ולכן $\gcd(m-x,n)=p$ גם ב-4 נקבל $\gcd(m-x,n)=q$

אם נבלון על מקרה 1,2 אז הבלבול לפעמים. על מקרה 1 יש לבן
בהסתברות שווה ומאין הסתברות הפעמה בכל רגע של האלגוריתם
ויהי $\frac{1}{2}$. כל הלבן מוסברת ל" ובוודאי $m-n$. כל קבוצת
m תופסת רק מהמרתה ולכן מרחב ה-$m-n$ "הטובים" הוא
$\frac{1}{2}$.