∈∧∨⇔⇒¬∀∃≡ pro tisknutí jako tahák je vhodnej font-size:4

- **Syn. Strom:** list je st. prom, nebo FS arity 0, nebo PS arity 0, je správně uzávorkováno, a algoritmus proběhl správně (zachována arita PS...)
- **Formule** je sentence iff **všechny** výskyty st. prom. vázané („výskyt x je vázaný, pokud cestou ke kořeni narazíme alespoň na jeden kvant. ∃x, nebo ∀x")
- **Jazyk PL:** Pred:={P} (ar.=2), Var:={x,y}, Const:={z}, Func:={f}
- **Interpretace:** U=N; [P]={(x,y); x+y∈ U}, [a]=2 („Predikát: součet x+y je taky N")
- **Res. Alg.: φ |=| tt** iff M∨{¬φ}nespl: Převedu na klausální tvar a utvořím resolventy:

1. Přejmenuju prom., aby každý kvantif. vázal jinou prom. (α-konverse, fresh proměnné)
2. a⇒b = ¬a∨b = ¬(a∧¬b); a⇔b = (¬a∨b)∧(a∨¬b); **3.** ¬∃xa=∀x¬a; **4.** ∨ dostanu co nejníž a∨(b∧c) = (a∨b)∧(b∨c); a∨(∀xb) = ∀x(a∨b); ∀x(a∧b) = ∀xa∧∀xb; ∃x(a∨b) = ∃xa∨∃xb; **5.** když tam bude ∃x∀y, tak c:=x; když ∀x∃y, tak f(x):=y; když bude ∃xP(x), tak P(a) (c–Skol. konst; f-Skol. fce), tím se zbavím ∃x skolemizací; poté se zbavím ∀x generalizací
Když se nepodaří subst, tak φ není vždy splněna, když najdu P∧¬P, tak je φ vždy splněna (resolventa je to, co zbyde, když škrtnu P a ¬P : když { }, tak je to ff)

- **Rozšířený Eukleidův algoritmus:**

Vstup: přirozená čísla a, b, kde a ≥ b ≥ 0.
Výstup: d = gcd(a;b) a celá čísla α, β, splňující d = α a + β b.
Do řádky: a,b,n,z 1 0 0 1 (α1=(α1-n*α2)) terminuje na řádku kde se objeví z=0
Koeficienty α,β jsou o řádek vejš, než je z=0 (klasicky z=1)

- **Spočtěte zbytek po dělení čísla 13^{1854} patnácti: a^e v Z_m**„scuknu exp. a pak čtverce"

Podle Eulerovy věty platí: $a^{\varphi(m)} \equiv 1$ (mod m), právě když gcd(a, m) = 1
gcd(13;15) = 1, tozn. že ji můžeme použít
φ(15) = φ(3)φ(5) = 2·4 = 8 → $a^8 \equiv 1$ (mod m) pro kaž. m nesoudě. s a
$13^{1854} = 13^{1151 \cdot 8 + 6} = (13^8)^{1151} \cdot 13^6 \equiv 1^{1151} 13^6 = 13^6$ (opakovaný čtverec)= $169^3 \equiv 4^3 \equiv 4$ (mod 15)

- **15x + 8y = 6**

Podle Bezoutovy rovnosti, gcd(a, b) = αa + βb
gcd(15,8) = 1 (= d); pokud d neděli pravou stranu, nemá řeš.
Takže existuje: 15a + 8b = 1
Koef. a a b najdeme pomocí rozšíř. Euklidova algoritmu (1; -2)
Abychom se dostali k původní rovnici:
15·(6a) + 8·(6b) = 6 //z toho je vidět x_p = 6a, y_p = 6b
To je jenom partikulární řešení, obecný najdem,
když prohodíme koef. pův. rovnice a jednomu dáme minus (-8; 15)t
Celkový řeš. je součet obecnýho a partikulárního řešení, takže:
(x; y) = (1; -2) + (-8; 15)t

- **4x ≡ 6 (mod 14)**

gcd (4,14) = 2 (= **d**), 2 dělí 6 → 2 řešení
Podle Eulerovy věty platí: $a^{\varphi(m)} \equiv 1$ (mod m), právě když gcd(a, m) = 1
$a \cdot a^{\varphi(m)-1} \equiv 1$ (mod m) → $a \cdot a^{\varphi(m)-1} b \equiv b$ (mod m) → $x = a^{\varphi(m)-1} b$ (mod m)

$$x_\kappa = \frac{1}{d} a^{\varphi\left(\frac{m}{d}\right)-1} \cdot \frac{b}{d} \pmod{\frac{m}{d}}$$, tozn. $x_\kappa = 2^{\varphi(7)-1} \cdot 3 = 2^5 3 \equiv 4 \cdot 3 \equiv 5$

x = x_κ + k (m/d), tozn. 5 + 7k (mod 14)
x_1 = 5 + 14t, x_2 = 12 + 14t

- **Malá Fermatova věta:**

Ať p je prvočíslo. Potom pro libovolné celé číslo nesoudělné s p platí:
$a^{p-1} \equiv 1$ v Z_p

- **Eulerova funkce:** pro kladné přirozené číslo n je φ(n) počet všech čísel z množiny {0; 1; : : : ; n-1}, která jsou s n nesoudělná.

Poznámka: Je zřejmé, že φ(1) = 1. Dále víme, že pro prvočíslo p platí φ(p) = p - 1.
Některé další vlastnosti Eulerovy funkce z tohoto faktu okamžitě plynou:
1. Pro prvočíslo p a přirozené číslo n ≥ 1 platí
φ(pn) = $p^n - p^{n-1}$ = $p^n(1 - 1/p)$
2. Jsou-li m_1 a m_2 nesoudělná čísla, potom platí:
$\varphi(m_1 m_2) = \varphi(m_1)\varphi(m_2)$
3. Z předchozí úvahy plyne rovnost
$\varphi(p_1^{\alpha_1} \cdot p_1^{\alpha_2} \cdots p_k^{\alpha_k}) = p_1^{\alpha_1}(1-1/p_1) \cdot p_2^{\alpha_2}(1-1/p_2) \cdots p_k^{\alpha_k}(1-1/p_k)$

- **Eulerova věta:** Pokud gcd(a;m) = 1, potom platí $a^{\varphi(m)} = 1$ v Z_m
- **Inversní matice:** $A^{-1} = (\det A)^{-1} \cdot D^t$; D: $a_{ij} = (-1)^{ij} \cdot \det(A_{ij})$
- **ISBN:** $x_1 x_2 \ldots x_{10}$, kde $\sum_{i=1}^{10} i x_i = 0$ v Z_{11}
- **Protokol RSA**

Tvorba klíče: A,B se veř. dohodnou na N a mění zprávy z 0 < z < N
A si zvolí **různá** prvočísla p,q tak, aby n=pq > N (**n=modul);** spočte φ(n)=φ(p-1)φ(q-1)
V $Z_{\varphi(n)}$ zvolí invertibilní prvek **d (d=dešifrovací exp.)** a tajně spočte $e=d^{-1}$ v $Z_{\varphi(n)}$
(e=šifrovací exp.) → veřejný klíč. (n,e) – slouží k zašifrování. soukromý klíč: (n,d) slouží k rozšifrování zprávy
Posílání zprávy: B posílá A: B si veme veřejný klíč Ačka a pošle **$x=z^e$ v Z_n**
Dešifrování zprávy: A přime zprávu x od B: a spočte **$z=x^d$ v Z_n**
- vždy se použije **alg. opakovaný čtverců**: 5=101→XSSX
- X=vynásobí se původním číslem a k exponentu se přičte jedna
- S=umocní se na druhou a exponent se zdvojnásobí

Útoky na RSA: Útok hrubou silou: E zachytí x=11 určenou pro A, zná Veřejný klíč A (n,e); postup: **1.** Hrubou silou fakt. n = p*q. **2.** Spočte φ(n)= φ(p)φ(q) **3.** spočte: e^{-1} v $Z_{\varphi(n)}$ a vyjde d. **4.** dešifruje x^d v Z_n (opak. čtverce, eulerova v.)
Útok outsidera při sdíleném n: E zachytí c1=694 (703,11) a c2=78 (703,7)
1. spočte gcd(11,7)=1 **2.** Bezoutem najde koef. a přepíše na: 7*3+1=11*2
3. zapíše $z^{7*3+1} = z^{11*2}$ v Z_{703} → $78^7 * z = 694^2$ v Z_{703} → 27*z=81 v Z_{703}
→ gcd(703,27)=1 ... jediné řeš: z=3. (když má řešení víc, tak z je dělitel n, čili jsme ho faktorizovali – postupujeme jako hrubou silou)
Útok při stejném exp.: E zachytí 86 (253,3); 9 (51,3); 40 (145,3) ze stejné zprávy z
1. Platí soustava rovnic: $x=z^3=86$ v Z_{253}; $x=z^3=9$ v Z_{51} $x=z^3=40$ v Z_{145} (pro nesoudělné n použije ČVOZ v $Z_{253*51*145}$: $x=86 \cdot 51 \cdot 145 \cdot (51 \cdot 145)^{-1} + 9 \cdot 253 \cdot 145 \cdot (\_)^{-1} + 40 \cdot 253 \cdot 51 \cdot (\_)^{-1}$)
2. vyjde x=3375 v $Z_{1870935}$ **3.** platí $3375=z^3$ <n1n2n3 **4.** takže z=$3375^{1/3}$ = 15
Útok „Alice je píča": známe **n** a **φ(n)**, faktorizujeme n: p*q=n, p+q=n-φ(n)+1, vyřešíme kvadratickou rovnici $q^2-(n-\varphi(n)+1)q+n=0$, $-b \pm (b^2-4ac)^{1/2}/2a$ – to vyhodí p;q

- **Grupy: Grupoid** – neprázdná množina M s operací *: M*M→M; **Pologrupa** – Grupoid <X,*> s asoc. *: (a*(b*c)=(a*b)*c) **∀a,b,c∈X**. **Monoid** – Pologrupa <X,*,e> s neutrálním prvkem e (Levý NP - n*e=n=e*n – Pravý NP) **Grupa** – Monoid <X,*,e,(-)^-1> s inversí vzhledem k definovanému „*" (a*a^-1=e= a^-1*a)

Centrum grupy - podgrupa, jejíž každý člen komutuje s libovolným členem grupy.
Důkaz komut: (a*b)*x=^{ASOC} a*(b*x)=^{KOMUT} a*(x*b)=^{AS} =(a*x)*b=^{KOM} =(x*a)*b=^{AS} =x*(a*b)
f: A→B je **PROSTÉ** iff ∀(x,y∈A)(x!=y)(f(x)!=f(y)) „různým prvkům různé obrazy"
f: A→B je **NA** iff ∀b∈B ∃a∈A; f(a)=b „zobrazí na **celou** cílovou množinu"
Skládání zobrazení: f°g: y=f(g(x)) – „to co je obraz z *f* je vzor pro *g*"

- **Důkaz malý Ferm.**: zobr. x→x·a je bijekce na invertibilních prvcích Z_p, což jsou {1,2,...p-1} proto {1a,2a...(p-1)a} = {1,2,...p-1}, proto součin musí být nutně stejný $a^{p-1} \cdot 1 \cdot 2 \cdot \ldots \cdot (p-1) = 1 \cdot 2 \cdot \ldots (p-1)$, čili **$a^{p-1} \equiv 1$ v Z_p**