Арифметика остатков

Квант-10. Математика

Михаил Хозин

ГРЦФМО, Лицей 40. г. Нижний Новгород

14 октября 2018 г.

Контактные данные

Группа в Телеграм

https://t.me/joinchat/F-8ewhB8v6j2nKDmgMlnzA
Это группа для вопросов и общения. Так же здесь будут появляться отдельные материалы и задания.

Почтовый адрес

kvant.math@gmail.com
Письменные задания отправлять сюда.

Контактные данные

Группа в Телеграм

https://t.me/joinchat/F-8ewhB8v6j2nKDmgMlnzA

Это группа для вопросов и общения. Так же здесь будут появляться отдельные материалы и задания.

Почтовый адрес

kvant.math@gmail.com

Письменные задания отправлять сюда.

ВНИМАНИЕ! По заданиям будет отчётность!

План занятия

Классы вычетов

Theorem

Классы вычетов Если мы выберем некоторый натуральный делитель $m > 1$, то все целые числа можно разбить на m не пересекающихся подгрупп таких, что внутри каждой из них разность любых двух чисел кратна m.

Доказательство.

Эти классы строятся конструктивно. Числа от 0 до $m-1$ попадают в разные классы. Все остальные сводятся к ним последовательным добавлением или вычитанием m. □

Эти группы называются классами вычетов

Классы вычетов

Theorem

Классы вычетов Если мы выберем некоторый натуральный делитель $m > 1$, то все целые числа можно разбить на m не пересекающихся подгрупп таких, что внутри каждой из них разность любых двух чисел кратна m.

Доказательство.

Эти классы строятся конструктивно. Числа от 0 до $m - 1$ попадают в разные классы. Все остальные сводятся к ним последовательным добавлением или вычитанием m. □

Эти группы называются классами вычетов

Сравнение по модулю

Представление элементов класса

Все элементы одного класса могут быть представлены как $n = N \cdot m + a$, где a – остаток от деления характеризующий класс

Сравнение по модулю

Принадлежность двух чисел одному классу записывается как

$$a \equiv b \pmod{m}$$

(a сравнимо с b по модулю m)

Отношение эквивалентности

Привычные свойства

- **Рефлексивность:** $a \equiv a \pmod{m}$.
- **Симметричность:** Если $a \equiv b \pmod{m}$, то $b \equiv a \pmod{m}$.
- **Транзитивность:** Если $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$, то $a \equiv c \pmod{m}$.

Отношение с такими свойствами называется *отношением эквивалентности*

Придумайте отношения не удовлетворяющие какому либо из свойств

Отношение эквивалентности

Привычные свойства

- **Рефлексивность:** $a \equiv a \pmod{m}$.
- **Симметричность:** Если $a \equiv b \pmod{m}$, то $b \equiv a \pmod{m}$.
- **Транзитивность:** Если $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$, то $a \equiv c \pmod{m}$.

Отношение с такими свойствами называется *отношением эквивалентности*

Придумайте отношения не удовлетворяющие какому либо из свойств

Кольцо

Арифметические операции с остатками

Мы можем проводить арифметические операции. Если $a \equiv b \pmod{m}$ и $c \equiv d \pmod{m}$, то:

- **Сложение** $a + c \equiv b + d \pmod{m}$
- **Умножение** $a \cdot c \equiv b \cdot d \pmod{m}$

Докажите эти свойства. Структура, в которой определены операции умножения и обратимого сложения называется *кольцом*.

А что же с вычитанием и делением? Они определяются через решение уравнений.

Кольцо

Арифметические операции с остатками

Мы можем проводить арифметические операции. Если $a \equiv b \pmod{m}$ и $c \equiv d \pmod{m}$, то:

- **Сложение** $a + c \equiv b + d \pmod{m}$
- **Умножение** $a \cdot c \equiv b \cdot d \pmod{m}$

Докажите эти свойства. Структура, в которой определены операции умножения и обратимого сложения называется *кольцом*.

А что же с вычитанием и делением? Они определяются через решение уравнений.

Обратный элемент по сложению. Вычитание

Решить уравнение - это предъявить все подходящие ответы (остатки)

Решение уравнения

$x + 7 \equiv 0 \pmod{13}$

$x + 7 + 6 \equiv 6 \pmod{13}$

$x \equiv 6 \pmod{13}$

Обратный элемент по сложению

$7 + 6 \equiv 0 \pmod{13}$ – можно интерпретировать как вычитание: $-7 \equiv 6 \pmod{13}$. Важно, что для любого элемента существует обратный.

Обратный элемент по сложению. Вычитание

Решить уравнение - это предъявить все подходящие ответы (остатки)

Решение уравнения

$x + 7 \equiv 0 \pmod{13}$
$x + 7 + 6 \equiv 6 \pmod{13}$
$x \equiv 6 \pmod{13}$

Обратный элемент по сложению

$7 + 6 \equiv 0 \pmod{13}$ – можно интерпретировать как вычитание: $-7 \equiv 6 \pmod{13}$. Важно, что для любого элемента существует обратный.

Обратный элемент по сложению. Вычитание

Решить уравнение - это предъявить все подходящие ответы (остатки)

Решение уравнения

$x + 7 \equiv 0 \pmod{13}$
$x + 7 + 6 \equiv 6 \pmod{13}$
$x \equiv 6 \pmod{13}$

Обратный элемент по сложению

$7 + 6 \equiv 0 \pmod{13}$ – можно интерпретировать как вычитание: $-7 \equiv 6 \pmod{13}$. Важно, что для любого элемента существует обратный.

Когда возможно деление?

Решение уравнения

$3x + 5 \equiv 0 \pmod{13}$

$3x \equiv 8 \pmod{13}$ – но что делать теперь?

$9 \cdot 3 \equiv 1 \pmod{13}$ – нашли обратный элемент.

$9 \cdot 3x \equiv 9 \cdot 8 \pmod{13}$

$x \equiv 7 \pmod{13}$

Делители единицы

a называется *делителем единицы* (обратимым элементом), если существует такой элемент b, что $a \cdot b \equiv 1 \pmod{m}$.

Не для все элементы обратимы по операции умножения.

Приведите пример ненулевого элемента, который не будет делителем единицы.

Когда возможно деление?

Решение уравнения

$3x + 5 \equiv 0 \pmod{13}$

$3x \equiv 8 \pmod{13}$ – но что делать теперь?

$9 \cdot 3 \equiv 1 \pmod{13}$ – нашли обратный элемент.

$9 \cdot 3x \equiv 9 \cdot 8 \pmod{13}$

$x \equiv 7 \pmod{13}$

Делители единицы

a называется *делителем единицы* (обратимым элементом), если существует такой элемент b, что $a \cdot b \equiv 1 \pmod{m}$.

Не для все элементы обратимы по операции умножения.

Приведите пример ненулевого элемента, который не будет делителем единицы.

Когда возможно деление?

Решение уравнения

$3x + 5 \equiv 0 \pmod{13}$

$3x \equiv 8 \pmod{13}$ – но что делать теперь?

$9 \cdot 3 \equiv 1 \pmod{13}$ – нашли обратный элемент.

$9 \cdot 3x \equiv 9 \cdot 8 \pmod{13}$

$x \equiv 7 \pmod{13}$

Делители единицы

a называется *делителем единицы* (обратимым элементом), если существует такой элемент b, что $a \cdot b \equiv 1 \pmod{m}$.

Не для все элементы обратимы по операции умножения.

Приведите пример ненулевого элемента, который не будет делителем единицы.

Когда возможно деление?

Решение уравнения

$3x + 5 \equiv 0 \pmod{13}$
$3x \equiv 8 \pmod{13}$ – но что делать теперь?
$9 \cdot 3 \equiv 1 \pmod{13}$ – нашли обратный элемент.
$9 \cdot 3x \equiv 9 \cdot 8 \pmod{13}$
$x \equiv 7 \pmod{13}$

Делители единицы

a называется *делителем единицы* (обратимым элементом), если существует такой элемент b, что $a \cdot b \equiv 1 \pmod{m}$.
Не для все элементы обратимы по операции умножения.
Приведите пример ненулевого элемента, который не будет делителем единицы.

Представление остатков. Биекция

Представление остатков

Важно, что различных классов остатков всегда ровно m. Мы можем выбирать любое удобное нам представлени. Обычно это набор $\{0,\ 1,\ \ldots,\ m-1\}$ но можно использовать и отрицательные числа, а так же числа превосходящие m. Но их должно быть ровно m и они должны принадлежать к различным классам.

Обратимость операции

Любая операция, переводящая различные остатки в различные является обратимой.

Квадратичные вычеты

Целое число a называется *квадратичным вычетом по модулю* m, если разрешимо сравнение $x^2 \equiv a \pmod{m}$, в противном случае оно называется *невычетом*.

Невычетов достаточно много. Т.к. $x^2 \equiv (-x)^2 \pmod{m}$, то есть операция возведения в квадрат не биективна. Для нечётных простых m получается ровно $(m-1)/2$ невычетов. Для составных может быть больше.

Задание

Составить таблицу квадратов и найти квадратичные вычеты для $m = \{2,\ 3,\ 4,\ 5,\ 8,\ 12\}$.

Квадратичные вычеты

Целое число a называется *квадратичным вычетом по модулю* m, если разрешимо сравнение $x^2 \equiv a \pmod{m}$, в противном случае оно называется *невычетом*.

Невычетов достаточно много. Т.к. $x^2 \equiv (-x)^2 \pmod{m}$, то есть операция возведения в квадрат не биективна. Для нечётных простых m получается ровно $(m-1)/2$ невычетов. Для составных может быть больше.

Задание

Составить таблицу квадратов и найти квадратичные вычеты для $m = \{2,\ 3,\ 4,\ 5,\ 8,\ 12\}$.

Задачи на квадратичные вычеты

Задание

Решить в целых числах уравнение $2^n + 7 = x^2$.

Задание

Решить в целых числах уравнение $m! + 12 = n^2$.

Задачи на квадратичные вычеты

Задание

Решить в целых числах уравнение $2^n + 7 = x^2$.

Решение

2^n с ростом n делится на всё большую степень двойки.

Тогда посмотрим на остатки от деления на степени двойки.

Как мы выписали раньше, только числа 0, 1 будут квадратичными вычетами по модулю 4. Значит левая часть может иметь только такие остатки.

Перенесём 7 вправо. Получаем, что 2^n должен иметь остаток 1, 2. Это возможно только при $n = 0$ и $n = 1$.

Проверяя получаем ответ: $n = 1$, $x = \pm 3$.

Задачи на квадратичные вычеты

Задание

Решить в целых числах уравнение $2^n + 7 = x^2$.

Решение

2^n с ростом n делится на всё большую степень двойки. Тогда посмотрим на остатки от деления на степени двойки. Как мы выписали раньше, только числа 0, 1 будут квадратичными вычетами по модулю 4. Значит левая часть может иметь только такие остатки.

Перенесём 7 вправо. Получаем, что 2^n должен иметь остаток 1, 2. Это возможно только при $n = 0$ и $n = 1$. Проверяя получаем ответ: $n = 1$, $x = \pm 3$.

Задачи на квадратичные вычеты

Задание

Решить в целых числах уравнение $2^n + 7 = x^2$.

Решение

2^n с ростом n делится на всё большую степень двойки. Тогда посмотрим на остатки от деления на степени двойки. Как мы выписали раньше, только числа $0,\ 1$ будут квадратичными вычетами по модулю 4. Значит левая часть может иметь только такие остатки.
Перенесём 7 вправо. Получаем, что 2^n должен иметь остаток $1,\ 2$. Это возможно только при $n = 0$ и $n = 1$.
Проверяя получаем ответ: $n = 1,\ x = \pm 3$.

Китайская теорема об остатках

Пусть $m_1,\ m_2, \ldots,\ m_n$ – попарно взаимнопростые натуральные числа. Обозначим $M = m_1 \cdot m_2 \cdot \ldots \cdot m_n$. Для любых целые числа $a_1,\ a_2, \ldots,\ a_n$ система сравнений

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

с обозначениями $M_i = M/m_i$, $\mu_i \equiv M_i^{-1} \pmod{m_i}$ будет единственное решение

$$x \equiv \sum_{i=1}^{n} a_i \mu_i M_i \pmod{M},$$

План доказательства

1. Покажем, что если целые числа x_1 и x_2 удовлетворяют системе сравнений, то $x_1 \equiv x_2 \pmod{M}$.
2. Покажем линейность системы сравнений по правой части
3. Найдём решение системы

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv 0 \pmod{m_2} \\ \dots \\ x \equiv 0 \pmod{m_n} \end{cases}$$

4. Докажем теорему

Задачи на китайскую теорему об остатках

Задания

1. Олег собрал мешочек монет. Саша пересчитал их, и оказалось, что если разделить все монеты на пять равных кучек, то останется две лишние монеты. А если на четыре равные кучки – останется одна лишняя монета. В то же время монетки можно разделить на три равные кучки. Какое наименьшее число монет могло быть у Олега?
2. Найдите наименьшее натуральное число, дающее при делении на 2, 3, 5, 7 остатки 1, 2, 4, 6 соответственно.
3. При каких целых n число $n^2 + 3n + 1$ делится на 55?

Решение задачи 1

Представиление задачи в виде сравнений

$$\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 1 \pmod 4 \\ x \equiv 0 \pmod 3 \end{cases}$$

Поиск ключевых параметров

$M = 5 \cdot 4 \cdot 3 = 60,$

$M_1 = 4 \cdot 3 = 12,\ M_2 = 5 \cdot 3 = 15,\ M_3 = 5 \cdot 4 = 20.$

$\mu_1 M_1 \equiv 1 \pmod 5,\ \mu_2 M_2 \equiv 1 \pmod 4,\ \mu_3 M_3 \equiv 1 \pmod 3$

$2\mu_1 \equiv 1 \pmod 5,\ 3\mu_2 \equiv 1 \pmod 4,\ 2\mu_3 \equiv 1 \pmod 3$

$\mu_1 \equiv 3 \pmod 5,\ \mu_2 \equiv 3 \pmod 4,\ \mu_3 \equiv 2 \pmod 3$

Решение задачи 1

Представиление задачи в виде сравнений

$$\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 1 \pmod 4 \\ x \equiv 0 \pmod 3 \end{cases}$$

Поиск ключевых параметров

$M = 5 \cdot 4 \cdot 3 = 60,$

$M_1 = 4 \cdot 3 = 12,\ M_2 = 5 \cdot 3 = 15,\ M_3 = 5 \cdot 4 = 20.$

$\mu_1 M_1 \equiv 1 \pmod 5,\ \mu_2 M_2 \equiv 1 \pmod 4,\ \mu_3 M_3 \equiv 1 \pmod 3$

$2\mu_1 \equiv 1 \pmod 5,\ 3\mu_2 \equiv 1 \pmod 4,\ 2\mu_3 \equiv 1 \pmod 3$

$\mu_1 \equiv 3 \pmod 5,\ \mu_2 \equiv 3 \pmod 4,\ \mu_3 \equiv 2 \pmod 3$

Решение задачи 1

Представиление задачи в виде сравнений

$$\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 1 \pmod 4 \\ x \equiv 0 \pmod 3 \end{cases}$$

Поиск ключевых параметров

$M = 5 \cdot 4 \cdot 3 = 60,$

$M_1 = 4 \cdot 3 = 12,\ M_2 = 5 \cdot 3 = 15,\ M_3 = 5 \cdot 4 = 20.$

$\mu_1 M_1 \equiv 1 \pmod 5,\ \mu_2 M_2 \equiv 1 \pmod 4,\ \mu_3 M_3 \equiv 1 \pmod 3$

$2\mu_1 \equiv 1 \pmod 5,\ 3\mu_2 \equiv 1 \pmod 4,\ 2\mu_3 \equiv 1 \pmod 3$

$\mu_1 \equiv 3 \pmod 5,\ \mu_2 \equiv 3 \pmod 4,\ \mu_3 \equiv 2 \pmod 3$

Решение задачи 1

Представиление задачи в виде сравнений

$$\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 1 \pmod 4 \\ x \equiv 0 \pmod 3 \end{cases}$$

Поиск ключевых параметров

$M = 5 \cdot 4 \cdot 3 = 60,$

$M_1 = 4 \cdot 3 = 12,\ M_2 = 5 \cdot 3 = 15,\ M_3 = 5 \cdot 4 = 20.$

$\mu_1 M_1 \equiv 1 \pmod 5,\ \mu_2 M_2 \equiv 1 \pmod 4,\ \mu_3 M_3 \equiv 1 \pmod 3$

$2\mu_1 \equiv 1 \pmod 5,\ 3\mu_2 \equiv 1 \pmod 4,\ 2\mu_3 \equiv 1 \pmod 3$

$\mu_1 \equiv 3 \pmod 5,\ \mu_2 \equiv 3 \pmod 4,\ \mu_3 \equiv 2 \pmod 3$

Решение задачи 1

Представиление задачи в виде сравнений

$$\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 1 \pmod 4 \\ x \equiv 0 \pmod 3 \end{cases}$$

По найденным параметрам решим задачу:

$\mu_1 M_1 = 3 \cdot 12 = 36$, $\mu_2 M_2 = 3 \cdot 15 = 45$, $\mu_3 M_3 = 2 \cdot 20 = 40$.

Теперь мы можем найти одно из решений:

$x = a_1\mu_1 M_1 + a_2\mu_2 M_2 + a_3\mu_3 M_3 = 2 \cdot 36 + 1 \cdot 45 + 0 \cdot 40 = 117$

Но подойдёт ли оно в качестве ответа задачи?

Все решения удовлетворяют условию $x \equiv 117 \pmod{60}$.

Ответом на задачу будет число 57.

Решение задачи 1

Представиление задачи в виде сравнений

$$\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 1 \pmod 4 \\ x \equiv 0 \pmod 3 \end{cases}$$

По найденным параметрам решим задачу:
$\mu_1 M_1 = 3 \cdot 12 = 36$, $\mu_2 M_2 = 3 \cdot 15 = 45$, $\mu_3 M_3 = 2 \cdot 20 = 40$.
Теперь мы можем найти одно из решений:
$x = a_1\mu_1 M_1 + a_2\mu_2 M_2 + a_3\mu_3 M_3 = 2 \cdot 36 + 1 \cdot 45 + 0 \cdot 40 = 117$
Но подойдёт ли оно в качестве ответа задачи?
Все решения удовлетворяют условию $x \equiv 117 \pmod{60}$.
Ответом на задачу будет число 57.

Решение задачи 1

Представиление задачи в виде сравнений

$$\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 1 \pmod 4 \\ x \equiv 0 \pmod 3 \end{cases}$$

По найденным параметрам решим задачу:
$\mu_1 M_1 = 3 \cdot 12 = 36$, $\mu_2 M_2 = 3 \cdot 15 = 45$, $\mu_3 M_3 = 2 \cdot 20 = 40$.
Теперь мы можем найти одно из решений:
$x = a_1\mu_1 M_1 + a_2\mu_2 M_2 + a_3\mu_3 M_3 = 2 \cdot 36 + 1 \cdot 45 + 0 \cdot 40 = 117$
Но подойдёт ли оно в качестве ответа задачи?
Все решения удовлетворяют условию $x \equiv 117 \pmod{60}$.
Ответом на задачу будет число 57.

Решение задачи 3

Напомним условие:

При каких целых n число $n^2 + 3n + 1$ делится на 55?

Необходимо найти связь между этой задачей и Китайской теоремой об сотатках.

Запишем условие в виде сравнений

$$\begin{cases} n^2 + 3n + 1 \equiv 0 \pmod 5 \\ n^2 + 3n + 1 \equiv 0 \pmod{11} \end{cases}$$

Необходимо решить эти сравнения.

Решение задачи 3

Напомним условие:

При каких целых n число $n^2 + 3n + 1$ делится на 55?

Необходимо найти связь между этой задачей и Китайской теоремой об сотатках.

Запишем условие в виде сравнений

$$\begin{cases} n^2 + 3n + 1 \equiv 0 \pmod 5 \\ n^2 + 3n + 1 \equiv 0 \pmod{11} \end{cases}$$

Необходимо решить эти сравнения.

Решение задачи 3

Эти квадратные уравнения можно решить простым подбором. Для этого составим таблицу вычисления:

Сравнение по модулю 5

n	n^2	$3n$	n^2+3n+1
0	0	0	1
1	1	3	0
2	4	1	1
3	4	4	4
4	1	2	4

Теперь мы можем то же самое сделать для 11. Попробуйте это самостоятельно.

Сравнение по модулю 11

n	n^2	$3n$	n^2+3n+1
0	0	0	1
1	1	3	5
2	4	6	0
3	9	9	8
4	5	1	7
5	3	4	8
6	3	7	0
7	5	10	5
8	9	2	1
9	4	5	10
10	1	8	10

Итог: $n \equiv 1 \pmod 5$, $n \equiv \{2,\ 6\} \pmod{11}$.

Решение задачи 3

Представиление задачи в виде сравнений

$$\begin{cases} n \equiv 1 \pmod 5 \\ n \equiv \{2,\ 6\} \pmod{11} \end{cases}$$

Можем повторить шаблон предыдущей задачи:
$M = 5 \cdot 11 = 55$, $M_1 = 11$, $M_2 = 5$.
$11\mu_1 \equiv 1 \pmod 5$, $5\mu_2 \equiv 1 \pmod{11}$
Решение: $\mu_1 \equiv 1 \pmod 5$, $\mu_2 \equiv 9 \pmod{11}$
Теперь мы можем записать ответы
$n_1 = 1 \cdot 1 \cdot 11 + 2 \cdot 9 \cdot 5 = 101$ $n_2 = 1 \cdot 1 \cdot 11 + 6 \cdot 9 \cdot 5 = 281$
Все решения удовлетворяют сравнению
$n \equiv \{6,\ 46\} \pmod{55}$.

Решение задачи 3

Представиление задачи в виде сравнений

$$\begin{cases} n \equiv 1 \pmod 5 \\ n \equiv \{2,\ 6\} \pmod{11} \end{cases}$$

Можем повторить шаблон предыдущей задачи:
$M = 5 \cdot 11 = 55$, $M_1 = 11$, $M_2 = 5$.
$11\mu_1 \equiv 1 \pmod 5$, $5\mu_2 \equiv 1 \pmod{11}$
Решение: $\mu_1 \equiv 1 \pmod 5$, $\mu_2 \equiv 9 \pmod{11}$
Теперь мы можем записать ответы
$n_1 = 1 \cdot 1 \cdot 11 + 2 \cdot 9 \cdot 5 = 101$ $n_2 = 1 \cdot 1 \cdot 11 + 6 \cdot 9 \cdot 5 = 281$
Все решения удовлетворяют сравнению
$n \equiv \{6,\ 46\} \pmod{55}$.

Решение задачи 3

Представиление задачи в виде сравнений

$$\begin{cases} n \equiv 1 \pmod 5 \\ n \equiv \{2,\ 6\} \pmod{11} \end{cases}$$

Можем повторить шаблон предыдущей задачи:
$M = 5 \cdot 11 = 55$, $M_1 = 11$, $M_2 = 5$.
$11\mu_1 \equiv 1 \pmod 5$, $5\mu_2 \equiv 1 \pmod{11}$
Решение: $\mu_1 \equiv 1 \pmod 5$, $\mu_2 \equiv 9 \pmod{11}$
Теперь мы можем записать ответы
$n_1 = 1 \cdot 1 \cdot 11 + 2 \cdot 9 \cdot 5 = 101$ $n_2 = 1 \cdot 1 \cdot 11 + 6 \cdot 9 \cdot 5 = 281$
Все решения удовлетворяют сравнению
$n \equiv \{6,\ 46\} \pmod{55}$.

Решение задачи 3

Представиление задачи в виде сравнений

$$\begin{cases} n \equiv 1 \pmod 5 \\ n \equiv \{2,\ 6\} \pmod{11} \end{cases}$$

Можем повторить шаблон предыдущей задачи:
$M = 5 \cdot 11 = 55$, $M_1 = 11$, $M_2 = 5$.
$11\mu_1 \equiv 1 \pmod 5$, $5\mu_2 \equiv 1 \pmod{11}$
Решение: $\mu_1 \equiv 1 \pmod 5$, $\mu_2 \equiv 9 \pmod{11}$
Теперь мы можем записать ответы
$n_1 = 1 \cdot 1 \cdot 11 + 2 \cdot 9 \cdot 5 = 101$ $n_2 = 1 \cdot 1 \cdot 11 + 6 \cdot 9 \cdot 5 = 281$
Все решения удовлетворяют сравнению
$n \equiv \{6,\ 46\} \pmod{55}$.

Решение задачи 3

Представиление задачи в виде сравнений

$$\begin{cases} n \equiv 1 \pmod 5 \\ n \equiv \{2,\ 6\} \pmod{11} \end{cases}$$

Можем повторить шаблон предыдущей задачи:
$M = 5 \cdot 11 = 55$, $M_1 = 11$, $M_2 = 5$.
$11\mu_1 \equiv 1 \pmod 5$, $5\mu_2 \equiv 1 \pmod{11}$
Решение: $\mu_1 \equiv 1 \pmod 5$, $\mu_2 \equiv 9 \pmod{11}$
Теперь мы можем записать ответы
$n_1 = 1 \cdot 1 \cdot 11 + 2 \cdot 9 \cdot 5 = 101$ $n_2 = 1 \cdot 1 \cdot 11 + 6 \cdot 9 \cdot 5 = 281$
Все решения удовлетворяют сравнению
$n \equiv \{6,\ 46\} \pmod{55}$.

Наверное в следующий раз...

Малая теорема Ферма и RSA-шифрование