Доп. дисциплины
Магистры весна 2021
Занятие 8
29.04.2021

КВАДРАТИЧНЫЙ ЗАКОН ВЗАИМНОСТИ

Удобным для вычислений является символ Лежандра

$$\left(\frac{a}{p}\right)=\begin{cases}1, & \text{если } a \text{ квадратичный вычет,}\\ -1, & \text{если } a \text{ квадратичный невычет,}\\ 0, & \text{если } a \text{ кратен } p.\end{cases}$$

Поскольку все вычисления производятся по модулю p, то очевидны следующие свойства символа Лежандра:

Если $a=b+kp,$ то $\left(\frac{a}{p}\right)=\left(\frac{b+pk}{p}\right)=\left(\frac{b}{p}\right)+\left(\frac{pk}{p}\right)=\left(\frac{b}{p}\right)$.

Далее, очевидно,

$$\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\Rightarrow\left(\frac{a^2}{p}\right)=1.$$

Очевидно, что $\left(\frac{1}{p}\right)=1$, т.к. из единицы квадратный корень всегда извлекается.

Так как по теореме Лагранжа

$$a^{p-1}=1(\mathrm{mod}\ p),$$

то корень квадратный из левой части равен 1 или -1.

Следовательно,

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

Эту формулу, часто, даже рассматривают, как определение символа Лежандра.
Запомним это для дальнейшего!

КВАДРАТИЧНЫЙ ЗАКОН ВЗАИМНОСТИ

Пусть p и q – нечетные простые числа, тогда имеют место три равенства:

$$\begin{cases}\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}\\ \left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}\\ \left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\end{cases}$$

Используя свойства символа Лежандра и квадратичный закон взаимности можно довольно быстро выяснить, извлекается ли квадратный корень из некоторого числа или нет.

Например, вернемся к нашему уравнению

$$x^2 \equiv 2011 (\mathrm{mod}\, 2161).$$

Вычислим $\left(\frac{2011}{2161}\right)$. Так как 2011 простое число, то сразу применяем третью (основную) формулу квадратичного закона взаимности. Поскольку,

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

$$\left(\frac{2011}{2161}\right)=(-1)^{\frac{2011-1}{2}\cdot\frac{2161-1}{2}}\left(\frac{2161}{2011}\right)=-\left(\frac{2011+150}{2011}\right)=-\left(\frac{150}{2011}\right)=$$

$$=-\left(\frac{2\cdot 3\cdot 5^2}{2011}\right)=-\left(\frac{2}{2011}\right)\left(\frac{3}{2011}\right)\left(\frac{5^2}{2011}\right)=-\left(\frac{2}{2011}\right)\left(\frac{3}{2011}\right)=-(-1)^{\frac{2011^2-1}{8}}\left(\frac{3}{2011}\right)=\left(\frac{3}{2011}\right).$$

Теперь нужно применить еще один раз квадратичный закон взаимности

$$\left(\frac{3}{2011}\right)=(-1)^{\frac{3-1}{2}\cdot\frac{2011-1}{2}}\left(\frac{2011}{3}\right)=-\left(\frac{2011}{3}\right)=-\left(\frac{3\cdot 670+1}{3}\right)=-\left(\frac{1}{3}\right)=-1.$$

Значит, из 2011 по модулю 2161 квадратный корень не извлекается.

Алгоритм извлечения квадратного корня по простому модулю.

Этот алгоритм важен и сам по себе, а также он применяется во многих важных криптографических протоколах.

Итак, практически решаем уравнение

$$x^2 \equiv a (\mathrm{mod}\, p).$$

Здесь имеются два, существенно, разных случая, в зависимости от того какой остаток от деления на 4 имеет число «р».

Вариант первый (легкий).

$p \equiv 3(\mathrm{mod}\, 4) \Rightarrow p = 4k+3$, для некоторого натурального числа k.

Пусть из числа «а» извлекается квадратный корень, т.е.

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

Тогда

$$a^{\frac{p-1}{2}}=a^{\frac{4k+3-1}{2}}=a^{2k+1}=1(\mathrm{mod}\, p) \Rightarrow a^{2k+2}=a(\mathrm{mod}\, p)$$

Мы просто умножили обе части равенства на «а».

Теперь можно легко извлечь квадратный корень из «а»: $\sqrt{a}=\pm a^{k+1}$.

Ответ для первого варианта.

Если $p \equiv 3(\mathrm{mod}\, 4)$**, то** $\sqrt{a}=\pm a^{k+1}=\pm a^{\frac{p-3}{4}+1}=a^{\frac{p+1}{4}}$ **.**

Кстати, во многих криптопротоколах сразу рекомендуют брать $p \equiv 3(\mathrm{mod}\, 4)$**, что бы можно было быстро извлекать квадратные корни.**

Простых чисел, с таким свойством, по известной теореме Дирихле, о простых числах в арифметических прогрессиях, бесконечно много.

Удовлетворяют условию $p \equiv 3(\bmod 4)$**,** например, **p = 3, 7, 11, 19, 23, 31, 43, 47, 59 и т.д.**

Однако, наше простое число 2161 имеет вид $p = 2161 = 4 \cdot 540+1 \Rightarrow p \equiv 1(\bmod 4)$, т.е. не подпадает под **Вариант первый.**

Вариант второй, сложный.

Пусть $p \equiv 1(\bmod 4) \Rightarrow p=4k+1$. В этом случае,

$a^{\frac{p-1}{2}} = a^{\frac{4k+1-1}{2}} = a^{2k} = a^{2^s t} = 1(\bmod p)$**,** где t – нечетное число.

В этом случае, фокус с умножением обеих частей равенства на «a» не проходит, т.к. в левой части равенства $a^{2^s t} = 1(\bmod p)$ находится четная степень числа «a» и при умножении на «a» она станет нечетной! И квадратный корень не извлечется!

Для дальнейших вычислений нам потребуется квадратичный невычет «b».

Вопрос в том, как его найти?

Так как, $p = 4k+1$, то $\frac{p-1}{2} = \frac{4k+1-1}{2} = 2k$ и $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{2k} = 1$ поэтому элемент «-1» будет квадратичным вычетом! А жаль, если бы невычетом был b = -1, то вычисления производились бы очень легко!

Второй соблазнительный кандидат – это число «2». И, действительно, если k – нечетное число, то в качестве b число «2» подходит!

В самом деле,

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{(4k+1)^2-1}{8}} = (-1)^{2k^2+k} = (-1)^{k(2k+1)} = -1.$$

Если же k – четно, то придется подбирать необходимый невычет b, перебирая числа 3, 5 и т.д., производя вычисления, используя квадратичный закона взаимности. Поскольку, невычетов ровно половина, среди всех остатков по модулю «p», то вероятность, что мы не найдем невычет, например, с четвертого раза, равна всего $\frac{1}{16}$.

Мораль. Искать невычет b – не проблема!

Итак, пусть b – квадратичный невычет по модулю p. Не забываем, что

$p=4k+1 \Rightarrow \frac{p-1}{2} = 2^s t$, где t – нечетное число.

Тогда, b - как невычет, удовлетворяет равенству $b^{2^s t} = -1(\bmod p)$**,** а элемент «a», в свою очередь, как вычет равенству $a^{2^s t} = 1(\bmod p)$.

Описание алгоритма извлечения квадратного корня для Второго варианта.

Поскольку, $a^{2^s t} = 1(\bmod p)$ то возможны два варианта извлечения квадратного корня из левой части

$$\begin{cases} a^{2^{s-1} t} = +1(\bmod p) \\ a^{2^{s-1} t} = -1(\bmod p) \end{cases}.$$

Но это только «фигура речи» – извлечение квадратного корня. Реально нам предстоит возвести элемент «a» в степень $2^{s-1}t$ и проверить, чему равна эта степень – или «+1» или «-1».

Случай 1. Когда $a^{2^{s-1}t} = +1 (\bmod p)$, мы можем опять «извлечь квадратный корень» (возвести элемент «a» в степень $2^{s-2}t$) и снова выяснить, какой из двух вариантов имеет место:

$$\begin{cases} a^{2^{s-2}t} = +1 (\bmod p) \\ a^{2^{s-2}t} = -1 (\bmod p) \end{cases}$$

Случай 2. Если $a^{2^{s-1}t} = -1 (\bmod p)$, то мы используем наш невычет b и умножаем это равенство на $b^{2^s t} = -1 (\bmod p)$ и получаем

$$a^{2^{s-1}t} \cdot b^{2^s t} = 1 (\bmod p) \Rightarrow (a^{2^{s-1}} \cdot b^{2^s})^t = 1 (\bmod p).$$

Теперь, если s-1>0 из левой части равенства $(a^{2^{s-1}} \cdot b^{2^s})^t = 1 (\bmod p)$ можно «извлечь квадратный корень» (т.е. возвести элемент ab^2 в степень $2^{s-2}t$). И опять получить один из двух возможных вариантов

$$\begin{cases} (a^{2^{s-2}} \cdot b^{2^{s-1}})^t = +1 (\bmod p) \\ (a^{2^{s-2}} \cdot b^{2^{s-1}})^t = -1 (\bmod p) \end{cases}$$

Например, если имеет место «плохой» случай с «-1», то умножаем второе равенство на $b^{2^s t} = -1 (\bmod p)$ и получаем

$$(a^{2^{s-2}} \cdot b^{2^{s-1}})^t \cdot b^{2^s t} = (-1)(-1) (\bmod p) \Rightarrow (a^{2^{s-2}} \cdot b^{2^{s-1}} \cdot b^{2^s})^t = 1 (\bmod p).$$

Извлекая квадратный корень из левой части получаем опять два варианта

$$\begin{cases} (a^{2^{s-3}} \cdot b^{2^{s-2}} \cdot b^{2^{s-1}})^t = +1 (\bmod p) \\ (a^{2^{s-3}} \cdot b^{2^{s-2}} \cdot b^{2^{s-1}})^t = -1 (\bmod p) \end{cases}$$ и т.д.

Пока не исчерпаются двойки в степени 2^s мы будем либо извлекать квадратный корень, когда правая часть будет равна «+1». Либо, в случае, если справа получается «-1» умножать равенство на $b^{2^s t} = -1 (\bmod p)$ и снова извлекать квадратный корень.

Поскольку на каждом шаге показатель степени «s» уменьшается на единицу, то на s-м шаге у нас получится один из двух вариантов.

Если очень повезет и «-1» ни разу не встретится, то у нас получится

$a^t = 1 (\bmod p) \Rightarrow a^{t+1} = a (\bmod p)$, и т.к. t – нечетное число

Ответ. $\sqrt{a} = \pm a^{\frac{t+1}{2}}$

Если же «-1» хотя бы один раз встретятся, то получится

$a^t \cdot b^{2m} = 1 (\bmod p) \Rightarrow a^{t+1} \cdot b^{2m} = a (\bmod p)$,

Ответ. $\sqrt{a} = \pm a^{\frac{t+1}{2}} \cdot b^m$, где m – некоторое натуральное число.

На практике, этот разветвляющийся алгоритм нужно применять с конца.

А именно, быстрым возведением в степень найти все встречающиеся в алгоритме степени элементов «a» и «b».

А встретиться могут только степени $a^t, a^{2t}, a^{2^2 t}, ..., a^{2^{s-1} t} (\mod p)$ и $b^t, b^{2t}, b^{2^2 t}, ..., b^{2^{s-1} t} (\mod p)$, а также известно, что $a^{2^s t} = 1(\mod p)$, $b^{2^s t} = -1(\mod p)$.

И имея все эти значения применять алгоритм.

ПРИМЕР ПРИМЕНЕНИЯ АЛГОРИТМА

Решим уравнение $x^2 \equiv 32(\mod 113)$.

Имеем, $p = 113 \Rightarrow \frac{p-1}{2} = 2^3 \cdot 7$, значит s = 3, t = 7.

Это плохой случай, $p \equiv 1(\mod 4)$

Проверим, извлекается ли из 32 квадратный корень по модулю 113. Используем квадратичный закон взаимности:

$$\left(\frac{32}{113}\right) = \left(\frac{4^2 \cdot 2}{113}\right) = \left(\frac{2}{113}\right) = (-1)^{\frac{113^2-1}{8}} = (-1)^{1596} = 1$$

Значит извлекается.

Найдем квадратичный невычет по модулю 113. Проверим, что подойдет b = 5:

$$\left(\frac{5}{113}\right) = (-1)^{\frac{5-1}{2} \cdot \frac{113-1}{2}} \left(\frac{113}{5}\right) = \left(\frac{3}{5}\right) = (-1)^{\frac{5-1}{2} \cdot \frac{3-1}{2}} \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = (-1)^{\frac{3^2-1}{8}} = -1.$$

Действительно, b = 5 – квадратичный невычет.

Вычислим требуемые для работы алгоритма степени элементов a = 32 и b = 5:

$a^7, a^{2 \cdot 7}, a^{2^2 \cdot 7} (\mod 113)$ и $b^7, b^{2 \cdot 7}, b^{2^2 \cdot 7} (\mod 113)$.

Так как $32 = 2^5$, то $32^7 = 2^{35}$ и $2^{35} = 2^3 \cdot 2^{32} (\mod 113)$. Последовательно вычисляем

$$2^1, 2^2 = 4, 2^4 = 16, 2^8 = 256 = 30(\mod 113), 2^{16} = 30^2 = -4(\mod 113), 2^{32} = 16(\mod 113).$$

Следовательно, $a^t = 32^7 = 2^{35} = 8 \cdot 16 = 15(\mod 113)$.

Аналогично, $b^t = 5^7$. Вычисляем последовательно

$5^7 = 5^1 \cdot 5^2 \cdot 5^4; 5^1 = 5, 5^2 = 25, 5^4 = 625 = 60(\mod 113)$ и в итоге

$5^7 = 5 \cdot 25 \cdot 60 = 12 \cdot 60(\mod 113) = 42(\mod 113)$.

Итак, $a^t = 15(\mod 113), b^t = 42(\mod 113)$. В итоге,

$\{a^7, a^{2 \cdot 7}, a^{2^2 \cdot 7}\} = \{15, 15^2, 15^4\} = \{15, -1, 1\}(\mod 113)$,

$\{b^7, b^{2 \cdot 7}, b^{2^2 \cdot 7}\} = \{42, 42^2, 42^4\} = \{42, 69, 15\}(\mod 113)$.

Теперь можно начать применять алгоритм.

ЗАДАНИЕ

Пусть a – количество букв в имени, b – фамилии, c – отчестве.

Задание для всех извлекается ли квадратный корень из числа $100a + 10b + c$ по модулю 2161.

Проверить извлекается ли квадратный корень из “F” по модулю «p» и если извлекается, то извлечь его

Группа 1. $F = 31$, $p = 331$; $F = 60$, $p = 109$.
Группа 2..$F = 32$, $p = 347$; $F = 87$, $p = 109$.
Группа 3..$F = 59$, $p = 359$; $F = 68$, $p = 101$.
Группа 4..$F = 42$, $p = 367$; $F = 95$, $p = 101$.
Группа 5. $F = 11$, $p = 379$; $F = 2$, $p = 97$.
Группа 6..$F = 34$, $p = 317$; $F = 72$, $p = 97$/