Квадратичный закон взаимности Гаусса. 22 июля

(Квадратичный закон взаимности Гаусса.) Для любых различных нечетных простых чисел p и q имеет место равенство $\left(\frac{q}{p}\right)\cdot\left(\frac{p}{q}\right)=(-1)^{\frac{(p-1)(q-1)}{4}}$.

Доказательство 1 было листочках про алгебраические числа.

Будем обозначать парой (a,b) такой остаток s при делении на pq, что выполнены $s\equiv a \pmod p$ и $s\equiv b \pmod q$.

Доказательство 2.

1. Рассмторим два подмножества остатков по модулю pq

$$S=\{(a,b): a=1,2,\dots,p-1; b=1,\dots\frac{q-1}{2}\}$$

$$T=\{(c\ mod\, p, c\ mod\, q): (c,pq)=1, c=1,2,\dots,\frac{pq-1}{2}\}.$$

Докажите, что произведения остатков в двух множествах либо совпадают, либо отличаются знаком.

2. Докажите, что

а) $\prod\limits_{(a,b)\in S}(a,b)\equiv((p-1)!^{\frac{q-1}{2}},((q-1)/2)!^{p-1}) \pmod{pq}$;

б) $\prod\limits_{c\in S}\equiv\frac{(1\cdot 2\dots\cdot p-1)\cdot(p+1\cdot\dots 2p-1)\dots(\dots\cdot\dots\cdot\frac{q-1}{2}p-1)(\dots\cdot\frac{q-1}{2}p+\frac{p-1}{2})}{q\cdot 2q\cdot\dots\frac{p-1}{2}q}\equiv$

$(p-1)!^{\frac{q-1}{2}}\left(\frac{q}{p}\right) \pmod p$

в) $\prod\limits_{c\in S}\equiv((p-1)!^{\frac{q-1}{2}}\left(\frac{q}{p}\right),(q-1)!^{\frac{p-1}{2}}\left(\frac{p}{q}\right)) \pmod{pq}$;

г) Выведите из этих сравнений квадратичный закон взаимности.

Доказательство 3.

3. Умножение всех элементов приведенной системы вычетов по нечетному простому модулю p на вычет $a\not\equiv 0 \pmod p$ производит в ней перестановку.

а) Докажите, что если a — квадратичный вычет по модулю p, то получившаяся подстановка четна.

б) Докажите, что если a — квадратичный невычет по модулю p, то она нечетна.

4. Рассмотрим пару отображений $f,g:\mathbb{Z}_{pq}\longrightarrow\mathbb{Z}_{pq}$, заданную следующими равенствами: $f(a,b)=a+pb$ и $g(a,b)=qa+b$.

а) Докажите, что f и g — перестановки на множестве $\mathbb{Z}_{pq}$.

б) Докажите, что перестановка f четна тогда и только тогда, когда $\left(\frac{p}{q}\right)=1$.

в) Рассмотрим перестановку $f\circ g^{-1}$ на множестве $\mathbb{Z}_{pq}$. Вычислите число инверсий этой перестановки.

г) **(Доказательство Золотарёва.)** При помощи предыдущих пунктов докажите квадратичный закон взаимности.

5. Пусть $x_1=1, y_1=100,\ x_{n+1}=x_n^{237}+y_n,\ y_{n+1}=y_n^{237}+x_n$. Докажите, что x_ny_n не делится на 239 ни при каком натуральном n.