O kongruencii $a^{p-1} \equiv 1 \mod p^k$

Peter Maličký
Univerzita Mateja Bela
Banská Bystrica

PRACOVNÉ STRETNUTIE V RÁMCI PROJEKTU
CaKS – Centrum excelentnosti informatických vied
a znalostných systémov
Nový Smokovec, 11.-13. októbra 2010

Podporujeme výskumné aktivity na Slovensku/
Projekt je spolufinancovaný zo zdrojov EÚ

Wieferichove prvočísla

Wieferichove prvočísla sa vyznačujú kongruenciou

$$2^{p-1} \equiv 1 \mod p^2 .$$

K dnešnému dňu sú známe iba dve

Wieferichove prvočísla

Wieferichove prvočísla sa vyznačujú kongruenciou

$$2^{p-1} \equiv 1 \mod p^2 .$$

K dnešnému dňu sú známe iba dve 1093 (Meissner, 1913),

Wieferichove prvočísla

Wieferichove prvočísla sa vyznačujú kongruenciou

$$2^{p-1} \equiv 1 \mod p^2 .$$

K dnešnému dňu sú známe iba dve 1093 (Meissner, 1913), a 3511 (Beeger, 1920).

Wieferichove prvočísla

Wieferichove prvočísla sa vyznačujú kongruenciou

$$2^{p-1} \equiv 1 \mod p^2 .$$

K dnešnému dňu sú známe iba dve 1093 (Meissner, 1913), a 3511 (Beeger, 1920). Wieferichove prvočísla boli zavedené v súvislosti s veľkou Fermatovou vetou v článku Zum letzten Fermat'schen Theorem, J. für Math. 136 (1909) 293-302. Nejaký čas sa prepokladalo, že neexistujú.

Wieferichove prvočísla

Wieferichove prvočísla sa vyznačujú kongruenciou

$$2^{p-1} \equiv 1 \mod p^2 .$$

K dnešnému dňu sú známe iba dve 1093 (Meissner, 1913), a 3511 (Beeger, 1920). Wieferichove prvočísla boli zavedené v súvislosti s veľkou Fermatovou vetou v článku Zum letzten Fermat'schen Theorem, J. für Math. 136 (1909) 293-302. Nejaký čas sa prepokladalo, že neexistujú.

Wieferichove prvočísla

My sme sa začali zaoberať Wieferichovými prvočíslami pri skúmaní periodických bodov zobrazenia

$$F : [x, y] \mapsto [x(4 - x - y),\, xy] \ ,$$

ktoré ležia vo vnútri trojuholníka

$$D = \{\, [x, y] : 0 \leq x,\, 0 \leq y,\, x + y \leq 4 \,\} .$$

O tom sme referovali na stretnutí CeXu v Herľanoch 16. apríla 2010.

Wieferichove prvočísla

My sme sa začali zaoberať Wieferichovými prvočíslami pri skúmaní periodických bodov zobrazenia

$$F : [x, y] \mapsto [x(4 - x - y),\, xy] \ ,$$

ktoré ležia vo vnútri trojuholníka

$$D = \{\, [x, y] : 0 \leq x,\, 0 \leq y,\, x + y \leq 4 \,\} \, .$$

O tom sme referovali na stretnutí CeXu v Herľanoch 16. apríla 2010.

Mirimanovove prvočísla

Mirimanovove prvočísla sa vyznačujú kongruenciou

$$3^{p-1} \equiv 1 \mod p^2 .$$

K dnešnému dňu sú známe iba dve

Mirimanovove prvočísla

Mirimanovove prvočísla sa vyznačujú kongruenciou

$$3^{p-1} \equiv 1 \mod p^2 .$$

K dnešnému dňu sú známe iba dve 11

Mirimanovove prvočísla

Mirimanovove prvočísla sa vyznačujú kongruenciou

$$3^{p-1} \equiv 1 \mod p^2 .$$

K dnešnému dňu sú známe iba dve 11 a 1006003 (Kloss, 1965).

Mirimanovove prvočísla

Mirimanovove prvočísla sa vyznačujú kongruenciou

$$3^{p-1} \equiv 1 \mod p^2 .$$

K dnešnému dňu sú známe iba dve 11 a 1006003 (Kloss, 1965). Aj Mirimanovove prvočísla boli zavedené v súvislosti s veľkou Fermatovou vetou.

Mirimanovove prvočísla

Mirimanovove prvočísla sa vyznačujú kongruenciou

$$3^{p-1} \equiv 1 \mod p^2 .$$

K dnešnému dňu sú známe iba dve 11 a 1006003 (Kloss, 1965). Aj Mirimanovove prvočísla boli zavedené v súvislosti s veľkou Fermatovou vetou.

Kongruencia $a^{p-1} \equiv 1 \mod p^k$

Uvažujme kongruenciu

$$a^{p-1} \equiv 1 \mod p^k .$$

Jej riešenia sa dajú opísať jednoducho.

Kongruencia $a^{p-1} \equiv 1 \mod p^k$

Uvažujme kongruenciu

$$a^{p-1} \equiv 1 \mod p^k .$$

Jej riešenia sa dajú opísať jednoducho. Nech $b = 1, 2, \cdots, p-1$.

Kongruencia $a^{p-1} \equiv 1 \mod p^k$

Uvažujme kongruenciu

$$a^{p-1} \equiv 1 \mod p^k .$$

Jej riešenia sa dajú opísať jednoducho. Nech $b = 1, 2, \cdots, p-1$.
Vezmime čísla a tak, by

$$\begin{aligned} a &\equiv b^{p^{k-1}} \mod p^k , \\ 1 &\leq a < p^k . \end{aligned}$$

Potom máme všetky riešenia.

Kongruencia $a^{p-1} \equiv 1 \mod p^k$

Uvažujme kongruenciu

$$a^{p-1} \equiv 1 \mod p^k .$$

Jej riešenia sa dajú opísať jednoducho. Nech $b = 1, 2, \cdots, p-1$. Vezmime čísla a tak, by

$$\begin{aligned} a &\equiv b^{p^{k-1}} \mod p^k , \\ 1 &\leq a < p^k . \end{aligned}$$

Potom máme všetky riešenia.

Kongruencia $a^{p-1} \equiv 1 \mod p^k$

Ak uvažujeme $1 < a < p^{k-1}$, potom riešení kongruencií

$$a^{p-1} \equiv 1 \mod p^k$$

je pomerne veľa.

Kongruencia $a^{p-1} \equiv 1 \mod p^k$

Ak uvažujeme $1 < a < p^{k-1}$, potom riešení kongruencií

$$a^{p-1} \equiv 1 \mod p^k$$

je pomerne veľa. Ak uvažujeme $1 < a < p^{k-2}$, potom poznáme len dve riešenia $a = 68$, $p = 113$, $k = 3$

Kongruencia $a^{p-1} \equiv 1 \mod p^k$

Ak uvažujeme $1 < a < p^{k-1}$, potom riešení kongruencií

$$a^{p-1} \equiv 1 \mod p^k$$

je pomerne veľa. Ak uvažujeme $1 < a < p^{k-2}$, potom poznáme len dve riešenia $a = 68$, $p = 113$, $k = 3$ a $p = 199$, $a = 363170837918927 7$, $k = 9$.

Kongruencia $a^{p-1} \equiv 1 \mod p^k$

Ak uvažujeme $1 < a < p^{k-1}$, potom riešení kongruencií

$$a^{p-1} \equiv 1 \mod p^k$$

je pomerne veľa. Ak uvažujeme $1 < a < p^{k-2}$, potom poznáme len dve riešenia $a = 68$, $p = 113$, $k = 3$ a $p = 199$, $a = 363170837918927 7$, $k = 9$. Skúmali sme prípady $k = 3, 4, \cdots, 10$.

Kongruencia $a^{p-1} \equiv 1 \mod p^k$

Ak uvažujeme $1 < a < p^{k-1}$, potom riešení kongruencií

$$a^{p-1} \equiv 1 \mod p^k$$

je pomerne veľa. Ak uvažujeme $1 < a < p^{k-2}$, potom poznáme len dve riešenia $a = 68$, $p = 113$, $k = 3$ a $p = 199$, $a = 363170837918927 7$, $k = 9$. Skúmali sme prípady $k = 3, 4, \cdots, 10$.

Kongruencia $a^{p-1} \equiv 1 \mod p^3$

Kongruencia

$$a^{p-1} \equiv 1 \mod p^3$$

je za predpokladu $1 < a < p < 2\,000\,000$ splnená len pri $a = 68$ a $p = 113$.

Kongruencia $a^{p-1} \equiv 1 \mod p^3$

Kongruencia

$$a^{p-1} \equiv 1 \mod p^3$$

je za predpokladu $1 < a < p < 2\,000\,000$ splnená len pri $a = 68$ a $p = 113$. Okrem toho trieda 68 generuje multiplikatívnu grupu $\mathbb{Z}_{113}^*$ rádu 112.

Kongruencia $a^{p-1} \equiv 1 \mod p^3$

Kongruencia

$$a^{p-1} \equiv 1 \mod p^3$$

je za predpokladu $1 < a < p < 2\,000\,000$ splnená len pri $a = 68$ a $p = 113$. Okrem toho trieda 68 generuje multiplikatívnu grupu $\mathbb{Z}^*_{113}$ rádu 112. Dôsledok uvedenej kongruencie je potom ten, že trieda 68 generuje v grupách $\mathbb{Z}^*_{113^2}$ a $\mathbb{Z}^*_{113^3}$ grupu rádu 112 izomorfnú $\mathbb{Z}^*_{113}$.

Kongruencia $a^{p-1} \equiv 1 \mod p^3$

Kongruencia

$$a^{p-1} \equiv 1 \mod p^3$$

je za predpokladu $1 < a < p < 2\,000\,000$ splnená len pri $a = 68$ a $p = 113$. Okrem toho trieda 68 generuje multiplikatívnu grupu $\mathbb{Z}^*_{113}$ rádu 112. Dôsledok uvedenej kongruencie je potom ten, že trieda 68 generuje v grupách $\mathbb{Z}^*_{113^2}$ a $\mathbb{Z}^*_{113^3}$ grupu rádu 112 izomorfnú $\mathbb{Z}^*_{113}$. Hranicu 2 000 000 by sme chceli zvýšiť použitím výkonného softwaru.

Kongruencia $a^{p-1} \equiv 1 \mod p^3$

Kongruencia

$$a^{p-1} \equiv 1 \mod p^3$$

je za predpokladu $1 < a < p < 2\,000\,000$ splnená len pri $a = 68$ a $p = 113$. Okrem toho trieda 68 generuje multiplikatívnu grupu $\mathbb{Z}^*_{113}$ rádu 112. Dôsledok uvedenej kongruencie je potom ten, že trieda 68 generuje v grupách $\mathbb{Z}^*_{113^2}$ a $\mathbb{Z}^*_{113^3}$ grupu rádu 112 izomorfnú $\mathbb{Z}^*_{113}$. Hranicu 2 000 000 by sme chceli zvýšiť použitím výkonného softwaru.