8ВМ, спецкурс, занятие 20
27 января 2023
Китайская теорема об остатках

Теорема (Китайская теорема об остатках, КТО)**.** Пусть НОД$(m,n)=1$. Тогда система сравнений

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

имеет единственное решение $x \equiv c \pmod{mn}$.

Доказательство 1: Рассмотрим все остатки по модулю mn, удовлетворяющие первому сравнению.

$$a,\ a+m,\ a+2m,\ \ldots,\ a+(n-1)m.$$

По модулю n все эти остатки различные. Действительно, остатки

$$0,\ 1,\ 2,\ \ldots,\ n-1$$

все различные. Далее, поскольку m взаимно просто с n, то остатки

$$0,\ m,\ 2m,\ \ldots,\ (n-1)m$$

тоже все различные. Наконец, от прибавления a остатки остаются различными. Итак, n чисел

$$a,\ a+m,\ a+2m,\ \ldots,\ a+(n-1)m$$

дают различные остатки по модулю n, поэтому среди них ровно один раз встречается остаток b. Это число и даст нам единственное решение нашей системы сравнений.

Доказательство 2:

1) Докажем существование решения, предъявив явную конструкцию. Рассмотрим диофантово уравнение $mx+ny=1$. Поскольку m и n взаимно просты, то у него есть какое-то решение x_0, y_0. То есть $mx_0+ny_0=1$. Возьмем

$$c \equiv mx_0b+ny_0a \pmod{mn}$$

Проверим, что это действительно решение системы. В самом деле,

$$c \equiv mx_0b+ny_0a \equiv ny_0a \equiv (1-mx_0)a \equiv a \pmod{m}$$

$$c \equiv mx_0b+ny_0a \equiv my_0b \equiv (1-ny_0)b \equiv b \pmod{n}$$

2) Докажем, что это решение единственно. Предположим, что у системы есть два различных решения $x \equiv c_1 \pmod{mn}$ и $x \equiv c_2 \pmod{mn}$. Тогда

$$\begin{cases} c_1 \equiv a \pmod{m} \\ c_2 \equiv a \pmod{m} \\ c_1 \equiv b \pmod{n} \\ c_2 \equiv b \pmod{n} \end{cases}$$

Значит, $c_1-c_2 \equiv 0 \pmod{m}$ и $c_1-c_2 \equiv 0 \pmod{n}$. То есть c_1-c_2 делится на m и на n, а значит и на mn (из-за взаимной простоты m и n). Тогда $c_1 \equiv c_2 \pmod{mn}$, и следовательно это было на самом деле одно и то же решение.

На примере разберем наиболее удобный способ решать такие системы сравнений

Пример.

$$\begin{cases} x \equiv 4 \pmod{15} \\ x \equiv 11 \pmod{28} \end{cases}$$

Домножим все первое сравнение (включая модуль) на 28, а все второе — на 15.

$$\begin{cases} 28x \equiv 112 \pmod{420} \\ 15x \equiv 165 \pmod{420} \end{cases}$$

Теперь будем вычитать сравнения друг из друга так, чтобы в итоге слева остался x. Вычтем второе из первого:

$$13x \equiv -53 \pmod{420}$$

Вычтем третье из второго:

$$2x \equiv 218 \pmod{420}$$

Обратите внимание, что нельзя делить это сравнение на 2, поскольку нам нужно решение по модулю 420, а не по модулю 210. Вместо этого вычтем из третьего четвертое шесть раз:

$$x \equiv -53 - 6 \cdot 218 = -1361 \equiv -101 \equiv 319 \pmod{420}$$

КТО можно использовать для нахождения остатков по непростым модулям.

Пример. Давайте найдем остаток от деления 20^{14} на 77. Обозначим $x = 20^{14}$ и вычислим $x \mod 7$ и $x \mod 11$.

$$20^{14} \equiv (-1)^2 = 1 \pmod{7}$$
$$20^{14} \equiv (-2)^4 \equiv 5 \pmod{11}$$

Решим систему

$$\begin{cases} x \equiv 1 \pmod{7} \\ x \equiv 5 \pmod{11} \end{cases}$$

Домножим сравнения, приведя их к модулю 77:

$$\begin{cases} 11x \equiv 11 \pmod{77} \\ 7x \equiv 35 \pmod{77} \end{cases}$$

Тогда

$$4x \equiv -24 \pmod{77}$$
$$8x \equiv -48 \equiv 29 \pmod{77}$$
$$x \equiv -6 \equiv 71 \pmod{77}$$

Еще КТО дает удобный инструмент, чтобы доказывать существование каких-то объектов, не конструируя их.

Пример. *Докажите, что существует 100 подряд идущих составных натуральных чисел.*

Пусть это числа $x, x+1, \ldots, x+99$. По КТО можно подобрать такой x, что $x \vdots 2$; $(x+1) \vdots 3$, $(x+2) \vdots 5$, $\ldots$, $(x+99) \vdots p_{100}$. Мы можем не знать, что именно это за x, но он точно существует.

1 Решите системы сравнений:

a $\begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 7 \pmod{17} \end{cases}$ b $\begin{cases} x \equiv 2 \pmod{13} \\ x \equiv 4 \pmod{19} \end{cases}$

2 По индукции докажите обобщенную КТО: пусть $m_1, m_2, \ldots, m_n$ — попарно взаимно простые числа. Тогда система сравнений

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \ldots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

имеет единственное решение по модулю $m_1 m_2 \ldots m_n$.

3 Известно, что число a при делении на 3 дает остаток 1, при делении на 5 дает остаток 3, а при делении на 7 — остаток 4. Найдите все возможные значения числа a.

4 Найдите остатки от деления:

a 2^{70} на 119; b 2023^{2022} на 1001

5 Решите сравнение $n^2 + 3n + 1 \equiv 0 \pmod{55}$.

6 Число 625 обладает забавным свойством «самовоспроизводимости»: $625^2 = 390\mathbf{625}$.

a Найдите еще одно такое трехзначное число и докажите, что других нет.

b Докажите, что при любом k существует ровно 4 набора из k цифр — $00\ldots00$, $00\ldots01$ и еще два, оканчивающиеся пятеркой и шестеркой, — обладающие таким свойством: если натуральное число оканчивается одним из этих наборов цифр, то его квадрат оканчивается тем же набором цифр.

7 У генерала есть n солдат, но от 1 до 37 солдат болеет. Генерал хочет построить солдат в одинаковые квадратные каре (каре должно содержать больше 1 человека; каре $k \times k$ содержит k^2 человек). Докажите, что существует такое n, что генерал сможет осуществить своё намерение независимо от количества больных солдат.

Подсказка: искать это n не обязательно.

8* Докажите, что на координатной плоскости можно отметить 10000 точек с целыми координатами, образующих квадрат 100×100, так, что у каждой точки координаты не взаимно просты.