Бабушкин А.

1 Обязательные задачи

1. Чтобы добиться ошибки e^{-1}, надо повторить n^3 раз, а чтобы затем $1/2^n$ – ещё n. Итого n^4 повторов, а всё решение за n^7.

2. Проверим Миллером-Рабином, простое ли число. Если оно составное, то затем тыкнем в случайное число, взаимно просто с n, и проверим, что оно свидетель простоты для Ферма.
   Если число простое, то Миллером-Рабином мы это найдём.
   Если составное и не Кармайкла, то с вероятностью $\leq 1/2$ ошибётся Миллер-Рабин, и мы его не найдём. И ещё с вероятностью $\leq 1/2$ ошибётся Ферма и выберет свидетеля простоты.
   Если составное и Кармайкла, то может ошибиться только Миллер-Рабин, а Ферма точно скажет, что оно простое.
   Ошибка двусторонняя, но $\log n$ проверок всё так же хватит.

3. Будем выбирать случайные y и вычислять g(x + y) - g(y), затем среди всех результатов выберем самый частый. Вероятность ошибиться у нас $2\epsilon - \epsilon^2$, будем понижать её, повторяя много раз.

4. Если в каждом клозе три различных переменных, то он выполняется с вероятностью 7/8, тогда матожидание числа выполненных – 7m/8. Если мы хотим выполнить $\geq 3m/4 = 6m/8$ клозов, то надо оступить от матожидания не больше чем на m/8, тогда хватит m запусков.

5. Если ответ нет, то RP не сможет ответить да. Если ответ да, то включим в подсказку случайные биты, на которых RP отвечает правильно.

6. На всех C1 тестах корректно Поллард отработает с вероятностью $(1 - 1/2)^{C1}$, а если повторить это k раз, то хотя бы раз победит с вероятностью $1-(1-(1/2)^{C1})^k$. $(1 - (1/2)^{C1})^k$ должно быть $\leq C2$, то есть $k \geq \log_{1-(1/2)^{C1}} C2$.

2 Дополнительные задачи

1. Пусть у них есть графы G и H, и они проведут несколько итераций таких действий:
   1. Алиса выбирает какой-то граф M, который изоморфен G, а значит, и H, и передаёт его Бобу.
   2. Боб выбирает случайный бит, и если он равен 0, то Алиса сообщает Бобу перестановку для изоморфизма G -> M, иначе перестановку для изоморфизма H -> M. Боб может легко проверить, сказала ли она правду. Она сможет ответить на оба эти запроса только в том случае, если G и H действительно

изоморфны.

2.