Федеральное государственное автономное
образовательное учреждение высшего образования
«Национальный исследовательский университет
«Высшая школа экономики»

Факультет математики

Беребердина Наталья Александровна

Обратимые элементы в кольцах вычетов

Курсовая работа студента 1 курса
образовательной программы бакалавриата «Математика»

Научный руководитель:
Левин Андрей Михайлович
Профессор: Факультет математики
Доктор физико-математических наук

Москва 2022

Содержание

1 Введение **3**

2 Разложение группы $(\mathbb{Z}/p^n\mathbb{Z})^*$ **3**
2.1 Справки 3
2.2 Отображение из $(\mathbb{Z}/p^n\mathbb{Z})^*$ в $(\mathbb{Z}/p\mathbb{Z})^*$ 3
2.3 Отображение групп корней 3
2.4 Разложение группы $(\mathbb{Z}/p^n\mathbb{Z})^*$ 4

3 p-адические числа **5**
3.1 Целые p-адические числа 5
3.2 Обратимые элементы в кольце p-адических чисел 5
3.3 Разложение группы $\mathbb{Z}_p^*$ 5

1 Введение

Целью данной работы является изучение групп обратимых элементов в кольце вычетов по модулю степени простого p ($(\mathbb{Z}/p^n\mathbb{Z})^*$) и обратимых элементов в p-адических числах ($\mathbb{Z}_p^*$).

2 Разложение группы $(\mathbb{Z}/p^n\mathbb{Z})^*$

2.1 Справки

Здесь и далее мы будем считать число p простым.

Для начала рассмотрим группу $(\mathbb{Z}/p\mathbb{Z})$. Обратимыми в ней будут все ненулевые элементы, таким образом $((\mathbb{Z}/p\mathbb{Z}^*), \cdot) \simeq ((\mathbb{Z}/(p-1)\mathbb{Z}), +)$. Рассмотрим теперь группу $(\mathbb{Z}/p^n\mathbb{Z})$. В ней обратимыми элементами будут все элементы взаимопростые с p^n, то есть

$$\{x \in (\mathbb{Z}/p^n\mathbb{Z}) : p \nmid x\} = (\mathbb{Z}/p^n\mathbb{Z})^*$$

Для начала заметим, что это действительно группа по умножению. Теперь мы хотим определить ее структуру, найдя более простую гомеоморфную ей.

2.2 Отображение из $(\mathbb{Z}/p^n\mathbb{Z})^*$ в $(\mathbb{Z}/p\mathbb{Z})^*$

Давайте заметим, что существует естественное отображение μ из $\mathbb{Z}/p^n\mathbb{Z}$ в поле $\mathbb{Z}/p\mathbb{Z}$. Рассмотрим его ограничение на множестве $(\mathbb{Z}/p^n\mathbb{Z})^*$ - оно перейдет в $(\mathbb{Z}/p\mathbb{Z})^*$. Кроме того, это отображение согласовано с операцией умножения в $\mathbb{Z}/p^n\mathbb{Z}$, то есть является гомоморфизмом. Давайте теперь посмотрим на его ядро. В единицу перейдут все элементы с остатком 1 при делении на p^{n-1}, а именно группа:

$$U_p[n] = \{x \in \mathbb{Z}_p^* : x \equiv 1 \pmod{p^n}\}$$

2.3 Отображение групп корней

Заведем теперь множество корней из единицы $p-1$ степени $\gamma_n \subset \mathbb{Z}/p^n\mathbb{Z}^*$, а именно:

$$\gamma_n = \{x \in \mathbb{Z}/p^n\mathbb{Z}^* : x^{p-1} \equiv 1 \pmod{p^n}\}$$

Нетрудно заметить, что они образуют группу.

Теперь построим отображение $\tau[i]$ из γ_{i-1} в γ_i. Будем строить его так, чтобы оно сохраняло результат малой теоремы Ферма, а именно

$$(\tau[i](\varepsilon))^{p-1} \equiv 1 \pmod{p^i}$$

Рассмотрим такое α, что

$$\alpha^{p-1} \equiv 1 \pmod{p^i} \Rightarrow \alpha^{p-1} \equiv 1 + lp^i \pmod{p^{i+1}}$$

Найдем $\alpha + kp^i$, такое что

$$(\alpha + kp^i)^{p-1} \equiv 1 \pmod{p^{i+1}}$$

Раскроем скобки

$$(\alpha + kp^i)^{p-1} \equiv \alpha^{p-1} + (p-1)\alpha^{p-2}kp^i \pmod{p^{i+1}}(\Rightarrow)$$

$$\circledRightarrow 1 + lp^i - \alpha^{p-2}kp^i \equiv 1 + p^i(l - \alpha^{p-2}k) \pmod{p^{i+1}} \Rightarrow p^i(l - \alpha^{p-2}k) \equiv 0 \pmod{p^{i+1}} \circledRightarrow$$

$$\circledRightarrow l - \alpha^{p-2}k \equiv 0 \pmod{p} \Rightarrow k = l\alpha$$

Значит для любого α найдет нужный k и при том единственный. Тогда построим $\tau[i] : \mathbb{Z}/p^{i-1}\mathbb{Z}^* \to \mathbb{Z}/p^i\mathbb{Z}^*$:

$$\tau[i](\alpha) = \alpha(1 + lp^i)$$

Не трудно заметить, что τ - гомоморфизм. Действительно, пусть есть два элемента α и β в $\mathbb{Z}/p^i\mathbb{Z}^*$:

$$\tau[i](\alpha) = \alpha(1 + lp^i),\ \tau[i](\beta) = \beta(1 + kp^i) \circledRightarrow$$

$$\circledRightarrow \tau[i](\alpha) \cdot \tau[i](\beta) = \alpha(1 + kp^i) \cdot \beta(1 + kp^i) =$$

$$= \alpha\beta(1 + kp^i + lp^i) = \alpha\beta(1 + kp^i + lp^i + lkp^{2i} = \tau[i](\alpha\beta)$$

Тогда образ τ образует группу:

$$im\ \tau[i] \simeq \gamma_{i-1}$$

2.4 Разложение группы $(\mathbb{Z}/p^n\mathbb{Z})^*$

Теперь давайте посмотрим на композицию отображений $\tau[i]$:

$$T[n] = \tau[n] \circ \tau[n-1] \circ ...\tau[2]$$

Заметим, что $T[n] : \gamma_1 \to \gamma_n$ является композицией гомоморфизмов, а значит и сам является гомоморфизмом.

Докажем теперь по индукции, что образ $T[n] = \gamma_1$.

База:

$$im\ T[2] = im\ \tau[2] = \gamma_1$$

Переход:

$$im\ T[n] = \tau[n](im\ T[n-1])$$

Т.к. $im\ T[n-1] = \gamma_1$ и $\tau[n]$ гомоморфизм, то $\tau[n](im\ T[n-1]) = \gamma_1$, что, в свою очередь изоморфно $\mathbb{Z}/p\mathbb{Z}^*$.

Таким образом:

$$im\ T[n] = \mathbb{Z}/p\mathbb{Z}$$

Теперь, когда мы построили два гомоморфизма $\mu : (\mathbb{Z}/p^n\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$ и $T : (\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p^n\mathbb{Z})^*$, мы можем задать структуру $(\mathbb{Z}/p^n\mathbb{Z})^*$:

$$(\mathbb{Z}/p^n\mathbb{Z})^* \simeq ker\ \mu \times im\ [n] \simeq U_p\ \times \mathbb{Z}/p\mathbb{Z}^*$$

Забегая вперед, скажем, что $U_p \simeq \mathbb{Z}/p^{n-1}Z$ (к доказательству этого факта мы вернемся в 3 пункте) и тогда последнее равенство завершается красивым результатом:

$$(\mathbb{Z}/p^n\mathbb{Z})^* \simeq \mathbb{Z}/p^{n-1}Z \times \mathbb{Z}/p\mathbb{Z}^*$$

3 p-адические числа

3.1 Целые p-адические числа

Целым p-адическим числом для простого p называется бесконечная последовательность x_n, где x_i - остаток по модулю p^n и выполняется условие:

$$x_n \equiv x_{n+1} \pmod{p^n}$$

Тогда если определить сложение и умножение целых p-адических чисел, как почленное сложение и умножение, на целых p-адических числах выполняются аксиомы кольца. Это кольцо обозначается $\mathbb{Z}_p$. Не трудно заметить, что целые числа естественно вкладываются в кольцо целых p-адических и являются в нем подкольцом. Таким образом, можно рассматривать $\mathbb{Z}_p$ как расширение $\mathbb{Z}$.

3.2 Обратимые элементы в кольце p-адических чисел

Заметим, что элемент x заданный последовательностью x_n - не обратим при $x_1 = 0$ (единица в $\mathbb{Z}_p$ задается последовательностью $x_n = 1$ для $\forall n$). Покажем, что для $\forall$ x заданного x_n с $x_1 \neq 0$ - элемент x обратим.

Действительно, если $x_1 \neq 0$, то для $\forall i$ $p \nmid x_i$. Тогда мы знаем, что каждый элемент последовательности обратим. Более того, мы умеем строить обратное p-адическое число. Рассмотрим α такой, что $x_1\alpha_1 \equiv 1 \pmod{p}$. Тогда построим $\alpha_2 = \tau[2](\alpha_1)$. Заметим, что по построению

$$\alpha_1 \equiv \alpha_2 \pmod{p^2} \alpha_2 x_2 = 1$$

Теперь построим аналогично все число α. Для этого зададим его последовательностью $\alpha_i = \tau[i](\alpha_i - 1)$. Тогда мы поняли вид всех обратимых элементов в $\mathbb{Z}_p$.

3.3 Разложение группы $\mathbb{Z}_p^*$

Из прошлого пункта мы поняли, что

$$\mathbb{Z}_p^* = \{x \in \mathbb{Z}_p : x_1 \neq 0 \pmod{p}\}$$

Тогда

$$\mathbb{Z}_p^* \simeq \mathbb{Z}_p \backslash p\mathbb{Z}_p \simeq \mathbb{F}_p^* \times p\mathbb{Z}_p$$

Заметим, что $\mathbb{Z}_p^*$ - группа по умножению. Теперь опишем ее структуру. Зададим такую группу

$$U_p = \{x \in \mathbb{Z}_p^* : x \equiv 1 \pmod{p^t}\}$$

где $t = 2$, при $p = 2$, $t = 1$ иначе.

Построим отображение, определяемое рядом

$$\exp x = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

Заметим, что подставляя туда элементы из $p^t\mathbb{Z}_p$ мы будем получать элементы U_p. Для этого введем обозначение степени вхождения простого числа p в число x : $deg_p(x)$. Докажем, что

$$deg_p(px)^n \geq n \geq deg_p(n!)$$

Для подсчета степени вхождения p в $n!$ посчитаем количество множителей делящихся на каждую степень p и воспользуемся суммой геометрической прогрессии:

$$deg_p(n!) \leq \frac{n}{p} + \frac{n}{p^2} + \frac{n}{p^3} + ... = \frac{n}{p(1-\frac{1}{p})} = \frac{n}{p-1} \leq n$$

Заметим, что последнее неравенство может обернуться в равенство только при $p = 2$. Отсюда берется необходимость $t = 2$ при $p = 2$. Действительно, $deg_p^2(px)^n = 2n > \frac{n}{p-1}$ при $\forall p$.

Таким образом, все слагаемые, начиная со второго, буду иметь вид $x' \cdot p^i/j$, причем $i > 0$, $j \in \mathbb{Z}_p^*$, значит деление на j определено и тогда

$$\exp x = \sum_{n=0}^{\infty} \frac{x^n}{n!} = 1 + \sum_{n=1}^{\infty} \frac{x^n}{n!} = 1 + p \cdot j \in U_p$$

Более того, это отображение задает гомоморфизм из $(p^t\mathbb{Z}_p, +)$ в $(U_p, \cdot)$.

Действительно, заметим, что

$$\exp x \cdot \exp y = \sum_{n=0}^{\infty} \frac{x^n}{n!} \cdot \sum_{m=0}^{\infty} \frac{y^m}{m!} =$$

$$= \sum_{n=0,m=0}^{\infty} \frac{x^n y^m}{n!m!} = \exp xy$$

На самом деле, это и изоморфизм, так как мы можем построить и обратное отображение (которое тоже будет гомоморфизмом), задаваемое рядом:

$$\log(x) = \sum_{i=0}^{\infty} (-1)^{n+1} \frac{(x-1)^{n+1}}{n}$$

Таким образом, $p^t\mathbb{Z}_p \simeq U_p$. Тогда, вернувшись к пункту 2.4, получим, что

$$U_p[n] \simeq U_p/p^n\mathbb{Z}_p \simeq p\mathbb{Z}_p/p^n\mathbb{Z}/p \simeq \mathbb{Z}/p^{n-t}Z$$

Тогда мы действительно получили разложение $\mathbb{Z}/p^n\mathbb{Z}^*$. Теперь вспомним рекурсивное разложение написанное выше:

$$\mathbb{Z}_p^* \simeq Z/p^tZ^* \times p^t\mathbb{Z}_p$$

Зная теперь разложение $p^t\mathbb{Z}_p$, наконец получим

$$\mathbb{Z}_p^* \simeq Z/p^tZ^* \times U_p$$

где $t = 2$, при $p = 2$, $t = 1$ иначе.

Список литературы

[1] Виноградов И.М. "Основы теории чисел"., *Объединенное научно-техническое издательство НКТП СССР*, (1936)