Критерий Люка простоты чисел Мерсенна

1. а) Докажите, что если p— простое число и $p \equiv \pm 1(\mod 8)$, то $2^{(p-1)/2} \equiv 1(\mathrm{mod} p)$.

б) Докажите, что если p— простое число и $p \equiv \pm 3(\mathrm{mod} 8)$, то $2^{(p-1)/2} \equiv -1(\mathrm{mod} p)$.

Указание. Пусть $z = (1+i)\sqrt{2}/2$. Тогда

$$(z+1/z)^p - (z^p + 1/z^p)$$

представимо в виде $p(A + B\sqrt{2})$, где A, B— целые числа.

2. а) Докажите, что если p— простое число и $p \equiv \pm 1(\mod 12)$, то $3^{(p-1)/2} \equiv 1(\mathrm{mod} p)$.

б) Докажите, что если p— простое число и $p \equiv \pm 5(\mod 12)$, то $3^{(p-1)/2} \equiv -1(\mathrm{mod} p)$.

Указание. Пусть $z = (1+\sqrt{3})/2$. Тогда

$$(z+1/z)^p - (z^p + 1/z^p)$$

представимо в виде $p(A + B\sqrt{3})$, где A, B— целые числа.

3. Обозначим $x_k = (2+\sqrt{3})^k + (2-\sqrt{3})^k$, $y_k = ((2+\sqrt{3})^k - (2-\sqrt{3})^k)/\sqrt{3}$. Докажите, что для любого целого k чсла x_k, y_k– целые.

В дальнейшем $p > 3$— простое число, $X = \{k : x_k \equiv 0(\mathrm{mod} p)\}$, $Y = \{k : y_k \equiv 0(\mathrm{mod} p)\}$.

4. а) Докажите, что если $z_1, z_2 \in X$, то $z_1 + z_2 \in Y$.

б) Докажите, что если $z_1, z_2 \in Y$, то $z_1 + z_2 \in Y$.

в) Докажите, что если $z_1 \in X, z_2 \in Y$, то $z_1 + z_2 \in X$.

5. Докажите, что $p+1 \in Y$ или $p-1 \in Y$.

6. а) Докажите, что если $X \neq \emptyset$ и z- минимальный положительный элемент множества X, то $X = \{(2k+1)z\}$, где k пробегает множество целых чисел.

б) Докажите, что если $X \neq \emptyset$ и z- минимальный положительный элемент множества X, то $z < p$.

7. Докажите, что если m— натуральное число и число $n = 2^m - 1$ является простым, то m— простое число.

В дальнейшем m— простое число, и мы будем проверять на простоту число $n = 2^m - 1$.

Построим последовательность Люка:

$$M_1 = 1, M_k = M_{k-1}^2 - 2.$$

Критерий Люка утверждает: число $n = 2^m - 1$ является простым тогда и только тогда, когда $M_{m-1} \equiv 0(\mathrm{mod} n)$.

8. Докажите, что $M_k = x_{2^{k-1}}$.

9. Докажите, что если n является простым, то $M_{m-1} \equiv 0(\mathrm{mod} n)$.

Указание. $2+\sqrt{3} = ((1+\sqrt{3})/\sqrt{2})^2$.

10. Докажите, что если $M_{m-1} \equiv 0(\mathrm{mod} n)$, то n является простым.