О законѣ взаимности простыхъ чиселъ.

В. П. Алексѣевскаго.

Между доказательствами закона взаимности простыхъ чиселъ заслуживаютъ большого вниманія доказательства Эйзенштейна, Шеринга и Кронекера; не смотря на различіе ихъ по формѣ, можно установить между ними преемственную связь. Къ этому же кругу идей относится и предлагаемое доказательство, которое мнѣ кажется болѣе простымъ и естественнымъ.

Пусть p и q числа простыя, h — одно изъ чиселъ натуральнаго рода отъ 1 до $\frac{p-1}{2}$, g_h — наиболѣе подходящее цѣлое число къ дроби $\frac{hq}{p}$, такъ что остатокъ r отъ дѣленія hq на p можетъ быть и положительнымъ, и отрицательнымъ, но абсолютная его величина меньше $\frac{p}{2}$; слѣдовательно

$$-\frac{p}{2} < hq - g_h p < \frac{p}{2},$$

откуда

$$g_h = E\left(\frac{hq}{p} + \frac{1}{2}\right).$$

Наименьшее значеніе g_h можетъ быть нулемъ; наибольше получится, полагая $h = \frac{p-1}{2}$, и изъ тождества

$$\frac{(p-1)q}{2p} + \frac{1}{2} = \frac{q-1}{2} + \frac{2p-q}{2p}$$

видно, что maximum g_h не можетъ быть болѣе $\frac{q-1}{2}$.

Изъ равенства

$$hq = g_h p + r$$

слѣдуетъ, что знакъ остатка r одинаковъ со знакомъ $(hq - g_h p)$, вслѣдствіе чего предыдущее равенство можно представить въ видѣ сравненія

$$hq \equiv \varrho \cdot \operatorname{sgn}(hq - g_h p), \qquad (\text{mod. } p)$$

гдѣ $\varrho = |r|$, а $\operatorname{sgn}(hq - g_h p) = \pm 1$.

Если въ этомъ сравненіи дадимъ h всѣ значенія отъ 1 до $\frac{p-1}{2}$ и перемножимъ результаты, то, основываясь на извѣстныхъ предложеніяхъ, получимъ:

$$\left(\frac{q}{p}\right) = \operatorname{sgn} \prod_{h=1}^{\frac{p-1}{2}} (hq - g_h p).$$

Каковъ бы ни былъ знакъ разности

$$hq - g_h p,$$

произведеніе

$$[hq - (g_h - 1)p][hq - (g_h - 2)p] \ldots [hq - p]$$

состоитъ изъ положительныхъ множителей, когда $g_h > 1$, поэтому

$$\operatorname{sgn}(hq - g_h p) = \operatorname{sgn} \prod_{k=1}^{g_h} (hq - kp),$$

или, переставивъ члены бимоновъ во второй части,

$$\operatorname{sgn}(hq - g_h p) = (-1)^{g_h} \operatorname{sgn} \prod_{k=1}^{g_h} (kp - hq).$$

Число множителей второй части можно сдѣлать постояннымъ, какова-бы ни было h. Дѣйствительно, maximum $g_h \leq \frac{q-1}{2}$, и въ произведеніи

$$[(g_h + 1)p - hq] \ldots \left[\frac{q-1}{2} p - hq\right]$$

всѣ множители положительные, поэтому отъ присоединенія ихъ къ предыдущему произведенію знакъ его не нарушится; слѣдовательно, можно написать:

$$\operatorname{sgn}(hq - g_h p) = (-1)^{g_h} \operatorname{sgn} \prod_{k=1}^{\frac{q-1}{2}} (kp - hq).$$

Не трудно убѣдиться, что формула эта остается справедливой и въ случаяхъ $g_h = 0$ или 1.

Отсюда, на основаніи замѣченнаго выше, находимъ, что

$$\left(\frac{q}{p}\right) = (-1)^{\sum g_h} \prod_{k,h} (kp - hq),$$

$$k = 1, 2 \ldots \frac{q-1}{2}, \quad h = 1, 2, \ldots \frac{p-1}{2}.$$

Складывая равенства вида

$$hq = g_h p + r$$

находимъ

$$q \sum h = p \sum g_h + \sum r.$$

Такъ какъ въ числѣ остатковъ существуютъ положительные ϱ' и отрицательные $-\varrho''$, а сумма абсолютныхъ величинъ всѣхъ вычетовъ, какъ извѣстно, равна $\sum h$, то предыдущее равенство можно написать въ видѣ:

$$q \sum h = p \sum g_h + \sum h - 2 \sum \varrho'',$$

откуда слѣдуетъ, что

$$\sum g_h \equiv 0 \pmod 2$$

когда $q > 2$. Поэтому выраженіе для символа Лежандра принимаетъ видъ:

$$\left(\frac{q}{p}\right) = \operatorname{sgn} \prod_{k,h} (kp - hq).$$

Вслѣдствіе этого и

$$\left(\frac{p}{q}\right) = \operatorname{sgn} \prod_{k,h} (hq - kp).$$

Перемноживъ эти равенства и замѣтивъ, что соотвѣтственныя пары множителей правыхъ частей отличаются знакомъ, а число ихъ $\frac{p-1}{2} \cdot \frac{q-1}{2}$, получимъ:

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