ДИСКРЕТНАЯ МАТЕМАТИКА

вспомогательные материалы
для студентов очного и дистанционного
обучения радиотехнического факультета

Екатеринбург 2008

УДК 373:53

Составители А.Л. Крохин

ДИСКРЕТНАЯ МАТЕМАТИКА./ А.Л. Крохин. Екатеринбург: , 2008.
20 с.

Рис. 69.

Подготовлено кафедрой
"Вычислительные методы и уравнения
математической физики".

1 Задание №2 по ДМ в потоке Крохина А.Л. Элементы теории чисел

Алгоритм шифрования с открытым ключом

1. Лицо А выбирает два простых числа. Например, $p = 23$ и $q = 41$, заметим, что реально эти числа имеют несколько десятков разрядов.

2. Лицо А пермножает эти числа и получает $pq = (23)(41) = 943$. 943 это и есть "открытый ключ который сообщается лицу В (и прочим жителям нашей планеты).

3. Лицо А также выбирает еще одно число e, которое должно быть взаимно простым с $(p-1)(q-1)$. В нашем примере, $(p-1)(q-1) = (22)(40) = 880$, поэтому подойдет $e = 7$. e также является частью открытого ключа, поэтому В получает и значение e.

4. Теперь лицо В имеет все необходимое для шифрования своего сообщения, направляемого А. Оно будет очень коротким М = 35.

5. В вычисляет шифротекст $C = M^e \pmod N) = 35^7 \pmod{943}$.

6. $35^7 = 64339296875$ and $64339296875 \pmod{943} = 545$. Шифротекст, т. е. число 545, В пересылает А.

7. Получив его, А хочет дешифровать 545. Для этого ему требуется такое число d, что $ed = 1 \pmod{(p-1)(q-1)}$, или в нашем случае, $7d = 1 \pmod{880}$. Решение будет $d = 503$, поскольку $7 \cdot 503 = 3521 = 4(880) + 1 = 1 \pmod{880}$.

8. Для дешифрования А должен вычислить $C^d \pmod N = 545^{503} \pmod{943}$. На первый взгляд это совершенно чудовищное вычисление, однако заметим, что $503 = 256+128+64+32+16+4+2+1$ (это всего лишь двоичная запись числа 503). Поэтому $545^{503} = 545^{256+128+64+32+16+4+2+1} = 545^{256}545^{128} \dots 545^1$.

Заметим, что нас интересует не само число, а его значение по (mod 943), поэтому мы можем вычислять все промежуточные значения по этому модулю. Этот технический прием называют "последовательное возведение в квадрат и состоит в том, что возводят в квадрат 545, берут результат по модулю, затем полученное число снова возводят в квадрат и так получаются все степени 2. Формальным обоснованием являются известные свойства сравнения. Считаем, $545^2 \pmod{943} = 545 \cdot 545 = 297025 \pmod{943} = 923$. Еще раз: $545^4 \pmod{943} = (545^2)^2 \pmod{943} = 923 \cdot 923 = 851929 \pmod{943} = 400$, и так далее. Получаем таблицу:

545	mod 943=	545
545^2	mod 943=	923
545^4	mod 943=	400
545^8	mod 943=	633
545^{16}	mod 943=	857
545^{32}	mod 943=	795
545^{64}	mod 943=	215
545^{128}	mod 943=	18
545^{256}	mod 943=	324

Итак, $545^{503} \pmod{943} = 324{\cdot}18{\cdot}215{\cdot}795{\cdot}857{\cdot}400{\cdot}923{\cdot}545 \pmod{943} = 35$.

1.1 Китайская теорема об остатках

Китайская теорема об остатках (Chinese Remainder Theorem) рассматривает следующую задачу. Мы ищем целое число x, которое при делении на 5 дает в остатке 4, при делении на 8 дает в остатке 7, а при делении на 9 дает в остатке 3.

Иначе говоря, требуется найти число $x \in \mathbb{N}$, которое удовлетворяет системе сравнений

$$x = 4 \pmod{5}; \tag{1}$$
$$x = 7 \pmod{8}; \tag{2}$$
$$x = 3 \pmod{9}. \tag{3}$$

Количество модулей может быть любым, но никакая пара не должна иметь общих множителей.

Теорема. Два сравнения $n \equiv n_1 \pmod{m_1}$ и $n \equiv n_2 \pmod{m_2}$ разрешимы только, если $n_1 \equiv n_2 \pmod{\gcd(m_1, m_2)}$

$$n = t \cdot m_1 + n_1 \; n = s \cdot m_2 + n_2.$$

$$t \cdot m_1 - s \cdot m_2 = n_2 - n_1. \tag{4}$$

Левая часть (4) делится на $\gcd(m_1, m_2)$, значит должна делиться и правая.

Вернемся к системе (1), разберемся, почему одним из решений будет число

$$144 + 135 + 120. \tag{5}$$

$$144 \equiv 4 \pmod 5),\ 5 \mid 120,\ 5 \mid 135.$$

Точно так же 144 и 120 делятся на 8, а 135 дает в остатке 7.

$$135 = 16 \cdot 8 + 7.$$

Наконец, и последнее сравнение также удовлетворяется, поскольку два слагаемых делятся на 9, а 120 дает в остатке 3.

Итак, 399=144+135+120 решение системы сравнений. Можно получить и другие решения прибавляя $k \cdot 5 \cdot 8 \cdot 9 = 360 \cdot k$, поскольку ни одно из сравнений не нарушается.

Получить решение (5) можно так. Перемножим второй и третий модули $8 \times 9 = 72$. Найдем число, кратное полученному и удовлетворяющее первому сравнению: $72 \times 2 = 144$. Теперь перемножим $5 \times 9 = 45$, второму сравнению удовлетворяет $45 \times 3 = 135$. Наконец, перемножая первые два модуля,найдем третье число: $5 \times 8 \times 3 = 120 \equiv 3 \pmod 9$.

Недостаток рассмотренной методики — перебор множителей для удовлетворения сравнениям.

Общий метод решения следующий. Найти x,

$$x \equiv x_i \pmod{m_i} \text{ для } 1 < i < k. \tag{6}$$

Построим алгоритм для вычисления x. Мы рассмотрим только случай взаимно простых модулей m_i. Пусть

$$M = \prod_{1 \le i \le k} m_i \text{ и } M_i = M/m_i. \tag{7}$$

Для рассматриваемого случая $\gcd(M_i, m_i) = 1$, $\forall m_i$, значит, с помощью расширенного алгоритма Евклида можно найти такие a_i, что $a_i \cdot M_i \equiv 1 \pmod{m_i}$. Если положить

$$x = \sum_i a_i M_i x_i, \tag{8}$$

то все сравнения (6) будут удовлетворяться. Действительно, сравнения можно почленно складывать, поэтому по $\mod m_l$ все слагаемые (8), кроме l-го, будут равны нулю в силу определения (7).

В рассматриваемом примере $M = 5 \cdot 8 \cdot 9 = 360$, $M_1 = 72$, $M_2 = 45$, $M_3 = 40$. Алгоритм Евклида дает $a_1 = 3$, $a_2 = 5$, $a_3 = 7$. Искомое число

$$x = 4 \cdot 3 \cdot 72 + 7 \cdot 5 \cdot 45 + 3 \cdot 7 \cdot 40 = 3279 \equiv 39 \pmod{5 \cdot 8 \cdot 9}.$$

Мы остановились на числе 39, как наименьшем положительном из всех возможных решений.

1.2 Задачи ИДЗ 2013 г.

В отчете приводить подробный протокол решения задачи! Сдать отчет во вторник 26 марта 2013г. Если что-то не решается — так и пишем в отчете!

Вариант №1

1. Найти НОД и НОК алгоритмом Евклида 1232, 1672.

2. Найти значение функции Эйлера от числа ддмм, где дд — двузначная дата, а мм — двузначное обозначение месяца вашего рождения.

3. Расшифровать сообщение 428. Элементы ключа RSA $\boxed{e = 7,\ p = 23,\ q = 41}$.

4. Найти наименьшее положительное решение системы сравнений

$$\begin{aligned} x &= 3 \pmod 5; \\ x &= 2 \pmod 8; \\ x &= 2 \pmod 9). \end{aligned}$$

5. Решить в целых числах уравнение(или обнаружить, что множество решений пусто) $11x + 23y = 24$.

Вариант №2

1. Найти НОД и НОК алгоритмом Евклида 132, 210.

2. Найти значение функции Эйлера от числа ддмм, где дд — двузначная дата, а мм — двузначное обозначение месяца вашего рождения.

3. Расшифровать сообщение 76. Элементы ключа RSA $\boxed{e = 7,\ p = 23,\ q = 41}$.

4.Найти наименьшее положительное решение системы сравнений

$$\begin{aligned} x &= 3 \pmod 5; \\ x &= 2 \pmod 7; \\ x &= 2 \pmod 9). \end{aligned}$$

5. Решить в целых числах уравнение(или обнаружить, что множество решений пусто) $15x + 19y = 1$.

Вариант №3

1. Найти НОД и НОК алгоритмом Евклида 135, 82 11.

2. Найти значение функции Эйлера от числа ддмм, где дд — двузначная дата, а мм — двузначное обозначение месяца вашего рождения.

3. Расшифровать сообщение 637. Элементы ключа RSA $\boxed{e = 7,\ p = 23,\ q = 41}$.

4. Найти наименьшее положительное решение системы сравнений

$$\begin{aligned} x &= 2 \pmod{3}; \\ x &= 3 \pmod{5}; \\ x &= 2 \pmod{7}. \end{aligned}$$

5. Решить в целых числах уравнение(или обнаружить, что множество решений пусто) $253x - 449y = 1$.

Вариант №4

1. Найти НОД и НОК алгоритмом Евклида 549, 387.

2. Найти значение функции Эйлера от числа ддмм, где дд — двузначная дата, а мм — двузначное обозначение месяца вашего рождения.

3. Расшифровать сообщение 354. Элементы ключа RSA $\boxed{e = 7,\ p = 23,\ q = 41}$.

4.Найти наименьшее положительное решение системы сравнений

$$\begin{aligned} x &= 1 \pmod{4}; \\ x &= 2 \pmod{3}; \\ x &= 3 \pmod{5}. \end{aligned}$$

5. Решить в целых числах уравнение(или обнаружить, что множество решений пусто) $53x + 47y = 11$.

Вариант №5

1. Найти НОД и НОК алгоритмом Евклида 589, 343.

2. Найти значение функции Эйлера от числа ддмм, где дд — двузначная дата, а мм — двузначное обозначение месяца вашего рождения.

3. Расшифровать сообщение 249. Элементы ключа RSA $\boxed{e = 7,\ p = 23,\ q = 41}$.

4. Найти наименьшее положительное решение системы сравнений

$$\begin{aligned} x &= 4 \pmod{7}; \\ x &= 5 \pmod{11}. \end{aligned}$$

5. Решить в целых числах уравнение(или обнаружить, что множество решений пусто) $38x + 114y = 209$.

Вариант №6

1. Найти НОД и НОК алгоритмом Евклида 12606,6494.

2. Найти значение функции Эйлера от числа ддмм, где дд — двузначная дата, а мм — двузначное обозначение месяца вашего рождения.

3. Расшифровать сообщение 34. Элементы ключа RSA $\boxed{e = 7,\ p = 23,\ q = 41}$.

4. Найти наименьшее положительное решение системы сравнений

$$\begin{aligned} x &= 3 \pmod 3; \\ x &= 3 \pmod 5; \\ x &= 5 \pmod 7). \end{aligned}$$

5. Решить в целых числах уравнение(или обнаружить, что множество решений пусто) $91x + 117y = 156$.

Вариант №7

1. Найти НОД и НОК алгоритмом Евклида 297, 765.

2. Найти значение функции Эйлера от числа ддмм, где дд — двузначная дата, а мм — двузначное обозначение месяца вашего рождения.

3. Расшифровать сообщение 133. Элементы ключа RSA $\boxed{e = 7,\ p = 23,\ q = 41}$.

4. Найти наименьшее положительное решение системы сравнений

$$\begin{aligned} x &= 3 \pmod 5; \\ x &= 7 \pmod 7; \\ x &= 3 \pmod 9). \end{aligned}$$

5. Решить в целых числах уравнение(или обнаружить, что множество решений пусто) $24x + 81y = 6$.

Вариант №8

1. Найти НОД и НОК алгоритмом Евклида 1628, 3217.

2. Найти значение функции Эйлера от числа ддмм, где дд — двузначная дата, а мм — двузначное обозначение месяца вашего рождения.

3. Расшифровать сообщение 710. Элементы ключа RSA $\boxed{e = 7,\ p = 23,\ q = 41}$.

4. Найти наименьшее положительное решение системы сравнений

$$\begin{aligned} x &= 2 \pmod 5; \\ x &= 5 \pmod 6; \\ x &= 3 \pmod 7). \end{aligned}$$

5. Решить в целых числах уравнение(или обнаружить, что множество решений пусто) $73x + 151y = 3$.

Вариант №9

1. Найти НОД и НОК алгоритмом Евклида 469459, 519302.

2. Найти значение функции Эйлера от числа ддмм, где дд — двузначная дата, а мм — двузначное обозначение месяца вашего рождения.

3. Расшифровать сообщение 857. Элементы ключа RSA $\boxed{e = 7,\ p = 23,\ q = 41}$.

4. Найти наименьшее положительное решение системы сравнений

$$\begin{aligned} x &= 2 \pmod 5; \\ x &= 7 \pmod 6; \\ x &= 2 \pmod 7. \end{aligned}$$

5. Решить в целых числах уравнение(или обнаружить, что множество решений пусто) $27x + 78y = 12$.

Вариант №10

1. Найти НОД и НОК алгоритмом Евклида 73808, 30826.

2. Найти значение функции Эйлера от числа ддмм, где дд — двузначная дата, а мм — двузначное обозначение месяца вашего рождения.

3. Расшифровать сообщение 153. Элементы ключа RSA $\boxed{e = 7,\ p = 23,\ q = 41}$.

4. Найти наименьшее положительное решение системы сравнений

$$\begin{aligned} x &= 3 \pmod 5; \\ x &= 5 \pmod 8; \\ x &= 8 \pmod 9. \end{aligned}$$

Вариант №11

1. Найти НОД и НОК алгоритмом Евклида 17937, 43351.

2. Найти значение функции Эйлера от числа ддмм, где дд — двузначная дата, а мм — двузначное обозначение месяца вашего рождения.

3. Расшифровать сообщение 90. Элементы ключа RSA $\boxed{e = 7,\ p = 23,\ q = 41}$.

4. Найти наименьшее положительное решение системы сравнений

$$\begin{aligned} x &= 3 \pmod 5; \\ x &= 5 \pmod 7; \\ x &= 8 \pmod 9. \end{aligned}$$

5. Решить в целых числах уравнение(или обнаружить, что множество решений пусто) $165x + 418y = 121$.

Вариант №12

1. Найти НОД и НОК алгоритмом Евклида 1403, 1058.

2. Найти значение функции Эйлера от числа ддмм, где дд — двузначная дата, а мм — двузначное обозначение месяца вашего рождения.

3. Расшифровать сообщение 33. Элементы ключа RSA $\boxed{e = 7,\ p = 23,\ q = 41}$.

4. Найти наименьшее положительное решение системы сравнений

$$\begin{aligned} x &= 2 \pmod 5; \\ x &= 5 \pmod 7; \\ x &= 5 \pmod 9. \end{aligned}$$

5. Решить в целых числах уравнение(или обнаружить, что множество решений пусто) $23x + 18y = 4$.

Вариант №13

1. Найти НОД и НОК алгоритмом Евклида 36372, 147 220.

2. Найти значение функции Эйлера от числа ддмм, где дд — двузначная дата, а мм — двузначное обозначение месяца вашего рождения.

3. Расшифровать сообщение 298. Элементы ключа RSA $\boxed{e = 7,\ p = 23,\ q = 41}$.

4. Найти наименьшее положительное решение системы сравнений

$$\begin{aligned} x &= 2 \pmod 5; \\ x &= 5 \pmod 7; \\ x &= 8 \pmod 9. \end{aligned}$$

5. Решить в целых числах уравнение(или обнаружить, что множество решений пусто) $39x + 299y = 27$.

Вариант №14

1. Найти НОД и НОК алгоритмом Евклида 10140, 92274.

2. Найти значение функции Эйлера от числа ддмм, где дд — двузначная дата, а мм — двузначное обозначение месяца вашего рождения.

3. Расшифровать сообщение 414. Элементы ключа RSA $\boxed{e = 7,\ p = 23,\ q = 41}$.

4. Найти наименьшее положительное решение системы сравнений

$$\begin{aligned} x &= 3 \pmod{11}; \\ x &= 5 \pmod{13}; \\ x &= 8 \pmod 9. \end{aligned}$$

5. Решить в целых числах уравнение(или обнаружить, что множество решений пусто) $122x + 129y = 156$.

Вариант №15

1. Найти НОД и НОК алгоритмом Евклида 420, 126.

2. Найти значение функции Эйлера от числа ддмм, где дд — двузначная дата, а мм — двузначное обозначение месяца вашего рождения.

3. Расшифровать сообщение 438. Элементы ключа RSA $\boxed{e = 7,\ p = 23,\ q = 41}$.

4. Найти наименьшее положительное решение системы сравнений

$$\begin{aligned} x &= 3 \pmod 5; \\ x &= 5 \pmod 7; \\ x &= 8 \pmod{11}. \end{aligned}$$

5. Решить в целых числах уравнение(или обнаружить, что множество решений пусто) $91x + 117y = 156$.

Вариант №16

1. Найти НОД и НОК алгоритмом Евклида 126, 525.

2. Найти значение функции Эйлера от числа ддмм, где дд — двузначная дата, а мм — двузначное обозначение месяца вашего рождения.

3. Расшифровать сообщение 933. Элементы ключа RSA $\boxed{e = 7,\ p = 23,\ q = 41}$.

4. Найти наименьшее положительное решение системы сравнений

$$\begin{aligned} x &= 3 \pmod 6; \\ x &= 5 \pmod 7; \\ x &= 8 \pmod{11}. \end{aligned}$$

5. Решить в целых числах уравнение(или обнаружить, что множество решений пусто) $15x+19y = 1$.

Вариант №17

1. Найти НОД и НОК алгоритмом Евклида 529, 1541.

2. Найти значение функции Эйлера от числа ддмм, где дд — двузначная дата, а мм — двузначное обозначение месяца вашего рождения.

3. Расшифровать сообщение 48. Элементы ключа RSA $\boxed{e = 7,\ p = 23,\ q = 41}$.

4. Найти наименьшее положительное решение системы сравнений

$$\begin{aligned} x &= 2 \pmod 5; \\ x &= 5 \pmod 7; \\ x &= 7 \pmod 9. \end{aligned}$$

5. Решить в целых числах уравнение(или обнаружить, что множество решений пусто) $81x - 48y = 33$.

Вариант №18

1. Найти НОД и НОК алгоритмом Евклида 1541, 1817.

2. Найти значение функции Эйлера от числа ддмм, где дд — двузначная дата, а мм — двузначное обозначение месяца вашего рождения.

3. Расшифровать сообщение 284. Элементы ключа RSA $\boxed{e = 7,\ p = 23,\ q = 41}$.

4. Найти наименьшее положительное решение системы сравнений

$$\begin{aligned} x &= 3 \pmod{5}; \\ x &= 5 \pmod{11}; \\ x &= 8 \pmod{9}. \end{aligned}$$

5. Решить в целых числах уравнение(или обнаружить, что множество решений пусто) $13x - 11y = 5$.

Вариант №19

1. Найти НОД и НОК алгоритмом Евклида 549, 493.

2. Найти значение функции Эйлера от числа ддмм, где дд — двузначная дата, а мм — двузначное обозначение месяца вашего рождения.

3. Расшифровать сообщение 753. Элементы ключа RSA $\boxed{e = 7,\ p = 23,\ q = 41}$.

4. Найти наименьшее положительное решение системы сравнений

$$\begin{aligned} x &= 3 \pmod{5}; \\ x &= 5 \pmod{7}; \\ x &= 6 \pmod{9}. \end{aligned}$$

5. Решить в целых числах уравнение(или обнаружить, что множество решений пусто) $81x - 48y = 33$.

Вариант №20

1. Найти НОД и НОК алгоритмом Евклида 1253, 252.

2. Найти значение функции Эйлера от числа ддмм, где дд — двузначная дата, а мм — двузначное обозначение месяца вашего рождения.

3. Расшифровать сообщение 716. Элементы ключа RSA $\boxed{e = 7,\ p = 23,\ q = 41}$.

4. Найти наименьшее положительное решение системы сравнений

$$\begin{aligned} x &= 3 \pmod{4}; \\ x &= 5 \pmod{7}; \\ x &= 8 \pmod{11}. \end{aligned}$$

5. Решить в целых числах уравнение(или обнаружить, что множество решений пусто) $23x + 18y = 4$.