Практическое занятие 11

Приложения алгебры вычетов в криптографии

ITMO University

Проверка простоты целых чисел по малой Т. Ферма

Малая теорема Ферма

p – *простое число* $\Rightarrow \forall a \in \mathbf{N} \quad a^{p} = a \,(mod\, p)$

Выводы:

- если Т. (сравнение) выполняется, то нельзя делать вывод о простоте числа p.
- если Т. (сравнение) не выполняется, то p – составное.

Тест на основе малой Т. Ферма является эффективным для обнаружения *составных* чисел.

Нахождение остатков от деления больших степеней целых чисел по Т. Эйлера

Теорема Эйлера

$\forall n$ и $\forall a \geq 1$ НОД$(a,n)=1$

$$a^{\varphi(n)} = 1 \ (mod\ n)$$

Если $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$

– каноническое разложение числа *n*, то

$$\varphi(n) = p_1^{\alpha_1 - 1} \cdot p_2^{\alpha_2 - 1} \cdot \ldots \cdot p_k^{\alpha_k - 1} \cdot (p_1 - 1) \cdot (p_2 - 1) \cdot \ldots \cdot (p_k - 1).$$

Задача:

Найти остаток от деления большой степени целого числа на n.

Обозначим x – остаток от деления, тогда исходную задачу можно записать в виде сравнения $a^N \equiv x \pmod n$ (1)

1. Проверяем выполнение условия Т. Эйлера. Если оно не выполняется, то применяем свойство 7 сравнений и тогда сравнение (1) примет вид:

$$a^N \equiv \frac{x}{k} \pmod n, \qquad (2)$$

где $k>0$, НОД$(a,n)=1$.

Записываем значения a,n,N.

2. Находим $\varphi(n)$, применяем Т. Эйлера, т.е. записываем сравнение:

$$a^{\varphi(n)} = 1 \ (mod\ n).$$

3. Находим числа q и r, число N записываем в виде

$$N = \varphi(n)q + r, \quad \text{где } 0 \le r < \varphi(n)$$

4. Выражаем a^N по Т. Эйлера:

$$a^N = a^{\varphi(n)q+r} = (a^{\varphi(n)})^q a^r = a^r \ (mod\ n)$$

5. Вычисляем $a^r \ (mod\ n)$ бинарным методом возведения в степень, т.е. находим $\frac{x}{k}$.

6. Находим x.

7. Записываем ответ.