קריטריון אוילר המוכלל

תומ"ס 12

<u>טענה</u>: אם עבור m יש ש"פ, $\gcd(a,m)=1$, אז a הוא שארית מחזקה n-ית $\Leftrightarrow$ $a^{\frac{\varphi(m)}{d}}\equiv 1(m)$ כאשר $d=\gcd(n,\varphi(m))$

<u>הוכחה</u>: יהי g ש"פ מודולו m, $a\equiv g^b(m)$. כותבים $x\equiv g^y(m)$, $x^n\equiv a(m)$ (*), $g^{ny}\equiv g^b(m)$ (#)

$ny\equiv b(\varphi(m))$ (**). שקולה (#) שקול ל- $g^{ny-b}\equiv 1(m)$. $\varphi(m)|ny-b$

כי $\operatorname{ord}(g)=\varphi(m)$. נגדיר $d=\gcd(n,\varphi(m))$.

ש- (**) קיים פתרון $\Leftrightarrow$ $d|b$.

$\boxed{\Rightarrow}$ אם $d|b$ אז $a^{\varphi(m)/d}\equiv g^{b\frac{\varphi(m)}{d}}=(g^{\varphi(m)})^{\frac{b}{d}}\equiv 1^{b/d}=1(m)$

$\boxed{\Leftarrow}$ אם $a^{\frac{\varphi(m)}{d}}\equiv 1(m)$ אז $g^{b\varphi(m)/d}\equiv 1(m)$ אבל $\operatorname{ord} g=\varphi(m)$ ולכן

$\varphi(m)|\frac{b\varphi(m)}{d}$ $\Leftarrow$ קיים $k\in\mathbb{Z}$ כך ש- $\frac{b\varphi(m)}{d}=k\varphi(m)$

$b=kd$

$d|b$

וכך הלאה $a^{\frac{\varphi(m)}{d}}\equiv 1(m)\Leftrightarrow d|b$ ☒

<u>מסקנה (קריטריון אוילר)</u>: יהי p ראשוני אי זוגי, $a\in\mathbb{Z}$, $\gcd(a,p)=1$

אז הקונג' $x^2\equiv a(p)$ ניתנת לפתרון $\Leftrightarrow$ $a^{\frac{p-1}{2}}\equiv 1(p)$

<u>הוכחה</u>: $\varphi(p)=p-1$. $d=\gcd(2,\varphi(p))=2$ $\Leftarrow$ $\varphi(p)/d=\frac{p-1}{2}$

התנאי הוא ש- $a^{\frac{p-1}{2}}\equiv 1(p)$. ולכן זה נובע ישירות מהקריטריון המוכלל.

<u>הוכחה ישירה של קריטריון אוילר</u>: $\Leftarrow$ אם $a\equiv b^2(p)$ אז $a^{\frac{p-1}{2}}\equiv b^{2\frac{p-1}{2}}=b^{p-1}\equiv 1(p)$ ✓

ראינו: אם a שארית ריבועית מודולו p אז $a^{\frac{p-1}{2}}\equiv 1(p)$

אם a אי-שארית (לא סתם) ריבועית מודולו p כותבים $a\equiv g^\gamma(p)$ כאשר

g ש"פ עבור p. אם γ זוגי אז a ריבועית. אבל a אי-ריבועית לכן γ אי זוגי, $\gamma=2\beta+1$ ואז:

$a^{\frac{p-1}{2}}\equiv(g^{2\beta+1})^{\frac{p-1}{2}}=(g^{p-1})^{\beta}\cdot g^{\frac{p-1}{2}}\equiv g^{\frac{p-1}{2}}\not\equiv 1(p)$

כי g הוא ש"פ וזו סתירה! ☒

<u>טענה</u>: יהי p ראשוני אי זוגי, $\ell\in\mathbb{Z}$, $\ell\geq 1$, $a\in\mathbb{Z}$, $p\nmid a$. אז הקונג'

$x^2\equiv a(p^\ell)$ (1) ניתנת לפתרון $\Leftrightarrow$ $x^2\equiv a(p)$ (2) ניתנת לפתרון

<u>הוכחה</u>: כל פתרון של (1) הוא גם פתרון של (2).

הפוך, נניח שיש פתרון של (2): $a\equiv b^2(p)$, $b\in\mathbb{Z}$. יהי g ש"פ מודולו p^ℓ,

הוכחנו ש״ע עבור p כותבים $a\equiv g^m (p^e)$.

מכיוון ו-a ריבוע מודולו p: $\exists b\ s.t\ a\equiv b^2(p)$

$b\equiv g^{m'}(p)$

$\Downarrow$

$g^m\equiv g^{2m'}(p)$

הסדר של g מודולו p הוא p-1. לכן $m\equiv 2m'\ (p-1)$

$m=2m'+k(p-1)$

p-1 זוגי לכן m זוגי, נסמן $m=2m''$

$a=g^{2m''}(p^e)$

מסקנה: יהי p ראשוני אי זוגי, $a\in\mathbb{Z}$, $p\nmid a$ אז הקונגר' $\overset{(1)}{x^2\equiv a(p^e)}$ ניתנת לפתרון $\Leftrightarrow$ $\underset{(2)}{a^{\frac{p-1}{2}}\equiv 1(p)}$

הוכחה: $(3)\ x^2\equiv a(p)$, $(1)\Leftrightarrow(3)\Leftrightarrow(2)$ ∎

② שאלה: $x^2\equiv a(2^e)$ ניתנת לפתרון? (a אי זוגי)

← $l=1$: 2 ⇐ כל a

← $l=2$: 4 ⇐ $a\equiv1(4)$

← $l\geq3$: אם $a\equiv b^2(2^e)$ אז $a\equiv b^2(8)$

טענה: אם $a\equiv1(8)$ אז הקונגר' $x^2\equiv a(2^e)$ ניתנת לפתרון עבור כל l.

הוכחה: אפשר להניח ש- $l\geq3$. לפי משפט שהוכחנו [illegible]! $a\equiv(-1)^u5^v(2^e)$,

כאשר $u=0,1$, $v\in\mathbb{Z}$. לכן $5\equiv1(4)$ $a\equiv(-1)^u1^v(4)$

אם $a\equiv1(8)$, לכן $a\equiv1(4)$. כמו קודם $(-1)^u\equiv1(4)$ ⇐ $u=0$.

אם v אי זוגי, $v=2k+1$ אז $a\equiv(5^2)^k\cdot5(2^e)$

לכן $a\equiv(5^2)^k\cdot5(8)$

אבל $5^2\equiv1(8)$

$a\equiv5(8)$ סתירה ($a\equiv1$)

לכן v זוגי, $v=2k$: $a\equiv5^v\equiv5^{2k}\equiv(5^k)^2(2^e)$ ⇐ a ריבוע מודולו 2^l

שאריות ריבועיות:

יהי $m\geq1$, $\gcd(a,m)=1$.

הגדרה: a הוא שארית ריבועית מודולו m אם הקונגר' $x^2\equiv a(m)$ ניתנת לפתרון.

דוגמה: 2 היא שארית ריבועית מודולו $\overset{7}{\cancel{m}}$. $3^2=7$. 3 אי שארית ריבועית מודולו 7.

המשך תומס 12:

טענה: יהי $m=2^e p_1^{e_1}\cdots p_t^{e_t}$ פירוק של m לראשוניים. אז התנאי

$x^2\equiv a(m)$ ניתנת לפתרון $\Leftrightarrow$ אם $e=2$ אז $a\equiv 1(4)$

אם $e\geq 3$ אז $a\equiv 1(8)$

עבור $i=1..t$: $a^{\frac{p_i-1}{2}}\equiv 1\,(p_i)$

הוכחה: לפי משפט השאריות הסיני הקונגרואנציה שלנו שקולה למערכת

$x^2\equiv a(2^e)$, $x^2\equiv a(p_i^{e_i})$ לכל $i=1,\dots,t$ $\leftarrow$ ואת זה הוכחנו.

2. p בדק ראשוני. איזה a הם שאריות ריבועיות מודולו p?

(נתון a. עבור איזה p הוא שארית ריבועית.)

⚠ מהיום זה ראשוני אי זוגי!

סימון לז'נדר: יהי p ראשוני. $a\in\mathbb{Z}$, a זר ל-p. נגדיר $\left(\frac{a}{p}\right)$ הוא

$+1$ אם a שארית ריבועית מודולו p, -1 אם לא.

דוגמאות: $\left(\frac{2}{7}\right)=1$, $\left(\frac{3}{7}\right)=-1$, $\left(\frac{14}{7}\right)$ לא מוגדר.

טענה: (א) $\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}}(p)$

(ב) $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

(ג) אם $a\equiv b(p)$, אז $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$

הוכחה: (ג) - ברור. ✓

(א) - נגדיר $b=a^{\frac{p-1}{2}}$. לפי פרמה $a^{p-1}\equiv 1(p)$, לכן $b^2\equiv 1(p)$ $\Leftarrow$ $\bar{b}=\bar{1}$ / $\bar{b}=-\bar{1}$

אם a ריבוע $a\equiv c^2(p)$ אז $a^{\frac{p-1}{2}}\equiv 1(p)$ לפי פרמה.

אם a לא שארית אז $a^{\frac{p-1}{2}}\not\equiv 1(p)$ לפי קריטריון אוילר. לכן $a^{\frac{p-1}{2}}\equiv -1(p)$

אם a ריבוע מודולו p אז $\left(\frac{a}{p}\right)=1$, $a^{p-1/2}\equiv 1(p)$ } בכל מקרה שווים ✓

אם a לא שארית p אז $\left(\frac{a}{p}\right)=-1$, $a^{\frac{p-1}{2}}\equiv -1(p)$