

ليكن لدينا نظام المعادلات

$$x = c_1 \pmod{m_1}$$

$$x = c_2 \pmod{m_2}$$

فاذا كان d هو القاسم المشترك الاكبر ل m_1 و m_2 وكان M هو المضاعف المشترك الاصغر ل m_1 و m_2 فبرهن ان

1. النظام السابق يملك حلا اذا فقط d يقسم المقدار $(c_1 - c_2)$
2. ان الحل يشكل صنف (Class) بترديد M في الواقع نحتاج الى برهان عدة نظريات قبل الوصول الى حل هذا السؤال

النظرية الاولى

اذا كان

$$a = b \pmod{m}$$

فان

$$ak = bk \pmod{mk}$$

البرهان

$$a = b \pmod{m} \Rightarrow m | (b - a) \Rightarrow km | k(b - a) \Rightarrow km | kb - ka \Rightarrow ka = kb \pmod{km}$$

وعكسها **النظرية الثانية**
اذا كان

$$ak = bk \pmod{mk}$$

فان

$$a = b \pmod{m}$$

البرهان

نتبع عكس الخطوات في البرهان السابق تماما

بالنظرية الثالثة

اذا كان

$$a = b \pmod{m}$$

فان مجموعة القواسم المشتركة ل a, m تساوي مجموعة القواسم المشتركة ل b, m
الاثبات
 $a = b \pmod{m} \Rightarrow a - b = mq \Rightarrow a - mq = b$

اذا فان اي قاسم مشترك ل a, m سيقسم العدد b وهو المطلوب اثباته

النظرية الرابعة

لنفرض اننا لدينا المعادلة او المقارنة

$$ax = b \pmod{m}$$

فاذا كان d القاسم المشترك الاكبر ل a, m وكان d لا يقسم b فان المعادلة السابقة لاتملك حلا

البرهان

لنفترض وجود حل x_0 لاحظ ان d يقسم a اذا d يقسم ax_0
فاذا كان d يقسم الطرف الايمن ويقسم m فلا بد انه يقسم b (حسب النظرية الثالثة) ولكن هذا يناقض الفرض
اذا وجود حل واحد ادى الى ظهور تناقض مما يعني نفي وجود الحل وهو المطلوب اثباته

ينتج من هذه النظرية انه لا نقوم بالبحث عن حلول المعادلة الا اذا كان $d|b$ كما يمكن تحويل المعادلة السابقة الى معادلة اخرى مكافئة لها حسب النظريات الاولى والثانية

$$a_1x = b_1 \pmod{m_1}$$

بحيث يكون

$$(a_1, m_1) = 1$$

وتقرا القاسم المشترك الاكبر لهما يساوي 1

اعتقد ان برهنة الجزء الاول من السؤال تم بشكل الي

$$x = a \pmod{m}$$

$$x = b \pmod{n}$$

نضع

$$x = tm + a \quad (2)$$

$$tm = b - a \pmod{n} \quad (3)$$

نفرض $(m, n) = d$

واضح من النظرية الرابعة ان هذه المعادلة قابلة للحل اذا وفقط اذا كان $d|(b-a)$

اذا نتسطيع تحويل المعادلة الاخيرة الى الشكل

$$m_1t = \alpha \pmod{n_1}$$

بقسمة الجميع على d

وواضح ان $(m_1, n_1) = 1$ كمان ان

$$m_1 = \frac{m}{d}; n_1 = \frac{n}{d}$$

اذا هذه المعادلة تملك حلا وحيدا

يمكن يكون بهذا الشكل

$$t = \beta + n_1y$$

وبتعويض هذه النتيجة في المعادلة (2)

$$x = m(\beta + n_1y) + a = m\beta + a + \frac{mn}{d}$$

هناك نظرية سنقبلها بدون برهان تقول

اذا كان $(a, m) = 1$ فان

$$ax = b \pmod{m}$$

تملك حلا وحيدا

هذا والله اعلم

