Review

Friday, November 17, 2023 4:24 PM

HW3 Ex. 6.5.7

Exercise 6.5.7 Use the fact that the period of $f_{7,247}$ is 12 to determine the factors of 247. $f(x) = 7^x \pmod{247} \Longrightarrow r = 12$ ■

$\text{GCD}((a^{\frac{r}{2}}+1), N)$ and $\text{GCD}((a^{\frac{r}{2}}-1), N)$

$\gcd(7^{12/2}+1, 247)$

$= \gcd(117650, 247)$

$\equiv 13$

$\gcd(117649-1, 247)$

$= 19$

$7^6+1 \mod 247$

$\equiv 78 \pmod{247}$

$247 = 3 \cdot 78 + 13$

$78 = \quad \cdot 13 + 0$

$12X \quad \frac{13}{2}$

Exer 6.5.5

$n = 8, \quad m = 16$

Exer 9.2.2

50% of the matched bases

$\Longrightarrow$ 25% of n.