21.1.2011

Kapitel 5

Der polynomiale Primzahltest v.a. ....

$Prim := \{ n \in \mathbb{N} \mid n \text{ prim} \} \in P$

$\vdots$

polynomiale Komplexitätsklasse

n in $poly(\log_2(n))$ Schritten bearbeitbar, ⊛ $((\log_2(n))^{11})$

$n \in Prim$? danach richtig beantworten $n = 2^{\log_2(n)}$

Lemma 5.1. $a \in \mathbb{Z}$, $n \in \mathbb{N}$, $n \geq 2$, $(a, n) = 1$. Dann

ist n prim gdw

$$(X + a)^n = \sum_{i=0}^{n} \binom{n}{i} X^i \cdot a^{n-i} = X^n + a \pmod{n}$$

$\vdots$

$0, 1, \ldots, n-1$

$a^n = a \pmod{n}$

$a^{n-1} = 1 \pmod{n}$

$q \ldots \quad (\log_2(n))^5$ $h(X)$

$$\sum_{i=1}^{n-1} \binom{n}{i} X^i a^{n-i} = 0 \mod n \quad \text{gdw } n \text{ prim.}$$

"$\Leftarrow$" n prim. $\binom{n}{i} = \frac{n!}{(n-i)\,i!} = \frac{1 \cdot \ldots \cdot p}{(1 \cdot \ldots \cdot (p-i))(1 \cdot \ldots \cdot i)}$

$p \mid \binom{p}{i}$ für p prim.

$\binom{n}{i} = 0 \mod n$

"$\Rightarrow$" n sei nicht prim. $n = q^k \cdot n'$. q prim

$q^k \| n$, d. h. $q^k \mid n$ und $q^{k+1} \nmid n$.

$$n = \prod_{i=0}^{r} q_i^{k_i} \qquad q_i \neq q_j$$

Für $q_i = q$ ist $k_i = k$

Koeffizient von X^q $\underbrace{\binom{n}{q} \cdot a^{n-q}}_{\not\equiv 0 \mod p}$.

$$\binom{n}{q} = \frac{(n' \cdot q^k)!}{(n' \cdot q^k - q)! \cdot q!}$$

Beh: Es gibt $a_k \in \mathbb{N}$

$$q^{(a_k)} \parallel (n' \cdot q^k)!$$

$$q^{a_k - k + 1} \parallel (n' \cdot q^k - q)!\, q!$$

$1 \cdot 2 \cdot \ldots \cdot 3 \cdot \ldots \cdot q$

$$(n' \cdot q^k)! = 1 \cdot \ldots \cdot \underbrace{(n' \cdot q^k - q + 1)\,(n' \cdot q^k - q + 2) \ldots \cdot n' \cdot q^k}_{\text{die letzten } q \text{ Faktoren}}$$

$a_1 = 1 n'$ $\qquad n' \cdot q$

$a_{k+1} = (q \cdot a_k + 1)\, n'$

$q^k!$

$q^{k+1}! = \overbrace{q^k \cdot (q^k + 1) \ldots \cdot (q^k + q^k)}^{q} (\quad)(\quad)$ ①

$$q^{a_k - (a_k - k + 1)} \parallel \binom{n}{q}$$

$$q^{k-1} \parallel \binom{n}{q}$$

$$q^{k} \nmid \binom{n}{q}$$

$$\vdots$$

$$n \nmid \binom{n}{q}$$

$$\binom{n}{q} \not\equiv 0 \pmod{q^k}.$$

$$a^{n-q} \not\equiv 0 \pmod{q^{**}}, \text{ da } \begin{matrix}(a, q) = 1 \\ (a, n) = 1\end{matrix}$$

$$\binom{n}{q} \cdot a^{n-q} \not\equiv 0 \pmod{q^k} \qquad \binom{n}{q} \cdot a^{n-q} \not\equiv 0 \pmod{n}$$

⊟

Sei p prim.

$\mathbb{F}_p = \left(\{0, 1, \dots, p-1\}, +_{\bmod p}, \cdot_{\bmod p}, 0, 1 \right) \models$ Körperaxiome

~~$x \cdot y = 0$~~

$h(X)$ sei ein irreduzibles Polynom vom Grad d über $\mathbb{F}_p$.

$$\underbrace{a_0 X^0 + \dots + a_d X^d}_{\in \mathbb{F}_p \quad \in \mathbb{F}_p} = h(X) \neq g(X) \cdot k(X)$$

$d+1$ Koeff.

Für jeden Koeff p Möglichk. $\Rightarrow p^{d+1}$

$\mathbb{F}_p[X]$ = Ring der Polynome über $\mathbb{F}_p$

~~$a X^{-n}$~~

$\mathbb{F}_p[X]/(h(X))$ = Restklassenkp. mit p^d Elemente.

q $f(X) = g(X) \cdot h(X) + r(X)$

$f(X) \equiv g(X) \pmod{p, h(X)}$

$\operatorname{grad} \leq d$ $\qquad X^r - 1$

$a_i \in \mathbb{F}_p$

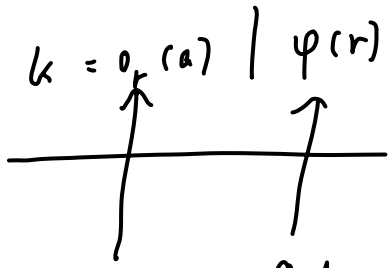
Def 5.2 Für $r \in \mathbb{N}$ und $a \in \mathbb{Z}$ mit $(a, r) = 1$

sei $o_r(a)$, die Ordnung von a modulo r, die kleinste

Zahl k o.d $a^k \equiv 1 \mod r$. ~~$a^{r-1} \equiv 1 \mod r$~~.

$\varphi(r)$ = Eulerzahl von r = $\#\{s \mid s < r, (s, r) = 1\}$ $\qquad a^{\varphi(r)} \equiv 1 \mod r$

(*) $k = \mathrm{ord}_r(a) \mid \varphi(r)$.



Ordnung der multiplikativen Gruppe $G = (\{s \mid s < r,\ (s,r)=1\}, \cdot)$

Ordnung von a

$\#G = \varphi(r) = r-1$ für r prim

$\{1, a, a^2, \ldots, a^{k-1}\}$ die von a in G erzeugte Untergruppe

Lemma 5.3. Sei $\mathrm{lcm}(m) = \mathrm{kleinstes\ gemeinsames\ Vielfaches}$ $\{1, \ldots, m\} = \min\{z \mid i \mid z \text{ für } i = 1, \ldots, m\} \leq m!$

$\Leftarrow$

$\mathrm{lcm}(m) \geq 2^{m-1}$ für $m \geq 9$.

Beweis: $m \leq n$, $\in \mathbb{N}$

$$(1-x)^{n-m} = \sum_{r=0}^{n-m} \binom{n-m}{r} \underbrace{1^{n-m-r}}_{1} \cdot (-x)^r$$

Für $m < n$

$$I(m,n) = \int_0^1 x^{m-1} (1-x)^{n-m} \, dx$$

$$= \int_0^1 x^{m-1} \sum_{r=0}^{n-m} \binom{n-m}{r} (-x)^r \, dx = \sum_{r=0}^{n-m} \binom{n-m}{r} \frac{1}{\underbrace{m+r}_{\leq n}} (-1)^r$$

Beobachtung: Alle Nenner in der Summe sind $\leq n$.

$I(m,n) \cdot \operatorname{lcm}(n) \in \mathbb{Z}$.

↑ Summe von Brüchen ↑ ~~kleinstes~~ Vielfaches gides Nenners des Bruches

$I(m,n)$ soll auf andere Weise ausgerechnet werden.

$$\left(\frac{x^m}{m}(1-x)^{n-m}\right)'$$

$$= \underbrace{x^{m-1}(1-x)^{n-m}}_{\cdots} - \frac{x^m}{m}(n-m)(1-x)^{n-m-1}$$

$$\left(\frac{x^{m+1}}{m(m+1)}(n-m)(1-x)^{n-m-1}\right)'$$

$$= \frac{x^m}{m}(n-m)(1-x)^{n-m-1} - \frac{x^{m+1}}{m(m+1)}(n-m)(n-m-1)(1-x)^{n-m-2}$$

$$\vdots$$

$n-m$

$$\left(\frac{x^n}{m(m+1)\cdots n-1}(n-m)(n-m-1)\cdots 2\,(1-x)^1\right)' = \frac{x^{n-1}}{\cdots(n-2)}(n-\cdots) - \frac{x^{n-1}}{m\cdots(n-1)}(n-m)\cdots 1\,x^{n-m-(n-m)}$$

$$\int \Sigma = \Sigma = \int \Sigma = I(n,m) - \int \frac{x^{n-1}(n-m)\cdots\cdot 1}{m\cdots\cdot(n-1)}$$

Also

$$\binom{n}{m} = \frac{m!\,(n-m)!}{m\;n!}$$

$$= \frac{1}{m\binom{n}{m}}$$