



SOLUTION OF EXERCISESHEET 2

Exercise 2-1

Test

Exercise 2-2

Exercise 2-3

f and g are negligible functions and g be a positive polynomial.

- (a) Is e^{-x} negligible? For any polynomial x^c , choose N=c, then for all x>N holds: $e^{-x}<\frac{1}{x^c}$, because $e^x>x^c$ for all x>N=c. $\Rightarrow e^{-x}$ is negligible.
- (b) Is $\frac{1}{x^{2021}}+1$ negligible? For the polynomial x^{2022} there is no N, that for all x>N holds: $\frac{1}{x^{2021}}+1<\frac{1}{x^{2022}}$, because x^{2021} is always smaller than x^{2022} . $\Rightarrow \frac{1}{x^{2021}}+1$ is not negligible.
- (c) Is h(x) negligible, when h(x) is a positive function such that h(x) < f(x) for all x? For f(x) holds: $f(x) < \frac{1}{p(x)}$ (Definition 0.1). Because of $h(x) < f(x) < \frac{1}{p(x)}$ for all x, h(x) is also negligible.
- (d) Is f(x)+g(x) negligible? f(x) negligible $\Rightarrow f(x)<\frac{1}{p(x)}$ (Definition 0.1). g(x) negligible $\Rightarrow g(x)<\frac{1}{p'(x)}$ (Definition 0.1).

$$\Rightarrow f(x) + g(x) < \frac{1}{p(x)} + \frac{1}{p'(x)}$$

$$= \frac{p'(x) + p(x)}{p(x) \cdot p'(x)}$$

$$= \frac{1}{\frac{p(x) \cdot p'(x)}{p'(x) + p(x)}}$$

Addition, multiplication and division of two polynomials results in another polynomial. Because of that the denominator $(\frac{p(x)\cdot p'(x)}{p'(x)+p(x)})$ can also be any polynomial. $\Rightarrow f(x)+q(x)$ is negligible.

- (e)
- (f)
- (g)

Introduction to Modern Cryptography Theresa, Celine, Prisca, Saibaba

October 26, 2022





SOLUTION OF EXERCISESHEET 2

(h)

(i)

Exercise 2-4

Exercise 2-5