Листок 13*

Короткое доказательство квадратичного закона взаимности Гаусса.

1. Алгебраическая форма китайской теоремы об остатках

В курсе элементарной теории чисел вы познакомились с китайской теоремой об остатках и квадратичным законом взаимности. В этом листке мы посмотрим на них с новой стороны. Автор берет на себя смелость утверждать, что изложенное здесь доказательство квадратичного закона взаимности является самым элементарным из всех известных элементарных доказательств[1]. Это доказательство принадлежит G. Rousseau[2]. Сначала нам потребуется несколько стандартных алгебраических определений и фактов.

Задача 1. Пусть R и S — кольца. Определим их *прямое произведение*. Как множество — это просто декартово произведение

$$R \times S = \{(r, s) : \ r \in R, \ s \in S\}.$$

Операции определим покомпонентно:

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2), \quad (r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2).$$

Проверьте, что получилось кольцо. Это нехитрая операция дает целую серию новых примеров колец.

Задача 2. Напомним, что изоморфизм колец — это биективный гомоморфизм между ними (см. Листок 11). Изоморфизм принято обозначать значком $\cong$.

(а) Пусть $n = mk$, где $(m, k) = 1$. Докажите, что отображение

$$\mathbb{Z}_n \to \mathbb{Z}_m \times \mathbb{Z}_k, \quad [a]_n \mapsto ([a]_m, [a]_k)$$

является изоморфизмом. Другими словами, при $(m, k) = 1$ имеем

$$\mathbb{Z}_m \times \mathbb{Z}_k \cong \mathbb{Z}_{mk}.$$

(б) В предположениях пункта (а), убедитесь, что

$$\mathbb{Z}_k^* \times \mathbb{Z}_m^* \cong \mathbb{Z}_{km}^*$$

Из Задачи 9а теперь легко извлекается алгебраическая форма китайской теоремы об остатках. А именно, если $n = n_1 \cdot \ldots \cdot n_k$, где $n_1, \ldots, n_k$ — попарно взаимно простые числа, то отображение

$$\pi : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}, \quad [a]_n \mapsto ([a]_{n_1}, \ldots, [a]_{n_k})$$

является изоморфизмом:

$$\mathbb{Z}_n \cong \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}.$$

[1] И, как и любое другое доказательство этого закона, оно не очень-то проливает свет на его природу.

[2] G. Rousseau, On the Quadratic Reciprocity Law, J. Austral. Math. Soc. Ser. A51 (1991), no. 3, 423–425. См. также http://mathoverflow.net/questions/1420/whats-the-best-proof-of-quadratic-reciprocity.

На элементарном языке это означает, что для любого набора $(r_1, \ldots, r_k)$ чисел с условием $0 \leq r_i < n_i$ найдется число x, которое при делении на n_i дает остаток r_i (сюръективность отображения π). Более того, если x_1, x_2 — два таких числа, то $x_1 \equiv x_2 \pmod{n}$ (инъективность отображения π).

2. Квадратичный закон взаимности Гаусса

2.1. **Квадратичные вычеты и символ Лежандра.** Если вы помните, что такое символ Лежандра и формула Эйлера для них — можете сразу переходить к доказательству закона Гаусса.

Рассмотрим сравнение

$$x^2 \equiv a \mod m, \quad (a, m) = 1. \tag{1}$$

Число a называется **квадратичным вычетом** по модулю m, если это сравнение имеет решение. В противном случае m называется **квадратичным невычетом**.

Пример 1. 4 является квадратичным вычетом по модулю 5 ($x = 3, 7$).

Далее мы будем рассматривать сравнения по простому *нечетному* модулю $m = p$:

$$x^2 \equiv a \mod p, \quad (a, p) = 1. \tag{$\star$}$$

Заметим, что если сравнение $f(x) \equiv 0 \mod p$ имеет более, чем $\deg f$ решений, то все коэффициенты f кратны p (эквивалентно, многочлен f тождественно равен 0 над полем $\mathbb{Z}/p\mathbb{Z}$). В частности, сравнение ($\star$) имеет не более двух решений.

Предложение 1. *Если a — квадратичный вычето по модулю p, то сравнение ($\star$) имеет ровно 2 решения.*

Доказательство. Если a — квадратичный вычет по простому модулю p, то наше сравнение имеет хотя бы одно решение $x \equiv x_0 \mod p$. Но тогда, ввиду $(-x_0)^2 = x_0^2$, то же сравнение имеет и второе решение $x \equiv -x_0 \mod p$. Это второе решение отлично от первого, так как из $x_0 \equiv -x_0 \mod p$ мы бы имели $2x_0 \equiv 0 \mod p$, что невозможно, ввиду $(2, p) = (x_0, p) = 1$. □

Предложение 2. *Приведенная система вычетов по модулю p состоит из $(p-1)/2$ квадратичных вычетов, сравнимых с числами*

$$1^2, \ 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$$

и $(p-1)/2$ невычетов.

Доказательство. Действительно, среди вычетов приведенной системы квадратичными являются те, и только те, которые сравнимы с квадратами чисел (приведенная система вычетов)

$$\pm 1, \ \pm 2, \ldots, \pm\frac{p-1}{2},$$

то есть как раз с теми числами, о которых идет речь в утвержденни. Заметим, что числа из утверждения не сравнимы между собой: если $k^2 \equiv l^2 \mod p$, то сравнению $l^2 \equiv x^2 \mod p$ удовлетворяет 4 числа $\pm k, \ \pm l$, вопреки сказанному ранее. □

Символ Лежандра для чисел a и p, таких что $(a, p) = 1$, определяется следующим образом:

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

Иногда дополнительно полагают символ Лежандра равным нулю, если a делится на p. Для вычисления символа Лежандра полезна следующая

Лемма 1 (Формула Эйлера). *При a не делящемся на p имеем*

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

Доказательство. Действительно, по теореме Ферма

$$a^{p-1} \equiv 1 \mod p, \quad \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \mod p.$$

Только один из сомножителей в левой части делится на p (иначе их разность 2 делилась бы на p). Значит, справедливо ровно одно из сравнений

$$(1)\ a^{\frac{p-1}{2}} \equiv 1 \mod p, \quad (2)\ a^{\frac{p-1}{2}} \equiv -1 \mod p.$$

Если a — квадратичный вычет по модулю p, то он удовлетворяет сравнению $a \equiv x^2 \mod p$ при некотором x и, следовательно, также получаемому из него возведением в степень $(p-1)/2$ сравнению (1). При этом квадратичными вычетами исчерпываются все решения этого сравнения (как мы видели выше, квадратичных вычетов ровно $(p-1)/2$), ибо оно не может иметь более чем $(p-1)/2$ решений. Следовательно, квадратичные невычеты удовлетворяют сравнению (2). □

Следствие 1. *Символ Лежандра удовлетворяет следующим свойствам:*

(1) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;

(2) *Если* $a \equiv b \mod p$, *то* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Пример 2. Имеем $5^14 \equiv 1 \mod 29$, поэтому $(5/29) = 1$ и 5 — квадратичный вычет по модулю 29. С другой стороны, $3^14 \equiv -1 \mod 29$, поэтому $(3/29) = -1$ и 3 — квадратичный невычет по модулю 29.

Теорема 1 (Квадратичный закон взаимности Гаусса). *Пусть p, q — различные нечетные простые числа. Тогда*

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

Доказательство. Рассмотрим группу $G = \mathbb{Z}_p^* \times \mathbb{Z}_q^* \cong \mathbb{Z}_{pq}^*$. Назовем половину элементов этой группы «хорошей», если для любого $x \in G$ этой половине принадлежит либо сам x, либо $-x$. Например, если элементы в группе $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$ упорядочены естественным образом, то «хорошей» оказывается первая половина. Для всей же группы G имеется как минимум три способа выделить «хорошую» половину:

(1) Взять первую половину элементов $\mathbb{Z}_p^*$ и всю $\mathbb{Z}_q^*$;
(2) Взять всю $\mathbb{Z}_p^*$ и первую половину элементов $\mathbb{Z}_q^*$;
(3) Взять первую половину элеметов $\mathbb{Z}_{pq}^*$.

Легко заметить, что в силу определения «хорошести», произведения всех элементов в каждой из этих половин отличается лишь знаком. Вычислим эти произведения как элементы группы $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$. Положив для краткости $P = (p-1)/2$, $Q = (q-1)/2$, получаем соответственно

(1) $\Pi_1 = (P!^{q-1}, (q-1)!^P)$;
(2) $\Pi_2 = ((p-1)!^Q, Q!^{p-1})$;
(3) $\Pi_3 = \left(\frac{(p-1)!^Q P!}{q^P P!}, \frac{(q-1)!^P Q!}{p^Q Q!}\right)$.

Первые два произведения считаются легко, покажем как посчитать третье. Имеем для первой координаты (то есть в $\mathbb{Z}_p^*$)

$$\prod_{\substack{k<pq/2\\(k,pq)=1}} k = \left(\prod_{\substack{k<pq/2\\p\nmid k}} k\right)\left(\prod_{\substack{k<pq/2\\q|k}} k\right)^{-1} =$$

$$\left(\prod_{0<k<p} k\right)\left(\prod_{p<k<2p} k\right)\dots\left(\prod_{(Q-1)p<k<Qp} k\right)\left(\prod_{Qp<k<pq/2} k\right)\left(\prod_{\substack{k<pq/2\\q|k}} k\right)^{-1}$$

$$= \frac{(p-1)!^Q P!}{q^P P!}$$

Для второй координаты — симметрично. По формуле Эйлера, $q^P = (q/p)$, $p^Q = (p/q)$. Сравнивая вторые координаты произведений, видим, что Π_1 отличается от Π_3 знаком (p/q). Аналогично, Π_2 отличается от Π_3 знаком (q/p). Значит, Π_1 отличается от Π_2 знаком $(p/q)(q/p)$. С другой стороны, эти два произведения отличаются тем, что мы у PQ множителей поменяли знак.

□

Пример 3. Вычислим $(79/101)$. Из закона взаимности, $(79/101) = (101/79)$. Но $101 \equiv 22 \mod 79$, поэтому $(101/79) = (22/79) = (2/79)(11/79)$. По закону взаимности, $(11/79) = -(79/11) = -(2/11)$. Последний символ уже легко вычисляется по формуле Эйлера: $(2/11) = -1$, поэтому $(11/79) = 1$.
Далее, $(2/79) = (-77/79) = (-1/79)(7/79)(11/79)$. По формуле Эйлера, $(-1/79) \equiv 1 \mod 79$, поэтому $(-1/79) = 1$. По закону взаимности, $(7/79) = (79/7) = (2/7) = 1$ (последнее равенство — формула Эйлера). Итого, получаем $(79/101) = 1$, то есть 79 — квадратичный вычет по модулю 101. На самом деле, $33^2 \equiv 79 \mod 101$.

Замечание 2.1. В этом примере мы пользовались тривиальным наблюдением $\left(\frac{2}{p}\right) = \left(\frac{2-p}{p}\right)$. На самом деле, можно показать, что

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