數播信箱

1. 薛昭雄、葉永南來函

數學傳播編輯委員:

前一陣子, 第一作者整理舊文找到一期數學傳播, 無意中翻到1997年6月第82期的一篇文章「質數三元數與同餘式組」, 作者爲羅春光教授及二位學生。他們的主要結果爲定理 3(p.68): 給定一任意整數 p, (a,b,c) 爲 (**) 的質數三元數解 iff $p \equiv (ab+bc+ca) (\mathrm{mod}\, abc)$, 其中 (**) 爲同餘式組

$$\begin{aligned} ab &\equiv p \,(\mathrm{mod}\, c) \\ bc &\equiv p \,(\mathrm{mod}\, a) \\ ca &\equiv p \,(\mathrm{mod}\, b) \end{aligned}$$

我們覺得此結果有誤。我們想也許我們 overlook, 否則這個結果"iff"是不成立的, 假使取 $a=3$, $b=4$, $c=5$, 則 $p=47$。(a,b,c) 滿足了 (**) 但他們不是質數三元數解, 事實上這個問題是解 (其實只要$(a,b,c)=1$, 任何解都成立)

$$\begin{cases} x \equiv ab \bmod c \\ x \equiv bc \bmod a \qquad (a,b,c)=1 \\ x \equiv ca \bmod b \end{cases}$$

它的解爲 $x \equiv ab+bc+ca \bmod abc$ 這個問題也可以推廣到一般性, 證明可見第一作者與二位教授合寫的文章: A fast algorithm of the Chinese remainder theorem and its app. to Fibonacci number. App. of Fibonacci Numbers, Proc. of the Fourth International conference on Fibonacci numbers and their App. 241-246, 1991, 這個文章收到 Handbook of Applied Cryptography by A. Menezes et al., CRC Press, Boca Raton, USA.

薛昭雄、葉永南 89.6.24

2. 羅春光回函

敬啓者:

有關本人以前的文章「質數三元數與同餘式組」之讀者來信, 原定理確是有一些漏洞。若我們先假設 a,b,c 皆爲互異質數, 則定理成立。故該文中定理3, 應改成:

定理3: 設 a,b,c 爲三個互異質數且 p 爲整數, 則 (a,b,c) 是 (**) 的質數三元數解若且唯若 $p \equiv ab+bc+ca (\mathrm{mod}\ abc)$。

很抱歉, 該文書寫上有疏漏, 也很感激二位先生指出錯誤, 並介紹相關文獻, 此致

數學傳播編輯部

羅春光 89.8.19