Лабораторная работа # 2

Возведение чисел в степень по модулю.

Цель лабораторной работы: используя результаты теории чисел, реализовать возведение числа в степень по модулю. Данные преобразования используются в криптографии, например, в алгоритме RSA.

Постановка задачи

Найти результат следующего преобразования:

$$c \equiv a^b \bmod M,$$

где числа a, b и M можно найти в вариантах к описанию лабораторной работы.

Порядок выполнения лабораторной работы

1. Факторизовать число M, по модулю которого производится возведение в степень.
2. Найти вектор остатков $\{r_i\}$ по модулям простых чисел $\{a_i\}$ таких, что $M = \prod_{i=1}^{k} a_i$.
3. Используя малую теорему Ферма найти $\tilde{r}_i \equiv r_i^b \bmod a_i$.
4. Реализовать восстановление числа c по его остаткам $\{\tilde{r}_i\}$ при помощи Китайской теоремы об остатках.

Рекомендации к выполнению

- Решение должно быть представлено на Python в Google Colab.
- Для факторизации натурального числа M можно реализовать самостоятельно любой из известных алгоритмов или воспользоваться готовыми реализациями из библиотеки SymPy.
- Малая теорема Ферма гласит:

  $$a^{m-1} \equiv 1 \bmod m$$

  откуда следует, что нет необходимости возводить даже остатки в большие степени.
- Китайская теорема об остатках должна быть реализована самостоятельно, даже если алгоритм не будет являться оптимальным.