Werk

Label: Abstract

Jahr: 1946

PURL: https://resolver.sub.uni-goettingen.de/purl?31311028X_0071|log11

Máme výsledek: náš polynom se rozpadl na faktor stupně prvního a na $\frac{q-1}{l}$ faktorů stupně l-tého.

Úhrnem máme větu:

Je dána kongruence $x^q - a \pmod p$, $q < p$. Nechť p a q jsou dvě různá prvočísla. Nechť p patří mod q k exponentu l. Je-li $l = 1$ a $a^{\frac{p-1}{q}} \equiv 1 \pmod p$, rozpadne se kongruence na samé lineární faktory. Je-li $l = 1$ a $a^{\frac{p-1}{q}} \not\equiv 1 \pmod p$, jest polynom ireducibilní. Je-li $l > 1$, rozpadne se $x^q - a \pmod p$ na jeden faktor lineární a na $\frac{q-1}{l}$ faktorů stupně l-tého.[3])

*

Contribution à la réductibilité des congruences binomiques.

(Résumé de l'article précédent.)

Soit (1) une congruence du degré n, $(n, p) = (a, p) = 1$. Soit k un nombre entier, $1 \leqq k \leqq n$. Posons $d_k = (p^k - 1, n)$. Soit σ_k le nombre des facteurs irréductibles du degré k de la congruence (1). Soient enfin $k' > k'' > \ldots > 1$ tous les diviseurs de k plus petits que k. Alors les relations suivantes ont lieu:

1. pour les k, pour lesquels

$$a^{\frac{p^k-1}{d_k}} \not\equiv 1 \pmod p,$$

on a $$k\sigma_k + k'\sigma_{k'} + k''\sigma_{k''} + \ldots + \sigma_1 \equiv 0 \pmod p;$$

2. pour les k, pour lesquels

$$a^{\frac{p^k-1}{d_k}} \equiv 1 \pmod p,$$

on a $$k\sigma_k + k'\sigma_{k'} + k''\sigma_{k''} + \ldots + \sigma_1 \equiv d_k \pmod p.$$

Ces relations forment une généralisation d'un résultat classique bien connu concernant le nombre des racines rationnelles de la congruence (1). Elles donnent des formules récurrentes, qui fournissent — en général — les nombres $\sigma_1, \sigma_2, \ldots, \sigma_n \pmod p$.

Quelques applications aux équations spéciales servent à illustrer la portée des résultats trouvés.

[3]) Jako speciální případ obsažen jest v této větě známý rozklad rovnice pro dělení kruhu $x^q - 1 \equiv 0 \pmod p$. Tady jest vždy $a^{\frac{p-1}{q}} \equiv 1$. Případ $l = 1$ a $l > 1$ lze formulovati jednotně: $x^q - 1 \equiv 0 \pmod p$ rozpadne se na jeden faktor lineární a $\frac{q-1}{l}$ faktorů stupně l-tého. (Lehce se dokáže, že platí ovšem i v případě $p < q$.)