## 10. Квадратичный закон взаимности: доказательство. 6 октября

**Определение.** Обозначим через $(\mathbb{Z}/m\mathbb{Z})\times(\mathbb{Z}/n\mathbb{Z})$ кольцо, элементами которого являются пары $(a,b)$, $a\in\mathbb{Z}/m\mathbb{Z}$, $b\in\mathbb{Z}/n\mathbb{Z}$ с покоординатным сложением и умножением: $(a_1,b_1)\cdot(a_2,b_2)=(a_1\cdot a_2, b_1\cdot b_2)$ и $(a_1,b_1)+$ $+(a_2,b_2)=(a_1+a_2,b_1+b_2)$.

**Китайская теорема об остатках.** Пусть $(p,q)=1$. Отображение $\alpha\colon(\mathbb{Z}/pq\mathbb{Z})\to(\mathbb{Z}/p\mathbb{Z})\times(\mathbb{Z}/q\mathbb{Z})$, $\alpha\colon a\mapsto(a \bmod p, a \bmod q)$ задаёт изоморфизм колец, т.е. является биекцией и сохраняет операции: $\alpha(a\cdot b)=$ $=\alpha(a)\cdot\alpha(b)$, $\alpha(a+b)=\alpha(a)+\alpha(b)$.

**$0_1$.** Убедитесь, что $\alpha(0)=(0,0)$, $\alpha(1)=(1,1)$, $\alpha(-a)=-\alpha(a)$.

**$0_2$.** Напомним, что через $(\mathbb{Z}/k\mathbb{Z})^\times$ обозначается мультипликативная группа вычетов, взаимно простых с $k$. Поймите, что $\alpha$ задает изоморфизм групп $(\mathbb{Z}/pq\mathbb{Z})^\times$ и $(\mathbb{Z}/p\mathbb{Z})^\times\times(\mathbb{Z}/q\mathbb{Z})^\times$ (с покоординатным умножением).

**1.** Пусть $p$ и $q$ — различные нечётные простые числа. Будем говорить, что некоторое подмножество $X$ множества $(\mathbb{Z}/pq\mathbb{Z})^\times$ удовлетворяет условию (*), если из $a$ и $-a$ в $X$ лежит ровно одно.

a) Пусть $X$ и $Y$ удовлетворяют условию (*). Докажите, что $\prod_{x\in X}x=$ $=\pm\prod_{y\in Y}y$ и $\prod_{x\in X}\alpha(x)=\pm\prod_{y\in Y}\alpha(y)$.

b) Пусть $X$ — такое подмножество $(\mathbb{Z}/pq\mathbb{Z})^\times$, что $\alpha(X)$ состоит из всевозможных пар $(a,b)$ таких, что $1\leqslant a\leqslant p-1$, $1\leqslant b\leqslant\frac{q-1}{2}$. Докажите, что $X$ удовлетворяет условию (*) и вычислите $\prod_{x\in X}\alpha(x)$ (т.е. вычислите, с чем сравнимо $\prod_{x\in X}x$ по модулям $p$ и $q$).

c) Пусть $Z=\left\{z\in(\mathbb{Z}/pq\mathbb{Z})^\times \mid 1\leqslant z\leqslant\frac{pq-1}{2}\right\}$. Докажите, что $Z$ удовлетворяет условию (*) и вычислите $\prod_{z\in Z}\alpha(z)$.

d) **(квадратичный закон взаимности, 1796)** Сравнивая результаты пунктов a), b) и c) докажите, что

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



*Октябрьская математическая программа, 11А «Сириус», октябрь 2021*

## 10. Квадратичный закон взаимности: доказательство. 6 октября

**Определение.** Обозначим через $(\mathbb{Z}/m\mathbb{Z})\times(\mathbb{Z}/n\mathbb{Z})$ кольцо, элементами которого являются пары $(a,b)$, $a\in\mathbb{Z}/m\mathbb{Z}$, $b\in\mathbb{Z}/n\mathbb{Z}$ с покоординатным сложением и умножением: $(a_1,b_1)\cdot(a_2,b_2)=(a_1\cdot a_2, b_1\cdot b_2)$ и $(a_1,b_1)+$ $+(a_2,b_2)=(a_1+a_2,b_1+b_2)$.

**Китайская теорема об остатках.** Пусть $(p,q)=1$. Отображение $\alpha\colon(\mathbb{Z}/pq\mathbb{Z})\to(\mathbb{Z}/p\mathbb{Z})\times(\mathbb{Z}/q\mathbb{Z})$, $\alpha\colon a\mapsto(a \bmod p, a \bmod q)$ задаёт изоморфизм колец, т.е. является биекцией и сохраняет операции: $\alpha(a\cdot b)=$ $=\alpha(a)\cdot\alpha(b)$, $\alpha(a+b)=\alpha(a)+\alpha(b)$.

**$0_1$.** Убедитесь, что $\alpha(0)=(0,0)$, $\alpha(1)=(1,1)$, $\alpha(-a)=-\alpha(a)$.

**$0_2$.** Напомним, что через $(\mathbb{Z}/k\mathbb{Z})^\times$ обозначается мультипликативная группа вычетов, взаимно простых с $k$. Поймите, что $\alpha$ задает изоморфизм групп $(\mathbb{Z}/pq\mathbb{Z})^\times$ и $(\mathbb{Z}/p\mathbb{Z})^\times\times(\mathbb{Z}/q\mathbb{Z})^\times$ (с покоординатным умножением).

**1.** Пусть $p$ и $q$ — различные нечётные простые числа. Будем говорить, что некоторое подмножество $X$ множества $(\mathbb{Z}/pq\mathbb{Z})^\times$ удовлетворяет условию (*), если из $a$ и $-a$ в $X$ лежит ровно одно.

a) Пусть $X$ и $Y$ удовлетворяют условию (*). Докажите, что $\prod_{x\in X}x=$ $=\pm\prod_{y\in Y}y$ и $\prod_{x\in X}\alpha(x)=\pm\prod_{y\in Y}\alpha(y)$.

b) Пусть $X$ — такое подмножество $(\mathbb{Z}/pq\mathbb{Z})^\times$, что $\alpha(X)$ состоит из всевозможных пар $(a,b)$ таких, что $1\leqslant a\leqslant p-1$, $1\leqslant b\leqslant\frac{q-1}{2}$. Докажите, что $X$ удовлетворяет условию (*) и вычислите $\prod_{x\in X}\alpha(x)$ (т.е. вычислите, с чем сравнимо $\prod_{x\in X}x$ по модулям $p$ и $q$).

c) Пусть $Z=\left\{z\in(\mathbb{Z}/pq\mathbb{Z})^\times \mid 1\leqslant z\leqslant\frac{pq-1}{2}\right\}$. Докажите, что $Z$ удовлетворяет условию (*) и вычислите $\prod_{z\in Z}\alpha(z)$.

d) **(квадратичный закон взаимности, 1796)** Сравнивая результаты пунктов a), b) и c) докажите, что

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

*Не забудьте перевернуть листочек!*

**Определение.** Пусть $n = p_1 \cdot p_2 \cdot \ldots \cdot p_s$ — нечетное число. *Символом Якоби* $\left(\frac{a}{n}\right)$ называется произведение

$$\left(\frac{a}{p_1}\right) \cdot \left(\frac{a}{p_2}\right) \cdot \ldots \cdot \left(\frac{a}{p_s}\right).$$

**$0_3$.** Поймите, что если $\left(\frac{a}{n}\right) = -1$, то $a$ является квадратичным невычетом по модулю $n$. Верно ли обратное утверждение?

**$0_4$.** Докажите, что $\left(\frac{-1}{4k+3}\right) = -1$.

**2.** Докажите, что если $m$ и $n$ — нечетные взаимно простые числа, то

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

**3.** Пусть $p$ — нечётное простое число. Докажите, что $\left(\frac{2}{p}\right) = 1$ если и только если $p \equiv \pm 1 \pmod 8$.

**$0_5$.** Вычислите $\left(\frac{219}{383}\right)$.

**Определение.** Пусть $n = p_1 \cdot p_2 \cdot \ldots \cdot p_s$ — нечетное число. *Символом Якоби* $\left(\frac{a}{n}\right)$ называется произведение

$$\left(\frac{a}{p_1}\right) \cdot \left(\frac{a}{p_2}\right) \cdot \ldots \cdot \left(\frac{a}{p_s}\right).$$

**$0_3$.** Поймите, что если $\left(\frac{a}{n}\right) = -1$, то $a$ является квадратичным невычетом по модулю $n$. Верно ли обратное утверждение?

**$0_4$.** Докажите, что $\left(\frac{-1}{4k+3}\right) = -1$.

**2.** Докажите, что если $m$ и $n$ — нечетные взаимно простые числа, то

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

**3.** Пусть $p$ — нечётное простое число. Докажите, что $\left(\frac{2}{p}\right) = 1$ если и только если $p \equiv \pm 1 \pmod 8$.

**$0_5$.** Вычислите $\left(\frac{219}{383}\right)$.