FEJEZETEK A SZÁMELMÉLETBŐL ELŐADÁS

Waldhauser Tamás

SZTE Bolyai Intézet

2021. március 16.

pr. Zahl mod 13: $\{2, 6, 7, 11\} \to g$

$\sigma_{13^2}(g) = \varphi(13^2) = 156$ vgl. $\sigma_{13^2}(g) = 12$

$g=2$: $2^{12} \equiv 5 \cdot 8 = 40 \pmod{169}$

$2^9 = 512 = 3 \cdot 169 + 5 = 507 + 5 \equiv 5 \pmod{169}$

$\Rightarrow \sigma_{169}(2) \neq 12 \Rightarrow$ 2 pr. Wzl mod $13^2, 13^3, \ldots$

$\Rightarrow 2 + 13^\alpha$ pr. Wzl mod $2p^\alpha$.

$g=7$: $7^{12} \equiv 125 \cdot 5 \equiv -44 \cdot 5 \equiv -220 \equiv 118 \not\equiv 1 \pmod{169}$

$7^3 = 343 = 2 \cdot 169 + 5 \equiv 5 \pmod{169}$

$\Rightarrow 7$ pr Wzl mod $13, 13^2, \ldots, 13^\alpha \Rightarrow$ mod $2 \cdot 13^\alpha$

p pk. prím, g pr. gyök mod p

a $\square$-es maradék. $\Leftrightarrow$ ind a pk.

a pr. gyök mod p $\Leftrightarrow$ ind a $\perp \varphi(p) = p-1$

A $(p-1)$-hez rel. prímek száma pk. maradék.

Ez akkor teljesül, ha $p-1 = 2^q$.

$p = 2^q + 1$ Fermat-prímek

$p = 2^{2^n} + 1$

TITKOSÍRÁSOK

$T: \mathbb{Z}_m \to \mathbb{Z}_m$

$x \mapsto x+2$

$T^{-1}: \mathbb{Z}_m \to \mathbb{Z}_m$

$x \mapsto x-2$

- 1874 W. S. JEVONS:

$n = a^2 - b^2 = (a+b)\cdot(a-b)$

$b^2 + n = a^2$

Fermat-faktorizáció

> Can the reader say what two numbers multiplied together will produce the number 8,616,460,799? I think it unlikely that any one but myself will ever know; for they are two large prime numbers, and can only be rediscovered by trying in succession a long series of prime divisors until the right one be fallen upon. The work would probably occupy a good computer for many weeks, but it did not occupy me many minutes to multiply the two factors together. Similarly there is no direct process

1889 C. J. BUSE: $96079 \times 89681 = 8616460799$

$96079 = a+b$ $\quad 89681 = a-b$

- 1970 J. H. ELLIS
- 1973 C. COCKS: RSA
- 1974 M. J. WILLIAMSON: D-H kulcscsere
- 1976 W. DIFFIE, M. HELLMANN: D-H kulcscsere
- 1977 R. RIVEST, A. SHAMIR, L. ADLEMAN: RSA

DIFFIE-HELLMANN-KULCSVÁLTÁS

$p = 13$, $g = 2$

A $a = 7$ $\quad g^a \equiv 11 \pmod{13}$ $\quad g^{ba} \equiv 6^a \equiv ? \pmod{13}$

B $b = 5$ $\quad g^b \equiv 6 \pmod{13}$ $\quad g^{ab} \equiv 11^b \equiv ? \pmod{13}$

RSA p, q prímek, $m = p \cdot q$

e nyilvános kitevő

$T: \mathbb{Z}_m \to \mathbb{Z}_m, x \mapsto x^e$

$T^{-1}: \mathbb{Z}_m \to \mathbb{Z}_m, x \mapsto \sqrt[e]{x} = x^{1/e} = x^{e^{-1}}$ ($e^{-1} = d$ titkos kitevő)

$ed \equiv 1 \pmod{m}$

TEZA p, q prim, $m = pq$, $ed \equiv 1 \pmod{\varphi(m)}$ cu φ Euler

$T: \mathbb{Z}_m \to \mathbb{Z}_m, x \mapsto x^e$ iune $T^{-1}: \mathbb{Z}_m \to \mathbb{Z}_m, x \mapsto x^d$.

Bij. $\forall a \in \mathbb{Z}: a^{ed} \overset{?}{\equiv} a \pmod{m}$. $\quad \varphi(p) \quad \varphi(q)$

Tocmai, $ed = 1 + k \cdot \varphi(m) = 1 + k \cdot (p-1) \cdot (q-1)$

1) HA $a \perp m$: $a^{ed} = a^{1+k\cdot\varphi(m)} \equiv a^1 \cdot \underbrace{\left(a^{\varphi(m)}\right)^k}_{\equiv 1 \text{ Euler}} \equiv a^1 \cdot 1^k \equiv a \pmod{m}$ ✓

$\equiv 1$

2) HA $p \mid a$, de ex. $a \perp q$: $\quad a \perp q \Rightarrow a^{ed} \equiv a^{1+k\cdot\varphi(p)(q-1)} \equiv a^1 \cdot \underbrace{\left(a^{\varphi(q)}\right)^{k\cdot\varphi(p)}}_{\equiv 1 \text{ Euler}} \equiv a \pmod{q}$

$\equiv 1$

$a \equiv 0 \pmod{p} \Rightarrow a^{ed} \equiv$ $\Big\} \Rightarrow \equiv a \pmod{p}$

$\Rightarrow a^{ed} \equiv a \pmod{pq}$. ✓

3)... 4)... ∎

$(\omega_A, e_A \rightsquigarrow T_A)$ $(\omega_B, e_B \rightsquigarrow T_B)$

$T_A(\ddot{u})$

$T_A(T_B^{-1}(\ddot{u}))$

A B

$\ddot{u}$

$p_A \cdot q_A = \omega_A$

$e_A d_A \equiv 1 \pmod{\varphi(\omega_A)}$

$(p_A - 1)(q_A - 1)$

Ell. alg. ✓

$p_B \cdot q_B = \omega_B$

$e_B d_B \equiv 1 \pmod{\varphi(\omega_B)}$

$(p_B - 1)(q_B - 1)$

$T_A : \mathbb{Z}_{\omega_A} \to \mathbb{Z}_{\omega_A}$

$x \mapsto x^{e_A}$

$T_A^{-1} : \mathbb{Z}_{\omega_A} \to \mathbb{Z}_{\omega_A}$

$x \mapsto x^{d_A}$

$T_B : \mathbb{Z}_{\omega_B} \to \mathbb{Z}_{\omega_B}$

$x \mapsto x^{e_B}$

$T_B^{-1} : x \mapsto x^{d_B}$

2002 PRIMESEP AKS

HF 13 Mikor a modulusból egyértelműen, hogy $ed \equiv 1 \pmod{\varphi(m)}$, akkor $\mathbb{Z}_m \to \mathbb{Z}_m$, $x \mapsto x^e$ és $\mathbb{Z}_m \to \mathbb{Z}_m$, $x \mapsto x^d$ egymás inverzei?

HF 14 $x^{275} \equiv 2 \pmod{4187}$

$p = \dots$, $q = \dots$ $\quad m = pq = 4187$

$e = 275$, $d = \dots$ $\quad ed \equiv 1 \pmod{\underbrace{\varphi(m)}_{(p-1)(q-1)}}$

$x \equiv 2^d \equiv \dots \pmod{4187}$

x 4 jegyű szám