Problema săptămânii 387

Găsiţi numerele prime p, q pentru care pq divide $(5^p - 2^p)(5^q - 2^q)$.

Olimpiadă Bulgaria, 1995-1996

Soluţie: Din ipoteză rezultă că $p \mid 5^p - 2^p$ sau $5 \mid 5^q - 2^q$ şi analog pentru q. Distingem 4 cazuri:
- $p \mid 5^p - 2^p$, $q \mid 5^q - 2^q$,
- $p \mid 5^p - 2^p$, $q \mid 5^p - 2^p$,
- $p \mid 5^q - 2^q$, $q \mid 5^q - 2^q$,
- $p \mid 5^q - 2^q$, $q \mid 5^p - 2^p$.

Din mica teoremă a lui Fermat, $5^p \equiv 5 \pmod{p}$ şi $2^p \equiv 2 \pmod{p}$, astfel că dacă $p \mid 5^p - 2^p$ atunci $0 \equiv 5^p - 2^p \equiv 5 - 2 = 3 \pmod{p}$, deci $p = 3$.
Atunci primul caz conduce la $p = q = 3$ care verifică într-adevăr condiţia dată.
Cazul 2 revine la $p = 3$ şi $q \mid 5^3 - 2^3 = 117 = 3^2 \cdot 13$. În afară de soluţia $p = q = 3$ găsită şi la cazul 1, mai obţinem $p = 3$, $q = 13$.
Cazul 3 este analog cazului 2 şi conduce la $p = 13$, $q = 3$.
Cazul 4. Evident, p, q nu pot fi nici 2, nici 5. De asemenea, considerăm $p, q \neq 3$, altminteri ne aflăm într-unul din primele trei cazuri.
Din mica teoremă a lui Fermat avem că $5^{p-1} \equiv 1 \pmod{p}$ şi $2^{p-1} \equiv 1 \pmod{p}$, deci $p \mid 5^{p-1} - 2^{p-1}$ şi totodată $p \mid 5^p - 2^q$. Se ştie că dacă p este un număr natural relativ prim cu a şi b atunci $p \mid a^m - b^m$ şi $p \mid a^n - b^n$ implică $p \mid a^d - b^d$, unde $d = (m, n)$. Deducem că, dacă $d = (p-1, q)$, atunci $p \mid 5^d - 2^d$. Cum $d = 1$ ar implica $p = 3$, caz pe care l-am exclus, rezultă că trebuie ca $(p-1, q) > 1$, adică $q \mid p - 1$, deci $q < p$. Analog obţinem că este necesar şi ca $p \mid q - 1$, deci ca $p < q$. Aşadar, acest din urmă caz nu aduce nicio soluţie în plus faţă de primele trei cazuri, astfel că singurele soluţii sunt

$$(p, q) \in \{(3, 3),\ (3, 13),\ (13, 3)\}.$$

Am primit soluţii de la: *Gheorghe Iurea, Cristian Muth, Eric-Dimitrie Cismaru* şi *Ioana Vlădoiu.*

Problem of the week no. 387

Determine all primes p, q such that pq divides $(5^p - 2^p)(5^q - 2^q)$.

Bulgarian Olympiad, 1995-1996

Solution: From the hypothesis it follows that $p \mid 5^p - 2^p$ or $5 \mid 5^q - 2^q$ and similarly for q. We distinguish 4 cases:
- $p \mid 5^p - 2^p$, $q \mid 5^q - 2^q$,
- $p \mid 5^p - 2^p$, $q \mid 5^p - 2^p$,
- $p \mid 5^q - 2^q$, $q \mid 5^q - 2^q$,

• $p \mid 5^q - 2^q$, $q \mid 5^p - 2^p$.
According to Fermat's Little Theorem, $5^p \equiv 5 \pmod{p}$ and $2^p \equiv 2 \pmod{p}$, therefore, if $p \mid 5^p - 2^p$ then $0 \equiv 5^p - 2^p \equiv 5 - 2 = 3 \pmod{p}$, hence $p = 3$.
The first case reduces to $p = q = 3$ which does indeed satisfy the given condition.
Case 2 comes down to $p = 3$ and $q \mid 5^3 - 2^3 = 117 = 3^2 \cdot 13$. Besides the solution $p = q = 3$, already found in the first case, we also get $p = 3$, $q = 13$.
Case 3 is similar to case 2 and leads to the solution $p = 13$, $q = 3$.
Case 4. Clearly, p, q can not be equal to 2 or 5. Also, we consider $p, q \neq 3$, otherwise we will find ourselves in one of the first three cases.
From Fermat's Little Theorem we have that $5^{p-1} \equiv 1 \pmod{p}$ and $2^{p-1} \equiv 1 \pmod{p}$, hence $p \mid 5^{p-1} - 2^{p-1}$ and also $p \mid 5^p - 2^q$. It is known that if $p \mid a^m - b^m$ and $p \mid a^n - b^n$, then $p \mid a^d - b^d$, where $d = (m, n)$. It follows that, if $d = (p-1, q)$, then $p \mid 5^d - 2^d$. But $d = 1$ would lead to $p = 3$, case that we have excluded, so we need to have $(p-1, q) > 1$, hence $q \mid p - 1$, i.e. $q < p$. Similarly, we also need $p \mid q - 1$, i.e. $p < q$. We conclude that this case does not lead to any new solution, so that the only solutions are

$$(p, q) \in \{(3, 3),\ (3, 13),\ (13, 3)\}.$$