السؤال(١): إذا كان $a = 2378$ و $b = 1769$ فاستخدم خوارزمية إقليدس لإيجاد $x, y \in \mathbb{Z}$ بحيث $(a,b) = ax + by$.

الإجابة:

$$2378 = 1 \cdot 1769 + 609$$
$$1769 = 2 \cdot 609 + 551$$
$$609 = 1 \cdot 551 + 58$$
$$551 = 9 \cdot 58 + 29$$
$$58 = 2 \cdot 29 + 0$$

$$29 = 2378(-29) + 1769(39)$$

السؤال(٢): إذا كان $a \mid c$ و $b \mid c$ فأثبت أن $[a,b] \mid c$.

الإجابة: لنفرض أن $c = ax$ و $c = by$ حيث $x, y \in \mathbb{Z}$. لنفرض أن $r, s \in \mathbb{Z}$ بحيث

$$(a,b) = ar + bs$$

باستخدام $[a,b] = \frac{ab}{(a,b)}$، لدينا

$$\begin{aligned}\frac{c}{[a,b]} &= \frac{c(a,b)}{ab} = \frac{car + cbs}{ab} = \tfrac{c}{b} r + \tfrac{c}{a} s \\ &= yr + xs \in \mathbb{Z} \\ &\Rightarrow [a,b] \mid c\end{aligned}$$

السؤال(٣): أثبت أن $(a,b) = (a, b-a)$.

الإجابة: $(a,b) \mid a$ و $(a,b) \mid b \Leftarrow (a,b) \mid a - b$، أي (a,b) قاسم لـ a و$(a-b) \Leftarrow (a,b) \le (a, a-b)$ ①

مـن ناحيـة أخـرى، $(a, a-b) \mid a$ و $(a, a-b) \mid a - b \Leftarrow (a, a-b) \mid a - (a-b)$ أي $(a, a-b) \mid b$. والآن $(a, a-b)$ قاسم لـ a و $b \Leftarrow (a, a-b) \le (a,b)$ ②.

من ① و ② ينتج $(a,b) = (a, b-a)$.

السؤال(٤): إذا كان $(a,c) = 1$ فأثبت أن $(a,bc) = (a,b)$.

الإجابة: بما أن $(a,bc) \mid a$ و $(a,c) = 1$ فإن $((a,bc), c) = 1$ وحيث $(a,bc) \mid bc$ إذن $(a,bc) \mid b$. إذا كان x قاسما لـ a و b فإن $x \mid a$ و $x \mid bc \Leftarrow x \mid (a,bc)$. وهذا يبرهن أن العدد (a,bc) هو القاسم المشترك الأعظم لـ a و b، أي $(a,bc) = (a,b)$.

السؤال(٥): استخدم ما ورد في السؤالين (٣) و(٤) لإثبات أن

$(2^m - 1, 2^n - 1) = 2^{(m,n)} - 1$ حيث $m, n \in \mathbb{Z}^+$.

الإجابة: سوف نثبت أكثر من ذلك.

$(a^m - 1, a^n - 1) = a^{(m,n)} - 1$ حيث $a, m, n \in \mathbb{Z}^+$ و $a \neq 1$

نلاحظ أولا: إذا كان $k_1, k_2 \geq 1$ عددين صحيحين، فإن

$$a^{k_1 k_2} - 1 = \left(a^{k_1} - 1\right)\left(a^{k_2 \cdot k_1 - k_1} + a^{k_2 \cdot k_1 - k_1 - 1} + a^{k_2 \cdot k_1 - k_1 - 2} + \ldots + 1\right)$$

هذا يعني أن $a^{(m,n)} - 1$ يقسم كلا من $a^m - 1$ و $a^n - 1$ ، بالتالي $\underline{a^{(m,n)} - 1 \mid (a^m - 1, a^n - 1)}$

لنفرض أن $x, y \in \mathbb{Z}$ بحيث $mx + ny = (m,n)$. العددين x و y لابد أنهما مختلفين في الإشارة(إن كانا سالين أصبح (m,n) سالبا، وإن كانا موجبين أصبح $(m,n) \geq m + n$)، ولنفرض أن $x > 0$ و $y \leq 0$:

- ❖ $a^m - 1 \mid a^{mx} - 1 \Leftarrow (a^m - 1, a^n - 1) \mid a^{mx} - 1$
- ❖ $a^n - 1 \mid a^{-ny} - 1 \Leftarrow (a^m - 1, a^n - 1) \mid a^{-ny} - 1$

$$\Leftarrow (a^m - 1, a^n - 1) \mid a^{mx} - 1 - a^{(m,n)}\left(a^{-ny} - 1\right)$$

$$\Leftarrow \underline{(a^m - 1, a^n - 1) \mid a^{(m,n)} - 1}$$

السؤال(٦): جد جميع حلول المعادلة الديوفنتية: $189x + 180y + 175z = 15750$

الإجابة: بما أن $(189, 180, 175) = 1$ يقسم 15750 فإن لهذه المعادلة حلول ويمكن إيجادها بالتطبيق المباشر لطريقة أويلر: نبدأ بكتابة z بدلالة باقي الحدود

$$z = 90 - x - \tfrac{14}{175}x - y - \tfrac{1}{15}y$$

- ➢ ضع $w_1 = -\frac{14}{175}x - \frac{1}{15}y \Leftarrow 175w_1 + 14x + 5y = 0$ ثم نعبر عن y: $y = -35w_1 - 2x - \frac{4}{5}x$
- ➢ ضع $w_2 = -\frac{4}{5}x \Leftarrow 5w_2 + 4x = 0$ ثم نعبر عن x: $x = -w_2 - \frac{1}{4}w_2$
- ➢ ضع $w_3 = -\frac{1}{4}w_2 \Leftarrow 4w_3 + w_2 = 0$ ثم نعبر عن w_2: $w_2 = -4w_3$ ، لنحصل

$$\Leftarrow \quad \begin{aligned} x &= 5w_3 \\ y &= -35w_1 - 14w_3 \\ z &= 36w_1 + 9w_3 + 90 \end{aligned}$$

السؤال(٧): إذا كان كل من p و $p+2$ عددا أوليا حيث $p>3$ فأثبت أن 12 يقسم $2p+2$.

الإجابة: لأن p فردي $\Leftarrow 2 \mid p+1 \Leftarrow 4 \mid 2(p+1)$. حيث $(3,4)=1$ ، يكفي إثبات $3 \mid 2(p+1)$.

الآن، بين كل ثلاثة أعداد متتالية يوجد عدد يقبل القسمة على 3 (إذا لم تقسم الأول فالباقي إما $1 \Leftarrow$ تقسم الثالث، أو $2 \Leftarrow$ تقسم الثاني). لنعتبر المتتالية p، $p+1$، $p+2$:

لما كان $p>3$ أوليا فإن $3 \nmid p$ وكذلك $3 \nmid p+2$ وبالتالي فإن $3 \mid p+1 \Leftarrow 3 \mid 2(p+1)$.

السؤال(٨): أثبت أن الأعداد الأولية على الصورة $3k+2$ عددها غير منته.

الإجابة: (البرهان بالتناقض) افرض أن $A=\{p_1,p_2,\ldots,p_n\}$ تتكون من جميع الأعداد الأولية التي على الصورة $3k+2$. اعتبر $N=3p_1p_2\ldots p_n-1$. لاحظ أن N على صورة $3k+2$ وبالتالي فلابد أن أحد قواسم N الأولية على الصورة $3k+2$ (لو أن جميع قواسمه الأولية على الصورة $3k+1$ لكان على الصورة $3k+1$). إذن يوجد $p\in A$ بحيث $p \mid N$ ولكن $p \mid 3p_1p_2\ldots p_n \Leftarrow p \mid 3p_1p_2\ldots p_n - N$ أي $p \mid 1$ وهذا مستحيل.

السؤال(٩): أثبت أن $F_0 \cdot F_1 \cdot F_2 \cdot \cdots \cdot F_{n-1} = F_n - 2$ لكل $n \geq 1$.

السؤال(١٠): زعم فيرما أن العدد $N=(2m)^{2^n}+1$ أولي ما لم يقبل القسمة على أحد أعداد فيرما، فهل كان زعم فيرما صحيحا؟

الإجابة: باعتبار $m=6$ و $n=2$ ، نجد أن

$$(2m)^{2^n}+1=12^4+1=20737=89\cdot 233$$

عدد مؤلف وكل من 89 و 233 ليس عدد فرما .