① Факторизация: Для зад. $n \in \mathbb{Z}^+$ найти $n = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$

↓

распознование чисел на простоту

② Задача RSA:

Для зад. $n = p \cdot q$ и $e \mid HOD(e; (p-1)(q-1)) = 1$

Найти: $m \mid m^e \equiv c \pmod n$

③ Задача квадратичи вычетов: Для зад. сост. нат. n и зад. цел. $a \mid \left(\frac{a}{n}\right) = 1$, определить явл-ся a – кв. вычет. или невычетом

$$\left(\frac{a}{p \cdot q}\right) = \underbrace{\left(\frac{a}{p}\right)}_{-1} \cdot \underbrace{\left(\frac{a}{q}\right)}_{-1} = 1$$

④ Вычисл. квадр. корня по mod n: Для зад. составн. n и квадр. выч. $a \pmod n$ найти $x \mid x^2 \equiv a \pmod n$

⑤ Задача дискр. логарифма: Для зад. прост p; α, где $\langle\alpha\rangle = \mathbb{Z}_p^*$ и $\beta \in \mathbb{Z}_p^*$ найти $x \in [0; p-2]$ | $\alpha^x \equiv \beta \pmod p$

(DLP)

$$\log_\alpha \alpha^x \equiv \log_\alpha \beta \pmod{p-1}$$

$$x \equiv \log_\alpha \beta \pmod{p-1}$$

⑥ Обобщ. задача дискр. логарифма

⑨ Задача суммы подмн-в: Для зад. мн-ва $\{a_1; a_2; \dots; a_n\}$ (положит. целые) и положит. целого S определить,

$\exists$-ет ли подмн-во $\{a_j\}_{j\in\{1;\dots;n\}} \subset \{a_1; a_2; \dots; a_n\}$ | $\sum a_j = S$

Гл 4. **Тесты чисел на простоту/непростоту**

$\pi(x)$ - число простых в $[2; x]$

$\pi(x) \sim \frac{x}{\ln x}$

Аппроксимация n-го прост. числа

$\exists p_n$ - n-е прост число $\Rightarrow p_n \sim n \cdot \ln n$

Кр. того, $n \cdot \ln n < p_n < n(\ln n + \ln(\ln n))$, $n \geq 6$

Теорема (Дирихле): Если $НОД(a; n) = 1 \Rightarrow$ $\exists$-ет бесконечно много простых $\equiv a \pmod n$

Предлож.: $\pi(x; n; a)$, $\pi(x; n; a) \sim \frac{x}{\varphi(n) \cdot \ln x}$.

§4.1. Тест Ферма.

Малая т. Ферма: Если n-прост., то $(*)$ $a^{n-1} \equiv 1 \pmod{n}$, $1 \le a \le n-1$

(n — прост)

Обратное в общем случае неверно

Опр

Если выполн. $(*)$ и n — не мол-ся прост. $\Rightarrow$ n наз-ся псевдопрост. по основ. a

Пример: $2^{340} \equiv 1 \pmod{341}$; $341 = 11 \cdot 31$

Алгоритм:

$a^{n-1} \equiv 1 \pmod n$

Вход: цел. $n \geq 3$ и пар-р без-ти $t \geq 1$

Выход: Вопрос: "Явл-ся ли n – прост" → ответ: "Вероятно прост"/"Составн".

① Для $i = \overline{1;t}$:

1.1 Выбир. случ. обр $a \in [2; n-2]$

1.2 Вычисл. $r := a^{n-1} \pmod n$

1.3 Если $r \neq 1 \Rightarrow$ возвращ. "n-составн"

② Возвращ. "n-вер. прост."

Опр: Составн. число n наз-ся числом Кармайкла, если

для всех $a \mid HOД(a;n)=1$: $a^{n-1} \equiv 1 \pmod n$

Св-ва (чисел Кармайкла).

Наим. число Кармайкла, $561 = 3 \cdot 11 \cdot 17$.

Эквив.

1. n – своб. от квадр
2. $(p-1) \mid (n-1)$, где p - прост. $\mid$ $p \mid n$.
3. $\forall$ число Кармайкла есть произвед, по кр. мере, $3^{\text{ех}}$ прост. (разных) чисел.
4. $\exists$-ет ∞ числа Кармайкла.
5. Кол-во чисел Кармайкла, $\leq n^{1-\{1+o(1)\}\cdot \ln\ln\ln n / \ln\ln n}$ меньших n

§4.2. Тест Соловея – Штрассена

Критерий Эйлера: $\exists$ n – неч. Тогда $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod n$. (**)

для $\forall a \mid НОД(a;n)=1$

Опр:
Если выполн. (**), то n наз-ся эйлеровым псевдопрост. по основ. a.

Пример: $9^{\frac{91-1}{2}} \equiv 1 = \left(\frac{9}{91}\right) \pmod{91}$; $91 = 7 \cdot 13$.

Факт: $\exists$ n-неч. составн. Тогда $\overset{\exists\text{-ет}}{\vee}$ не более $\frac{\varphi(n)}{2}$ всех чисел a $\left(1 \le a \le n-1\right)$, для котор n явл-ся Эйлер. псевдопрост.

Алгоритм:

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod n$$

Вход: нат. $n \geq 3$ и $t \geq 1$ – нар-р безопасности.

Выход: ответ на вопрос "n – прост?"

① Для $i = \overline{1;t}$:

1.1 Выбир. случ. обр. $a \in [1; n-1]$

1.2 Вычисл. $r := a^{\frac{n-1}{2}} \pmod n$

1.3 Если $r \neq 1$ и $r \neq n-1$ $\Rightarrow$ возвращ "n-составн"

1.4 Вычисл. $S := \underbrace{\left(\frac{a}{n}\right)}_{\text{символ Якоби}}$.

1.5 Если $r \neq S \Rightarrow$ возвращ. "n-составн".

② Возвращ. "n – вероятно прост".

$\left(\frac{1}{2}\right)^t$

§4.3. Тест Миллера - Рабина

(***)

Diz

Предлож: $\exists\ n$ - неч. прост.; $n-1 = 2^s \cdot \underbrace{r}_{\text{неч}}$; $\forall\ a \in [1; n-1]$ $НОД(a; n) = 1$

Тогда либо $a^r \equiv 1 \pmod n$ или $a^{2^j \cdot r} \equiv -1 \pmod n$ для некотор. $0 \le j \le s-1$

Опр: $\exists\ n$ – неч. составн: $n-1 = 2^s \cdot r$.

Если для n выполн. (***), то n наз-ся сильн. псевдопрост. числом по основ. a

Предлож: Если n - неч. сост., то для не более, чем $\frac{1}{4}$ всех чисел a, n - явл-ся сильн. псевдопрост. по основ. a

Пример: $n = 91$.

$n-1 = 90 = 2 \cdot \underbrace{45}_{r}$

$a = 9$; ... (для 18)

$9^r = 9^{45} \equiv 1 \pmod{91}$

$a^r \equiv 1 \pmod n$ или $a^{2^i \cdot r} \equiv -1 \pmod n$

Алгоритм:

Вход и Выход как ранее

① $n-1 = 2^{\textcircled{r}} \cdot \textcircled{s}$ ← находим r и s

② Для $i = \overline{1;t}$:

②.① Выбор случ. обр. $a \in [2; n-2]$

②.② $y := a^r \pmod n$

②.③ Если $y \neq 1$ и $y \neq n-1 \Rightarrow j := 1$.

Пока $j \leq s-1$ и $y \neq n-1$:

$y := y^2 \pmod n$

Если $y = 1 \Rightarrow$ Возвращ. "n-сост"; $j := j+1$;

Если $y \neq n-1 \Rightarrow$ возвращ. "n-сост"

③. Возвращ. "n-вер. прост"

Утверждение: $\exists$ n – нечет. составн.

продумать:

① Если n – эйлеров. псевдопрост. по основ. $a \Rightarrow$ n – псевдопрост. по основ. a.

② Если n – сильн. псевдопрост по основ. $a \Rightarrow$ n – эйлер. псевдопрост. по осн. a.

Утверждение: Если $n \equiv 3 \pmod 4$, то

n – эйлеров. псевдопрост. по основ. $a \Leftrightarrow$ n – строгое псевдопрост. по основ. a.

продумать