Sets avoiding squares in $\mathbb{Z}_m$

Mikhail Gabdullin
Lomonosov Moscow State University

Recently I.Ruzsa and M.Matolcsi proved that if m is a square-free positive integer and $A \subset \mathbb{Z}_m$ is such that $A - A$ does not contain non-zero squares, then $|A| \le me^{-c\sqrt{\log m}}$, and, under an additional assumption that all prime divisors of m are equal to $1 \pmod 4$, $|A| \le m^{1/2}$. We present the following result.

Theorem. *For all square-free m and $A \subset \mathbb{Z}_m$ such that $A - A$ does not contain non-zero squares we have $|A| \le m^{1/2}(3n)^{1.5n}$, where n denotes the number of odd prime divisors of m.*

Corollary 1. *Let m and A obey the conditions of the Theorem.*
If $n = o(\frac{\log m}{\log\log m})$, then $|A| \le m^{1/2+o(1)}$;
if $n \le (\frac{1}{3} - \varepsilon)\frac{\log m}{\log\log m}$, then $|A| \le m^{1-1.5\varepsilon+o(1)}$.

Corollary 2. *We have $|A| \le me^{-c\log m/\log\log m}$ for all m and A obeying the conditions of the Theorem.*