# Алгоритмы и модели вычислений.
# Задание 10: теория чисел

Сергей Володин, 272 гр.

задано 2014.04.17

## (каноническое) Задача 41

**Модель вычислений: RAM, трудоемкость $C$ — суммарное количество арифметических операций, присваиваний, сравнений.**
Мое решение задания 2 $\Rightarrow$

1. $g_n = 2g_{n-1} + g_{n-2}$, $g_0 = 1$, $g_1 = 3$
2. $g_n = \frac{1}{2}\left[(1+\sqrt{2})^{n+1} + (1-\sqrt{2})^{n+1}\right]$

1. (a) Алгоритм:

```
1  number g(number n, number p)
2  {
3    number a = 1;
4    number b = 3;
5
6    if(n == 0) return(a);
7    if(n == 1) return(b);
8
9    number i, bt;
10   for(i = 2; i <= n; i++)
11   {
12     bt = 2 * b + a;
13     a = b;
14     b = bt;
15   }
16
17   return(b);
18 }
```

   (b) Корректность

      i. $g_0 = 1 = g(0)$ (строка 6)

      ii. $g_1 = 3 = g(1)$ (строка 7)

      iii. $n \geqslant 2$:

         A. $P_i =$ [после $i$-й итерации цикла $a = g_{i-1}$, $b = g_i$]. $i$-я итерация цикла — при таком значении переменной $i$.

         B. $P_1$ (до цикла) верно: (строки 3, 4): $a = g_{1-1} = 1$, $b = g_1 = 3$.

         C. Пусть $P_k$. Тогда $a \equiv a_{\text{old}} = g_{k-1}$, $b \equiv b_{\text{old}} = g_k$ после $k$-й итерации. После следующей $(k+1)$ итерации $a = b_{\text{old}} = g_k$, $b = 2b_{\text{old}} + a_{\text{old}} = 2g_k + g_{k-1} \overset{1}{=} g_{k+1}$ $\blacksquare$ $\forall k \geqslant 2 \hookrightarrow P(k)$

         D. В конце (после $n$-й итерации) $P(n) \Rightarrow b = g_n$ $\blacksquare$ $\forall n \geqslant 2 \hookrightarrow g(n) = g_n$ (строка 17)

   (c) Время работы. При $n \in \{0, 1\}$ $C(0) = 3$, $C(1) = 4$. На каждой итерации цикла трудоемкость константная $c = 8$, поэтому общее количество арифметических операций

$$C(n) = \begin{cases} 3, & n = 0 \\ 4, & n = 1 \\ 5 + 8(n-1), & n \geqslant 2 \end{cases}$$

   (d) Вычисление по модулю: вычислим $g(n)$, вычислим $g(n) \mod p$. Добавляется одна единица трудоемкости.

   (e) Асимптотика $C(n) = O(n)$

   (f) Трудоемкость вычисления $A = g_{10000} \mod 19$: $C(10000) = 5 + 8(9999) = 79997$

2. (a) Фиксируем $p \in \mathbb{N}$. Рассмотрим функцию $f\colon \mathbb{N} \to \overline{0, p-1}^2$: $f(k) = (g_{k-1} \mod p, g_k \mod p)$. Область определения $|D_f| = \infty$, множество значений $|E_f| = p^2$, откуда $|E_f| < |D_f|$, получаем, что $f$ — не инъективна, то есть, $\exists \mathbb{N} \ni i \neq j \in \mathbb{N}\colon f(i) = f(j) \Leftrightarrow (g_{i-1} \mod p, g_i \mod p) = (g_{j-1} \mod p, g_j \mod p)$

(b) Фиксируем эти $i \neq j$: $f(i) = f(j)$. $P(t) \overset{\text{def}}{=} [f(i+t) = f(j+t)]$. $P(0)$ выполнено. Пусть $P(t)$. Тогда $f(i+t) = f(j+t) \Leftrightarrow \begin{cases} g_{i+t-1} = g_{j+t-1} \mod p \\ g_{i+t} = g_{j+t} \mod p \end{cases}$. Тогда $g_{i+t+1} \overset{1}{=} 2g_{i+t} + g_{i+t-1} \overset{P(t)}{=} 2g_{j+t} + g_{j+t-1} \overset{1}{=} g_{j+t+1}$, откуда $f(i+t+1) = f(j+t+1)$ (второе условие из $P(t)$). Значит, $P(t+1)$. По индукции $\forall t \in \mathbb{N} \cup \{0\} \hookrightarrow P(t) \Rightarrow \forall t \in \mathbb{N} \cup \{-1, 0\} \hookrightarrow g_{i+t} = g_{j+t}$

(c) То есть, последовательности $\{g_n\}_{n=i-1}^{\infty} = \{g_n\}_{n=j-1}^{\infty}$, откуда следует, что $\{g_n \mod p\}_{n=0}^{\infty}$ — периодическая с периодом $|i-j|$, начиная с $\min(i-1, j-1)$. Используя рекуррентность «в обратную сторону» получаем, что она периодическая с начала (с $n = 0$).

(d) Оценим период $|i-j|$. $|E_f| = p^2$, откуда $|i-j| \leqslant p^2$. Пусть иначе: $|i-j| \geqslant p^2 + 1$. Без ограничения общности, $i < j$. Тогда $f(i), f(i+1), ..., f(j-1)$ — все различны. Их количество $j - i \geqslant p^2 + 1$, и они из $E_f$ — противоречие, $|E_f| = p^2$.

(e) Для $p = 19$: $|i-j| \leqslant 19^2 = 361$.

(f) Алгоритм: вычисляем период: храним $f(1)$, сравниваем $f(i)$ с $f(1)$. Вычисляем $g_i$ через рекуррентность (см. выше). Ищем место от начала периода для $n$ и выдаем ответ. Сложность $O(p^2)$ (величина периода). Для $A$: $p^2 = 361$, откуда $C \leqslant 2 \times (\underbrace{5 + 8(361-1)}_{\text{период}}) = 5770$ (2 — т.к. в два прохода, сначала поиск периода, потом вычисление $A$).

3. $p = 23$. $x = 5$: $x^2 = 25 \equiv 2 \mod p$. $2 \Rightarrow g_n = |t \overset{\text{def}}{=} \sqrt{2}| = \frac{1}{2}\left[(1+t)^{n+1} + (1-t)^{n+1}\right] = \frac{1}{2}\left[\sum_{k=0}^{n+1}\binom{n+1}{k}t^k - \sum_{k=0}^{n+1}\binom{n+1}{k}(-t)^k\right] = \sum_{k=0}^{n+1}\binom{n+1}{k}\frac{1+(-1)^k}{2}t^k \boxed{=}$. $1 + (-1)^k = \begin{cases} 2, & k = 2l \\ 0, & k = 2l+1 \end{cases}$, поэтому $\boxed{=} \sum_{l=0}^{\lfloor\frac{n+1}{2}\rfloor}\binom{n+1}{2l}t^{2l} \equiv \sum_{l=0}^{\lfloor\frac{n+1}{2}\rfloor}\binom{n+1}{2l}2^l$. Поэтому $g_n \mod p = \left[\sum_{l=0}^{\lfloor\frac{n+1}{2}\rfloor}\binom{n+1}{2l}2^l\right] \mod p = |x^2 \equiv 2 \mod p| = \sum_{l=0}^{\lfloor\frac{n+1}{2}\rfloor}\left[\binom{n+1}{2l}x^{2l}\right] \mod p$. Раскрывая обратно по той же формуле, получаем

$$g_n \mod p = \frac{(1+x)^{n+1} + (1-x)^{n+1}}{2} \mod p.$$

Для конкретной задачи

$$g_n \mod 23 = \frac{6^{n+1} + 19^{n+1}}{2} \mod 23$$

Возводим в степень Быстрым возведением в степень. Количество операций $O(\log n)$. Алгоритм:

```
number n = 10000;
number p = 23;
number x = 5;
number pow1(number a, number n)
{
  if(n == 0) return(1 % p);
  else if(n % 2 == 0)
  {
    number m = pow1(a, n / 2);
    return((m * m) % p);
  }
  else return((a * pow1(a, n - 1)) % p);
}

number g(n)
{
  return((pow1(6, n + 1) + pow1(19, n + 1)) / 2);
}

print(g(n));
```

Ответ: $g_{10000} \mod 23 = 10$.

4. Вернемся к формуле $g_n \mod p = \left[\sum_{l=0}^{\lfloor\frac{n+1}{2}\rfloor}\binom{n+1}{2l}2^l\right] \mod p$, посчитаем по ней **???**

## (каноническое) Задача 42

*(Кормен)*

1. $N \in \mathbb{N}, a$: $(a, N) = 1, a^{N-1} \neq 1 \mod N$. $\mathbb{Z}_N^* = \{a | a < N, (a, N) = 1\}$. Рассмотрим множество $G = \{x | x^{N-1} = 1\}$. Пусть $x \in G$. Тогда $x \cdot x^{N-2} = 1 \mod N$, то есть, существует обратный элемент к $x$, откуда $x \in \mathbb{Z}_N^*$. Значит, $G \subseteq \mathbb{Z}_N^*$. Пусть $x_1, x_2 \in G \Rightarrow x_1^{N-1} = 1 \mod p$, $x_2^{N-1} = 1 \mod p$. Тогда $x_1 x_2 = 1 \mod p$, и $x_1 x_2 \in G$. Получаем, что $G$ — замкнута, значит, $G$ — подгруппа $\mathbb{Z}_N^*$. Теорема Лагранжа $\Rightarrow |\mathbb{Z}_N^*| = k|G|$. По условию, $a \in \mathbb{Z}_N^* \setminus G$, откуда $|G| < |\mathbb{Z}_N^*|$. Значит, $k \geqslant 2$, и $|G| \leqslant \frac{|\mathbb{Z}_N^*|}{2}$. Но $|\mathbb{Z}_N^*| = \varphi(N) \leqslant N - 1$, откуда $|G| \leqslant \frac{N-1}{2}$. Рассмотрим $\overline{G} = \overline{1, N-1} \setminus G$. Очевидно, $1 \notin \overline{G}$, так как $1^{N-1} = 1 \mod p$. Тогда $\overline{G} \subseteq \overline{2, N-1}$, причем $|\overline{G}| = |\overline{1, N-1}| - |G| \geqslant N - 1 - \frac{N-1}{2} = \frac{N-1}{2}$ ■

2. НОД$(a, b)$ — полиномиален по $|a|$, $|b|$ (лекции), вычисление $a^{N-1} \mod N$ — также (быстрое возведение в степень, см. мое решение задачи 12).

3. $P(a = i \in \overline{2, N-1}) = \frac{1}{N-1} = p$. Пусть $N$ — составное. Тогда $\exists a < N\colon (a, N) = 1$.

   (a) С вероятностью $\frac{1}{N-1}$ алгоритм выдаст правильный ответ (угадан делитель)

   (b) В противном случае с вероятностью $\geqslant \frac{1}{2}$ (см. первый пункт. По условию, хотя бы одно такое $a$ существует, значит, таких $a$ не меньше половины) будет выбрано $a\colon a^{N-1} \neq 1 \mod p$, и будет выдан правильный ответ.

   Поэтому $P \geqslant \frac{1}{N-1} + (1 - \frac{1}{N-1})\frac{1}{2} = 1 - \frac{1}{2(N-1)}$. $N \geqslant 2 \Rightarrow N - 1 \geqslant 1 \Rightarrow P \geqslant \frac{1}{2}$ ■

## (каноническое) Задача 43

Открытый ключ $(e, n) = (11, 899)$. $M \in \mathbb{Z}_n$ — сообщение.
Чтобы вычислить цифровую подпись сообщения $M$, необходимо вычислить $S(M) = M^d \mod n$,
где $d\colon ed = 1 \mod \varphi(n)$. $n = \underbrace{29}_{p} \cdot \underbrace{31}_{q}$, $p$, $q$ — простые, поэтому $\varphi(n) = (p-1)(q-1) = 28 \cdot 30 = 840$.
Подбором найдем $d = 611$, проверим: $ed = 6721 \equiv 1 \mod 840 \Rightarrow$ Ответ: в степень $d = 611$.

## (каноническое) Задача 44

1. $8\varphi(n) \geqslant \sqrt{n}$ при $n \notin \{2, 6\}$. Получим, что $n \leqslant 8^2 = 64$. Перебором найдем $n \in \{15, 16, 20, 24, 30\}$.

2. Перебором найдем

| Порядок | Элементы |
|---|---|
| 1 | 1 |
| 11 | 2, 3, 4, 6, 8, 9, 12, 13, 16, 18 |
| 22 | 5, 7, 10, 11, 14, 15, 17, 19, 20, 21 |

3. Перебором найдем множество первообразных корней {5, 7, 10, 11, 14, 15, 17, 19, 20, 21}

## (каноническое) Задача 45

$\mathbb{Z}_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$, $\mathbb{Z}_9^* = \{x \big| x < 9,\ (x, 9) = 1\} = \{1, 2, 4, 5, 7, 8\}$. $h_{a,b}(k) \stackrel{\text{def}}{=} [(ak + b) \mod 8] \mod 5$.
$H \stackrel{\text{def}}{=} \{h_{a,b} \big| a \in \mathbb{Z}_9^*,\ b \in \mathbb{Z}_9\}$.

1. $n_2 = 5$, так как $\forall a, b, k \hookrightarrow h_{a,b}(k) \in \overline{0, 4}$.

2. $|H| \leqslant |\mathbb{Z}_9 \times \mathbb{Z}_9^*| = 9 \cdot 6 = 54$.

3. $h_{a_1,b_1}(k) = h_{a_2,b_2}(k) \Leftrightarrow ((a_1 k + b_2) \mod 8) \mod 5 = ((a_2 k + b_2) \mod 8) \mod 5 \Leftrightarrow ([(a_1 - a_2)k + (b_1 - b_2)] \mod 8) \mod 5 = 0$.

4. Функции $h_{a_1,b_1}$, $h_{a_2,b_2}$ совпадают $\Leftrightarrow \forall k \in U \hookrightarrow h_{a_1,b_1}(k) = h_{a_2,b_2}(k)$.

5. $((ak + b) \mod 8) \mod 5 = 0 \Leftrightarrow \exists l_1\colon 5 \big| (ak + b) \mod 8 \Leftrightarrow \left[\begin{array}{l} ak + b \equiv 5 \mod 8 \\ ak + b \equiv 0 \mod 8 \end{array}\right.$ **???**

6. Перебором найдем $|H| = 45$ (количество различных хеш-функций).

7. $n_1 = 8$ $(k = k_0 + 8l \Rightarrow h_{a,b}(k) = h_{a,b}(k_0))$

8. Нет, $H$ — не универсальное (например, для $k = 0$, $l = 2$ количество функций $h \in H\colon h(k) = h(l)$ равно $13 > \frac{|H|}{n_2} = \frac{45}{5} = 9$).