1 Квадратичные сравнения.

Замечание. Вопрос о разрешимости квадратичных сравнений был рассмотрен в Лекции 3. Там также были приведены некоторые утверждения и понятия используемые в этой лекции, такие как символ Якоби(Лежандра), квадратичный закон взаимности Гаусса, критерий Эйлера и другие.

Далее будем считать, что p - простое число отличное от 2.

Лемма 1. Сравнение $z^2 \equiv 1(mod\, p)$ имеет следующие решения: $z \equiv \pm 1(mod\, p)$.

Доказательство

Перепишем исходное сравнение в виде $(z-1)(z+1) \equiv 0(mod\, p)$. Отсюда следует, что либо $z \equiv 1(mod\, p)$ либо $z \equiv -1(mod\, p)$.

Замечание. Рассмотрим сравнение $x^2 \equiv a(mod\, p)$. Оно не имеет решений, если $\left(\frac{a}{p}\right) = -1$, имеет единственное решение($x \equiv 0(mod\, p)$), если $\left(\frac{a}{p}\right) = 0$. Если же $\left(\frac{a}{p}\right) = 1$, то оно имеет 2 решения.

Действительно, пусть $b^2 \equiv a(mod\, p)$. Тогда $(x-b)(x+b) \equiv 0(mod\, p)$, то есть $x \equiv \pm b(mod\, p)$.

Пример. Сравнение $x^2 \equiv 15(mod\, 5)$ имеет единственное решение по модулю 5: $x \equiv 0(mod\, 5)$.

Сравнение $x^2 \equiv 7(mod\, 19)$ не имеет решений, так как

$$\left(\frac{7}{19}\right) = (-1)^{\frac{7-1}{2}\frac{19-1}{2}} \left(\frac{19}{7}\right) = -\left(\frac{5}{7}\right) = \left(\frac{2}{5}\right) = -1.$$

Сравнение $x^2 \equiv 9(mod\, 19)$ имеет ровно два решения по модулю 19, так как

$$\left(\frac{9}{19}\right) = (-1)^{\frac{9-1}{2}\frac{19-1}{2}} \left(\frac{19}{9}\right) = \left(\frac{1}{19}\right) = 1.$$

Сравнение $x^2 \equiv 1(mod\, 19)$ имеет следующих два решения по модулю 19:$x \equiv \pm 1(mod\, 19)$.

Замечание. Если x_0 - решение сравнения $x^2 \equiv a(mod\, p)$, то $-x_0$ также решение этого сравнения.

Теорема 1. Пусть p - число вида $4k+3$, $k \in \mathbb{N}$. Тогда если сравнение $x^2 \equiv a(mod\, p)$ разрешимо, то оно имеет следующие решения по модулю p:

$$x \equiv \pm a^{\frac{p+1}{4}}(mod\, p).$$

Доказательство

Если $a \equiv 0(mod\, p)$, то это действительно верно. В противном случае оно имеет ровно два решения по модулю p. Заметим, что $\left(\pm a^{\frac{p+1}{4}}\right)^2 \equiv a^{\frac{p+1}{2}} \equiv a \cdot a^{\frac{p-1}{2}} \equiv a\left(\frac{a}{p}\right) \equiv a(mod\, p)$, что и требовалось доказать.

Пример. Ранее было показано, что сравнение $x^2 \equiv 9(mod\, 19)$ разрешимо. Используя данную теорему можно показать, что решениями являются $x \equiv \pm 16(mod\, 19)$.

Далее построим алгоритм нахождения одного из решений сравнения $x^2 \equiv a(mod\, p)$, где p - произвольное простое нечётное и $\left(\frac{a}{p}\right) = 1$. Отметим, что если найдено одно решение, то второе находится домножением первого на -1. Для начала введём некоторые определения.

Определение 1. Будем говорить, что число a является *корнем из единицы степени k по модулю p*, если $a^k \equiv 1(mod\, p)$.

Пример. 4 является корнем степени 2 из единицы по модулю 5, а 2 является корнем степени 4 из единицы по модулю 5.

Замечание. Нетрудно видеть, что k всегда кратно δ, где δ - показатель, которому a принадлежит по модулю p.

Определение 2. Будем говорить что, a является *первообразным корнем по модулю p степени k*, если для любого корня из единицы степени k существует j, такое что $a^j \equiv b(mod\, p)$.

Пример. Любой первообразный корень по модулю p является первообразным корнем степени $p-1$.

Далее будем считать, что n - квадратичный невычет по модулю p. Заметим, что $\varphi(p) = p-1$. Запишем $p-1$ в виде $p-1 = 2^\alpha s$, $(s,2) = 1$. Далее вычислим остаток n^s при делении на p, обозначим его за b. Так же вычислим остаток $a^{\frac{s+1}{2}}$ при делении на p и обозначим его за r.

Утверждение 1. $(r^2a^{-1})^{2^{\alpha-1}} \equiv 1(mod\, p)$, то есть $(r^2a^{-1})^{2^{\alpha-1}}$ - корень степени $2^{\alpha-1}$ из единицы по модулю p.

Доказательство

$$\left(r^2a^{-1}\right)^{2^{\alpha-1}} \equiv \left(a^s\right)^{2^{\alpha-1}} \equiv a^{2^{\alpha-1}s} \equiv a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \equiv 1(mod\, p).$$

Далее попытаемся найти такое число θ, что оно является корнем степени 2^α из единицы по модулю p и $x \equiv \theta r(mod\, p)$ - решение исходного сравнения.

Утверждение 2. b является первообразным корнем степени 2^α по модулю p.

Доказательство

Для начала покажем, что b - корень степени 2^α из единицы по модулю p. Действительно

$$b^{2^\alpha} \equiv n^{s2^\alpha} \equiv n^{p-1} \equiv 1(mod\, p).$$

Далее покажем, что b принадлежит показателю 2^α по модулю p. Предположим, что это не так. Пусть δ - показатель, которому b принадлежит по модулю p.

Разделим 2^α с остатком на δ: $2^\alpha = \delta q + r$, $0 \le r < \delta$. Если r отлично от 0, то получаем, что $1 \equiv b^{2^\alpha} \equiv b^{\delta q + r} \equiv \left(b^\delta\right)^q b^r \equiv b^r(mod\, p)$, но $r < \delta$. Получаем противоречие с минимальностью δ. Отсюда $\delta | 2^\alpha$.

Так как $\delta | 2^\alpha$ получаем, что $\delta = 2^k$, $0 \le k < \alpha$. Тогда $b^{2^{\alpha-1}} \equiv 1(mod\, p)$, но с другой стороны используя критерий Эйлера получаем, что

$$b^{2^{\alpha-1}} \equiv n^{s2^{\alpha-1}} \equiv n^{\frac{p-1}{2}} \equiv \left(\frac{n}{p}\right) \equiv -1(mod\, p).$$

Получаем противоречие, то есть $\delta = 2^\alpha$.

Найдём число корней степени 2^α из единицы по модулю p. Это тоже самое что найти число решений сравнения $x^{2^\alpha} \equiv 1(mod\, p)$ по модулю p. Число его решений равно числу решений сравнения $2^\alpha y \equiv 0(mod\, p-1)$ по модулю $p-1$, что в свою очередь равно $(2^\alpha, p-1) = (2^\alpha, 2^\alpha s) = 2^\alpha$. Таким образом число корней степени 2^α из единицы по модулю p равно 2^α.

Также заметим, что все числа b, $b^2, \ldots, b^{2^\alpha}$ - корни из единицы степени 2^α по модулю p. Все они не сравнимы по модулю p, так как $\delta = 2^\alpha$ и их число совпадает с числом различных корней из единицы степени 2^α по модулю p. Значит все эти числа представляют собой всё множество корней из единиц степени 2^α по модулю p. Таким образом, b является первообразным корнем степени 2^α по модулю p.

Таким образом $\theta \equiv b^j(mod\, p)$. Отметим, что можно считать, что $j < 2^\alpha$, так как $b^{2^\alpha} \equiv 1(mod\, p)$. Более того можно считать, что $j < 2^{\alpha-1}$. Действительно, пусть $j \geq 2^{\alpha-1}$. Тогда $j = 2^{\alpha-1} + j'$. Отметим, что $b^{2^{\alpha-1}} \equiv n^{2^{\alpha-1}s} \equiv n^{\frac{p-1}{2}} \equiv \left(\frac{n}{p}\right) \equiv -1(mod\, p)$. Но тогда

$$b^j r \equiv b^{2^{\alpha-1}+j'} r \equiv -b^{j'} r(mod\, p).$$

Нетрудно видеть, что, если $b^j r$ - корень, то и $b^{j'} r$ - корень. Так как цель алгоритма - нахождение одного корня, то можно считать $j < 2^{\alpha-1}$.

Исходя из того, что $b^{2^{\alpha-1}} \equiv -1(mod\, p)$ при изменении j на $2^{\alpha-1}$ мы получим новое значение j', которое нам даст второе решение исходного сравнения.

Далее запишем j в двоичной системе исчисления: $j = (\overline{j_{\alpha-2} j_{\alpha-3} \ldots j_1 j_0})_2 = j_0 + 2j_1 + \cdots + 2^{\alpha-3} j_{\alpha-3} + 2^{\alpha-2} j_{\alpha-2}$.

Предложим алгоритм нахождения j_i.

1)Возведём $r^2 a^{-1}$ в степень $2^{\alpha-2}$. Отметим, что полученный результат будет сравним с ± 1 по модулю p. Действительно $\left(r^2 a^{-1}\right)^{2^{\alpha-1}} \equiv 1(mod\, p)$ по Утверждению, далее возьмём $z = \left(r^2 a^{-1}\right)^{2^{\alpha-2}}$ и воспользуемся Леммой 1. Если мы получим 1, то возьмём $j_0 = 0$, иначе $j_0 = 1$. Отметим, что j_0 было выбрано так, что $(b^{j_0} r)^2 a^{-1}$ является корнем степени $2^{\alpha-2}$ из единицы по модулю p.

2)Пусть уже выбраны $j_0, j_1, \ldots, j_{k-1}$ так, что $\left(b^{j_0+2j_1+\cdots+2^{k-1}j_{k-1}} r\right)^2 a^{-1}$ является корнем степени $2^{\alpha-k-1}$ из единицы по модулю p. Возведём данное выражение в степень $2^{\alpha-k-2}$(полученный результат будет сравним с ± 1 по модулю p исходя из Леммы 1, это можно показать руссуждениями аналогичными рассуждениям в первом пункте). Если 1, то выбираем $j_k = 0$, иначе $j_k = 1$. Покажем, что выражение $\left(b^{j_0+2j_1+\cdots+2^{k-1}j_{k-1}+2^k j_k} r\right)^2 a^{-1}$ будет корнем степени $2^{\alpha-k-2}$ из единицы по модулю p:

$$\left(\left(b^{j_0+2j_1+\cdots+2^{k-1}j_{k-1}+2^k j_k} r\right)^2 a^{-1}\right)^{2^{\alpha-k-2}} \equiv$$

$$\equiv \left(\left(b^{j_0+2j_1+\cdots+2^{k-1}j_{k-1}}r\right)^2 a^{-1}\right)^{2^{\alpha-k-2}} \left(b^{2^{\alpha-1}j_k}\right) \equiv 1(mod\, p).$$

3)На $\alpha-2$ шаге получим, что

$$\left(b^{j_0+2j_1+\cdots+2^{\alpha-3}j_{\alpha-3}+2^{\alpha-2}j_{\alpha-2}}r\right)^2 a^{-1} \equiv 1(mod\, p).$$

То есть решение будет найдено.

Формализуем полученный алгоритм.

Алгоритм.

Дано: a, $\left(\frac{a}{p}\right)=1$, p - простое нечётное, n - квадратичный невычет по модулю p.

Требуется: Найти все решения сравнения $x^2 \equiv a(mod\, p)$ по модулю p.

Алгоритм:

1. Если $a \equiv 1(mod\, p)$, то $x \equiv \pm 1(mod\, p)$. Выход.
2. Если $p = 4k+3$, то $x \equiv \pm a^{\frac{p+1}{4}}(mod\, p)$. Выход.
3. Вычисляем a^{-1}.
4. Записываем $p-1$ в виде $p-1=2^\alpha s$, $(s,2)=1$.
5. Находим b - остаток n^s по модулю p.
6. Находим r - остаток $a^{\frac{s+1}{2}}$ по модулю p.
7. for $k = 0, 1, \ldots, \alpha-2$ do
8. Выбираем такое j_k, что $\left(b^{j_0+2j_1+\cdots+j_k2^k}\right)^2 a^{-1}$ является корнем степени $2^{\alpha-k-2}$(делаем это по схеме указанной в обосновании алгоритма).
9. $x_1 \equiv b^{j_0+2j_1+\cdots+j_{\alpha-2}2^\alpha}$, $x_2 \equiv -x_1(mod\, p)$. Выход.

Пример. Решить сравнение $x^2 \equiv 186(mod\, 401)$.

Решение

Отметим, что 401 является простым числом, так как не делится ни на одно из чисел 2, 3, 5, 7, 11, 13, 17, 19.

Заметим, что

$$\left(\frac{186}{401}\right) = \left(\frac{2}{401}\right)\left(\frac{93}{401}\right) = \left(\frac{93}{401}\right) = \left(\frac{29}{93}\right) = \left(\frac{6}{29}\right) = -\left(\frac{3}{29}\right) = -\left(\frac{2}{3}\right) = 1.$$

То есть 186 - квадратичный вычет по модулю 401.

Найдём квадратичный невычет по модулю 401. Нетрудно проверить, что это 3, так как

$$\left(\frac{3}{401}\right) = \left(\frac{401}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

Найдём a^{-1}. С помощью алгоритма Евклида получаем, что оно равно 235.

$p-1 = 2^4 \cdot 25$. $3^25 \equiv 268(mod\, 401)$, то есть $b = 268$. $168^{13} \equiv 103(mod\, 401)$, то есть $r = 103$.

$r^2a^{-1} \equiv 98(mod\, 401)$, $98^4 \equiv -1(mod\, 401)$. Согласно алгоритму получаем, что $j_0 = 1$.

$\left((br)^2a^{-1}\right)^2 \equiv \left((268 \cdot 103)^2 \cdot 235\right)^2 \equiv 1(mod\, 401)$. Таким образом $j_1 = 0$.

$(br)^2a^{-1} \equiv -1(mod\,401)$. Таким образом $j_2 = 1$.

Значит $j = j_0 + 2j_1 + 4j_2 = 5$. Таким образом $x \equiv b^5r \equiv 268^5 \cdot 103 \equiv 304(mod\,401)$. Второе решение $x \equiv 97(mod\,401)$.

Замечание. Рассмотрим произвольное квадратичное сравнение $ax^2 + bx + c \equiv 0(mod\,n)$, $a \not\equiv 0(mod\,n)$ по произвольному модулю. Пусть $n = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_r^{\alpha_r}$ - каноническое разложение n. Тогда данное сравнение равносильно системе сравнений $ax^2 + bx + c \equiv 0(mod\,p_i^{\alpha_i})$, $i \in \overline{1,r}$.

Далее рассмотрим сравнение $ax^2 + bx + c \equiv 0(mod\,p^\alpha)$, где p - простое. Исходя из рассуждений приведённых на прошлой лекции зная решения $ax^2 + bx + c \equiv 0(mod\,p)$ с помощью метода подъёма можно найти все решения исходного сравнения. Заметим, что решения сравнения $ax^2 + bx + c \equiv 0(mod\,2)$ могут быть найдены тривиальным перебором. Далее считаем, что $p \neq 2$. Тогда проведём некоторые преобразования:

$$ax^2+bx+c \equiv 0(mod\,p^\alpha) \Leftrightarrow a(x^2+2b(2a)^{-1}x+b^2(4a^2)^{-1})+(c-b^2(4a)^{-1}) \equiv 0(mod\,p) \Leftrightarrow$$

$$(x + b(2a)^{-1})^2 \equiv b^2(4a^2)^{-1} - ca^{-1}(mod\,p).$$

Воспользовавшись заменой $y \equiv x + b(2a)^{-1}(mod\,p)$, получим сравнение $y^2 \equiv b^2(4a^2)^{-1} - ca^{-1}(mod\,p)$б которое может быть решено с помощью приведённого ранее алгоритма.

Замечание. В лекции 3 были приведены формулы для нахождения всех решений сравнения $x^2 \equiv 1(mod\,p^\alpha)$, где p - произвольное простое, а также формулы для нахождения общего числа решений по модулю n сравнения $x^2 \equiv a(mod\,n)$.

Замечание. Данный алгоритм имеет сложность равную $O\left(\log^4 n\right)$. Это строго доказано в книге Н.Коблица Курс теории чисел и криптографии.

2 Задачи для самостоятельного решения.

Задача 1

a)Решить сравнение $x^2 \equiv 34(mod\,37)$.
b)Решить сравнение $x^2 + 2x + 7 \equiv 0(mod\,121)$.
c)Решить сравнение $x^2 \equiv 1(mod\,32)$.