0 1 1

0 1 0 1

1 0 1 0

1 1 0 1

0 1 1 0

0 0 1 1

1 0 0 1

0 1 0 0

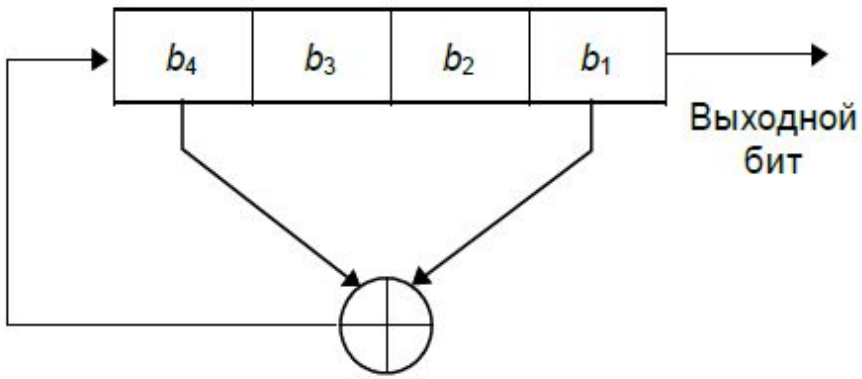
0 0 1 0

0 0 0 1

1 0 0 0

1 1 0 0

1 1 1 0



Свойства ЛРП

1. В криптографии применяются ЛРП максимального периода, формируемые характеристическими многочленами, являющимися примитивными многочленами над соответствующими полями.

2. ЛРП максимальной длины имеют равномерный спектр, статистическую равномерность.

3. Предельно большая длина периода q^k-1

4. Отсутствие скрытой периодичности