Тексты на диске O: Miller–Rabin Test

1. Если $n > 1$ нечетное, то докажите, что каждый свидетель Ферма n является свидетелем Миллера–Рабина n. (Это нетрудно. *Не* используйте упражнение во втором листке, что свидетели Ферма подмножество свидетелей Эйлера плюс трудный результат, что каждый свидетель Эйлера является свидетелем Миллера–Рабина.)

2. Докажите, что 2 свидетель Миллера–Рабина 12801.

3. Вот все нечетные составные $n < 10000$, для которых 2 не свидетель Эйлера:

   561, 1105, 1729, 1905, 2047, 2465, 3277, 4033, 4681, 6601, 8321, 8481.

   Для каждого из этих 12 чисел вычислите, является ли 2 свидетелем Миллера–Рабина; если нет, то проверьте, что 3 является свидетелем Миллера–Рабина.

   (Подсказка: 2 является свидетелем Миллера–Рабина семи из этих чисел.)

4. Проверьте, что 8 и 47 лжесвидетели Миллера–Рабина 65, а $8 \cdot 47 \equiv 14 \bmod 65$ является свидетелем Миллера–Рабина. Это иллюстрирует, что лжесвидетели Миллера–Рабина иногда не сохраняются при умножении.

5. Докажите, что если a свидетель Миллера–Рабина n, то $-a$ и $1/a \bmod n$ тоже свидетели Миллера–Рабина n.

6. Во втором листке было упражнение, что если существуют бесконечно много пар простых p и $2p-1$, то плотность свидетелей Ферма их произведений $p(2p-1)$ стремится к $1/2$ при $p \to \infty$ (по таким p). Что можно сказать о плотности свидетелей Эйлера или Миллера–Рабина таких произведений?

   а) Если p и $2p-1$ простые и $p \equiv 3 \bmod 4$, то $p(2p-1) \equiv 3 \bmod 4$, откуда следует, что понятия свидетеля Эйлера и свидетеля Миллера–Рабина такого произведения $p(2p-1)$ совпадают (см. текста по тесту Миллера–Рабина). Докажите, что плотность свидетелей Эйлера чисел вида $p(2p-1)$ среди

обратимых по модулю $n := p(2p-1)$

$$\frac{|\{1 \leqslant a \leqslant n-1 : \text{НОД}(a,n) = 1 \text{ и } a^{(n-1)/2} \not\equiv (\frac{a}{n}) \bmod n\}|}{|\{1 \leqslant a \leqslant n-1 : \text{НОД}(a,n) = 1\}|}$$

ровно $3/4$.

Выведите, что плотность всех свидетелей Миллера–Рабина таких чисел стремится к $3/4$ при $p \to \infty$, предполагая, что есть бесконечно много таких p. (Например, $12403 = p(2p-1)$ для $p = 79$ и плотность его свидетелей Миллера–Рабина равна $9360/12402 \approx 75.4\%$.)

б) Что происходит, если p и $2p-1$ простые и $p \equiv 1 \bmod 4$? (напр., $p = 37$ и $p(2p-1) = 2701$).

(Подсказка для пункта а: Рассмотрите лжесвидетели вместо свидетелей.)

7. Пусть p нечетное простое и $s \geq 1$.

   а) Докажите, что $x^2 \equiv 1 \bmod p^s \Longrightarrow x \equiv \pm 1 \bmod p^s$ (т.е., нет нетривиальных корней из единицы по модулю p^s).

   б) Докажите, что множество свидетелей Миллера–Рабина p^s описывается так: $\{1 \leq a \leq p^s - 1 : a^{p-1} \equiv 1 \bmod p^s\}$. В частности, это множество является группой по умножению.

8. Мы хотим доказать, что когда $-1 \equiv \square \bmod n$ и у n есть по крайней мере два различных простых делителя, то лжесвидетели Милера–Рабина n сохраняются при умножении. Пусть p простой делитель n; запишем $n = p^s m$, где m не делится на p ($m > 1$, т.к. n не степень простого).

   а) Пусть $a \equiv -1 \bmod p^s$ и $a \equiv 1 \bmod m$ (такое a есть по китайской теореме об остатках). Докажите, что a является свидетелем Миллера–Рабина n.

   б) Пусть $b^2 \equiv -1 \bmod n$. Определите c (в силу китайской теоремы об остатках) условиями $c \equiv b \bmod p^s$ и $c \equiv -b \bmod m$. Докажите, что b и c свидетели Миллера–Рабина n и $bc \equiv a \bmod n$.

   в) Возникает ли в этом построении пример $n = 65$, $b = 8$, $c = 47$ из 4-го упражнения? (Ответ: да, а для какого p?)

   (Подсказка для пункта а: Из того, что $-1 \equiv \square \bmod n$ выведите, что $n \equiv 1 \bmod 4$. Поэтому в представлении $n - 1 = 2^e k$ обязательно $e \geq 2$.)