Квадратичный закон взаимности Гаусса

Кристина Оганесян

В работе доказывается квадратичный закон взаимности Гаусса:

Теорема. Для простых нечётных p и q верно равенство $(\frac{p}{q})(\frac{q}{p})=(-1)^{(p-1)(q-1)/4}$

Этот результат дает простой способ решения сравнения $x^2 \equiv a\ (p)$ в целых числах. Доказательство следует плану, предложенному в сборнике «Математика в задачах», и основывается на критерии Эйлера и теореме Эйзенштейна.

Введём необходимые определения и докажем несколько лемм:

Определение 1: Остаток a≠0 называется квадратичным вычетом (квадратичным невычетом) по модулю p, если сравнение $x^2 \equiv a(p)$ разрешимо (неразрешимо).

Определение 2: Введём символ Лежандра $(\frac{a}{p})$:=1, если a является квадратичным вычетом по модулю p, $(\frac{a}{p})$:=-1 – если не является.

Лемма 1: Количество квадратичных вычетов по модулю p равно (p-1)/2.

Доказательство: Их не более (p-1)/2, так как $1^2 \equiv (-1)^2(p); 2^2 \equiv (-2)^2(p); \ldots; ((p-1)/2)^2 \equiv (-(p-1)/2)^2(p)$.

Предположим, что какие-то 2 из данных остатков совпадают. Тогда существуют такие $k^2 \equiv a(p), l^2 \equiv b(p)$, $k,l \leq (p-1)/2$, что $k^2-l^2 \vdots p$, а тогда одно из чисел (k-l) и (k+l) делится на p, но поскольку k≠l, то $0<(k-l),(k+l)<p$, противоречие! Значит, наше предположение неверно, и никакие 2 вычета не совпадают, => вычетов ровно (p-1)/2, а значит, невычетов p-1-(p-1)/2=(p-1)/2. Требуемое доказано.

Лемма 2: сравнение $ax^n+a_1x^{n-1}+\ldots+a_n \equiv 0(p)$, не все коэффициенты которого кратны p, не может иметь более, чем n решений

Доказательство: Предположим, что $ax^n+a_1x^{n-1}+\ldots+a_n \equiv 0(p)$ имеет хотя бы n+1 решение. Тогда $ax^n+a_1x^{n-1}+\ldots+a_n=a(x-x_1)(x-x_2)\ldots(x-x_n)+b(x-x_1)\ldots(x-x_{n-1})+c(x-x_1)\ldots(x-x_{n-2})+\ldots+k(x-x_1)+l$,где b – коэффициент при x^{n-1} многочлена $ax^n+a_1x^{n-1}+\ldots+a_n-a(x-x_1)(x-x_2)\ldots(x-x_n)$, c – коэффициент при x^{n-2} многочлена $ax^n+a_1x^{n-1}+\ldots+a_n-a(x-x_1)(x-x_2)\ldots(x-x_n)-b(x-x_1)\ldots(x-x_{n-1})$и т.д. Последовательно подставляя $x_1,x_2,\ldots,x_{n+1}$ вместо x получим, что l,k,…,c,b,a делятся на p, а значит, каждое из чисел $a_1,a_2,\ldots,a_n$ делится на p, как сумма чисел, кратных p.

Критерий Эйлера: $(\frac{a}{p}) \equiv a^{(p-1)/2} \pmod p$.

Доказательство: По малой теореме Ферма $a^{p-1} \equiv 1(p)$.

Тогда $(a^{(p-1)/2}-1)(a^{(p-1)/2}+1) \equiv 1(p)$. Значит, либо $a^{(p-1)/2} \equiv 1(p)$ (1), либо $a^{(p-1)/2} \equiv -1(p)$ (2).

Если a – вычет, то $\exists x: x^2 \equiv a(p)$. Тогда $a^{(p-1)/2} \equiv x^{p-1} \equiv 1(p)$ (по малой теореме Ферма), => все вычеты являются решениями сравнения (1), а так как по лемме 1 вычетов всего (p-1)/2, то, (сравнение $ax^n+a_1x^{n-1}+\ldots+a_n \equiv 0(p)$, не все коэффициенты которого кратны p, не может иметь более, чем n решений по лемме 2), других решений у данного сравнения нет, => невычеты являются решениями сравнения (2), и требуемое доказано.

Лемма 3a: Если число p=8k+5 простое, то $2^{4k+2} \equiv -1(p)$

Доказательство следует из цепочки сравнений:

$(8k+4)!=2^{4k+2}1*2*\ldots*(4k+2)*1*3*\ldots*(8k+3) \equiv 2^{4k+2}(4k+2)!(-1)^{2k+1}(8k+5-1)(8k+5-3)\ldots$

$(8k+5-(4k+1))*(4k+3)(4k+5)\ldots(8k+3)=2^{4k+2}(-1)(8k+4)!(\text{mod } p)$

Лемма 3b: Если число p=8k+1 простое, то $2^{4k} \equiv 1(p)$

Доказательство: $(-1)(8k)!=(-1)2^{4k}1*2*\ldots*4k*1*3*\ldots*(8k-1) \equiv (-1)2^{4k}(4k)!(-1)^{2k}(8k+1-1)(8k+1-3)\ldots$

$(8k+1-(4k-1))*(4k+1)(4k+3)\ldots(8k-1)=(-1)2^{4k}(-1)^{2k}(8k)!(\text{mod } p)$

Лемма 3c: Если число p=8k-1 простое, то $2^{4k-1} \equiv 1(p)$

Доказательство: $(-1)(8k-2)!=(-1)2^{4k-1}1*2*\ldots*(4k-1)*1*3*\ldots*(8k-3) \equiv (-1)2^{4k-1}(4k-1)!(-1)^{2k}(8k-1-1)(8k-1-3)\ldots(8k-1-(4k-1))*(4k+1)(4k+3)\ldots(8k-3)=(-1)2^{4k-1}(-1)^{2k}(8k-2)!(\text{mod } p)$

Лемма 3d: Если число p=8k+3 простое, то $2^{4k+1} \equiv -1(p)$

Доказательство: $(8k+2)!=2^{4k+1}1*2*\ldots*(4k+1)*1*3*\ldots*(8k+1) \equiv 2^{4k+1}(4k+1)!(-1)^{2k+1}(8k+3-1)(8k+3-3)\ldots(8k+3-(4k+1))*(4k+3)(4k+5)\ldots(8k+1)=2^{4k+1}(-1)^{2k+1}(8k+2)!(\text{mod } p)$

Докажем теперь основную лемму, на базе которой будем доказывать квадратичный закон взаимности:

Основная лемма: $(\frac{a}{p})$*= (-1) ^*$\sum_{n=1}^{\frac{p-1}{2}} \left[\frac{an}{p}\right]$

Доказательство: Из критерия Эйлера следует, что $(\frac{a}{p}) \equiv a^{(p-1)/2}$ (mod p). Покажем сначала, что $a^{(p-1)/2} \equiv (-1)^{\sum_{n=1}^{(p-1)/2}[\frac{2an}{p}]}$:

$a^{(p-1)/2}$ $(p-1)!=a*(2a)*\ldots*((p-1)a/2)*((p+1)/2)*((p+3)/2)*\ldots*(p-1)$

Никакая из попарных сумм или разностей чисел a,2a,…,(p-1)a/2 не может делиться на p, так как в противном случае для некоторых $1 \le k < m \le (p-1)/2$ либо $ka+ma \vdots p \Leftrightarrow (k+m)a \vdots p \Leftrightarrow (k+m) \vdots p$, что невозможно, так как $0<k+m<p$, либо $ma-ka \vdots p \Leftrightarrow a(m-k) \vdots p \Leftrightarrow m-k \vdots p$, что также невозможно в силу $0<m-k<p$. Тогда каждое из чисел a,2a,…,(p-1)a/2 имеет свой остаток при делении на p, равный ±r, где $0<r \le (p-1)/2$. Причём знак перед r положителен (отрицателен) у числа n такого, что [2n/p]-чётно (нечётно) ([2n/p]=[2[n/p]+2{n/p}]=2[n/p]+[2{n/p}]=2[n/p]+[2r/p]). Тогда

$a^{(p-1)/2}$ $(p-1)!=a*(2a)*\ldots*((p-1)a/2)*((p+1)/2)*((p+3)/2)*\ldots*(p-1) \equiv$

$1*(-1)^{[2a/p]}*2*(-1)^{[4a/p]}*\ldots*((p-1)/2)*(-1)^{[(p-1)a/p]}*((p+1)/2)*((p+3)/2)*\ldots*(p-1)=(p-1)!*(-1)^{\sum_{n=1}^{(p-1)/2}[\frac{an}{p}]}$.

Далее поскольку a и (p-a) разной чётности, то мы можем считать, что a – нечётно. Тогда

$(\frac{2a}{p})= (\frac{2a+2p}{p})= (\frac{4(a+p)/2}{p})= (\frac{(a+p)/2}{p})$=(-1) ^$\sum_{n=1}^{(p-1)/2}[\frac{(a+p)n}{p}]$= (-1) ^$(\sum_{n=1}^{\frac{p-1}{2}}\left[\frac{an}{p}\right]+\sum_{n=1}^{(p-1)/2} n)$

Отсюда $(\frac{2}{p})(\frac{a}{p})$= (-1) ^$(\sum_{n=1}^{\frac{p-1}{2}}\left[\frac{an}{p}\right]+\frac{p^2-1}{8})$

По лемме 3 и критерию Эйлера 2 является вычетом при p=8k±1 (при p=8k±1 $(p^2-1)/8=(64k^2+16k)/8=2(4k^2\pm k)$- чётно), и невычетом при p=8k±3 (при p=8k±3 $(p^2-1)/8=(64k^2\pm 48k+8)/8=2(4k^2+3k)+1$- нечётно). Тогда $(\frac{2}{p})$= (-1) ^$(\frac{p^2-1}{8})$. Отсюда $(\frac{a}{p})$= (-1) ^$\sum_{n=1}^{\frac{p-1}{2}}\left[\frac{an}{p}\right]$, ч.т.д.

***Доказательство квадратичного закона взаимности Гаусса*.** Теперь нетрудно доказать и сам квадратичный закон взаимности:

По основной лемме $(\frac{p}{q})$ $(\frac{q}{p})$= (-1)^$\sum_{x=1}^{(q-1)/2}[\frac{px}{q}]$+$\sum_{y=1}^{(p-1)/2}[\frac{qy}{p}]$. Для завершения доказательства достаточно доказать следующую лемму:

Лемма 4 (теорема Эйзенштейна): $\sum_{x=1}^{(q-1)/2}[\frac{px}{q}]$+$\sum_{y=1}^{(p-1)/2}[\frac{qy}{p}]$*=(p-1)(q-1)/4*

Доказательство: Рассмотрим прямоугольник 1≤x≤(p-1)/2, 1≤y≤(q-1)/2 и прямую y=qx/p (заметим, что на данной прямой нет ни одной целочисленной точки). $\sum_{x=1}^{(q-1)/2}[\frac{px}{q}]$ есть число целочисленных точек над данной прямой внутри данного прямоугольника, (так как число целочисленных точек над данной прямой с ординатой y есть [py/q]), а $\sum_{y=1}^{(p-1)/2}[\frac{qy}{p}]$ - число целочисленных точек под данной прямой внутри данного прямоугольника, (так как число целочисленных точек под данной прямой с абсциссой x есть [qx/p]). А всего целочисленных точек внутри данного прямоугольника (p-1)/2*(q-1)/2. Требуемое доказано.

Благодарности:

Хочется выразить огромную благодарность Михаилу Скопенкову за неоценимую помощь в подготовке работы, а также поблагодарить рецензента на данную работу за ценные советы.

Литература:

- Заславский А.А., Пермяков Д.А., Скопенков А.Б., Скопенков М.Б., Шаповалов А.В. (под ред.). «Математика в задачах. Сборник материалов выездных школ команды Москвы на Всероссийскую математическую олимпиаду». М.; МЦНМО, 2009.488 с.
- Виноградов И.М. «Основы теории чисел». М.-Л.; Гостехиздат, 1952. 180 с.