Date: ۱۴۰۰/۸/۲۳ Subject: یادداشت کلاسی راستین احسانی ۹۷۵۲۱۰۱۸

* با داشتن بلوک‌های $n=30$ چگونه عملیات جایگشتی را انجام دهیم؟

اگر $r_1, r_2, \dots, r_{\varphi(n)}$ مجموع کاهش یافته‌ها

↳ جایگشت کامل $\rightarrow \{a r_1, a r_2, \dots, a r_{\varphi(n)}\}$

↳ اگر $(a,n)=1$

* اویلر ← ریاضی‌دان ـ فیزیک‌دان ← سوئیسی

↳ یکی از آثار ← پس از نابینا شدن

* چگونه تابع اویلر را حساب کنیم؟ ← اعداد اول ← $\varphi(p) = p-1$

↳ اگر $n = pq$ ← p, q عدد اول

↳ $\boxed{\varphi(n) = (p-1)(q-1)}$ ← چرا؟

* اثبات ← اول ← $(q-1)\times 1, (q-1)\times 2, \dots, (q-1)\times(p-1)$

شبیه n

$(p-1)\times 1, (p-1)\times 2, \dots, (p-1)(q-1)$

$n - (p-1) - (q-1) + 1 = pq - (p-1) - (q-1)$

■

Date: / / Subject:

* اگر $n = p_1^{e_1} p_2^{e_2} \dots p_t^{e_t}$ ← n را به فاکتورهای اول تجزیه کنیم

$$\varphi(n) = \prod_{i=1}^{T} p_i^{e_i - 1} (p_i - 1)$$

* مثال

$n = 72 = 2^3 \times 3^2$

$\varphi(72) = 2^2 \times (2-1) \times 2^1 \times (3-1) = \boxed{24}$

* معکوس در هنگ n ← $ax \equiv 1 \pmod n$

اگر $(a,n) = 1$ ← معادله جواب یکتا دارد

مثال ← معکوس عدد ۵ در هنگ ۷

$(5,7) = 1 \rightarrow ax \equiv 1 \pmod 7 \rightarrow 5x^3 \equiv 1 \pmod 7$

* قضیه اویلر - فرمت ← اگر n, a نسبت به هم اول باشند

$$a^{\varphi(n)} \equiv 1 \pmod n$$

* اگر p ← عدد اول $a^{p-1} \equiv 1 \pmod p$

Date: / / Subject:

* معادلات همنهشتی ← دو عدد a و n اول نسبت به یکدیگر

$ax \equiv b \rightarrow x = b a^{\varphi(n)-1} \pmod n$

← ما کمک می‌کند معکوس پیدا کنیم

* RSA ← ۱۹۷۷ — $n = pq$ → حاصل‌ضرب

e → Public key

d → Private " ⇝ $ed \equiv 1 \pmod{\varphi(n)}$

← معکوس یکدیگر

$e < \varphi(n)$
$(e, \varphi(n)) = 1$

* حلقه n, e را دارد

← نمی‌توانند تجزیه کنند ← مسئله NP

* کاربر با کلید عمومی ← رمز — $C = m^e \bmod n$

↳ ciphertext

گیرنده → $m = C^d \bmod n = (m^e)^d \bmod n$