Тексты на диске O: Legendre Symbol, Jacobi Symbol.

1. В тексте Legendre Symbol доказано, что если существует бесконечно много пар простых $p$ и $2p-1$, то плотность свидетелей Ферма соответствующих чисел $p(2p-1)$ стремится к $1/2$ при $p \to \infty$. Докажите, что если для фиксированного целого $c \geq 2$ существует бесконечно много пар простых $p$ и $cp-(c-1)$, то плотность свидетелей Ферма соответствующих чисел $p(cp-(c-1))$ стремится к $1-1/c$ при $p \to \infty$. Используйте то, что при $q$ простом и $c \mid (q-1)$, существуют $(q-1)/c$ ненулевых $c$-ых степеней $a \bmod q$, характеризующиеся условием $a^{(q-1)/c} \equiv 1 \bmod q$.

2. а) Вычислите символы Лежандра $(\frac{15}{71})$, $(\frac{30}{97})$ и $(\frac{43}{101})$, используя квадратичный закон взаимности и разложение числителя на простые. (Ответы: 1, $-1$, 1)

   б) Перечислите символы Лежандра предыдущей части, используя квадратичный закон взаимности символа Якоби, не разлагая число на простые множители, кроме степеней двойки.

   в) Вычислите еще символы Якоби, не разлагая число на простые множители, кроме степеней двойки: $(\frac{53}{93})$, $(\frac{65}{119})$, $(\frac{1001}{2015})$. (Ответы: 1, $-1$, 0)

3. Если $n > 1$ нечетное и не квадрат, то докажите, что $(\frac{a}{n}) = -1$ для некоторого $a \in \mathbf{Z}$. Выведите, что $(\frac{a}{n}) = 1$ и $(\frac{a}{n}) = -1$ одинаково часто, при $1 \leqslant a \leqslant n-1$ и $\text{НОД}\,(a,n) = 1$. (Подсказка: У $n$ есть простой делитель $p$ нечетной кратности. Используйте идеи из доказательства существования свидетелей Эйлера в случае, что $n$ свободно от квадратов.)

4. Докажите, что если $a$ является свидетелем Ферма целого $n$, то $a$ является также и свидетелем Эйлера $n$. (Подсказка: Легче доказать контрапозицию, что лжесвидетели Эйлера являются лжесвидетелями Ферма.)

5. Если нечетное число $n > 1$ удовлетворяет условию $(a,n) = 1 \Longrightarrow a^{(n-1)/2} \equiv 1 \bmod n$, то оно составное, так как $a^{(n-1)/2} \equiv -1 \bmod n$ для половины ненулевых вычетов $a$ по модулю $n$, когда $n$ простое. Ясно, что такое $n$ является числом Кармайкла специального типа. На самом деле говорят, что $n$ является *специальным числом Кармайкла*. Существует бесконечно много таких

чисел (это следует из доказательства теоремы, что существует бесконечно много чисел Кармайкла). Первые три примера специальных чисел Кармайкла 1729, 2465, и 15841.

а) Докажите следующее обобщение критерия Корсельта: $n$ специальное число Кармайкла тогда и только тогда, когда (i) $n$ свободно от квадратов и (ii) $p \mid n \Longrightarrow (p-1) \mid (n-1)/2$ для простых $p$.

б) Выведите с помощью упр. 3, что для каждого специального числа Кармайкла $n$ плотность его свидетелей Эйлера среди *обратимых по модулю* $n$

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

ровно $1/2$. (Подсказка: легче вычислить плотность дополнительного множества лжесвидетелей Эйлера среди обратимых по модулю $n$.)

в) Пусть $n := (6k+1)(12k+1)(18k+1)$, где все три сомножителя простые (первые примеры: $k = 1, 6, 35, 45$). По первому листку $n$ является числом Кармайкла. Докажите, что такое $n$ является специальным числом Кармайкла тогда и только тогда, когда $k$ нечетное.

Докажите, что плотность свидетелей Эйлера

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

стремится к $1/2$ при $k \to \infty$. Полагают, что есть бесконечно много таких $k$, но это еще не доказано. Если это верно, то $1/2$ является оптимальной оценкой снизу для плотности свидетелей Эйлера для *всех* нечетных составных $n$. (Подсказка: докажите, что плотность равна $1/2 + (11k+1)/(72k^2+22k+2)$.)