Углы в плоскости над конечным простым полем

А. Р. Исмаилов*

С вещественными числами связана евклидова геометрия. Возникает вопрос: какая геометрия будет связана с остатками по простому модулю? В этой ситуации аналогом плоскости служит $\mathbb{Z}_p \times \mathbb{Z}_p$. Прямые можно определить как решения уравнения вида

$$ax + by + c \equiv 0 \pmod{p}.$$

Аналогично евклидову случаю, прямые могут быть параллельны и перпендикулярны. В классическом случае (плоскость $\mathbb{R}^2$) естественно определяется понятие угла между прямыми. В $\mathbb{Z}_p \times \mathbb{Z}_p$ возникает аналогичный вопрос: как ввести углы? Единичная окружность задаётся уравнением

$$x^2 + y^2 \equiv 1 \pmod{p}.$$

Оказывается, за множеством его решений скрывается структура, которая чем-то напоминает обычные углы. Можно даже определить синусы и косинусы. Однако что с этим дальше делать? Казалось бы, просто получается аналогичная тригонометрия.

Возьмём угол в 45°:

$$\sin \frac{\pi}{4} = \cos \frac{\pi}{4} = \frac{1}{\sqrt{2}}.$$

Если в нашей структуре углов по модулю p имеется аналог угла в 45 градусов, то $\sqrt{2}$ будет среди остатков по модулю p, и наоборот. Получается критерий того, будет ли число 2 квадратичным вычетом по модулю p.

Отсюда начинает раскрываться основная тема нашей статьи: как можно использовать структуру, возникающую в поле остатков $\mathbb{Z}_p$, чтобы получать факты, выходящие за рамки обычной тригонометрии?

* На момент написания статьи автор был учеником школы «Воробьёвы горы», г. Москва.

§ 1. Введение

Мы начнём с построения аналога обычных углов над полем $\mathbb{Z}_p$ и затем тригонометрических функций над $\mathbb{Z}_p$ (сами углы не будут принадлежать $\mathbb{Z}_p$). Проводя аналогию между тем, что происходит с обычными углами, и тем, что происходит с углами нового вида, мы докажем в § 4 ряд фактов: наличие $\sqrt{2}$, $\sqrt{3}$ по модулю p, несоизмеримость некоторых углов с 2π. В дальнейшем мы сможем показать, что существует бесконечно много простых чисел вида $kn-1$, используя аналог многочлена деления круга (теорема 3, следствие 1).

§ 2. Углы

Пусть $p > 2$ — простое число. В этом разделе мы будем работать в поле $\mathbb{Z}_p$. Чтобы ввести углы, рассмотрим решения уравнения $x^2+y^2=1$, которые образуют единичную окружность.

Случай $p = 4n + 1$. В этом случае имеются два квадратных корня из -1, которые мы обозначим j и $-j$. Тогда

$$x^2 + y^2 = 1 \quad \Leftrightarrow \quad (x + jy)(x - jy) = 1.$$

Заметим, что существует биекция между упорядоченными парами $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ и упорядоченными парами $(a, b) \in \mathbb{Z}_p \times \mathbb{Z}_p$, где (x, y) сопоставляется точке $(a, b) = (x + jy, x - jy)$. Действительно, (x, y) восстанавливается по (a, b) как $\left(\frac{a+b}{2}, \frac{a-b}{2j}\right)$. Назовём последнее выражение прообразом (a, b). Заключаем, что пары (x, y), являющиеся решениями уравнения $x^2 + y^2 = 1$, биективно соответствуют парам (a, b), у которых $ab = 1$, или, другими словами, парам вида $(a, 1/a)$ при $a \neq 0$. Поэтому уравнение $x^2 + y^2 = 1$ имеет ровно $p - 1$ решение.

Две пары (a_1, b_1) и (a_2, b_2) можно поэлементно перемножить:

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1a_2, b_1b_2).$$

Такое произведение соответствует «комплексному» умножению их прообразов (x_1, y_1) и (x_2, y_2) соответственно:

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1),$$

результатом которого будет прообраз пары (a_1a_2, b_1b_2). Последнее утверждение следует из тождеств

$$a_1a_2 = (x_1 + jy_1)(x_2 + jy_2), b_1b_2 = (x_1 - jy_1)(x_2 - jy_2).$$

Эти равенства можно переписать как

$$a_1a_2 = (x_1x_2 - y_1y_2) + j(x_1y_2 + x_2y_1),$$
$$b_1b_2 = (x_1x_2 - y_1y_2) - j(x_1y_2 + x_2y_1).$$

При рассмотрении образов, т. е. пар (a, b), под умножением будем понимать поэлементное умножение. При рассмотрении прообразов, т. е. пар (x, y), под умножением будем подразумевать «комплексное» умножение. Назовём $(x, -y)$ парой, сопряжённой паре (x, y); если образ первой — это (a, b), то образом второй будет (b, a).

Все ненулевые пары (a, b), где $a \neq 0$ и $b \neq 0$, образуют группу по умножению. Пары (a, b) с $ab = 1$ образуют её подгруппу; поскольку они имеют вид $(a, 1/a)$, подгруппа изоморфна мультипликативной группе $(\mathbb{Z}_p)^*$, которая, в свою очередь, изоморфна циклической группе C_{p-1}, т. е. группе $(\mathbb{Z}_{p-1}, +)$ по сложению. Тогда решения (x, y) уравнения $x^2 + y^2 = 1$ образуют группу по «комплексному» умножению, изоморфную $\mathbb{Z}_{p-1}$.

Случай $p = 4n + 3$. Многочлен $x^2 + 1$ неприводим над полем $\mathbb{Z}_p$. Его полем разложения является $\mathbb{Z}_p(i)$, где через i мы обозначаем корень из поля разложения (другим корнем будет $-i$). Зададим сопряжение как операцию, сопоставляющую элементу $z = x + iy \in \mathbb{Z}_p(i)$ элемент $\bar{z} = x - iy$, где $x, y \in \mathbb{Z}_p$. Сопряжение является автоморфизмом поля $\mathbb{Z}_p(i)$. Пусть норма элемента z имеет вид

$$N(z) = z\bar{z} = x^2 + y^2 \in \mathbb{Z}_p.$$

У нас $p \equiv 3 \pmod 4$, и по теореме Жирара $N(z) = 0 \Leftrightarrow z = 0$. Также $N(z_1z_2) = N(z_1)N(z_2)$. Следовательно, N — это гомоморфизм из группы $\mathbb{Z}_p(i)^*$ в группу $\mathbb{Z}_p^*$. Мощность множества $A = \{x^2 \mid x \in \mathbb{Z}_p\}$ равна $(p+1)/2$. По принципу Дирихле множество $A + A$ содержит все остатки по модулю p: для любого $r \in \mathbb{Z}_p$ множество $r - A$ должно иметь хотя бы один общий элемент с A. Образ отображения N — это множество $\mathrm{Im}(N) = \mathbb{Z}_p^*$. Ядром отображения N является множество $\ker(N) = \{z \mid N(z) = 1\}$. Из изоморфизма $\mathrm{Im}(N) \cong \mathbb{Z}_p(i)^*/\ker(N)$ (первая теорема об изоморфизме) следует равенство

$$|\ker(N)| = |\mathbb{Z}_p(i)^*| : |\mathrm{Im}(N)| = |\mathbb{Z}_p(i) \setminus \{0\}| : |\mathbb{Z}_p^*| = \frac{p^2 - 1}{p - 1} = p + 1.$$

Так как ядро отображения N — это подгруппа из $p + 1$ элемента в группе $\mathbb{Z}_p(i)^*$, согласно теореме Лагранжа получаем $z^{p+1} = 1$ для всякого $z \in N$. Однако многочлен $z^{p+1} - 1$ имеет не более $p + 1$ корней, поэтому

$$N(z) = 1 \quad \Leftrightarrow \quad z^{p+1} = 1.$$

Следовательно, имеет место изоморфизм $\ker(N) \cong \mathbb{Z}_{p+1}$, где $\mathbb{Z}_{p+1}$ понимается как группа по сложению.

Количество решений уравнения $N(z) = l$ равно $p+1$ при $l \in \mathbb{Z}_p \setminus \{0\}$, так как N является гомоморфизмом из $\mathbb{Z}_p(i)^*$ в $\mathbb{Z}_p^*$ с образом $\mathbb{Z}_p \setminus \{0\}$ и мощностью ядра $|\ker(N)| = p+1$. Поэтому существует всего $2(p+1)$ чисел z с нормой $N(z) = \pm 1$. Они тоже образуют подгруппу в $\mathbb{Z}_p(i)^*$. Это группа по умножению, изоморфная группе $\mathbb{Z}_{2(p+1)}$ по сложению.

Вводим углы. С этого момента выражение $p \pm 1$ будет совмещать оба случая: в случае $p = 4n+1$ будет подразумеваться число $p-1$, а в случае $p = 4n+3$ — число $p+1$. В обоих случаях изоморфизм, установленный между $\mathbb{Z}_{p\pm1}$ и группой решений уравнения $x^2 + y^2 = 1$, сопоставляет остаткам по модулю $p \pm 1$ решения уравнения $x^2 + y^2 = 1$. Решение $(1, 0)$ соответствует остатку 0. Решению $(-1, 0)$ соответствует $(p \pm 1)/2$, так как это элементы порядка 2 в своих группах. Паре решений $(0, 1)$ и $(0, -1)$ соответствует либо $(p \pm 1)/4$, $-(p \pm 1)/4$, либо $-(p \pm 1)/4$, $(p \pm 1)/4$, так как это элементы порядка 4. Заметим, что мы можем заменить наш изоморфизм на другой так, что если остатку r соответствует какое-то решение $x^2 + y^2 = 1$ при исходном изоморфизме, то остатку $-r$ соответствует это же решение при новом изоморфизме. Поэтому можно выбрать изоморфизм, который отображает $(p \pm 1)/4$ в $(0, 1)$ и $-(p \pm 1)/4$ в $(0, -1)$. Итак, определим *негеометрические углы* как остатки по модулю $\mathbb{Z}_{p\pm1}$, причём этим остаткам в результате некоторого изоморфизма, удовлетворяющего нашим условиям (отображающего $(p \pm 1)/4$ в $(0, 1)$ и $-(p \pm 1)/4$ в $(0, -1)$), будут сопоставляться решения уравнения $x^2 + y^2 = 1$.

В случае $p = 4n+3$ мы можем дополнительно ввести то, что здесь будет называться *геометрическими углами*. Подгруппа по умножению, состоящая из чисел z с нормой $N(z) = \pm 1$, изоморфна группе $\mathbb{Z}_{2(p+1)}$ по сложению, из чего следует, что её элементы являются решениями уравнения $z^{2(p+1)} = 1$. Заметим, что верно равенство $N(z^2) = N(z)^2 = (\pm 1)^2 = 1$, поэтому чётные остатки являются прообразами чисел с нормой 1. Но тогда нечётные остатки являются прообразами элементов с нормой -1. Рассуждая аналогично, придём к тому, что решение $(1, 0)$ уравнения $x^2 + y^2 = \pm 1$ соответствует нулевому остатку, а решение $(-1, 0)$ — остатку $p+1$. Как и в предыдущем случае, можно считать, что остатки $(p+1)/2$ и $-(p+1)/2$ сопоставлены решениям $(0, 1)$ и $(0, -1)$ соответственно. Итак, определим геометрические углы как остатки по модулю $2(p+1)$, причём этим остаткам при некотором изоморфизме, удовлетворяющем нашим условиям (отображающем

$(p+1)/2$ в $(0,1)$ и $-(p+1)/2$ в $(0,-1)$), будут сопоставляться решения уравнения $x^2+y^2=\pm 1$.

§ 3. Модулярные синусы и косинусы

Теперь введём синус и косинус. Как для геометрических, так и для негеометрических углов определим косинус угла как x, а синус угла как y из сопоставляемой этому углу пары (x,y). Обозначим их через $\cos_p$ и $\sin_p$ соответственно. Для негеометрических углов получим набор значений:

α	0	$\frac{p\pm 1}{4}$	$\frac{p\pm 1}{2}$	$3\frac{p\pm 1}{4}$
$\sin_p \alpha$	0	1	0	-1
$\cos_p \alpha$	1	0	-1	0

Остатки α и $-\alpha$ соответствуют паре взаимно обратных элементов из группы решений уравнения $x^2+y^2=1$, но тогда они сопряжены друг с другом, так как в обоих случаях произведение элемента группы решений $x^2+y^2=1$ на его сопряжённый даёт единичный элемент. Поэтому $\cos_p \alpha = \cos_p(-\alpha)$ и $\sin_p(-\alpha) = -\sin_p \alpha$. Сумма углов α и β как остатков соответствует умножению соответствующих элементов группы решений, но тогда, рассмотрев формулу для этого умножения, мы получим формулы

$$\cos_p(\alpha+\beta) = \cos_p \alpha \cos_p \beta - \sin_p \alpha \sin_p \beta,$$
$$\sin_p(\alpha+\beta) = \sin_p \alpha \cos_p \beta + \sin_p \beta \cos_p \alpha.$$

Если мы заменим β на $-\beta$, то получим формулы синуса и косинуса разности. Прибавление $(p\pm 1)/2$ к углу соответствует умножению всех решений на элемент $(-1,0)$:

$$\cos_p\Big(\alpha+\frac{p\pm 1}{2}\Big) = -\cos_p \alpha, \quad \sin_p\Big(\alpha+\frac{p\pm 1}{2}\Big) = -\sin_p \alpha.$$

Если угол α соответствует паре (x,y), то угол $-\alpha$ соответствует паре $(x,-y)$. Прибавление числа $(p\pm 1)/4$ к углу $-\alpha$ сопоставляется умножению решения, которое соответствует этому углу, на $(0,1)$. Поэтому

$$\cos_p\Big(\frac{p\pm 1}{4}-\alpha\Big) = \sin_p \alpha \quad \text{и} \quad \sin_p\Big(\frac{p\pm 1}{4}-\alpha\Big) = \cos_p \alpha.$$

Синус равен 0 тогда и только тогда, когда косинус равен ± 1, т. е.

$$\sin_p \alpha = 0 \quad \Leftrightarrow \quad \alpha \in \Big\{0, \frac{p\pm 1}{2}\Big\}.$$

Аналогично

$$\cos_p \alpha = 0 \quad \Leftrightarrow \quad \alpha \in \left\{ \frac{p \pm 1}{4}, -\frac{p \pm 1}{4} \right\}.$$

Используя формулы суммы углов и равенство $\sin_p^2 \alpha + \cos_p^2 \alpha = 1$, можно получить стандартные тригонометрические тождества:

$$\sin_p 2\alpha = 2 \sin_p \alpha \cos_p \alpha, \qquad \cos_p 2\alpha = \cos_p^2 \alpha - \sin_p^2 \alpha,$$
$$\sin_p 3\alpha = -4 \sin_p^3 \alpha + 3 \sin_p \alpha, \quad \cos_p 3\alpha = 4 \cos_p^3 \alpha - 3 \cos_p \alpha.$$

Геометрические углы. Пусть $p \equiv 3 \pmod 4$. В отличие от геометрических углов, мы позволяем выражению $x^2 + y^2$ быть равным не только 1, но и -1 (подробнее на с. 70). Поэтому $z\bar{z} = \pm 1$. Тогда

$$\cos_p(-\alpha) = \pm \cos_p \alpha \quad \text{и} \quad \sin_p(-\alpha) = \mp \sin_p \alpha,$$

где знак зависит от того, на что надо умножить z, чтобы получить 1: на $\bar{z}$ или на $-\bar{z}$. Формулы синуса и косинуса суммы углов не меняются. Рассмотрим синус разности двух углов:

$$\sin_p(\alpha - \beta) = \sin_p \alpha \cos_p(-\beta) + \cos_p \alpha \sin_p(-\beta).$$

Мы уже знаем, что $1/z = \pm\bar{z}$. Поэтому при умножении угла на -1 противоположное значение примет либо только косинус, либо только синус (значения синуса в первом и косинуса во втором случае останутся неизменными). Следовательно, верна формула

$$\sin_p(\alpha - \beta) = \pm(\sin_p \alpha \cos_p \beta - \sin_p \beta \cos_p \alpha).$$

Аналогично в случае косинуса разности углов имеем

$$\cos_p(\alpha - \beta) = \sin_p \alpha \sin_p(-\beta) - \cos_p \alpha \cos_p(-\beta) =$$
$$= \pm(\cos_p \alpha \cos_p \beta + \sin_p \alpha \sin_p \beta).$$

Мы также знаем следующие значения косинуса и синуса:

α	0	$\frac{p+1}{2}$	$p+1$	$3\frac{p+1}{2}$
$\sin_p \alpha$	0	1	0	-1
$\cos_p \alpha$	1	0	-1	0

Следовательно,

$$\sin_p(\alpha + (p+1)) = -\sin_p \alpha \quad \text{и} \quad \cos_p(\alpha + (p+1)) = -\cos_p \alpha.$$

Также

$$\sin_p\left(\alpha + \frac{p+1}{2}\right) = \cos_p \alpha \quad \text{и} \quad \cos_p\left(\alpha + \frac{p+1}{2}\right) = -\sin_p \alpha.$$

Синус равен нулю при $\cos_p^2 \alpha = \pm 1$. Так как число -1 не является квадратичным вычетом по модулю p, мы заключаем, что $\cos_p \alpha = \pm 1$, и тогда $\sin_p \alpha = 0 \Leftrightarrow \alpha \in \{0, p+1\}$. Аналогичным образом для косинуса мы выводим следующее:

$$\cos_p \alpha = 0 \quad \Leftrightarrow \quad \alpha \in \Big\{\frac{p+1}{2}, -\frac{p+1}{2}\Big\}.$$

Геометрические и негеометрические углы представляют из себя объекты, которые мы будем называть углами по модулю p, хотя связанные с ними структуры, вообще говоря, отличаются от поля $\mathbb{Z}_p$.

§ 4. Некоторые приложения

Можно провести аналогию между обычными углами и углами по модулю p. Например, далее мы увидим, как с помощью аналогии между углами по модулю p и такими углами, как например $\pi/4$ и $\pi/3$, можно понять что-то про квадратичные вычеты. В этом разделе рассматриваются негеометрические углы. Покажем, как с их помощью можно получить некоторые известные факты.

Существование $\sqrt{2}$ по модулю p. Мы докажем, что число 2 — квадратичный вычет по простому модулю $p > 2$, если и только если $p \equiv \pm 1 \pmod 8$. Пусть $p \equiv \pm 1 \pmod 8$. Тогда существует остаток $(p \pm 1)/8$ по модулю $p \pm 1$. Рассмотрим его синус:

$$\sin_p\Big(\frac{p\pm1}{8}\Big) = \sin_p\Big(\frac{p\pm1}{4} - \frac{p\pm1}{8}\Big) = \cos_p\Big(\frac{p\pm1}{8}\Big).$$

Однако сумма квадратов синуса и косинуса равна

$$1 = \sin_p^2\Big(\frac{p\pm1}{8}\Big) + \cos_p^2\Big(\frac{p\pm1}{8}\Big) = 2\sin_p^2\Big(\frac{p\pm1}{8}\Big) \quad \Rightarrow \quad 2 = \Big(\sin_p \frac{p\pm1}{8}\Big)^{-2}.$$

Поэтому 2 будет квадратичным вычетом по модулю p.

Теперь предположим, что число 2 является квадратичным вычетом по модулю p. Через $\sqrt{2}$ обозначим один из корней многочлена $x^2 - 2$, который мы рассматриваем над полем $\mathbb{Z}_p$. Так как пара $(1/\sqrt{2}, 1/\sqrt{2})$ удовлетворяет уравнению $x^2 + y^2 = 1$, найдётся такой угол $\alpha \in \mathbb{Z}_{p\pm1}$, что $\cos_p \alpha = \sin_p \alpha = 1/\sqrt{2}$. Тогда

$$\cos_p 2\alpha = \cos_p^2 \alpha - \sin_p^2 \alpha = 0 \quad \Rightarrow \quad 2\alpha \equiv \pm\frac{p\pm1}{4} \pmod{p\pm1}.$$

Отсюда следует, что

$$2 \mid \frac{p\pm1}{4} \quad \Rightarrow \quad p \equiv \pm 1 \pmod 8.$$

Существование $\sqrt{3}$ по модулю p. Докажем, что число 3 — квадратичный вычет по простому модулю $p>3$, если и только если $p\equiv\pm1 \pmod{12}$. Пусть $12 \mid p\pm1$. Тогда мы можем рассмотреть угол $(p\pm1)/6$. Отметим, что

$$0=\sin_p\Big(3\frac{p\pm1}{6}\Big)=-4\sin_p^3\Big(\frac{p\pm1}{6}\Big)+3\sin_p\Big(\frac{p\pm1}{6}\Big)=$$
$$=\sin_p\Big(\frac{p\pm1}{6}\Big)\Big(3-4\sin_p^2\Big(\frac{p\pm1}{6}\Big)\Big).$$

Ясно, что $\sin_p((p\pm1)/6)\neq0$, но тогда число $3=(2\sin_p((p\pm1)/6))^2$ будет квадратичным вычетом по модулю p.

Пусть теперь число 3 является квадратичным вычетом по модулю p, причём $p>3$. Обозначим через $\sqrt{3}$ один из корней многочлена x^2-3, лежащего в поле $\mathbb{Z}_p$. Уравнение $x^2+y^2=1$ имеет решение $(-1/2, \sqrt{3}/2)$, связанное с углом α. Угол 2α можно сопоставить решению $(-1/2,-\sqrt{3}/2)$, а угол 3α — решению $(1,0)$. Следовательно, $\alpha\not\equiv0 \pmod{p\pm1}$, но $3\alpha\equiv0 \pmod{p\pm1}$, значит, модуль должен делиться на 3. Так как для $p\equiv1 \pmod 4$ под $p\pm1$ мы договорились подразумевать $p-1$, а для $p\equiv-1 \pmod 4$ под $p\pm1$ подразумевается $p+1$, получим $4\mid p\pm1$. Комбинируя делимость на 3 и на 4, получаем, что $p\equiv\pm1 \pmod{12}$.

Иррациональность и обычные углы. Докажем, что для таких натуральных c и d, что $d^2-2c^2=1$, число $1/(2\pi)\cdot\arcsin(1/d)$ иррационально, причём arcsin здесь понимается в стандартном смысле. Например, в качестве c и d можно взять числа 2 и 3 соответственно.

Во-первых, имеет место равенство

$$\Big(\frac{\sqrt{2}c}{d}\Big)^2+\Big(\frac{1}{d}\Big)^2=1.$$

Обозначим $\arcsin(1/d)$ через θ. Мы покажем, что число $\theta/(2\pi)$ иррационально, предположив обратное. Пусть $\theta=2\pi\frac{n}{m}$, где $n,m\in\mathbb{N}$. Выберем любое простое p, взаимно простое с d и такое, что $8\mid p+1$. Позже (в этом разделе) мы поймём, почему таких простых бесконечно много. Работая в $\mathbb{Z}_p(i)$ или $\mathbb{Z}_p$, под $\sqrt{2}$ мы подразумеваем один из корней многочлена x^2-2 в поле $\mathbb{Z}_p$, под делением подразумеваем умножение на обратный элемент, и так как $(p,d)=1$, возможно деление на d. Элемент

$$z=\frac{\sqrt{2}c}{d}+i\frac{1}{d}$$

принадлежит $\mathbb{Z}_p(i)$. В поле $\mathbb{C}$ из равенства

$$e^{i\theta}=\frac{\sqrt{2}c}{d}+i\frac{1}{d}$$

следует тождество

$$\Big(\frac{\sqrt{2}c}{d}+i\frac{1}{d}\Big)^m = e^{i\theta m} = e^{i\cdot 2\pi n} = 1.$$

Докажем аналогичное утверждение для $\mathbb{Z}_p(i)$.

Лемма 4.1. *В поле $\mathbb{Z}_p(i)$ имеет место равенство*

$$\Big(\frac{\sqrt{2}c}{d}+i\frac{1}{d}\Big)^m = 1.$$

Доказательство. Если рассматривать $\mathbb{Q}(i,\sqrt{2})$ как векторное пространство над $\mathbb{Q}$, то числа $1, i, \sqrt{2}, \sqrt{2}\,i$ образуют базис расширения $\mathbb{Q}(i,\sqrt{2})$. Тогда из равенства

$$\Big(\frac{\sqrt{2}c}{d}+i\frac{1}{d}\Big)^m = 1$$

в $\mathbb{Q}(i,\sqrt{2})$ следует, что

$$\Big(\frac{\sqrt{2}c}{d}+i\frac{1}{d}\Big)^m = 1$$

в $\mathbb{Z}_p(i)$. Действительно, пусть

$$e^{i\theta k} = t_{k1} + t_{k2}i + t_{k3}\sqrt{2} + t_{k4}\sqrt{2}\,i$$

в $\mathbb{C}$, где все $t_{ki} \in \mathbb{Q}$. Нетрудно видеть, что $t_{01} = 1$, $t_{02} = t_{03} = t_{04} = 0$. Следовательно, мы можем получить $e^{i\theta(k+1)}$ из $e^{i\theta k}$, рассмотрев в $\mathbb{Q}(i,\sqrt{2})$ произведение

$$\big(t_{k1} + t_{k2}i + t_{k3}\sqrt{2} + t_{k4}\sqrt{2}\,i\big)\Big(\frac{\sqrt{2}c}{d}+i\frac{1}{d}\Big).$$

Раскрывая скобки и приводя подобные в этом выражении, для всех четырёх новых «координат» можно получить выражения в виде линейных комбинаций предыдущих четырёх координат с рациональными коэффициентами, чьи знаменатели взаимно просты с p, так как $(p,d)=1$. В случае рациональных чисел, у которых знаменатели взаимно просты с p, все их преобразования можно рассмотреть по модулю p (дробь a/b соответствует остатку $a\cdot b^{-1}$). Поэтому, например, если мы посредством сложения и умножения получили 1 в $\mathbb{Q}$, то, применив этот способ к соответствующим остаткам, мы получим 1 по модулю p. В $\mathbb{Q}(i,\sqrt{2})$ имеют место равенства $t_{m1} = 1$, $t_{m2} = t_{m3} = t_{m4} = 0$. Если мы теперь рассмотрим преобразования, которые произошли с нашими «координатами» по модулю p, получим

$$\Big(\frac{\sqrt{2}c}{d}+i\frac{1}{d}\Big)^m = 1\cdot 1 + 0\cdot i + 0\cdot\sqrt{2} + 0\cdot i\sqrt{2} = 1$$

по модулю p. □

Вернёмся к $\mathbb{Z}_p(i)$: количество элементов группы решений уравнения $x^2 + y^2 = 1$ равно $p + 1$, поэтому верно равенство

$$\left(\frac{\sqrt{2}\,c}{d} + i\frac{1}{d}\right)^{\gcd(m,\,p+1)} = 1.$$

Чтобы воспользоваться последним утверждением, докажем следующую лемму.

Лемма 4.2. *Существует бесконечно много простых p таких, что $8 \mid p+1$ и $(m, p+1) \mid 8$, и $(p, d) = 1$.*

Доказательство. Для всех r_i рассмотрим систему сравнений

$$\begin{cases} p \equiv 7 \pmod{16}, \\ p \equiv 1 \pmod{r_i}, \end{cases}$$

где r_i — все нечётные простые делители чисел m и d. По китайской теореме об остатках существует арифметическая прогрессия натуральных чисел, удовлетворяющая этим сравнениям, причём разность этой прогрессии взаимно проста с её элементами. Тогда по теореме Дирихле о простых числах в арифметической прогрессии имеется бесконечно много простых чисел, удовлетворяющих условиям леммы. □

Если $(m, p+1) \mid 8$, то в $\mathbb{Z}_p(i)$ верно равенство

$$\left(\frac{\sqrt{2}c}{d} + i\frac{1}{d}\right)^{8} = 1.$$

В нашем случае это означает, что $(\sqrt{2}\,c/d, 1/d)$ имеет вид либо $(\pm 1, 0)$, либо $(0, \pm 1)$, либо $(\pm 1/\sqrt{2}, \pm 1/\sqrt{2})$. Первый случай невозможен, второй означает, что $c \equiv 0 \pmod{p}$, а третий даст нам условие $d^2 - 2 \equiv 0 \pmod{p}$. Тогда по лемме 4.2 найдётся нужное нам простое число, для которого последние два случая невозможны. Это приводит к противоречию. Отсюда получаем, например, что число $1/(2\pi) \cdot \arcsin(1/3)$ иррационально. То же самое верно для любого такого натурального числа d, что при некотором натуральном c выполнено уравнение Пелля $d^2 - 2c^2 = 1$.

Аналогично мы можем доказать, что для таких $c, d \in \mathbb{N}$, что $d^2 - 3c^2 = 1$ и $d \neq 2$, число $1/(2\pi) \cdot \arcsin(1/d)$ иррационально. В частности, по системе сравнений

$$\begin{cases} p \equiv 11 \pmod{6 \cdot 12}, \\ p \equiv 1 \pmod{r_i} \quad \forall\, r_i, \end{cases}$$

где r_i — все простые делители чисел m и d, превосходящие 3, мы можем построить нужную арифметическую прогрессию. Исходя из по-

хожих соображений, можно доказать, что пересечение $\mathbb{Q}(i)$ и множества всех комплексных чисел вида $e^{i2\pi\theta}$, где θ рационально, — это $\{1, i, -1, -i\}$. Действительно, пусть $\theta = n/m$ и $e^{i\theta} = a/d + ib/d$, где $n, a, b \in \mathbb{Z}$ и $m, d \in \mathbb{N}$. Мы можем рассмотреть систему сравнений

$$\begin{cases} p \equiv 3 \pmod 8, \\ p \equiv 1 \pmod{r_i} \end{cases}$$

для всех r_i, где r_i — все нечётные простые делители чисел m и d. Найдётся бесконечно много простых, удовлетворяющих этой системе сравнений. Обозначим одно из них через p. Тогда из равенства

$$1 = e^{i\theta m} = \left(\frac{a}{d} + i\frac{b}{d}\right)^m$$

в $\mathbb{C}$ мы также, как и в лемме 4.1, получаем, что

$$\left(\frac{a}{d} + i\frac{b}{d}\right)^m = 1$$

в $\mathbb{Z}_p(i)$. Но, так как $(m, p+1) = 4$, имеет место равенство

$$\left(\frac{a}{d} + i\frac{b}{d}\right)^4 = 1$$

в $\mathbb{Z}_p(i)$, поэтому один из двух остатков $a/d, b/d$ должен быть равен 0 в $\mathbb{Z}_p$. Тогда если $e^{i\theta} \notin \{1, i, -1, -i\}$, то, так как в нашей арифметической прогрессии бесконечно много простых чисел, среди них найдётся такое, при котором мы получим противоречие.

§ 5. Модулярный тангенс

В случае геометрических углов значения $\sin_p(-\alpha)$ могут быть равны $-\sin_p \alpha$ или $\sin_p \alpha$. Более того, нельзя сказать, что любой остаток $a \in \mathbb{Z}_p$ — например, остаток 2 по модулю 11 — представим как синус некоторого угла ($a = \sin_p \alpha$). Оказывается, что в случае тангенса картина более приятная. Однако начнём с более простого типа углов.

Негеометрические углы. Тангенсом угла $\alpha \neq \pm(p \pm 1)/4$ будем называть функцию $\operatorname{tg}_p \alpha = \sin_p \alpha / \cos_p \alpha$ (деление в поле $\mathbb{Z}_p$). Когда $\cos_p \alpha = 0$, тангенс не определён. Кроме того, можно заметить, что равенство $\operatorname{tg}_p \alpha = 0$ имеет место лишь при $\sin_p \alpha = 0$. Тогда $\alpha \in \{0, (p \pm 1)/2\}$.

Верны тождества $\operatorname{tg}_p(-\alpha) = -\operatorname{tg}_p \alpha$ и $\operatorname{tg}_p(\alpha + (p \pm 1)/2) = \operatorname{tg}_p \alpha$. Также

$$\operatorname{tg}_p\left(\frac{p \pm 1}{4} - \alpha\right) = \frac{1}{\operatorname{tg}_p \alpha},$$

когда $\operatorname{tg}_p \alpha \neq 0$. Формула тангенса суммы углов, которая выполнена в стандартном случае, тоже верна; если тангенсы углов α, β, $\alpha+\beta$ определены, то имеем

$$\frac{\operatorname{tg}_p \alpha + \operatorname{tg}_p \beta}{1-\operatorname{tg}_p \alpha \operatorname{tg}_p \beta} = \frac{\sin_p \alpha \cos_p \beta + \sin_p \beta \cos_p \alpha}{\cos_p \alpha \cos_p \beta - \sin_p \alpha \sin_p \beta} = \operatorname{tg}_p(\alpha+\beta).$$

Заметим, что

$$\operatorname{tg}_p \alpha = \operatorname{tg}_p \beta \quad \Leftrightarrow \quad \sin_p \alpha \cos_p \beta - \sin_p \beta \cos_p \alpha = 0 \quad \Leftrightarrow \quad \sin_p(\alpha-\beta) = 0.$$

Поэтому $\alpha - \beta \in \{0, (p \pm 1)/2\}$. Так как $(p \pm 1)/2$ — период нашего тангенса, множество значений последнего равно

$$\left\{ \operatorname{tg}_p \alpha \colon \alpha \in \left[0, \frac{p \pm 1}{2}\right) \setminus \left\{\frac{p \pm 1}{4}\right\} \right\}.$$

Значения, которые принимает тангенс на

$$\left\{0, \ldots, \frac{(p \pm 1)}{2} - 1\right\} \setminus \left\{\frac{(p \pm 1)}{4}\right\},$$

отличаются попарно, поэтому он имеет ровно $(p \pm 1)/2 - 1$ различных значений.

Геометрические углы. Напомним, что под геометрическими углами подразумевается тип углов, возникающий при рассмотрении решений уравнения $x^2 + y^2 = \pm 1$. Тангенс геометрических углов при $\alpha \neq \pm(p+1)/2$ определяется как $\operatorname{tg}_p \alpha = \sin_p \alpha / \cos_p \alpha$. Снова

$$\operatorname{tg}_p \alpha = 0 \quad \Leftrightarrow \quad \alpha \in \{0, p+1\}.$$

По-прежнему верно равенство $\operatorname{tg}_p(\alpha + (p+1)) = \operatorname{tg}_p \alpha$. Так как обратное к z — это $\bar{z}$ или $-\bar{z}$, имеем $\operatorname{tg}_p(-\alpha) = -\operatorname{tg}_p \alpha$. Также верно, что

$$\operatorname{tg}_p\left(\alpha + \frac{p+1}{2}\right) = -\frac{1}{\operatorname{tg}_p \alpha}, \quad \text{если} \quad \operatorname{tg}_p \alpha \neq 0.$$

Формула тангенса суммы углов верна, так как верны формулы синуса и косинуса суммы углов. Однако тогда верна и формула для разности: если тангенсы углов α, β, $\alpha - \beta$ определены, то

$$\operatorname{tg}_p(\alpha + (-\beta)) = \frac{\operatorname{tg}_p \alpha + \operatorname{tg}_p(-\beta)}{1 - \operatorname{tg}_p \alpha \operatorname{tg}_p(-\beta)} = \frac{\operatorname{tg}_p \alpha - \operatorname{tg}_p \beta}{1 + \operatorname{tg}_p \alpha \operatorname{tg}_p \beta}.$$

Отметим, что

$$\operatorname{tg}_p \alpha = \operatorname{tg}_p \beta \quad \Leftrightarrow \quad \sin_p \alpha \cos_p \beta - \sin_p \beta \cos_p \alpha = 0 \quad \Leftrightarrow \quad \pm \sin_p(\alpha-\beta) = 0.$$

Поэтому $\alpha - \beta \in \{0, p+1\}$. Следовательно, значения тангенса возникают ровно по одному разу для углов от 0 до p включительно, и тангенс

не определён в точке $\alpha = (p+1)/2$. Но тогда получаем, что множество значений тангенса — все остатки по модулю p. Другими словами, каждый остаток по модулю p появляется ровно два раза среди всех значений тангенса, и соответствующих ему два угла отличаются на $p+1$; также тангенс не определён для двух углов, отличающихся на $p+1$.

Корни уравнения. Снова рассмотрим геометрические углы. Нетрудно заметить, что верны формулы

$$\frac{2\operatorname{tg}_p \alpha}{1+\operatorname{tg}_p^2 \alpha} = \frac{2\sin_p \alpha \cos_p \alpha}{\sin_p^2 \alpha + \cos_p^2 \alpha} = \pm \sin_p 2\alpha,$$
$$\frac{1-\operatorname{tg}_p^2 \alpha}{1+\operatorname{tg}_p^2 \alpha} = \frac{\cos_p^2 \alpha - \sin_p^2 \alpha}{\sin_p^2 \alpha + \cos_p^2 \alpha} = \pm \cos_p 2\alpha.$$

Тогда получим пару $(-\sin_p 2\alpha, -\cos_p 2\alpha)$, когда угол нечётный, так как в этом случае $\sin_p^2 \alpha + \cos_p^2 \alpha = -1$, и пару $(\sin_p 2\alpha, \cos_p 2\alpha)$, когда угол чётный, так как в этом случае $\sin_p^2 \alpha + \cos_p^2 \alpha = 1$ (вспомним, что для геометрических углов верны формулы синуса и косинуса суммы углов). Так как тангенс может быть равен любому остатку, у нас есть возможность получать решения уравнения $z^{p+1} = 1$, сопоставляя остаток t по модулю p элементу из $\mathbb{Z}_p(i)$ вида

$$\pm\frac{1-t^2}{1+t^2} \pm i\frac{2t}{1+t^2}.$$

Рассмотрим негеометрические углы в случае $p = 4n+1$. Их тангенс не может быть равен $\pm j$, где под j подразумевается один из корней многочлена x^2+1 в поле $\mathbb{Z}_p$: иначе выполнялось бы равенство $\sin_p^2 \alpha + \cos_p^2 \alpha = 0$. Заметим, что мы можем снова получать решения уравнения $x^2 + y^2 = 1$ из остатков по модулю p: если взять $t \neq \pm j$, то

$$\left(\frac{1-t^2}{1+t^2}\right)^2 + \left(\frac{2t}{1+t^2}\right)^2 = 1.$$

Если также $t \neq \pm 1$, то существует тангенс данного угла, равный $\dfrac{2t}{1-t^2}$.

§ 6. Многочлены для тангенса

Мы знаем, что $\operatorname{tg} 2\theta = 2\operatorname{tg}\theta/(1-\operatorname{tg}^2\theta)$. Представим $\operatorname{tg} n\theta$ как рациональную функцию от $\operatorname{tg}\theta$.

Рассмотрим следующую рекуррентную последовательность пар многочленов $p_n, q_n \in \mathbb{Z}[x]$

$$p_0 = 0, \quad p_{n+1} = p_n + q_n x,$$
$$q_0 = 1, \quad q_{n+1} = q_n - p_n x.$$

Приведём несколько первых элементов последовательности:

n	0	1	2	3	4	5
p_n	0	x	$2x$	$3x-x^3$	$4x-4x^3$	$5x-10x^3+x^5$
q_n	1	1	$1-x^2$	$1-3x^2$	$1-6x^2+x^4$	$1-10x^2+5x^4$

Лемма 6.1. *При $n>0$ верно следующее*:

Случай		*Степень*	*Старший коэффициент*
$2 \mid n$	p_n	$n-1$	$(-1)^{n/2-1}n$
	q_n	n	$(-1)^{n/2}$
$2 \nmid n$	p_n	n	$(-1)^{(n-1)/2}$
	q_n	$n-1$	$(-1)^{(n-1)/2}n$

Младший моном многочлена q_n равен x^0. Младший моном многочлена p_n равен nx.

Доказательство. Проведём индукцию по n. Для случая $n=1$ наше утверждение верно. Опишем переход от n к $n+1$. Если $2 \mid n$, то

$$p_{n+1}=p_n+q_nx \quad \text{и} \quad \deg p_n<\deg q_n \quad \Rightarrow \quad \deg p_{n+1}=n+1.$$

При этом $(-1)^{n/2}=(-1)^{((n+1)-1)/2}$. Перейдём к многочлену q_{n+1} следующим образом:

$$q_{n+1}=q_n-p_nx \quad \Rightarrow \quad \deg q_{n+1}\leqslant \max(\deg q_n, \deg(-p_nx))=n=(n+1)-1.$$

Коэффициент при старшей степени многочлена q_{n+1} равен

$$(-1)^{n/2}-(-1)^{n/2-1}n=(-1)^{((n+1)-1)/2}(n+1).$$

Если $2 \nmid n$, то $p_{n+1}=p_n+q_nx$, и поэтому

$$\deg p_{n+1}\leqslant \max(\deg p_n, \deg(q_nx))=n=(n+1)-1.$$

Коэффициент при старшей степени многочлена p_{n+1} равен

$$(-1)^{(n-1)/2}+(-1)^{(n-1)/2}n=(-1)^{(n+1)/2-1}(n+1).$$

Далее,

$$q_{n+1}=q_n-p_nx, \deg p_n>\deg q_n \quad \Rightarrow \quad \deg q_{n+1}=n+1.$$

Старший коэффициент равен $(-1)^{(n-1)/2}(-1)=(-1)^{(n+1)/2}$. Так как $q_{n+1}=q_n-p_nx$, коэффициент при x^0 остается неизменным, следовательно, тождественно равен 1. Так как $p_{n+1}=p_n+q_nx$, коэффициент при x^0 тождественно равен 0, а коэффициент при x^1 увеличивается на 1 на каждом шаге. □

Так как мы собираемся рассматривать соотношение p_n и q_n, желательно избежать случая $0/0$. Докажем, что такой ситуации не возникает.

Лемма 6.2. *Многочлены p_n и q_n взаимно просты. Для любого простого $p > 2$ их редукции по модулю p взаимно просты как многочлены в $\mathbb{Z}_p[x]$.*

Доказательство. Взаимная простота двух многочленов равносильна тому, что у них нет общих корней ни в одном расширении поля. Докажем последнее по индукции. База индукции при $n \leqslant 1$ верна. Опишем переход от n к $n+1$. Пусть многочлены $p_n + q_n x$ и $q_n - p_n x$ имеют общий корень z. Если $z = 0$, то $p_n(z) = q_n(z) = 0$, что приводит к противоречию. Когда $z \neq 0$, из равенства $p_n(z) = 0$ или равенства $q_n(z) = 0$ следует $p_n(z) = q_n(z) = 0$. Значит, $p_n(z)q_n(z) \neq 0$. Тогда

$$p_n(z) = -q_n(z)z = -p_n(z)z^2 \quad \Rightarrow \quad z^2 = -1.$$

Теперь покажем, что p_n и q_n не могут одновременно быть равны 0, когда $z^2 = -1$. Чтобы это сделать, посмотрим на значения, которые они принимают:

n		0	1	2	3
i	$p_n(i)$	0	i	$2i$	$4i$
	$q_n(i)$	1	1	2	4
$-i$	$p_n(-i)$	0	$-i$	$-2i$	$-4i$
	$q_n(-i)$	1	1	2	4

Ясно, что, начиная с $n = 1$, ненулевые значения p_n и q_n удваиваются на каждом шаге, и потому два многочлена никогда не будут одновременно равны 0 в $\pm i$. Заметим, что это рассуждение работает во всех трёх случаях: $\mathbb{C}$, $\mathbb{Z}_p(i)$ при $p \equiv 3 \pmod 4$ и $\mathbb{Z}_p$ при $p \equiv 1 \pmod 4$, причём в каждом случае под i подразумевается корень из -1 в соответствующем поле. □

В следующей лемме под tg будем подразумевать как обычный тангенс, так и tg_p; аналогично для синуса и косинуса.

Лемма 6.3. *В случае углов из $\mathbb{R}$ и в случае углов по модулю простых чисел (как геометрических, так и негеометрических) формула*

$$\frac{p_n(\mathrm{tg}\,\alpha)}{q_n(\mathrm{tg}\,\alpha)} = \mathrm{tg}\, n\alpha$$

верна, когда тангенс углов α и $n\alpha$ определён. Случай, когда $\mathrm{tg}\,\alpha$ определён, а $\mathrm{tg}\, n\alpha$ — нет, встречается тогда и только тогда, когда

$$q_n(\mathrm{tg}\,\alpha) = 0.$$

Доказательство. Проведём индукцию по n. База в случае $n \leqslant 1$ ясна. Опишем переход от $n-1$ к n. Предположим, что $\operatorname{tg}\alpha$ определён. Если $\operatorname{tg}(n-1)\alpha$ тоже определён, то $q_{n-1}(\operatorname{tg}\alpha) \neq 0$, и мы имеем

$$\operatorname{tg} n\alpha = \operatorname{tg}(\alpha + (n-1)\alpha) = \frac{\operatorname{tg}\alpha + \dfrac{p_{n-1}(\operatorname{tg}\alpha)}{q_{n-1}(\operatorname{tg}\alpha)}}{1 - \operatorname{tg}\alpha\,\dfrac{p_{n-1}(\operatorname{tg}\alpha)}{q_{n-1}(\operatorname{tg}\alpha)}} =$$

$$= \frac{p_{n-1}(\operatorname{tg}\alpha) + \operatorname{tg}\alpha \cdot q_{n-1}(\operatorname{tg}\alpha)}{q_{n-1}(\operatorname{tg}\alpha) - \operatorname{tg}\alpha \cdot p_{n-1}(\operatorname{tg}\alpha)} = \frac{p_n(\operatorname{tg}\alpha)}{q_n(\operatorname{tg}\alpha)}.$$

Заметим, что

$$q_n(\operatorname{tg}\alpha) = 0 \quad \Leftrightarrow \quad q_{n-1}(\operatorname{tg}\alpha) - p_{n-1}(\operatorname{tg}\alpha)\operatorname{tg}\alpha = 0 \quad \Leftrightarrow$$
$$\Leftrightarrow \quad \operatorname{tg}\alpha \operatorname{tg}(n-1)\alpha = 1 \quad \Leftrightarrow$$
$$\Leftrightarrow \quad \cos\alpha\cos(n-1)\alpha - \sin\alpha\sin(n-1)\alpha = 0 \quad \Leftrightarrow \quad \cos n\alpha = 0.$$

Отсюда следует, что $\operatorname{tg} n\alpha$ не определён. Если $\operatorname{tg}(n-1)\alpha$ не определён, то $\cos(n-1)\alpha = 0$, при этом $q_{n-1}(\operatorname{tg}\alpha) = 0$, но тогда $p_{n-1}(\operatorname{tg}\alpha) \neq 0$. Отсюда получаем формулу

$$\operatorname{tg}(\alpha + (n-1)\alpha) = -\frac{1}{\operatorname{tg}\alpha} = \frac{p_{n-1}(\operatorname{tg}\alpha)}{-p_{n-1}(\operatorname{tg}\alpha)\operatorname{tg}\alpha} = \frac{p_n(\operatorname{tg}\alpha)}{q_n(\operatorname{tg}\alpha)}. \qquad \square$$

Из этой леммы следует равенство

$$\operatorname{tg}(n \operatorname{arctg} x) = \frac{p_n(x)}{q_n(x)}$$

для действительных x. Заметим, что ввиду взаимной простоты многочленов $p_n(x)$ и $q_n(x)$ любое представление $\operatorname{tg}(n \operatorname{arctg} x)$ в виде отношения двух многочленов должно иметь вид

$$\frac{p_n(x)K(x)}{q_n(x)K(x)},$$

где $K(x)$ — некоторый отличный от p_n и q_n многочлен.

Теперь мы можем представить p_n и q_n в виде произведения линейных множителей.

Лемма 6.4. *Пусть A — старший коэффициент в p_n, а B — старший коэффициент в q_n. Тогда в $\mathbb{R}$ верны равенства*

$$p_n(x) = A\prod_{\substack{k=0\\k\neq n/2}}^{n-1}\Big(x - \operatorname{tg}\frac{\pi}{n}k\Big), \quad q_n(x) = B\prod_{\substack{k=0\\k\neq n,\,2\nmid k}}^{2n-1}\Big(x - \operatorname{tg}\frac{\pi}{2n}k\Big).$$

Доказательство. Нетрудно заметить, что $x_k = \operatorname{tg}(\pi k/n)$ — корни многочлена p_n, $0 \leqslant k \leqslant n-1$, $k \neq n/2$. Их количество совпадает со степенью p_n. Отсюда вытекает первая формула из утверждения леммы. Теперь заметим, что $\operatorname{tg} n \operatorname{arctg} x$ не определён лишь при $x = \operatorname{tg}(\pi k/(2n))$, где k нечётно и не кратно n. Для такого x имеем $q_n(x) = 0$. При чётных n имеем $\deg q_n = n$, а при нечётных $\deg q_n = n-1$. Другими словами, мы только что рассмотрели корни многочлена q_n, количество которых равно $\deg q_n$. □

Если мы умножим угол на n, а потом на m, то получим, что

$$\operatorname{tg}\bigl(n\bigl(\operatorname{arctg}(\operatorname{tg}(m \operatorname{arctg} x))\bigr)\bigr)$$

равен $\operatorname{tg} nm \operatorname{arctg} x$, если определён. Покажем теперь, что композиция дробей $p_m(x)/q_m(x)$ и $p_n(x)/q_n(x)$ даёт дробь $p_{nm}(x)/q_{nm}(x)$.

Лемма 6.5. *Верны равенства многочленов*

$$p_{nm}(x) = p_n\Bigl(\frac{p_m(x)}{q_m(x)}\Bigr)q_m(x)^n, \quad q_{nm}(x) = q_n\Bigl(\frac{p_m(x)}{q_m(x)}\Bigr)q_m(x)^n.$$

Доказательство. Ясно, что

$$p_n\Bigl(\frac{p_m(x)}{q_m(x)}\Bigr)q_m(x)^n, q_n\Bigl(\frac{p_m(x)}{q_m(x)}\Bigr)q_m(x)^n \in \mathbb{R}[x].$$

Рассмотрим старшие коэффициенты и степени этих многочленов. Используем лемму 6.1. Если $2 \mid m$, то $\deg p_m = m-1$ и $\deg q_m = m$. Многочлен p_n можно записать как $a_0 + a_1 x + a_2 x^2 + \ldots$, тогда многочлен

$$p_n\Bigl(\frac{p_m(x)}{q_m(x)}\Bigr)q_m(x)^n$$

можно записать как

$$a_0 q_m(x)^n + a_1\Bigl(\frac{p_m(x)}{q_m(x)}\Bigr)q_m(x)^n + a_2\Bigl(\frac{p_m(x)}{q_m(x)}\Bigr)^2 q_m(x)^n + \ldots$$

Нас интересует старший моном в многочлене

$$p_n\Bigl(\frac{p_m(x)}{q_m(x)}\Bigr)q_m(x)^n.$$

Чтобы его найти, мы можем посмотреть отдельно на старшие степени x в каждом из слагаемых суммы, приведённой выше. Так как $\deg q_m > \deg p_m$, старшая степень x появляется только внутри монома

$$a_k\Bigl(\frac{p_m(x)}{q_m(x)}\Bigr)^k q_m(x)^n$$

с минимальным k, при котором $a_k \neq 0$. Тогда старший член

$$p_n\left(\frac{p_m(x)}{q_m(x)}\right)q_m(x)^n$$

совпадает со старшим членом $np_m(x)q_m(x)^{n-1}$, т. е. с мономом

$$(-1)^{\frac{m}{2}-1+\frac{m}{2}(n-1)}nmx^{nm-1} = (-1)^{nm/2-1}nmx^{nm-1}.$$

Аналогичным образом старший член многочлена

$$q_n\left(\frac{p_m(x)}{q_m(x)}\right)q_m(x)^n$$

будет присутствовать только внутри $q_m(x)^n$, что даёт моном $(-1)^{nm/2}x^{nm}$.

Если $2 \nmid m$: $\deg p_m = m$ и $\deg q_m = m-1$. Теперь в приведённых рассуждениях старшая степень x появляется лишь в слагаемом с максимальным k, при котором $a_k \neq 0$. Если $2 \mid n$: в случае многочлена

$$p_n\left(\frac{p_m(x)}{q_m(x)}\right)q_m(x)^n$$

мы рассматриваем слагаемое $(-1)^{n/2-1}np_m(x)^{n-1}q_m(x)$, из которого получаем моном

$$(-1)^{n/2-1+(n-1)(m-1)/2+(m-1)/2}nmx^{nm-1} = (-1)^{nm/2-1}nmx^{nm-1}.$$

Аналогичным образом для многочлена

$$q_n\left(\frac{p_m(x)}{q_m(x)}\right)q_m(x)^n$$

мы рассматриваем слагаемое $(-1)^{n/2}p_m(x)^n$, из которого получаем моном

$$(-1)^{(n+(m-1)n)/2}x^{nm} = (-1)^{nm/2}x^{nm}.$$

Если $2 \nmid n$: для полинома

$$p_n\left(\frac{p_m(x)}{q_m(x)}\right)q_m(x)^n$$

мы рассмотрим $(-1)^{(n-1)/2}p_m(x)^n$, получим моном

$$(-1)^{(n-1)/2}(-1)^{(m-1)n/2}x^{nm} = (-1)^{(nm-1)/2}x^{nm}.$$

Далее, в случае многочлена

$$q_n\left(\frac{p_m(x)}{q_m(x)}\right)q_m(x)^n$$

мы будем работать со слагаемым $(-1)^{(n-1)/2} n p_m(x)^{n-1} q_m(x)$. Оно должно дать моном

$$(-1)^{(n-1)/2} n (-1)^{(n-1)(m-1)/2} (-1)^{(m-1)/2} m x^{nm-1} = (-1)^{(nm-1)/2} nm x^{nm-1}.$$

Таким образом, оба многочлена

$$p_n\left(\frac{p_m(x)}{q_m(x)}\right) q_m(x)^n \quad \text{и} \quad q_n\left(\frac{p_m(x)}{q_m(x)}\right) q_m(x)^n$$

имеют старшие члены, идентичные старшим членам многочленов p_{nm} и q_{nm} соответственно. Теперь значение рациональной дроби

$$\frac{p_n\left(\frac{p_m(x)}{q_m(x)}\right) q_m(x)^n}{q_n\left(\frac{p_m(x)}{q_m(x)}\right) q_m(x)^n}$$

совпадает с $p_{nm}(x)/q_{nm}(x)$ для бесконечно большого количества значений x. Используя доказанное выше, получаем нужное равенство. □

Доказанный факт позволяет выразить p_{2n} через p_n и q_n. Воспользуемся этим, чтобы доказать следующую лемму. Через $\nu_p(n)$ обозначим степень вхождения простого p в ненулевое целое n.

Лемма 6.6. *Пусть $n = 2^k n' > 0$, где $k = \nu_2(n)$. Тогда $c(p_n) = 2^k$, где $c(p_n)$ — содержание многочлена p_n.*

Доказательство. Проведём индукцию по $\nu_2(n)$. База индукции: для нечётного n старший коэффициент многочлена p_n равен ± 1, так что $c(p_n) = 1$. Опишем индукционный переход от $\nu_2(n)$ к $\nu_2(n) + 1$. В лемме 6.5 поменяем местами n и m, после этого положим $m = 2$ и воспользуемся формулами для p_2, q_2. В итоге получим $p_{2n} = 2p_n q_n$. Но тогда $c(p_{2n}) = 2c(p_n)c(q_n) = 2c(p_n)$, так как младший коэффициент многочлена q_n равен 1. □

§ 7. Фундаментальные многочлены

При разложении многочлена $x^n - 1$ на множители получим многочлены деления круга, которые имеют полезные приложения. Многочлены деления круга связаны с мультипликативной группой $\mathbb{Z}_p^*$, вследствие чего удаётся установить связь с её мощностью $p - 1$. Однако группы, связанные с углами, помимо мощности $p - 1$ могут иметь мощность $p + 1$. Поэтому попытаемся разложить $p_n(x)$ в произведение многочленов меньшей степени.

Для нечётного n положим $s(n) = (-1)^{(n-1)/2}$. Так как $s(n) \equiv n \pmod 4$, имеем $s(nm) = s(n)s(m)$, когда n и m нечётны.

Определение. Определим n-й фундаментальный многочлен, где $n \in \mathbb{N}$, следующим образом:

$$\varphi_1(x) = x, \quad \varphi_2(x) = 2;$$

при $n > 2$

$$\varphi_n(x) = A \prod_{\substack{k=0 \\ (k,n)=1 \\ 2k \neq n}}^{n-1} \left(x - \operatorname{tg} \frac{\pi}{n} k\right),$$

где

$$A = \begin{cases} -2, & \text{если } n = 4, \\ +2, & \text{если } n = 2^k, \text{ где } k \neq 2 \text{ и } k > 0, \\ s(p), & \text{если } n = p^k, \text{ где } p > 2, \\ s(p)p, & \text{если } n = 2p^k, \text{ где } p > 2, \\ 1, & \text{иначе.} \end{cases}$$

Лемма 7.1. *Для всех $n \in \mathbb{N}$ справедлива формула*

$$p_n(x) = \prod_{d|n} \varphi_d(x).$$

Доказательство. Мы знаем, что корни многочлена p_n — числа вида $\operatorname{tg} \frac{\pi}{n} k$ при $2k \neq n$, $0 \leqslant k < n$, но каждое из них встречается в произведении в правой части по одному разу: для $\operatorname{tg} \frac{\pi}{n} k$ надо взять $d = (k, n)$. Поэтому надо проверить только равенство старших коэффициентов.

Для нечётного $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, где p_i — простые числа, большие 2, старший коэффициент в правой части имеет вид

$$s(p_1)^{\alpha_1} \cdot \ldots \cdot s(p_k)^{\alpha_k} = s(n) = (-1)^{(n-1)/2}.$$

Для $n = 2p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ старший коэффициент в правой части будет иметь вид

$$2 \underbrace{s(p_1)^{\alpha_1} \cdot \ldots \cdot s(p_k)^{\alpha_k}}_{\text{от } d = p^\alpha} \underbrace{p_1^{\alpha_1} s(p_1)^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k} s(p_k)^{\alpha_k}}_{\text{от } d = 2p^\alpha} = (-1)^{n/2-1} n.$$

Для $n = 2^k p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ при $k > 1$ имеем

$$-2^k \underbrace{s(p_1)^{\alpha_1} \cdot \ldots \cdot s(p_k)^{\alpha_k}}_{\text{от } d = p^\alpha} \underbrace{p_1^{\alpha_1} s(p_1)^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k} s(p_k)^{\alpha_k}}_{\text{от } d = 2p^\alpha} = (-1)^{n/2-1} n,$$

где отрицательный знак перед 2^k обусловлен тем, что старший коэффициент в $\varphi_{2^2}(x)$ равен -2. □

Через $c(P)$ обозначим содержание многочлена P.

Лемма 7.2. *Пусть $P, Q \in \mathbb{Z}[x]$. Если $Q \mid P$ как многочлен в $\mathbb{Q}[x]$, и $c(Q) \mid c(P)$, то $P/Q \in \mathbb{Z}[x]$, и $c(P/Q) = c(P)/c(Q)$.*

Доказательство. Без ограничения общности можно предположить, что $c(Q) = 1$: иначе мы можем разделить и P, и Q на $c(Q)$. Пусть $P(x) = Q(x)R(x)$, где $R(x) \in \mathbb{Q}[x]$. Через t обозначим такое наименьшее натуральное число, что $tR(x) \in \mathbb{Z}[x]$. Тогда $(t, c(tR(x))) = 1$, так как иначе нашлось бы меньшее t. Поэтому

$$tP(x) = Q(x)(tR(x)) \quad \Rightarrow \quad tc(P) = c(Q)c(tR(x)) = c(tR(x)) \quad \Rightarrow$$
$$\Rightarrow \quad t = 1 \quad \Rightarrow \quad R(x) \in \mathbb{Z}[x]. \quad \square$$

Используя эту лемму, мы можем показать, что фундаментальные многочлены имеют целые коэффициенты.

Лемма 7.3. *Верно, что $\varphi_n(x) \in \mathbb{Z}[x]$, причём*

$$c(\varphi_n) = \begin{cases} 2, & \text{если } n = 2^k \text{ для } k \in \mathbb{N}, \\ 1, & \text{иначе}, \end{cases}$$

$$\varphi_n(0) = \begin{cases} p, & \text{если } n = p^\alpha \text{ при простом } p \text{ и } \alpha \in \mathbb{N}. \\ 0, & \text{если } n = 1, \\ 1, & \text{иначе}. \end{cases}$$

Доказательство. Проведём индукцию по n. База индукции $n = 1$ очевидна. Чтобы осуществить индуктивный переход, выведем наше утверждение для n из всех предыдущих. Мы знаем, что

$$p_n(x) = \varphi_n(x) \prod_{\substack{d \mid n \\ d < n}} \varphi_d(x).$$

Пусть $k = \nu_2(n)$. В лемме 6.6 было показано, что $c(p_n) = 2^k$. По предположению индукции имеем

$$c\left(\prod_{d \mid n,\, d < n} \varphi_d(x) \right) = \prod_{\substack{d \mid n \\ d < n}} c(\varphi_d(x)) = \begin{cases} 2^{k-1}, & \text{если } n = 2^k, \\ 2^k, & \text{иначе.} \end{cases}$$

Число 2^k делит $c(p_n(x))$. Применим предыдущую лемму 7.2. В качестве многочлена P рассмотрим $p_n(x)$, а в качестве многочлена Q — произведение всех $\varphi_d(x)$, где $d < n$ и d делит n. Выбранные многочлены P и Q имеют целые коэффициенты, в частности, для Q это верно по предположению индукции. По лемме 7.2 получаем $\varphi_n(x) \in \mathbb{Z}[x]$. Кроме того, $c(\varphi_n) = 2$, когда $n = 2^k$, так как $c(p_n) = 2^k$.

Пусть $D(x) = p_n(x)/x$. Тогда $D(x) \in \mathbb{Z}[x]$ и $D(0) = n$ согласно лемме 6.1. Поэтому

$$D(0) = \varphi_n(0) \prod_{\substack{d|n \\ 1<d<n}} \varphi_d(0) = \varphi_n(0) \begin{cases} \frac{n}{p}, & \text{если } n = p^\alpha, \\ n, & \text{иначе.} \end{cases}$$

Отсюда следует требуемое. □

Ясно, что $p_n(x)$ не имеет кратных корней как многочлен из $\mathbb{C}[x]$ по лемме 6.4. Оказывается, то же верно при рассмотрении $p_n(x)$ как многочлена из $\mathbb{Z}_p[x]$.

Теорема 1. *Для простого $p \nmid n$ многочлен p_n не имеет кратных корней ни в одном расширении $\mathbb{Z}_p$.*

Доказательство. Предположим противное. Обозначим через z кратный корень из некоторого расширения $\mathbb{Z}_p$. Ясно, что $z^2 + 1 \neq 0$, так как иначе $p_n(z) \neq 0$ (см. таблицу из леммы 6.2). Если z — кратный корень, то $p_n'(z) = 0$. Тогда $p_n'(z)q_n(z) - p_n(z)q_n'(z) = 0$. Найдём последний многочлен.

Лемма 7.4. *Верно следующее равенство многочленов*:

$$p_n'(x)q_n(x) - p_n(x)q_n'(x) = n\frac{p_n^2(x) + q_n^2(x)}{x^2 + 1}.$$

Доказательство. Пусть $n \neq 0$. Для любого такого x, что $q_n(x) \neq 0$, верны равенства

$$\frac{p_n'(x)q_n(x) - p_n(x)q_n'(x)}{q_n^2(x)} = \left(\frac{p_n(x)}{q_n(x)}\right)' = (\operatorname{tg} n \operatorname{arctg} x)' = \\ = (n \operatorname{arctg} x)' \left(\frac{d}{dx} \operatorname{tg}\right)(n \operatorname{arctg} x).$$

Мы также знаем, что

$$\frac{d}{dx} \operatorname{tg} x = \frac{1}{\cos^2 x} = 1 + \operatorname{tg}^2 x,$$

поэтому

$$(n \operatorname{arctg} x)' \left(\frac{d}{dx} \operatorname{tg}\right)(n \operatorname{arctg} x) = \frac{n}{x^2+1}\left(1 + \left(\frac{p_n(x)}{q_n(x)}\right)^2\right) = \\ = \frac{n}{x^2+1}\frac{p_n^2(x) + q_n^2(x)}{q_n^2(x)} = n\frac{\frac{p_n^2(x) + q_n^2(x)}{x^2+1}}{q_n^2(x)}.$$

Можно заметить, что $p_n^2(\pm i) + q_n^2(\pm i) = 0$, а также $c(x^2+1) = 1$. Тогда x^2+1 делит $p_n^2(x) + q_n^2(x)$ как многочлен в $\mathbb{Z}[x]$, так как

$$\frac{p_n^2(x) + q_n^2(x)}{x^2+1} \in \mathbb{Z}[x].$$

Поэтому для бесконечного количества значений x выполнено равенство

$$p_n'(x)q_n(x) - p_n(x)q_n'(x) = n\frac{p_n^2(x) + q_n^2(x)}{x^2+1}. \qquad \square$$

Значит,

$$0 = p_n'(z)q_n(z) - p_n(z)q_n'(z) = n\frac{p_n^2(z) + q_n^2(z)}{z^2+1} = n\frac{q_n^2(z)}{z^2+1} \neq 0,$$

так как $p_n(z)$ и $q_n(z)$ не могут равняться нулю одновременно. Это приводит к противоречию. $\square$

Порядком угла α будем называть такое наименьшее натуральное m, что $\operatorname{tg} m\alpha = 0$. Порядок определён не только для обычных углов, соизмеримых с 2π, но и для углов по модулю. Корни многочлена $\varphi_n(x)$ как элемента из $\mathbb{R}[x]$ связаны с углами порядка n. Докажем аналогичное утверждение для поля $\mathbb{Z}_p$.

Теорема 2. *Пусть p — нечётный простой делитель многочлена $\varphi_n(x)$ для некоторого $x \in \mathbb{Z}$. Если p не делит n, то $p - 1 \equiv 0 \pmod n$ при $p \equiv 1 \pmod 4$ и $p + 1 \equiv 0 \pmod n$ при $p \equiv -1 \pmod 4$.*

Доказательство. Пусть $p \nmid n$. Рассмотрим возможные ситуации.

Предположим, что $p \equiv -1 \pmod 4$. Тогда по лемме 7.1 и лемме 6.2 имеем

$$\varphi_n(x) \equiv 0 \pmod p \quad \Rightarrow \quad p_n(x) \equiv 0 \pmod p \ \text{ и } \ q_n(x) \not\equiv 0 \pmod p.$$

Пусть $x \equiv \operatorname{tg}_p \alpha \pmod p$ для некоторого геометрического угла α. Тогда из леммы 6.3 следует сравнение $\operatorname{tg}_p n\alpha \equiv 0 \pmod p$, что даёт нам $n\alpha \in \{0, p+1\}$. Пусть m — такое наименьшее натуральное число, что $\operatorname{tg}_p m\alpha \equiv 0 \pmod p$. Это равносильно сравнению $m\alpha \equiv l(p+1) \pmod{2(p+1)}$, где l — некоторое целое число. Ясно, что $m \mid p+1$. Также $m \mid n$, так как $n\alpha \in \{0, p+1\}$, и m — такое наименьшее число, что $m\alpha \equiv l(p+1) \pmod{2(p+1)}$. Допустим, что $m < n$, но тогда $p_m(x) \equiv \equiv 0 \pmod p$. Так как p_m представимо как произведение фундаментальных многочленов, для некоторого $d \mid m$ получим $\varphi_d(x) \equiv 0 \pmod p$, причём $m \mid n$. Так как p_n тоже представимо как произведение фундаментальных многочленов, в котором $\varphi_d(x)$ и $\varphi_n(x)$ имеют общий

корень в поле $\mathbb{Z}_p$, мы получаем, что p_n имеет кратный корень в $\mathbb{Z}_p$. Это приводит к противоречию (см. теорему 1). Поэтому $m = n$ и $n \mid p+1$.

Предположим, что $p \equiv 1 \pmod 4$. Имеем

$$\varphi_n(x) \equiv 0 \pmod p \quad \Rightarrow \quad p_n(x) \equiv 0 \pmod p.$$

Тогда $x \not\equiv \pm j \pmod p$, где j — корень многочлена x^2+1 в $\mathbb{Z}_p$. Если $x \equiv \pm 1 \pmod p$, то $\varphi_4(x) \equiv 0 \pmod p$. Приведём значения многочленов p_n и q_n при $x \equiv \pm 1 \pmod p$:

n		0	1	2	3	4
1	$p_n(1)$	0	1	2	2	0
	$q_n(1)$	1	1	0	-2	-4
-1	$p_n(-1)$	0	-1	-2	-2	0
	$q_n(-1)$	1	1	0	-2	-4

При $n = 4$ получаем значения, которые отличаются от значений в случае $n = 0$ умножением на -4. Так как $p_n(x) \equiv 0 \pmod p$, получаем, что $4 \mid n$. Но тогда $n = 4$: иначе многочлен $p_n(x)$ будет иметь кратный корень, так как $\varphi_n(x) \equiv \varphi_4(x) \equiv 0 \pmod p$. Требуемое утверждение выполняется. Теперь можем считать, что $x \not\equiv \pm 1 \pmod p$ и $x \not\equiv \pm j \pmod p$. Тогда

$$\frac{p_2(x)}{q_2(x)} = \frac{2x}{1-x^2} = \operatorname{tg}_p \alpha$$

для некоторого угла α (конец § 5).

Пусть $n = 2n'$ — чётное число. Мы доказали следующее равенство многочленов:

$$p_n(x) = p_{n'}\left(\frac{p_2(x)}{q_2(x)}\right) q_2(x)^{n'},$$

где $q_2(x) \not\equiv 0 \pmod p$. Отсюда получаем

$$p_{n'}\left(\frac{p_2(x)}{q_2(x)}\right) \equiv 0 \pmod p \quad \Rightarrow \quad \operatorname{tg}_p n'\alpha \equiv 0 \pmod p.$$

Пусть m — порядок угла α. Ясно, что $m \mid (p-1)/2$ и $m \mid n'$. Предположим, что $m < n'$, тогда имеет место равенство

$$p_{2m}(x) = p_m\left(\frac{p_2(x)}{q_2(x)}\right) q_2(x)^m = 0.$$

Однако $2m$ делит n, и поэтому найдётся такое d, что $d \mid n$, $d < n$ и $\varphi_d(x) \equiv \equiv 0 \pmod p$, из чего следует, что $p_n(x)$ имеет кратный корень. Поэтому $m = n' \Rightarrow n \mid p-1$.

Пусть n — нечётное число. Мы уже доказали равенство многочленов

$$p_n\Big(\frac{p_2(x)}{q_2(x)}\Big)q_2(x)^n = p_{2n}(x) = p_2\Big(\frac{p_n(x)}{q_n(x)}\Big)q_n(x)^2 = 2p_n(x)q_n(x).$$

Правая часть даёт 0. Поэтому

$$p_n\Big(\frac{p_2(x)}{q_2(x)}\Big) \equiv 0 \pmod p \quad \Rightarrow \quad \operatorname{tg}_p n\alpha \equiv 0 \pmod p.$$

Пусть m — порядок α. Ясно, что $m \mid (p-1)/2$ и $m \mid n$. Пусть $m < n$. Тогда

$$p_m\Big(\frac{p_2(x)}{q_2(x)}\Big) \equiv 0 \pmod p.$$

Отсюда следует равенство

$$p_{2m}(x) = p_m\Big(\frac{p_2(x)}{q_2(x)}\Big)q_2(x)^m = 0.$$

Кроме того, $2m$ делит $2n$. Найдётся такое d, что $d \mid 2m$ и $\varphi_d(x) \equiv 0 \pmod p$, причём $d \neq n$, так как иначе $n \mid 2m \Rightarrow n \mid m \Rightarrow m \geqslant n$. Тогда $p_{2m}(x)$ будет иметь кратный корень, что приводит к противоречию. Следовательно, $n = m \mid (p-1)/2$, из чего получаем $n \mid p-1$. □

Наконец, мы можем доказать следующее утверждение.

Теорема 3. *Для любого натурального k найдётся такое простое p, что $k \mid p+1$.*

Доказательство. Мы можем заменить k на любое его кратное, не теряя общности. Тогда будем считать, что $4 \mid k$ и k не является степенью простого числа. Заметим, что $\varphi_k(0) = 1$. Следовательно, $4 \mid x$. Отсюда получаем сравнение $\varphi_k(x) \equiv 1 \pmod 4$.

Пусть $k = 4k'$. Так как старший коэффициент многочлена $\varphi_k(x)$ равен 1, на интервале от его наибольшего корня до $+\infty$ выполнено неравенство $\varphi_k(x) \geqslant 0$. Поэтому между двумя наибольшими корнями имеем $\varphi_k(x) < 0$. Отметим, что $(2k'-1, 4k') = 1$, поэтому

$$\operatorname{tg} \frac{\pi}{4k'}(2k'-1) = \frac{1}{\operatorname{tg}(\pi/(4k'))}$$

будет максимальным корнем, а значение второго по величине корня будет не больше

$$\operatorname{tg} \frac{\pi}{4k'}(2k'-2) = \frac{1}{\operatorname{tg}(2\pi/(4k'))}.$$

Пусть $\alpha = \pi/(4k')$. Тогда длина интервала между двумя наибольшими корнями будет не меньше

$$\frac{1}{\operatorname{tg}\alpha} - \frac{1}{\operatorname{tg} 2\alpha} = \frac{1}{\operatorname{tg}\alpha} - \frac{1-\operatorname{tg}^2\alpha}{2\operatorname{tg}\alpha} \geqslant \frac{1}{\operatorname{tg}\alpha} - \frac{1}{2\operatorname{tg}\alpha} = \frac{1}{2\operatorname{tg}\alpha}.$$

Отметим, что $\operatorname{tg}\alpha \leqslant 1$ для нашего k. Обозначим текущее значение числа k через k_0. Посмотрим, как изменится наше рассуждение, если бы вместо k_0 была его степень k_0^t: в этом случае мы бы получили интервал длины не меньше $1/(2\operatorname{tg}(\pi/k_0^t))$. Так как $\operatorname{tg}\alpha \to 0$ при $\alpha \to 0$, найдётся такое t, что на нашем интервале мы найдём целое x, делящееся на k_0. Тогда для него $-\varphi_{k_0^t}(x)$ — натуральное число, и верны сравнения

$$-\varphi_{k_0^t}(x) \equiv -\varphi_{k_0^t}(0) \equiv -1 \pmod{k_0}.$$

Отсюда $-\varphi_{k_0^t}(x) \equiv 3 \pmod 4$ и $(-\varphi_{k_0^t}(x), k_0) = 1$. Поэтому среди простых делителей числа $-\varphi_{k_0^t}(x)$ найдётся такое p, что $p \equiv 3 \pmod 4$, p взаимно просто с k_0^t, и тогда $k \mid p+1$ по теореме 2. □

Следствие 1. *Для любого натурального k имеется бесконечно много простых вида $kn-1$.*

Доказательство. Предположим противное. По теореме 1 множество, состоящее из простых чисел требуемого вида, непусто. Тогда обозначим через p' наибольшее простое вида $p' = n'k - 1$. Согласно теореме 1 найдётся такое простое p, что $p+1$ кратно $k(n'+1)$. Поэтому существует натуральное m, для которого $p = k(n'+1)m - 1$. Так как $p > p'$, мы получаем противоречие. □

Мы уже знаем, что $p_n(x)$ можно разложить в произведение фундаментальных многочленов. Однако можно ли провести дальнейшее разложение многочлена $p_n(x)$, оставаясь в $\mathbb{Z}[x]$? Ответ на этот вопрос даёт

Лемма 7.5. *При $\nu_2(n) \leqslant 1$ многочлен $\varphi_n(x)$ неприводим над кольцом $\mathbb{Z}$. При $\nu_2(n) \geqslant 2$ многочлен $\varphi_n(x)$ представляется в виде произведения двух приведённых неприводимых многочленов, принадлежащих $\mathbb{Z}[x]$, и константы A следующим образом*:

$$\varphi_n(x) = A \prod_{\substack{k=0\\(k,n)=1\\s(k)=+1}}^{n-1} \Big(x - \operatorname{tg}\frac{\pi}{n}k\Big) \prod_{\substack{k=0\\(k,n)=1\\s(k)=-1}}^{n-1} \Big(x - \operatorname{tg}\frac{\pi}{n}k\Big),$$

где константа A равна старшему коэффициенту многочлена $\varphi_n(x)$.

Доказательство. Рассмотрим расширение $\mathbb{Q}\Big(\operatorname{tg}\frac{\pi}{n}k\Big)$, где $\operatorname{tg}\frac{\pi}{n}k$ — один из корней многочлена $\varphi_n(x)$. Мы можем подставить $\operatorname{tg}\frac{\pi}{n}k$ в формулу $p_r(x)/q_r(x)$, и тогда если $\operatorname{tg}\frac{\pi}{n}t$ определено, то оно принадлежит $\mathbb{Q}\Big(\operatorname{tg}\frac{\pi}{n}k\Big)$. Через $\operatorname{tg}\frac{\pi}{n}t$ можно выразить $\sin\frac{2\pi}{n}t$ и $\cos\frac{2\pi}{n}t$. Заметим,

что $\sin\frac{2\pi}{n}\frac{ln}{2}$ и $\cos\frac{2\pi}{n}\frac{ln}{2}$ принадлежат $\mathbb{Q}$ для любого $l\in\mathbb{Z}$. Поэтому при всех $t\in\mathbb{Z}$ числа $\sin\frac{2\pi}{n}t$ и $\cos\frac{2\pi}{n}t$ входят в $\mathbb{Q}\left(\operatorname{tg}\frac{\pi}{n}k\right)$.

Расширим поле $\mathbb{Q}\left(\operatorname{tg}\frac{\pi}{n}k\right)$ до поля $\mathbb{Q}\left(\operatorname{tg}\frac{\pi}{n}k\right)(i)$. Заметим, что

$$\dim_{\mathbb{Q}}\mathbb{Q}\left(\operatorname{tg}\frac{\pi}{n}k\right)(i)=\dim_{\mathbb{Q}}\mathbb{Q}\left(\operatorname{tg}\frac{\pi}{n}k\right)\dim_{\mathbb{Q}(\operatorname{tg}\frac{\pi}{n}k)}\mathbb{Q}\left(\operatorname{tg}\frac{\pi}{n}k\right)(i)=$$
$$=2\dim_{\mathbb{Q}}\mathbb{Q}\left(\operatorname{tg}\frac{\pi}{n}k\right),$$

где $\dim_K L$ — размерность поля L над его подполем K. Также заметим, что $\mathbb{Q}\left(\operatorname{tg}\frac{\pi}{n}k,i\right)$ содержит все корни из единицы

$$e^{i2\pi t/n}=\cos\frac{2\pi}{n}t+i\sin\frac{2\pi}{n}t.$$

Пересечение $\mathbb{Q}\left(\operatorname{tg}\frac{\pi}{n}k,i\right)$ и множества корней из единицы содержит все корни 4-й степени из единицы, т. е. $\pm1,\pm i$, и все корни n-й степени из единицы. Если в $\mathbb{Q}\left(\operatorname{tg}\frac{\pi}{n}k,i\right)$ перемножить два корня из единицы, мы снова получим корень из единицы. Поэтому в нашем расширении все корни из единицы будут иметь порядок $[n,4]$, и тогда размерность этого расширения будет делиться на $\varphi([n,4])$, так как, обозначив $[n,4]$ через m, имеем

$$\dim_{\mathbb{Q}}\mathbb{Q}\left(\operatorname{tg}\frac{\pi}{n}k\right)(i)=\dim_{\mathbb{Q}(e^{2\pi i/m})}\mathbb{Q}\left(\operatorname{tg}\frac{\pi}{n}k\right)(i)\dim_{\mathbb{Q}}\mathbb{Q}(e^{2\pi i/m})=$$
$$=\dim_{\mathbb{Q}(e^{2\pi i/m})}\mathbb{Q}\left(\operatorname{tg}\frac{\pi}{n}k\right)(i)\varphi(m).$$

Отсюда

$$\dim_{\mathbb{Q}}\mathbb{Q}(\operatorname{tg}\frac{\pi}{n}k)\geqslant\frac{\varphi([n,4])}{2}.$$

Поэтому степень минимального многочлена $\operatorname{tg}\frac{\pi}{n}k$ будет не меньше $\frac{1}{2}\varphi([n,4])$.

Если $\nu_2(n)\leqslant1$, то $\deg\varphi_n(x)=\varphi(n)=\frac{1}{2}\varphi([n,4])$, за исключением случая $n=2$, когда $\operatorname{tg}(\pi/2)$ не определён и $\varphi_2(x)=2$. Иначе положим $n=4n'$. Тогда

$$q_{2n'}(x)=q_{n'}^2(x)-p_{n'}^2(x)=(q_{n'}(x)-p_{n'}(x))(q_{n'}(x)+p_{n'}(x)).$$

Мы также знаем, что

$$p_{4n'}(x)=2p_{2n'}(x)q_{2n'}(x).$$

Ясно, что $\varphi_n(x)$ не входит в разложение многочлена $p_{2n'}(x)$ на фундаментальные многочлены, но присутствует в разложении многочлена $p_{4n'}(x)$, поэтому

$$\varphi_n(x)\mid2q_{2n'}(x)=2(q_{n'}(x)-p_{n'}(x))(q_{n'}(x)+p_{n'}(x)),$$

где под делимостью понимается делимость многочленов в $\mathbb{Z}[x]$. Заметим, что многочлен $q_{n'}(x) - p_{n'}(x)$ не имеет общих корней с $q_{n'}(x)$, поэтому его корни соответствуют $1 = p_{n'}(x)/q_{n'}(x)$; другими словами, $\operatorname{tg}(n' \operatorname{arctg} x) = 1$, но тогда все его корни — это числа вида $\operatorname{tg} \frac{\pi}{4n'}k$, где k нечётно и $s(k) = +1$. Аналогично все корни многочлена $q_{n'}(x) + p_{n'}(x)$ — числа вида $\operatorname{tg} \frac{\pi}{4n'}k$, где k нечётно и $s(k) = -1$. Понятно, что

$$q_{n'}(x) + p_{n'}(x), q_{n'}(x) - p_{n'}(x) \in \mathbb{Z}[x].$$

Рассмотрим разложение $\varphi_n(x)$ на неприводимые многочлены над $\mathbb{Z}[x]$. Так как $\varphi_n(x) \mid 2(q_{n'}(x) - p_{n'}(x))(q_{n'}(x) + p_{n'}(x))$, каждый неприводимый множитель в этом разложении будет иметь корни вида $\operatorname{tg} \frac{\pi}{4n'}k$, где $2 \nmid k$, и либо все они имеют $s(k) = 1$, либо $s(k) = -1$. Тогда $\varphi_n(x)$ представим как произведение хотя бы двух многочленов. Так как степень минимального многочлена $\operatorname{tg} \frac{\pi}{n}k$, где $(k, n) = 1$, должна быть хотя бы $\frac{1}{2}\varphi(n)$, мы заключаем, что $\varphi_n(x)$ представим в виде произведения ровно двух многочленов степени $\frac{1}{2}\varphi(n)$. Также если n — степень двойки, то $c(\varphi_n(x)) = 2$, и мы можем представить $\varphi_n(x)$ как $\pm 2\left(\frac{1}{\pm 2}\varphi_n(x)\right)$, где $\frac{1}{\pm 2}\varphi_n(x) \in \mathbb{Z}[x]$. Старший коэффициент многочлена $\frac{1}{\pm 2}\varphi_n(x)$ равен 1 (знак зависит от того, равно ли число n четырём). Отсюда следует требуемое. □

Приложение

§ 1. Другой подход к вопросу о несоизмеримости углов

Результаты о несоизмеримости углов (с. 74–77) могут быть получены другим способом. Известно, что размерность $\mathbb{Q}(e^{(2\pi i/n)+m})$ над полем $\mathbb{Q}$ равна $\varphi(n)$, где m и n взаимно просты. Заметим, что если n имеет ровно k простых делителей $p_1, \ldots, p_k$, то верно неравенство

$$\varphi(n) = n \cdot \prod_{i=1}^{k} \frac{p_i - 1}{p_i} \geqslant n \cdot \prod_{i=2}^{k+1} \frac{i-1}{i} = \frac{n}{k+1} \geqslant \frac{n}{\log_2 n + 1}.$$

Поэтому для всякого M существует такое N, что $\varphi(n) > M$ при $n > N$. Тогда пересечение любого конечного расширения поля $\mathbb{Q}$ и множества $\{e^{i2\pi\theta} \mid \theta \in \mathbb{Q}\}$ образует группу по умножению. Она конечна: иначе найдётся элемент l, для которого значение $\varphi(l)$ превосходит размерность

расширения. Обозначим эту группу через G. Для любого элемента $z \in G$ верно равенство $z^{|G|} = 1$, из чего получаем, что G состоит из корней уравнения $z^{|G|} = 1$. Тогда $\varphi(|G|)$ делит размерность расширения.

Если мы рассмотрим пересечение $\mathbb{Q}(i)$ и $\{e^{i2\pi\theta} \mid \theta \in \mathbb{Q}\}$, то получим, что 4 делит $|G|$, так как подмножество $\{1, i, -1, -i\} \subseteq G$ образует подгруппу из четырёх элементов. В то же время $\varphi(|G|) \leqslant 2$, из чего следует $|G| = 4$.

Если рассматриваемое расширение есть $\mathbb{Q}(e^{2\pi i/n})$ при $2 \mid n$, то $n \mid |G|$, и в то же время $\varphi(|G|) \leqslant \varphi(n)$. Так как $2 \mid n$, значение $\varphi(nt)$ не превосходит $\varphi(n)$ лишь при $t = 1$. Поэтому G состоит из чисел вида $\{e^{i2\pi k/n} \mid k \in \mathbb{Z}\}$. Это можно применить к расширениям

$$\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(e^{2\pi i/8}) \quad \text{и} \quad \mathbb{Q}(i, \sqrt{3}) = \mathbb{Q}(e^{2\pi i/12}).$$

§ 2. Быстрое преобразование Фурье

Быстрое преобразование Фурье (FFT) рассматривается в статье М. Я. Кельберта [1]. Известно, что существует обобщение дискретного преобразования Фурье для случая конечных полей. Рассмотрим это обобщение. Пусть $p \equiv 3 \pmod 4$.

Ортогональный базис. Наличие корней из единицы позволяет построить базис в пространстве функций, действующих из $\mathbb{Z}/(p+1)\mathbb{Z}$ в $\mathbb{Z}_p(i)$. Определим билинейное отображение, действующее на функциях f и g, следующим образом:

$$\langle f, g \rangle = \sum_{k=0}^{p} f(k) g(-k). \tag{1}$$

В качестве базиса рассмотрим набор функций вида $f_z(k) = z^k$, где через z обозначен один из корней уравнения $z^{p+1} - 1$: для любой пары корней z_1 и z_2 имеем

$$\langle f_{z_1}, f_{z_2} \rangle = \sum_{k=0}^{p} (z_1 z_2^{-1})^k.$$

Если $z_1 \neq z_2$, то $\langle f_{z_1}, f_{z_2} \rangle = 0$, иначе получим $p + 1 \equiv 1 \pmod p$. Если существует линейная комбинация наших функций, дающая 0, в которой при некотором f_z стоит ненулевой коэффициент, то применение к ней и к $f(z)$ билинейного отображения (1) дает 0, так как $\langle 0, f_z \rangle = 0$. С другой стороны, мы получим ненулевой коэффициент перед f_z, что противоречит выбору линейной комбинации.

FFT. Мы можем рассмотреть аналоги FFT по модулю простого числа, включая многомерные преобразования Фурье. Интерес могут представлять случаи простых чисел Мерсенна, например, числа $2^{19}-1$ и $2^{31}-1$. Если $p=2^q-1$, то существует алгоритм для преобразования Фурье, который использует корни уравнения $z^{2^t}=1$, $t\leqslant q$, $t\in\mathbb{N}$, принадлежащие $\mathbb{Z}_p(i)$. Отметим, что в этом случае можно найти корень из единицы порядка 2^q: произвольно выбранный корень из единицы с вероятностью $1/2$ окажется корнем порядка 2^q. При достаточном количестве повторений этой операции вероятность получить корень порядка 2^q стремится к 1. Кроме того, если размерности рассматриваемых объектов (многочленов, матриц и т. д.) достаточно малы, то можно сначала применить преобразование Фурье по модулю $2^{19}-1$ и по модулю $2^{31}-1$, а затем восстановить числа по двум остаткам. Стоит отметить, что возможны более эффективные реализации операции взятия остатка по модулю простых чисел данного вида, так как модуль имеет вид 2^q-1.

Заключение

Нами были рассмотрены аналоги углов и тригонометрических функций в $\mathbb{Z}_p$. В дальнейшем можно попробовать ввести гиперболические углы, для которых, вероятно, мощность группы решений будет равна $p-1$ в обоих случаях. Далее можно попытаться задать аналоги гиперболических функций sinh, cosh, tanh.

Благодарности

Автор признателен А. Я. Канель-Белову за помощь в работе над статьёй.

Список литературы

[1] *Кельберт М. Я.* Что такое преобразование Фурье? // Математическое просвещение. Сер. 3. Вып. 4. М.: МЦНМО, 2000. С. 188–202. http://mi.mathnet.ru/mp66

Абдуламин Русланович Исмаилов, студент матфака ВШЭ
nameundefinednamovich@gmail.com