7. Китайская теорема об остатках (окончание)

Китайская теорема об остатках.

Пусть $t \in \mathbb{N}_0$, $n_1, \ldots, n_t \in \mathbb{N}$ *и числа* $n_1, \ldots, n_t$ *попарно взаимно просты.*

Обозначим через n *число* $n_1 \cdot \ldots \cdot n_t$*; тогда отображение, действующее из* $\mathbb{Z}/n$ *в* $\mathbb{Z}/n_1 \times \ldots \times \mathbb{Z}/n_t$ *по правилу* $a \mapsto (a \bmod n_1, \ldots, a \bmod n_t)$ *для любых* $a \in \mathbb{Z}/n$, *— изоморфизм колец.*

Доказательство.

• Легко видеть, что рассматриваемое отображение — гомоморфизм колец.

• Числа $n_1, \ldots, n_t$ попарно взаимно просты $\Rightarrow$ рассматриваемое отображение — инъекция.

• Из предыдущих двух фактов, принципа Дирихле и того, что $|\mathbb{Z}/n| = |\mathbb{Z}/n_1 \times \ldots \times \mathbb{Z}/n_t| < \infty$, следует, что рассматриваемое отображение — изоморфизм колец. $\square$

Замечания.

• Для каждого числа $j \in \{1, \ldots, t\}$ зафиксируем соотношение Безу для чисел $\frac{n}{n_j}$ и n_j: $u_j \frac{n}{n_j} + v_j n_j = 1$, где $u_j, v_j \in \mathbb{Z}$. Пусть $a_1 \in \mathbb{Z}/n_1, \ldots, a_t \in \mathbb{Z}/n_t$; обозначим через a число $(u_1 \frac{n}{n_1} a_1 + \ldots + u_t \frac{n}{n_t} a_t) \bmod n$; тогда $\forall\, j \in \{1, \ldots, t\}$ $(a \bmod n_j = a_j)$. Отсюда следует, что отображение, действующее из $\mathbb{Z}/n_1 \times \ldots \times \mathbb{Z}/n_t$ в $\mathbb{Z}/n$ по правилу $(a_1, \ldots, a_t) \mapsto (u_1 \frac{n}{n_1} a_1 + \ldots + u_t \frac{n}{n_t} a_t) \bmod n$ для любых $(a_1, \ldots, a_t) \in \mathbb{Z}/n_1 \times \ldots \times \mathbb{Z}/n_t$, — изоморфизм колец, обратный к изоморфизму, рассматриваемому в китайской теореме об остатках.

• Пусть $p, q \in \mathbb{P}$, $p \neq q$ и числа p и q имеют порядка N знаков в двоичной записи (например, $N = 1024$ или $N = 2048$); обозначим через n число pq. Китайская теорема об остатках дает явный и эффективный изоморфизм между кольцами $\mathbb{Z}/n$ и $\mathbb{Z}/p \times \mathbb{Z}/q$; при этом производить вычисления в кольце $\mathbb{Z}/p \times \mathbb{Z}/q$ (в этом кольце мы имеем дело с парами чисел длины порядка N) можно быстрее, чем в кольце $\mathbb{Z}/n$ (в этом кольце мы имеем дело с числами длины порядка $2N$).

8. Элементарная теория чисел

Определение. *Функция Эйлера* ϕ есть отображение, действующее из $\mathbb{N}$ в $\mathbb{N}$ по следующему правилу: $n \mapsto$ $\mapsto |\{a \in \{0, \ldots, n-1\} \mid \gcd(a, n) = 1\}|$ для любых $n \in \mathbb{N}$.

Примеры: $\phi(1) = 1$; для любого простого числа p выполнено $\phi(p) = p - 1$.

Лемма об обратимых остатках.

Пусть $n \in \mathbb{N}$ *и* $a \in \mathbb{Z}/n$*; тогда* $a \in (\mathbb{Z}/n)^\times \Leftrightarrow \gcd(a, n) = 1 \Leftrightarrow \langle a \rangle = (\mathbb{Z}/n)^+$.

Доказательство.

• $a \in (\mathbb{Z}/n)^\times \Rightarrow \exists\, u, v \in \mathbb{Z}\ (ua + vn = 1) \Rightarrow \gcd(a, n) = 1$.

• $\gcd(a, n) = 1 \Rightarrow \operatorname{ord}(a) = \frac{n}{\gcd(a,n)} = n$ (в группе $(\mathbb{Z}/n)^+$) $\Rightarrow \langle a \rangle = (\mathbb{Z}/n)^+$.

• $\langle a \rangle = (\mathbb{Z}/n)^+ \Rightarrow 1 \in \langle a \rangle \Rightarrow \exists\, u, v \in \mathbb{Z}\ (ua + vn = 1) \Rightarrow a \in (\mathbb{Z}/n)^\times$. $\square$

Замечания.

• Пусть $n \in \mathbb{N}$; тогда $|(\mathbb{Z}/n)^\times| = \phi(n) = |\{d \in \mathrm{C}_n \mid \mathrm{C}_n = \langle d \rangle\}|$.

• Пусть $n \in \mathbb{N}$, $a \in \mathbb{Z}/n$ и $\gcd(a, n) = 1$; тогда (a^{-1} в группе $(\mathbb{Z}/n)^\times$) = (коэффициент перед a в соотношении Безу для чисел a и n). В вопросе 7 курса было доказано, что коэффициенты Безу можно находить эффективно, используя расширенный алгоритм Евклида.

• Пусть R — коммутативное кольцо, в котором имеется алгоритм деления с остатком (примеры: кольца $\mathbb{Z}$, $\mathbb{Z}[\mathrm{i}]$ и $\mathbb{Z}[\frac{1+\sqrt{3}\mathrm{i}}{2}]$; кольца $K[x]$, где K — поле), и $r, s \in R$; тогда $s + rR \in (R/rR)^\times \Leftrightarrow \gcd(r, s) \in R^\times$. Доказательство импликации "$\Rightarrow$" аналогично доказательству для кольца $\mathbb{Z}$; доказательство импликации "$\Leftarrow$": $\gcd(r, s) \in R^\times \Rightarrow \exists\, u, v \in R\ (us + vr = 1)$ (из наличия алгоритма деления с остатком для кольца R следует наличие соотношения Безу) и $\exists\, u, v \in R\ (us + vr = 1) \Rightarrow s + rR \in (R/rR)^\times$ (это очевидно).

Теорема Эйлера. *Пусть* $n \in \mathbb{N}$, $a \in \mathbb{Z}$ *и* $\gcd(a, n) = 1$*; тогда* $a^{\phi(n)} \equiv 1 \pmod{n}$.

Доказательство.

Для любой конечной группы G выполнено $\forall\, g \in G\ (g^{|G|} = 1)$; в частности, в случае группы $(\mathbb{Z}/n)^\times$ имеем $\forall\, a \in (\mathbb{Z}/n)^\times\ (a^{\phi(n)} = 1)$; переходя к кольцу $\mathbb{Z}$, получаем требуемое сравнение по модулю n. $\square$

Замечания.

• Пусть $n \in \mathbb{N}$, $a \in \mathbb{Z}$, $\gcd(a, n) = 1$ и $k \in \mathbb{Z}$; тогда $a^k \equiv a^{k \bmod \phi(n)} \pmod{n}$.

• Малая теорема Ферма: пусть $p \in \mathbb{P}$, $a \in \mathbb{Z}$ и $p \nmid a$; тогда $a^{p-1} \equiv 1 \pmod{p}$.

• Пусть $p \in \mathbb{P}$, $a \in \mathbb{Z}$, $p \nmid a$ и $k \in \mathbb{Z}$; тогда $a^k \equiv a^{k \bmod (p-1)} \pmod{p}$.

• Вычислим 2^{340} в кольце $\mathbb{Z}/341$, используя то, что $341 = 11 \cdot 31$ и $2^{10} - 1 = 3 \cdot 11 \cdot 31$: $2^{340} \overset{\mathrm{CRT}}{\longmapsto} (2^{340} \bmod 11, 2^{340} \bmod 31) = (1, 2^{10} \bmod 31) = (1,1) \Rightarrow 2^{340} = 1$.

• Вычислим 2^{1638} в кольце $\mathbb{Z}/3277$, используя то, что $3277 = 29 \cdot 113$ и $2^{14} + 1 = 5 \cdot 29 \cdot 113$: $2^{1638} \overset{\mathrm{CRT}}{\longmapsto} (2^{1638} \bmod 29, 2^{1638} \bmod 113) = (2^{14} \bmod 29, 2^{70} \bmod 113) = (-1,-1) \Rightarrow 2^{1638} = -1$.

Теорема о функции Эйлера.

1. Пусть $m, n \in \mathbb{N}$ и $\gcd(m,n) = 1$; тогда $\phi(mn) = \phi(m)\phi(n)$.

2. Пусть $n \in \mathbb{N}$; представим число n в виде $p_1^{\omega_1} \cdot \ldots \cdot p_t^{\omega_t}$, где $t \in \mathbb{N}_0$, $p_1, \ldots, p_t \in \mathbb{P}$, числа $p_1, \ldots, p_t$ попарно различны и $\omega_1, \ldots, \omega_t \in \mathbb{N}$; тогда $\phi(n) = n\bigl(1 - \frac{1}{p_1}\bigr) \cdot \ldots \cdot \bigl(1 - \frac{1}{p_t}\bigr)$.

Доказательство.

1. Китайская теорема об остатках $\Rightarrow \mathbb{Z}/mn \cong \mathbb{Z}/m \times \mathbb{Z}/n \Rightarrow$ $\Rightarrow (\mathbb{Z}/mn)^\times \cong (\mathbb{Z}/m)^\times \times (\mathbb{Z}/n)^\times \Rightarrow |(\mathbb{Z}/mn)^\times| = |(\mathbb{Z}/m)^\times|\,|(\mathbb{Z}/n)^\times| \Rightarrow \phi(mn) = \phi(m)\phi(n)$.

2. Пусть $p \in \mathbb{P}$ и $\omega \in \mathbb{N}$; тогда $(\mathbb{Z}/p^\omega)^\times = \mathbb{Z}/p^\omega \setminus p\,(\mathbb{Z}/p^\omega)$ (и, значит, $\phi(p^\omega) = p^{\omega-1}(p-1)$).

Пункт 1 $\Rightarrow \phi(n) = \phi(p_1^{\omega_1}) \cdot \ldots \cdot \phi(p_t^{\omega_t})$; соображение из предыдущей строки $\Rightarrow \phi(p_1^{\omega_1}) \cdot \ldots \cdot \phi(p_t^{\omega_t}) = p_1^{\omega_1-1}(p_1-1) \cdot \ldots \cdot p_t^{\omega_t-1}(p_t-1) = p_1^{\omega_1}\bigl(1-\frac{1}{p_1}\bigr) \cdot \ldots \cdot p_t^{\omega_t}\bigl(1-\frac{1}{p_t}\bigr) = n\bigl(1-\frac{1}{p_1}\bigr) \cdot \ldots \cdot \bigl(1-\frac{1}{p_t}\bigr)$. □

Теорема о группах обратимых остатков.

1. Пусть $n \in \mathbb{N}$; представим число n в виде $p_1^{\omega_1} \cdot \ldots \cdot p_t^{\omega_t}$, где $t \in \mathbb{N}_0$, $p_1, \ldots, p_t \in \mathbb{P}$, числа $p_1, \ldots, p_t$ попарно различны и $\omega_1, \ldots, \omega_t \in \mathbb{N}$; тогда $(\mathbb{Z}/n)^\times \cong (\mathbb{Z}/p_1^{\omega_1})^\times \times \ldots \times (\mathbb{Z}/p_t^{\omega_t})^\times$.

2. Пусть $p \in \mathbb{P} \setminus \{2\}$ и $\omega \in \mathbb{N}$, или $p = 2$ и $\omega \in \{1,2\}$; тогда $(\mathbb{Z}/p^\omega)^\times \cong \mathrm{C}_{p^{\omega-1}(p-1)}$.

3. Пусть $\omega \in \mathbb{N} \setminus \{1,2\}$; тогда $(\mathbb{Z}/2^\omega)^\times \cong \mathrm{C}_2 \times \mathrm{C}_{2^{\omega-2}}$.

Доказательство.

1. Китайская теорема об остатках $\Rightarrow \mathbb{Z}/n \cong \mathbb{Z}/p_1^{\omega_1} \times \ldots \times \mathbb{Z}/p_t^{\omega_t} \Rightarrow (\mathbb{Z}/n)^\times \cong (\mathbb{Z}/p_1^{\omega_1})^\times \times \ldots \times (\mathbb{Z}/p_t^{\omega_t})^\times$.

2. Следующее утверждение будет доказано позже (в доказательстве будет использоваться задача 21 у группы SE): пусть $p \in \mathbb{P}$; тогда существует первообразный корень по модулю p (и, значит, $(\mathbb{Z}/p)^\times \cong \mathrm{C}_{p-1}$). Зафиксируем некоторый первообразный корень d по модулю p; тогда, если $p \in \mathbb{P} \setminus \{2\}$ и $\omega \in \mathbb{N}$, или $p = 2$ и $\omega \in \{1,2\}$, то $(\mathbb{Z}/p^\omega)^\times = \langle (p+1)\, d^{p^{\omega-1}} \rangle$ (и, значит, $(\mathbb{Z}/p^\omega)^\times \cong \mathrm{C}_{p^{\omega-1}(p-1)}$); это задача 19 у группы CS.

3. $(\mathbb{Z}/2^\omega)^\times \cong \langle -1 \rangle \times \langle 5 \rangle$ и, если $\omega \in \mathbb{N} \setminus \{1\}$, то $\langle -1 \rangle \cong \mathrm{C}_2$ и $\langle 5 \rangle \cong \mathrm{C}_{2^{\omega-2}}$; это задача 19 у группы SE. □

Замечания.

• Пусть $n \in \mathbb{N}$; представим число n в виде $p_1^{\omega_1} \cdot \ldots \cdot p_t^{\omega_t}$, где $t \in \mathbb{N}_0$, $p_1, \ldots, p_t \in \mathbb{P}$, числа $p_1, \ldots, p_t$ попарно различны и $\omega_1, \ldots, \omega_t \in \mathbb{N}$, а также, если $2 \mid n$, то $p_1 = 2$; тогда

$$(\mathbb{Z}/n)^\times \cong \begin{cases} \mathrm{C}_{p_1^{\omega_1-1}(p_1-1)} \times \ldots \times \mathrm{C}_{p_t^{\omega_t-1}(p_t-1)}, \text{ если } 2 \nmid n \,\vee\, (4 \mid n \,\wedge\, 8 \nmid n); \\ \mathrm{C}_{p_2^{\omega_2-1}(p_2-1)} \times \ldots \times \mathrm{C}_{p_t^{\omega_t-1}(p_t-1)}, \text{ если } 2 \mid n \,\wedge\, 4 \nmid n; \\ \mathrm{C}_2 \times \mathrm{C}_{2^{\omega_1-2}} \times \mathrm{C}_{p_2^{\omega_2-1}(p_2-1)} \times \ldots \times \mathrm{C}_{p_t^{\omega_t-1}(p_t-1)}, \text{ если } 8 \mid n. \end{cases} \qquad (\triangle)$$

• Теорема о группах обратимых остатков полностью описывает структуру групп $(\mathbb{Z}/n)^\times$, где $n \in \mathbb{N}$; с ее помощью можно построить явные изоморфизмы между этими группами и указанными выше произведениями циклических групп. Однако, эти изоморфизмы не являются эффективными, так как зависят от первообразных корней по простым модулям, для поиска которых в настоящее время не существует алгоритма, который работал бы за полиномиальное время от длины двоичной записи модуля.

9. Теоретико-числовые алгоритмы (начало)

Критерий существования дискретного логарифма по модулю n.

Пусть $n \in \mathbb{N}$; тогда следующие свойства эквивалентны:

• *существует дискретный логарифм по модулю n (то есть группа $(\mathbb{Z}/n)^\times$ циклическая);*

• *число n нечетное примарное, или число $\frac{n}{2}$ нечетное примарное, или $n \in \{1,2,4\}$.*

Доказательство.

Порядки циклических групп, указанных в разложении $(\triangle)$, четны, поэтому $(\mathbb{Z}/n)^\times \cong \mathrm{C}_{\phi(n)} \Leftrightarrow$ (количество сомножителей в прямых произведениях, указанных в разложении $(\triangle)$, равно 1 или 0).

• Если $2 \nmid n \,\vee\, (4 \mid n \,\wedge\, 8 \nmid n)$, то $(\mathbb{Z}/n)^\times \cong \mathrm{C}_{\phi(n)} \Leftrightarrow n \in \{p^\omega \mid p \in \mathbb{P} \setminus \{2\} \,\wedge\, \omega \in \mathbb{N}\} \cup \{1,4\}$.

• Если $2 \mid n \,\wedge\, 4 \nmid n$, то $(\mathbb{Z}/n)^\times \cong \mathrm{C}_{\phi(n)} \Leftrightarrow n \in \{2p^\omega \mid p \in \mathbb{P} \setminus \{2\} \,\wedge\, \omega \in \mathbb{N}\} \cup \{2\}$.

• Если $8 \mid n$, то $(\mathbb{Z}/n)^\times \ncong \mathrm{C}_{\phi(n)}$ (в данном случае обязательно имеется хотя бы 2 сомножителя). □