بسم الله الرحمن الرحيم

* الأعداد الأولية:

- العدد الأولي: هو عدد أكبر من الواحد ولا يقبل القسمة إلا على نفسه والعدد واحد.

* خواص:

1- p عدد أولي فإن $p \in \mathbb{P}$

- $p \nmid n$ إذا كان $(p,n)=1$
- $p \mid n$ إذا كان $(p,n)=p$

2- p عدد أولي فإن $p \mid ab$ فإن p يقسم أحدهما على الأقل.

3- $p \mid a_1,a_2,\dots a_n$ فإن p يقسم أحد الأعداد a_i على الأقل.

4- $p_1, p_2, \dots, p_n$ أعداد أولية مختلفة وكان $p \mid p_1 . p_2 \dots p_n$ فإن p يساوي أحد هذه الأعداد الأولية.

* المبرهنة الأساسية في الحساب:

إذا كان $n>1$ عدد صحيح موجب فإنه يكون عدد موجب مؤلف يكتب على شكل جداء منتهٍ لعوامله الأولية أو إما أن يكون أولي وهذا التمثيل يكون وحيد.

الإثبات:

2 أولي، 3 أولي، $4=2\times 2$، 5 أولي $6=2.3$.

خطوة الاستقراء:

نفرض أن العدد n مؤلف ونفرض أنه من أجل $n \geq k$ محققة $k=p_1 p_2 \dots p_k$

وإذا كان k أولي تم المطلوب.

لنثبت أن $n=k+1$ محققة من أجلها

إذا كان $k+1$ أولي تم المطلوب

، $k+1$ مؤلف $\Leftarrow$ $k+1=a \times b$ أي $1<a \leq b<k+1$

فإن a,b يكتب كل منها على شكل جداء منتهٍ لعوامل أولية أي أن $k+1$ يكتب على جداء منتهٍ لعوامله الأولية.

لنثبت أن هذا الجداء لعوامله الأولية وحيد.

- إذا كان $n>1$ فإن n يكتب بالشكل القانوني: $n=p_1^{\alpha_1} \cdot p_2^{\alpha_2}, \dots, p_k^{\alpha_k}$

/ /

الموضوع: ....

حيث $p_1, p_2, \dots, p_k$ اعداد أولية مختلفة و α_i اعداد صحيحة موجبة $\alpha_i \geq 1$

أي $p_1 < p_2 < \dots < p_k$

*** نتيجة:**

① إذا كان $n > 1$ فإنّ n على الأقل عامل أولي أي يوجد عدد $p | n$.

② إذا كان $n > 1$ مؤلف فإنه عامل أولي p حيث $p \leq \sqrt{n}$ ،

الإثبات:

n عدد مؤلف أي $n = a b$ و $p | n$ ولنفرض أن $1 < a \leq b < n$

$p | a \Rightarrow p \leq a$

$n \geq a \Rightarrow n \geq a^2 \Rightarrow \sqrt{n} > a \Rightarrow \sqrt{n} \geq p$

*** نتيجة:**

إذا كان $n > 1$ ولم يكن عامل p أصغر من $\sqrt{n}$ فإنه عدد أولي.

*** مبرهنة:**

عدد الاعداد الأولية غير منتهٍ.

الإثبات: نفرض أنّ عدد الاعداد الأولية منتهٍ ولتكن $k \in \mathbb{N}$; $p_1, p_2, \dots, p_k$

نؤلف العدد التالي:

$$N = p_1 p_2 \cdots p_k + 1$$

لعامل أولي p و $p | N$ وسيكون احد الاعداد الأولية $p_1, p_2, \dots, p_k$ أي $p | N$ و $p | p_1 \cdots p_k$

$\Rightarrow p | N - p_1 \cdots p_k$ أي $p | 1$ وهذا يناقض الفرض الخاطئ وبالتالي عدد الأعداد الأولية غير منتهٍ:

*** صيغة اقليدس:** $N = p_1 \cdot p_2 \cdots p_k + 1$

تعطي أعداد أولية. $N_2 = 2 \cdot 3 + 1 = 7$ ، $N_1 = 2 + 1 = 3$ ، $N_3 = 2 \cdot 3 \cdot 5 + 1 = 31$

$N_4 = 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$ ، $N_6 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \times 509$

صيغة اقليدس تعطينا أعداداً أولية.

الصيغة التالية تعطينا أعداداً أولية $F(x) = x^2 - x + 41$ تعطينا أعداداً أولية من أجل

/ /   الموضوع: ....

$x = 0, 1, \ldots, 40$

- صيغة أخرى:

$F(n) = x^2 - 79x + 1601$ تعطينا اعداداً أولية من أجل $x = 0, 1, \ldots, 79$

العددان الأوليان الفرق بينهما (2) مثل (3, 2) يسمى التوأم

- العددان المتقابلان:

مجموع قواسم العدد الأول مساوياً نفسه مساوي العدد الثاني

* ديرطيه $(a, b) = 1 \Leftarrow ax + b$ تعطي اعداد أولية $a = 5 \quad b = 4$

$5(3) + 4 = 19$ تكون صحيحة عندما $x = 3$

$5(5) + 4 = 29$ $\quad x = 5$

$5(11) + 4 = 59$ $\quad x = 11$

* فيرما $F_n = 2^{2^n} + 1$

$n = 0 \Rightarrow F_0 = 3, \; F_1 = 5, \; F_2 = 17, \; F_3 = 257$

$F_4 = 2^{16} + 1 = 65537, \quad F_5 = 641 \times 6700417$

* غربلة ايراتوستين $x = 100$

نرمز لـ $\pi(x)$ بعدد الاعداد الأولية التي هي أقل من x

$\pi(x) \simeq \dfrac{x}{\log x}$

$$\lim_{x \to \infty} \frac{\pi(x)}{\dfrac{x}{\log(x)}} = 1$$

انتهت المحاضرة

Yehia D.