ⵜⴰⴳⵍⴷⵉⵜ ⵏ ⵍⵎⵖⵔⵉⴱ المملكة المغربية

أكاديمية الحسن الثاني للعلوم والتقنيات

وزارة التربية الوطنية والتكوين المهني

المباراة العامة للعلوم والتقنيات 2014

يوليوز 2014	الرياضيات	مدة الإنجاز: 4 ساعات

يشتمل موضوع مادة الرياضيات لهذه المباراة على مسألة تتكوّن من أربعة أجزاء مترابطة فيما بينها؛ ويمكن لأي مترشح، من أجل الإجابة على سؤال ما، أن يقبل نتائج الأسئلة السابقة ولو لم يُجِب عنها، وأن يستعمل هذه النتائج شريطة الإشارة بدقّة إلى أرقام الأسئلة المعنية.

وتجدر الإشارة إلى أنّ مدى حرص الترشح على اعتماد الوضوح والضبط في تقديم الأجوبة وتحريرها، ومدى التزامه بالدّقة في الاستدلال والبرهان تعتبر من العناصر المهمّة التي سيتمّ أخذها بعين الاعتبار أثناء القيام بعملية التصحيح. وفي هذا الاطار، يجب ضبط أرقام الأسئلة التي تم الإجابة عنها بكل دقّة.

لا يسمح باستعمال حاسوب أو آلة حاسبة أو لوحة إلكترونية.

إذا بدا لأحد المترشحين أثناء الاختبار على أنّ هناك خطأً ما في موضوع المباراة فَلْيُشِر إلى ذلك على ورقة تحريره وليواصل اختباره مبرزا أسباب المبادرات التي قد يقوم باتخاذها.

تـعــاريف ورموز

- لكل r و k من $\mathbb{N}$ حيث $k \leqslant r$، نرمز بـ $\binom{r}{k}$ للمعامل الحدّاني المعرّف بـ $\frac{r!}{k!(r-k)!} = \binom{r}{k}$.
- لكل p و q من $\mathbb{Z}^*$، نرمز للقاسم المشترك الأكبر للعددين p و q بـ $p \wedge q$.
- لكل عدد طبيعي غير منعدم n نرمز بـ $\varphi(n)$ لرئيسي المجموعة المكونة من الأعداد k المنتمية إلى المجموعة $\{1,\dots,n\}$ حيث n و k أوليان فيما بينهما :

$$\varphi(n) = \operatorname{card}\{k \in \{1,\dots,n\},\ \ k \wedge n = 1\}.$$

الدّالّة $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ تُسمَّى بالدّالة المُخبِرة لأُولِر[1] .

- لكل n من $\mathbb{N}^*$ ولكل k من $\mathbb{Z}$، نرمز لصنف العدد k بترديد n بـ $\bar{k}$، ونذكر أنّ

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{(n-1)}\}.$$

نرمز للحلقة $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ بـ $\mathbb{Z}_n$، ونذكر أنّ العمليتين $+$ و $\times$ معرّفتين بما يلي :

$$\bar{a} + \bar{b} = \overline{a+b}\ ;\ \ \bar{a} \times \bar{b} = \overline{ab},\ \ (a,b) \in \mathbb{Z}^2.$$

نضع

$$\mathbb{Z}_n^* = \{\bar{a} \in \mathbb{Z}_n\ ;\ \exists \bar{b} \in \mathbb{Z}_n,\ \ \bar{a} \times \bar{b} = \bar{1}\}$$

أو بمعنى آخر، $\mathbb{Z}_n^*$ هي مجموعة العناصر المنتمية إلى الحلقة $\mathbb{Z}_n$ والقابلة للقلب بالنسبة للقانون الداخلي $\times$.

[1] EULER, math. suisse (1707-1783)

الجــزء الأول

أسئــلة تمــهيدية حـول الدّالة المُخبِرة لأُولِر

1.1. أحسب $\varphi(1)$ و $\varphi(13)$ و $\varphi(20)$.

2.1. ليكن n من $\mathbb{N}\setminus\{0,1\}$. بيّن أنّ $\varphi(n)=n-1$ إذا وفقط إذا كان n عددا أوّليا.

3.1. ليكن p عددا أوّليا.

1.3.1. ليكن m و k عددين من $\mathbb{N}^*$. بيّن أنّ $m\wedge p^k\neq 1$ إذا وفقط إذا كان p يقسم العدد m.

2.3.1. استنتج أنّ $\varphi(p^n)=p^n-p^{n-1}$ لكل عدد n من $\mathbb{N}^*$.

نهدف في ما تبقى من هذا الجزء إلى تبيان بعض خاصّيات الدّالة المُخبِرة لأُولِر باستعمال حساب الاحتمالات.

نعتبر عددا صحيحا طبيعيا n يكون تفكيكه إلى جداء أعداد أوّلية على شكل $n=p_1^{\alpha_1}\dots p_r^{\alpha_r}$، بحيث $\alpha_1,\dots,\alpha_r$ أعداد صحيحة طبيعية غير منعدمة و $p_1,\dots,p_r$ أعداد أوّلية مختلفة مثنى مثنى، و$r\geq 2$.

يحتوي صندوق على n كرة مرقمة من 1 إلى n. نسحب عشوائيّا كرة من هذا الصندوق، ونفترض أنّه لا يمكن التميز بين هذه الكرات باللّمس.

4.1. لكل k من $\{1,\dots,r\}$، نعتبر الحدث A_k أسفله، ونرمز بـ $P(A_k)$ إلى احتمال هذا الحدث :
A_k : " سحب كرة تحمل رقما مضاعفا للعدد p_k ".

1.4.1. بيّن أنّ $P(A_k)=\frac{1}{p_k}$ لكل k من $\{1,\dots,r\}$.

2.4.1. بيّن أنّ لكل k من $\{2,\dots,r\}$ ولكل جزء $\{i_1,\dots,i_k\}$ من المجموعة $\{1,\dots,r\}$، لدينا
$P(A_{i_1}\cap\dots\cap A_{i_k})=P(A_{i_1})\dots P(A_{i_k})$.

3.4.1. لكل k من $\{1,\dots,r\}$، نرمز للحدث المضاد للحدث A_k بـ $\overline{A}_k$. بيّن أنّ
$P(\overline{A}_1\cap\dots\cap\overline{A}_r)=P(\overline{A}_1)\dots P(\overline{A}_r)$.

5.1. نعتبر الحدث A : " سحب كرة تحمل رقما يكون أوّليا مع n "، ونرمز بـ $P(A)$ إلى احتماله.

1.5.1. بيّن أنّ $P(A)=\frac{\varphi(n)}{n}$.

2.5.1. تحقّق من أنّ $A=\overline{A}_1\cap\dots\cap\overline{A}_r$ و استنتج أنّ
$$\varphi(n)=n\prod_{k=1}^{r}\Big(1-\frac{1}{p_k}\Big).$$

6.1. ليكن m من $\mathbb{N}\setminus\{0,1\}$ وليكن $m=p_1^{\alpha_1}\dots p_s^{\alpha_s}$ تفكيك هذا العدد إلى جداء أعداد أوّلية، حيث $\alpha_1,\dots,\alpha_s$ أعداد صحيحة طبيعية غير منعدمة و $p_1,\dots,p_s$ أعداد أوّلية مختلفة مثنى مثنى. بيّن أنّ
$$\varphi(m)=m\prod_{k=1}^{s}\Big(1-\frac{1}{p_k}\Big).$$

7.1. ليكن m_1 و m_2 عددين من $\mathbb{N}\setminus\{0,1\}$.

1.7.1. نفترض هنا أنّ $m_1\wedge m_2=1$. بيّن أنّ $\varphi(m_1m_2)=\varphi(m_1)\varphi(m_2)$.

2.7.1. نضع هنا $d = m_1 \wedge m_2$. أحسب $\varphi(m_1 m_2)$ بدلالة d و $\varphi(m_1)$ و $\varphi(m_2)$ و $\varphi(d)$.

8.1. ليكن X المتغيّر العشوائي الذي يربط كل نتيجة بالعدد الذي تحمله الكرة المسحوبة. نذكّر أنّ $n \in \mathbb{N} \setminus \{0, 1\}$.

1.8.1. ليكن m و a من $\mathbb{N}^*$ و ليكن d قاسما للعدد m. بيّن أنّ

$$a \wedge m = d \Longleftrightarrow (\exists k \in \mathbb{N}^*)\ \left(a = kd,\ \ k \wedge \frac{m}{d} = 1\right).$$

2.8.1. ليكن d من $\mathbb{N}^*$ قاسما للعدد n ؛ نضع $\Delta_d = \{a \in \{1, \dots, n\}\ ;\ a \wedge n = d\}$. بيّن أنّ

$$\mathrm{Card}\, \Delta_{\mathrm{d}} = \varphi(\frac{\mathrm{n}}{\mathrm{d}}).$$

3.8.1. ليكن d من $\mathbb{N}^*$ قاسما للعدد n ؛ نعتبر الحدث C_d : " $X \wedge n = d$ " . عَبِّرْ عن $P(C_d)$ بواسطة n و d والدّالة φ .

4.8.1. بيّن أنّ $\sum_{d|n} \varphi(d) = n$ (متطابقة أُولِر) . يمكن استعمال نِظْمَة تامّة من الأحداث.

الجــزء الثــاني

الرُّتْبَــة الضَّــرْبِية لعــدد

الهدف من هذا الجزء هو تعريف الرّتْبَة الضّربية لعدد ودراسة بعض التطبيقات.

أ. مبرهنتا أُولِر و فِيرْمَا[2]

1.2. ليكن n عددا صحيحا طبيعيا غير منعدم و a من $\mathbb{Z}^*$. بيّن أنّ
$\bar{a} \in \mathbb{Z}_n^* \Longleftrightarrow n \wedge a = 1.$

2.2. ليكن p عددا أوّليا. بيّن أنّ $\mathbb{Z}_p^* = \{\bar{1}, \dots, \overline{(p-1)}\}$.

3.2. بيّن أنّ $(\mathbb{Z}_n^*, \times)$ زمرة تبادلية عدد عناصرها $\varphi(n)$ (أي أنّ رتبتها هي $\varphi(n)$).

4.2. نضع $\mathbb{Z}_n^* = \{\bar{u}_1, \dots, \bar{u}_{\varphi(n)}\}$. ليكن a من $\mathbb{N}^*$ بحيث a و n أوّليان فيما بينهما.

1.4.2. بيّن أنّ لكل عدد i من $\{1, \dots, \varphi(n)\}$ يوجد عنصر وحيد j من $\{1, \dots, \varphi(n)\}$ بحيث $\bar{a} \times \bar{u}_j = \bar{u}_i$.

2.4.2. استنتج أنّ $a^{\varphi(n)}$ يوافق 1 بترديد n : $a^{\varphi(n)} \equiv 1[n]$. (مبرهنة أُولِر).

5.2. ليكن p عددا أوّليا. بيّن أنّ لكل عدد صحيح طبيعي a، أوّلي مع p ، لدينا $a^{p-1} \equiv 1[p]$. (المبرهنة الصغرى لِفِيرْمَا).

[2] FERMAT, math. fran. (1601-1665)

ب. ألرُّتْبة الضَّربية لعدد

ليكن n عددا صحيحا طبيعيا غير منعدم ويخالف 1 .

6.2. بيّن أنّ لكل عدد a من $\mathbb{N}^*$ لدينا

$$a \wedge n = 1 \iff \exists k \in \mathbb{N}^*,\ \ a^k \equiv 1[n].$$

7.2. ليكن a عددا صحيحا طبيعيا غير منعدم ؛ نفترض أنّ $a \wedge n = 1$ ونعتبر العدد $w_n(a)$ المعرّف بـ

$$w_n(a) = \min\{k \in \mathbb{N}^*,\ \ a^k \equiv 1[n]\}.$$

العدد $w_n(a)$ معرّف لكون المجموعة $\{k \in \mathbb{N}^*,\ \ a^k \equiv 1[n]\}$ جزءا غير فارغ من $\mathbb{N}$ ، ويسمّى **بالرّتبة الضّربية** للعدد a بترديد n.

1.7.2. بيّن أنّ لكل r من $\mathbb{N}^*$ لدينا

$$w_n(a) = r \iff \begin{cases} a^r \equiv 1[n], \\ \forall k \in \mathbb{N}^*,\ \ a^k \equiv 1[n] \implies r|k. \end{cases}$$

2.7.2. بيّن أنّ $w_n(a)$ يقسم العدد $\varphi(n)$.

3.7.2. بيّن أنّه إذا كان n أوّليا فإنّ $w_n(a)$ يقسم العدد $n-1$.

4.7.2. بيّن أنّ لكل عدد صحيح طبيعي غير منعدم k لدينا $w_n(a^k) = \frac{w_n(a)}{k \wedge w_n(a)}$.

8.2. ليكن a و b عددين صحيحين طبيعيين غير منعدمين. نفترض أنّ $a \wedge n = b \wedge n = 1$ و أنّ $w_n(a) \wedge w_n(b) = 1$. بيّن أن $w_n(ab) = w_n(a)w_n(b)$.

ج. بعض التطبيقات

9.2. **التطبيق الأول** : ليكن p و q عددين أوّليين مختلفين بحيث يكون العدد $3^p - 2^p$ قابلا للقسمة على q .

1.9.2. بيّن أنّ $q \geq 5$.

2.9.2. بيّن أنّه يوجد $u \in \mathbb{N}^*$ بحيث $u \wedge q = 1$ و $3 \equiv 2u\,[q]$ ، ثمّ استنتج أنّ $w_q(u)|p$.

3.9.2. بيّن أنّ $p|(q-1)$.

10.2. **التطبيق الثاني** :

1.10.2. ليكن k عددا صحيحا طبيعيا. أوجد جميع البواقي الممكنة للقسمة الإقليدية للعدد k^3 على 9.

2.10.2. احسب $w_9(7)$ ثم بيّن أنّه لا وجود لاي عدد صحيح طبيعي n بحيث يكون العدد $7^n + n^3$ قابلا للقسمة على 9 .

11.2. **التطبيق الثالث** : ليكن p عددا أوّليا يخالف 2 . نضع $m = \frac{p^p - 1}{p-1}$.

1.11.2. بيّن أنّ m عدد صحيح طبيعي فردي.

2.11.2. ليكن q عددا أوّليا يقسم m . بيّن أنّ $p|(q-1)$ ثم استنتج أنّ العدد q يُكتب على شكل $q = 2\ell p + 1$ بحيث $\ell \in \mathbb{N}^*$. يمكن أن تبيّن أنّ $q \neq p$ وتعتبر $w_q(p)$.

3.11.2. ليكن r عددا صحيحا طبيعيا فرديا. بيّن أنّ العدد $p^p - 1$ لا يقبل القسمة على $rp+1$.

الجـزء الثـالث

دراسـة الزمرة $(\mathbb{Z}_n^*, \times)$ في حالة $n = p^\alpha$، حيث p عدد أولي و $\alpha \in \mathbb{N}^*$

في هذا الجزء، نرمز بـ p إلى عدد أوّلي فردي .

أ. أسئـلة تمـهيدية حـول تعميل الحدوديات ذات المعاملات في $\mathbb{Z}_p$

1.3. ليكن n عنصرا من $\mathbb{N} \setminus \{0,1\}$. بين أنّ الحلقة $\mathbb{Z}_n$ جسم إذا وفقط إذا كان العدد n أوّليا.

2.3. لتكن P و Q دالّتين حدوديتين من الدرجة $n \geqslant 0$ و $m \geq 0$ على التوالي، حيث

$$\begin{cases} P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = \sum_{k=0}^{n} a_k x^k \\ Q(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0 = \sum_{k=0}^{m} b_k x^k \end{cases}$$

و a_0 ، a_1 ، … ، a_n و b_0 ، b_1 ، … ، b_m عناصر من الجسم $\mathbb{Z}_p$.

بيّن أنّ الجداء PQ دالّة حدودية من الدرجة $m+n$.

3.3. لتكن $P(x) = \sum_{k=0}^{n} a_k x^k$ دالّة حدودية من الدرجة $n \geqslant 2$ حيث a_0 ، a_1 ، … ، a_n عناصر من الجسم $\mathbb{Z}_p$.

1.3.3. ليكن α و β عنصرين مختلفين من الجسم $\mathbb{Z}_p$ ، و $k \in \mathbb{N}^*$. أوجد تعبيرا للفرق $\alpha^k - \beta^k$ على شكل جداء $\alpha - \beta$ ومجموع يُعَبَّر عنه بدلالة العنصرين α و β .

2.3.3. ليكن α عنصرا من الجسم $\mathbb{Z}_p$. بيّن أنّ $P(\alpha) = 0$ إذا وفقط إذا وُجِدت دالّة حدودية Q من الدرجة $n-1$، معاملاتها عناصر من $\mathbb{Z}_p$ ، حيث

$$P(x) = (x-\alpha)Q(x).$$

3.3.3. بيّن أنّ عدد جذور الدالّة الحدودية P في الجسم $\mathbb{Z}_p$ لا يتعدى n .

4.3. أوجد في الحلقة $\mathbb{Z}_6$ جميع جذور الدالّة $P(x) = x^2 - x$ ثم أوجد تعميلين مختلفين للدالّة $P(x)$ على شكل $P(x) = (x-\alpha)(x-\beta)$. ماذا يمكنك استنتاجه بالنّظر إلى ما سبق؟

ب. الزمرة $(\mathbb{Z}_p^*, \times)$ دوريّة

نذكر هنا بأنّ رتبة الزمرة $(\mathbb{Z}_p^*, \times)$ هي $\varphi(p) = p-1$ وأنّ $\mathbb{Z}_p^* = \{\bar{1}, \bar{2}, \ldots, \overline{(p-1)}\}$.

5.3. ليكن q عددا أوّليا و $\alpha \in \mathbb{N}^*$ بحيث $p-1$ يقبل القسمة على q^α ($q^\alpha | p-1$). لكل k من المجموعة $\{1, \ldots, p-1\}$ نضع $y_k = k^{\frac{p-1}{q^\alpha}}$.

1.5.3. بيّن أنّ $y_k^{q^\alpha} \equiv 1\,[p]$ واستنتج أنّه يوجد n_k من $\{0, \ldots, \alpha\}$ بحيث $w_p(y_k) = q^{n_k}$.

2.5.3. نضع $m=\max\{n_k\ ;\ k\in\{1,\dots,p-1\}\}$. بيّن أنّ كل عناصر المجموعة $\mathbb{Z}_p^*$ هي جذور للدالّة الحدودية $P(x)=x^{\frac{p-1}{q^\alpha}q^m}-1$ ثم استنتج أنّ $m=\alpha$.

6.3. ليكن $p-1=p_1^{\alpha_1}\dots p_s^{\alpha_s}$ تفكيكا للعدد $p-1$ إلى جداء أعداد أوّلية، حيث $\alpha_1,\dots,\alpha_s$ أعداد صحيحة طبيعية غير منعدمة و $p_1,\dots,p_s$ أعداد أوّلية مختلفة مثنى مثنى.

1.6.3. بيّن أنّ لكل i من $\{1,\dots,s\}$ يوجد a_i من $\{1,\dots,p-1\}$ بحيث $w_p(a_i)=p_i^{\alpha_i}$ ثم أوجد عنصرا a من $\mathbb{N}^*$ بحيث $a\wedge p=1$ و $w_p(a)=p-1$.

2.6.3. بيّن أنّ $\mathbb{Z}_p^*=\{1,\bar a,\dots,\bar a^{p-1}\}$ ، أي أنّ لكل $\bar b$ من $\mathbb{Z}_p^*$ يوجد k من $\{0,1,\dots,p-1\}$ بحث $\bar b=\bar a^k$. (الزّمرة $(\mathbb{Z}_p^*,\times)$ دورية).

ج. الزمرة $(\mathbb{Z}_{p^\alpha}^*,\times)$ دوريّة لكل $2\le\alpha$

ليكن α من $\mathbb{N}\setminus\{0,1\}$.

7.3. بيّن أنّ لكل k من $\mathbb{N}^*$ يوجد $\lambda_k\in\mathbb{N}^*$ بحث $p\wedge\lambda_k=1$ و $(1+p)^{p^k}=1+\lambda_k p^{k+1}$.

8.3. استنتج أنّ $w_{p^\alpha}(1+p)=p^{\alpha-1}$.

9.3. تحقق أنه يوجد عدد x من $\mathbb{N}^*$ بحث $p\wedge x=1$ و $w_p(x)=p-1$.

10.3. بيّن أنّ $p-1|w_{p^\alpha}(x)$ واستنتج أنّه يوجد x_1 من $\mathbb{N}^*$ بحيث $p\wedge x_1=1$ و $w_{p^\alpha}(x_1)=p-1$.

11.3. بيّن أنّه يوجد عدد y من $\mathbb{N}^*$ بحيث $w_{p^\alpha}(y)=p^{\alpha-1}(p-1)$. (الزمرة $(\mathbb{Z}_{p^\alpha}^*,\times)$ دوريّة).

الجـــزء الرابـــع
في شــــأن أعــداد كـارميــكائيـل[3]

تعريف : نسمّي عدد كارميكائيل كل عدد صحيح طبيعي n يحقّق ما يلي :

- n غير أوّلي،
- لكل k من $\mathbb{Z}^*$ بحيث $k\wedge n=1$ ، لدينا $k^{n-1}\equiv 1\,[n]$.

1.4. لتكن $p_1,\dots,p_s$ ، $3\le s$ ، أعدادا أوّلية فردية ومختلفة مثنى مثنى. نضع $n=p_1\dots p_s$ ونفترض أن $(p_j-1)|(n-1)$ لكل j من المجموعة $\{1,\dots,s\}$. بيّن أنّ n عدد من أعداد كارميكائيل.

2.4. بيّن أنّ 561 عدد من أعداد كارميكائيل.

نعتبر في ما يلي عددا n من أعداد كارميكائيل، وليكن $n=p_1^{\alpha_1}\dots p_r^{\alpha_r}$ تفكيك العدد n إلى جداء أعداد أوّلية، حيث $\alpha_1,\dots,\alpha_r$ أعداد صحيحة طبيعية غير منعدمة و $p_1,\dots,p_r$ أعداد أوّلية مختلفة مثنى مثنى.

3.4. بيّن أن الأعداد $p_1,\dots,p_r$ كلها فردية.

[3] CARMICHAEL, math. americain. (1879-1967)

4.4. ليكن i من $\{1,\ldots,r\}$ وليكن a_i من $\mathbb{N}\setminus\{0,1\}$ بحيث $a_i \wedge p_i = 1$ و $w_{p_i^{\alpha_i}}(a_i) = p_i^{\alpha_i-1}(p_i-1)$.

1.4.4. علّل وجود العدد a_i وبيّن أنّه يوجد $t\in\mathbb{N}\setminus\{0,1\}$ بحيث

$$\begin{cases} t \equiv a_i\,[p_i^{\alpha_i}], \\ t \equiv 1\,[p_j^{\alpha_j}],\ \ j\neq i. \end{cases}$$

2.4.4. بيّن أنّ $t^{n-1}\equiv 1[n]$ ثم استنتج أنّ $p_i^{\alpha_i-1}(p_i-1)|(n-1)$.

3.4.4. بيّن أنّ $\alpha_i = 1$ و أنّ $(p_i-1)|(n-1)$.

4.4.4. بيّن أنّ $3\le r$.

5.4. حل في $\mathbb{Z}^2$ المعادلة $85x-16y=1$ ذات المجهولين x و y ، ثم أوجد أصغر عدد من أعداد كارميكائيل يقبل القسمة على العددين 5 و 17 .

نهـايــة الــموضــوع

لمحة تاريخية عن أعداد كارميكائيل

بدأ الإهتمام بأعداد كارميكائيل منذ زمن بعيد انطلاقا من أبحاث فيرما خلال القرن السابع عشر. فقد بيّن فيرما أنّه إذا كان n عددا أوّليا، فإنّ لكل a من $\mathbb{N}^*$ بحيث $n\wedge a=1$ ، لدينا $a^{n-1}\equiv 1\,[n]$. وانكبّت بعد ذلك مجموعة من الباحثين على دراسة الخاصية العكسية محاولين الجواب على السؤال التالي :

هل توجد أعداد n تحقق الخاصية $\mathcal{P}$ التالية، وكيف يمكن تمييزها؟

$\mathcal{P}$: " n عدد غير أوّلي ويحقق $a^{n-1}\equiv 1\,[n]$ لكل عدد a أوّلي مع n . "

في سنة 1899 تمكن كورسيلت من البرهان على ما يلي : " n عدد يحقق الخاصية $\mathcal{P}$ إذا وفقط إذا كان n لا يقبل القسمة على مربّع أيّ عدد اوّلي ولكل قاسم أوّلي p للعدد n لدينا $(p-1)|(n-1)$ "، لكنه لم يستطع رغم ذلك إعطاء أيّ مثال ملموس لهذه الأعداد.

في سنة 1909 تمكن كارميكائيل من تحديد أصغر عدد يحقق الخاصية $\mathcal{P}$ ، والذي هو 561 ؛ ومن تم أصبحت هذه الأعداد تحمل إسم أعداد كارميكائيل .

في سنة 1939 بيّن شيرنيك مبرهنة مفادها أنّ لكل عدد k من $\mathbb{N}$ بحيث تكون الأعدد $6k+1$ و $12k+1$ و $18k+1$ أوّلية، فإنّ الجداء $(6k+1)(12k+1)(18k+1)$ عدد من أعداد كارميكائيل.

في سنة 1956 بيّن إيردوس أنّه يوجد عدد حقيقي K يحقق $C(n)\le ne^{\frac{-K\ln n\ln\ln\ln n}{\ln\ln n}}$ ، بحيث $C(n)$ هو عدد أعداد كارميكائيل التي هي أصغر أو تساوي n . وفي سنة 1994 بيّن ألفورد و كرانفيل و بوميرانس أنّ $n^{\frac{2}{7}}\le C(n)$ لكلّ عدد n، كبير بما فيه الكفاية.

في سنة 2013 تم إثبات وجود ما لا نهاية من أعداد كارميكائيل في كل متتالية $(an+b)_n$ حيث a و b عددان أوّليان بينهما.