10.1. Докажите, что на каждом шаге расширенного алгоритма Евклида верно gcd(x, y) = 1.

Решение:

Будем брать алгоритм с лекции и каждый раз при выходе из рекурсии x, y будут пересчитываться следующим образом.

$$\begin{cases} y' = x - \lfloor a / b \rfloor y \\ x' = y \end{cases}$$

Заметим что, если gcd(x, y) = 1, то очевидно, что gcd(x’, y’) = 1 так как,

gcd(x, y) == gcd(x’, y’) == (y, x - ky)

И в итоге в конце рекурсии мы должны найти такие x и y, что ax + 0y = d и тут подходит только (1, y) тогда gcd(x, y) = 1

11.4. Покажите, что зная n и $\varphi(n)$ можно восстановить разложение $n = pq$.

$\varphi(n) = \varphi(pq) = \varphi(p) * \varphi(q)$ (Так как функция мультипликативная).

Так как p и q простые числа, то

$\varphi(n) = \varphi(p) * \varphi(q) = (p - 1) * (q - 1) = pq – p – q + 1 = n – p – q + 1$

$p + q = n - \varphi(n) + 1$

Зная сумму и произведение p и q, по теореме Виета мы можем найти корни уравнения, а именно уравнение вида

$x^2 + (n - \varphi(n) + 1) * x + n = 0$ будет иметь два корня p и q.