

$$|GF(2^n)| = 2^n$$

n-bit strings

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 1 \\ \hline 2^4 \end{pmatrix} \sim x^4 + x^3 + x + 1$$

\emptyset

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 1 \\ \hline 2^7 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & 1 & 0 & 1 \\ \hline 5 \end{pmatrix}$$

$$(x^4 + x^3 + x + 1) \cdot (x^2 + 1) \pmod{p(x)}$$

$$= 155$$



irreducible polynomial of degree 5

$$a \in GF(2^n)$$

order of $GF(2^n)$

$$a^e \text{ in } GF(2^n)$$

$$\underbrace{f_1(x) \cdot f_2(x) \cdot \dots \cdot f_n(x)}_e \quad \emptyset$$

$$a^{e/n} \pmod{n} \equiv 1 \quad \text{iff } \gcd(a, n) = 1$$

$$a^{p-1} \pmod{p} \equiv 1$$

$$(a^e)^d \equiv a^{e \cdot d} \pmod{p-1} \equiv a^1 \pmod{p}$$

order of multiplication

group of \mathbb{F}_p with

p prime is $(p-1)$

$$(1)^e = 1$$

$$(-1)^e = 2$$

$$\text{order}(\mathbb{F}_p) = p-1 \Rightarrow \text{th } \mathbb{F}_p \quad a^{p-1} \equiv 1 \pmod{p}$$

$$a \equiv a^{(e \pmod{p-1})} \pmod{p}$$

$$d = e^{-1} \pmod{p-1}$$

1 1 k... . 1 1

$$d = e \pmod{p-1}$$

$$\text{order}(F_p) = p-1 \Rightarrow \forall a \in F_p \ a^{p-1} \equiv 1 \pmod{p}$$

by Lagrange's theorem order of multiplicative group of $GF(2^n) = 2^n - 1$

$$a \in GF(2^n) \quad \boxed{a^{2^n-1} \equiv 1 \quad (\text{in } GF(2^n))}$$

$$\gcd(e_A, 2^n-1) = 1$$

$$\exists d_A \text{ st. } d_A = e_A^{-1} \pmod{2^n-1}$$

Randomized factoring algorithm

$$\sqrt{n}$$

$A(n) \sim$ chooses a random number $\{2, \dots, \lfloor \sqrt{n} \rfloor\}$ (assume $n = p \cdot q$)

$$\Pr(A(n) \text{ giving a factor}) = \frac{1}{\sqrt{n}} \quad \forall n$$

A' has a table T of factors for all numbers $n \leq 100$

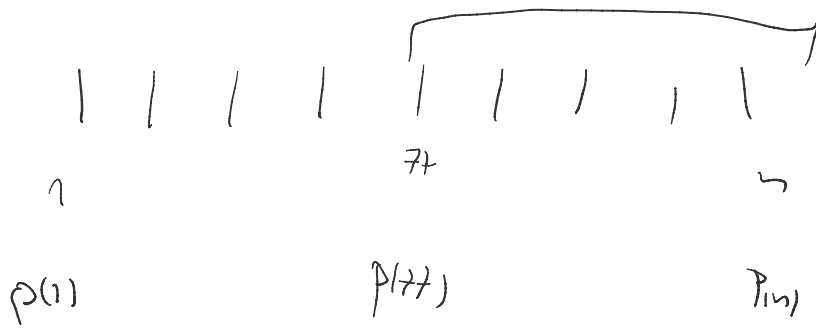
$A'(n) =$ if $n \leq 100$ look up table T and return an answer

otherwise call $A(n)$

$\Pr(A'(n) \text{ giving a correct answer}) \Rightarrow$ depends on n

for each c (here $c = 1/2$) $\exists n_c$ (here $n_c = 100$)

$$\forall n > n_c \quad \Pr(\text{correct answer}) \leq \frac{1}{nc}$$



$$P(X \geq 77) = \sum_{i=77}^n p(i)$$

$$P(X = 77) = p(77)$$

$$P(X \geq 77) - P(X = 77) = \sum_{i=77}^n (p(i) - p(77))$$

$$= \sum_{i=78}^n p(i) = P(X \geq 78)$$