Integers of prescribed arithmetic structure in residue classes

Igor Shparlinski

The University of New South Wales

Primes in Progressions: In the Dream Word

Let

$$\pi(x;q,a) = \#\{p \le x : p \equiv a \bmod q\}$$

We believe that if $\gcd(a,q) = 1$ then

$$\pi(x;q,a) \sim \frac{1}{\varphi(q)}\pi(x)$$

provided $q \le x^{1-\varepsilon}$, and

$$\pi(x;q,a) > 0$$

provided $q \le x(\log x)^{-1-\varepsilon}$:

the smallest prime $p \equiv a \bmod q$ **is** $O\left(q(\log q)^{1+\varepsilon}\right)$

Primes in Progressions: Harsh Real Word

Let

$$\pi(x;q,a) = \#\{p \le x : p \equiv a \bmod q\}$$

If $\gcd(a,q) = 1$ then

$$\pi(x;q,a) \sim \frac{1}{\varphi(q)}\pi(x)$$

provided $q \le x^{1/2-\varepsilon}$ under the GRH or provided $q \le (\log x)^A$ with some fixed A, unconditionally, and

$$\pi(x;q,a) > 0$$

provided $q \le x^{1/5.2}$ (perhaps $5.2 \to 5$ — PhD Thesis by Xylouris, never published):

the smallest prime $p \equiv a \bmod q$ **is** $O\left(q^{5.2}\right)$

Special moduli

Highly composite moduli: $\max_{p|q} p = q^{o(1)}$

Chang (**2014**):

$$\pi(x; q, a) > 0$$

provided $q \le x^{5/12-\varepsilon}$ $(5/12 = 0.4167)$.

Prime power moduli: $q = p^\gamma$, *for a fixed* p.

Banks & Shparlinski (**2015**):

$$\pi(x; q, a) \gg \frac{x}{\varphi(q) \log x}$$

provided $q \le x^{0.4736-\varepsilon}$.

Recall: $A \ll B \;\Leftrightarrow\; B \gg A \;\Leftrightarrow\; A = O(B) \;\Leftrightarrow\; |A| \le cB$

The exponent 0.4736 comes from a result of *Harman* (**2008**) on *Carmichael numbers* combined with a new bound on the zero-free region.

This lower bound

$$\pi(x; p^\gamma, a) \gg \frac{x}{p^\gamma \log x}, \qquad p^\gamma \le x^{0.4736-\varepsilon},$$

implies that there are *many* primes ℓ such that $\ell - 1$ contains a very large power of a small prime. Such primes appear in some algorithmic applications and cryptographic construction

- fast primality proving for *many* primes: *Pintz, Steiger & Szemerédi* 1989, *Konyagin & Pomerance* (**1997**),
- factoring polynomials modulo such primes: *Źrałek* (**2010**),
- fast integer multiplication algorithms: *Harvey, van der Hoeven* (**2019**),
- quantum-resistant cryptosystems from supersingular elliptic curve isogenies, *De Feo, Jao and J. Plût* (**2014**).

Relaxations

Since studying one prime if **very hard** it is natural to consider some *relaxations*.

There several possible ways to relax the original question

- Consider expressions with *more than one prime*.
- Consider denser and easier to handle sequences, e.g. *square-free* numbers or *almost-primes* P_k (products of *at most* k primes).
- Do both!

Sums of two primes in residue classes $\equiv$ Goldbach numbers in residue classes

Let $G(q)$ be the smallest integer such that the sums $p_1 + p_2$, with primes $p_1, p_2 \le G(q)$ fall in all non-zero residue classes modulo q.

Conditional result

Linnik (**1952**): GRH $\Longrightarrow G(q) \ll q(\log q)^5$

. . . which is very close to $G(q) = q + 3$ which follows from the **Binary Goldbach Conjecture**

Unconditional results

Jutila (**1968**): For a prime p, $G(p) \ll p^{6/5+o(1)}$

Rakhmonov (**1986**): For any odd q, $G(q) \ll q^{\alpha}$ for any

$$\alpha > \frac{3}{32}(9+\sqrt{17}) = 1.23029\ldots .$$

Rakhmonov (**1987**): For prime p, there is $\approx$ a right number of sums p_1+p_2 with $p_1, p_2 \le p^{\beta}$ in each residue class modulo p for any $\beta > 3/2$.

Mikawa (**2000**): Proved $G(p) \ll p^{14/13+o(1)}$ for a prime p, and wrote:

> *We control the arising parameters so that all numerical calculations can be done by hand . . . So there would be some room for a further refinement, by pushing our method more.*

nobody has ever revisited this.

The above results are based on:

bounds of character sums with shifted primes & *sieve methods*

— both have recently been advanced.

Products of two primes in residue classes: Erdős, Odlyzko & Sárközy Problem

Erdős, Odlyzko & Sárközy (**1987**):
Question: Do the products p_1p_2, with primes $p_1, p_2 < p$ fall in all non-zero residue classes modulo a prime p?

The *EOS*-question seems to be too hard even for the GRH . . . so several *further relaxations* have been considered:

$$p_1p_2(p_3 + a), \quad p_1(p_2 + p_3), \quad p_1p_2 + p_1p_3 + p_2p_3$$

by *Friedlander, Kurlberg & Shparlinski* (**2008**), *Fouvry & Shparlinski* (**2010**), *Baker* (**2012**), *Garaev* (**2012**).

Products $p_1 \dots p_\nu$, p_i is prime or $p_i = 1$

Shparlinski (**2013**), via Kloosterman sums & sieve methods:

one can take $\nu = 18$ and both $P_{17} = p_1 \dots p_{17},\ p_{18} \le p^{0.977}$

(that is, we have a product of a small prime and a small almost prime)

Walker (**2016**) via methods of additive combinatorics:

one can take $\nu = 6$ and $p_i \le p^{15/16+o(1)} = p^{0.9375+o(1)}$;

For any $\varepsilon > 0$, one can take large ν and $p_i \le p^{3/4+\varepsilon}$.

Shparlinski (**2018**) via Kloosterman sums & sieve methods:

one can take $\nu = 5$ and $p_i \le p^{0.905+o(1)}$;

one can take $\nu = 6$ and $p_i \le p^{0.864+o(1)}$;

one can take $\nu = 7$ and $p_i \le p^{0.760+o(1)}$;

one can take $\nu = 8$ and $p_i \le p^{0.673+o(1)}$.

For any $\varepsilon > 0$, one can take large ν and $p_i \le p^{1/2+\varepsilon}$.

Question: Can we do anything in the **Burgess range** $p_i \le p^{1/(4e^{1/2})+\varepsilon}$?

The results are much harder if $p_i = 1$ is not allowed

Ramaré & Walker (**2016**) via additive combinatorics:

one can take $\nu = 3$ and $1 < p_i \ll p^{16/3}$

Ramaré & Srivastav (**2018**)

via character sums & sieve:

one can take $\nu = 3$ and $1 < p_i \ll p^3$

Balasubramanian, Ramaré & Srivastav (**2022**)

via additive combinatorics and sieve:

one can take $\nu = 3$ and $1 < p_i \ll p^{3/2}$

one can take $\nu = 4$ and $1 < p_i \ll p(\log p)^6$

Szabó (**2022**)

via character sums, sieve and additive combinatorics:

one can take $\nu = 3$ and $1 < p_i \ll p^{6/5}$

Approximation by p_1p_2

Irving (**2014**) via bounds of sums of incomplete Kloosterman sums:
For any integers a and q with $\gcd(a, q) = 1$, here are p_1 and p_2 with $p_1p_2 \le q^{46/31+o(1)}$ and such that

$$ap_1p_2 \equiv k \pmod q$$

for some k with $|k| \le q^{15/31+o(1)}$.

Question: What are the gaps between $ap_1p_2 \pmod q$?

Question: Can one get stronger results for almost all q (prime or composite)?

Square-free numbers in residue classes

Let

$$\sigma(x;q,a) = \#\{s \le x : s \equiv a \bmod q,\ \ s \text{ square-free}\}$$

— and analogue of $\pi(x;q,a)$ for square-free integers — and

$$\sigma^*(x;q) = \#\{s \le x : \gcd(s,q) = 1,\ \ s \text{ square-free}\}$$

Nunes (**2016-2017**)

$$\sigma(x;q,a) \sim \frac{1}{\varphi(q)}\sigma^*(x;q), \quad \text{for } q \le x^{13/19-\varepsilon},$$

and

$$\sigma(x;q,a) > 0, \qquad \text{for } q \le x^{25/36-\varepsilon},$$

$$\boxed{25/26 > 13/19 > \mathbf{2/3}}$$

$\mathbf{2/3}$ is a notoriously *difficult* threshold, which remains unbeaten for related problems, e.g. in the *Dirichlet divisor problem in progressions*.

Mangerel (**2022**):
If q is reasonably smooth and square-free then

$$\sigma(x; q, a) \sim \frac{1}{\varphi(q)}\sigma^*(x; q), \quad \text{for } q \leq x^{196/261-\varepsilon}$$

Note that

$$196/261 = 0.7509578\ldots$$

For smooth but not square-free q one can replace it with $3/4$.

Question: What can we say for prime powers $q = p^k$ with a fixed p?

The other extreme: Smooth numbers in residue classes

As usual, we say that n is y-**smooth** if $p \mid n \Longrightarrow p \le y$ and define

$$\psi(x, y; q, a) = \#\{n \le x \ ; \ n \text{ is } y\text{-smooth and } n \equiv a \bmod q\}$$
$$\psi_q(x, y) = \#\{n \le x \ ; \ n \text{ is } y\text{-smooth and } \gcd(n, q) = 1\}.$$

Balog & Pomerance; Munsch, Shparlinski & Yau, Fouvry & Tenenbaum; Granville; Harper; Soundararajan; . . .: various results in different ranges of (q, x, y). All these results have a natural limitation if one looks at the range $q \le y^A$

$$A \le 4e^{1/2} \qquad \text{— } \textit{Burgess Barrier}$$

Conjecture *(Soundararajan (2007))*

For any fixed $A > 1$, for $q \le y^A$ uniformly over a with $\gcd(a, q) = 1$:

$$\psi(x, y; q, a) \sim \frac{1}{\varphi(q)} \psi_q(x, y) \qquad \textit{as} \quad \frac{\log x}{\log q} \to \infty$$

Let $P(q)$ denote the largest prime divisor of q.

Banks & Shparlinski (2021)

For every fixed value of $A > 0$, there is a number $Q_A > 0$, such that if

$$P(q)^{Q_A} < q \le y^A \quad \text{and} \quad (a, q) = 1,$$

then we have asymptotic relation

$$\psi(x, y; q, a) \sim \frac{1}{\varphi(q)} \psi_q(x, y) \qquad \text{as} \quad \frac{\log x}{\log q} \to \infty$$

Let $\mathcal{Q}$ be a set of natural numbers q with the property that

$$\log P(q) = o(\log q) \qquad (q \to \infty,\ q \in \mathcal{Q}).$$

Then *Soundararajan's Conjecture* holds over $q \in \mathcal{Q}$.

Remark

The set $\mathcal{Q}$ is "almost" of positive density.

Small smooth numbers in residue classes

Harman (1999) via character sums & sieve

For any $\varepsilon > 0$ each non-zero residue class $\bmod p$ contains a $p^{1/(4e^{1/2})+\varepsilon}$-smooth $s \le p^{9/4+\varepsilon}$

Remark

Reducing $1/(4e^{1/2})$ for **any** *size of s is impossible until the Burgess (1957) bound on the smallest quadratic non-residue is improved. However improving $9/4$ is not limited by anything.*

Short products of small integers in residue classes

Motivated by applications to *Fermat Quotients*

$$q_p(a) = \frac{a^{p-1} - 1}{p}$$

and an improvement of a result of *Chen & Winterhof* (**2014**):

Harman & Shparlinski (2014) via character sums & sieve

For any $\varepsilon > 0$ each non-zero residue class $\bmod p$ can be represented as a product of 14 integers from $[1, p^{1/(4e^{1/2})+\varepsilon}]$.

Comment: The above result of *Harman* (**1999**) can be used directly but it gives 17 factors, making our application weaker.

Fermat quotients modulo p

Fermat Quotients:

$$q_p(a) = \frac{a^{p-1} - 1}{p}, \quad \gcd(a, p) = 1, \quad \text{and} \quad q_p(kp) = 0,$$

are mysterious objects whose p-divisibility properties keep re-appearing in different areas:

- Fermat Last Theorem — *Wieferich* (**1909**) primes: $p \mid q_p(2)$:

$$1093, \quad 3511, \quad (??) > 10^{17};$$

- Euler-Kronecker constants of the unique cyclic extension of degree p over $\mathbb{Q}$, *Ihara* (**2006**);
- Testing for squarefreeness, *Lenstra* (**1979**).

Motivated by the above applications, various questions about $q_p(a) \bmod p$ have been studied:

- The smallest $a \geq 2$ with $q_p(a) \not\equiv 0 \bmod p$: *Lenstra; Granville; Ihara; Bourgain, Ford, Konyagin & Shparlinski; Shkredov* (**1979–2017**)
- The smallest $A \geq 2$ with $\{q_p(a) \bmod p : \ 1 \leq a \leq A\} = \mathbb{F}_p$: *Chen–Winterhof; Shparlinski* (**2012–2017**)
- The number of $a \in [1, A]$ with $q_p(a) \equiv 0 \bmod p$: *Granville; Shparlinski* (**1990–2012**).
- The number of fixed points $a \in [1, A]$ with $q_p(a) \equiv a \bmod p$: *Ostafe & Shparlinski, Chen & Winterhof* (**2011–2014**).
- Exponential and character sums: *Chang; Shparlinski* (**2011–2014**).
- Additive properties $\bmod p$ (*á la* Waring Problem): *Chen & Winterhof; Harman & Shparlinski* (**2014**)

Smooth square-free numbers in progressions

Recall that an integer n is called

- *y-smooth* if all prime divisors of n do not exceed y;
- *square-free* if it is not divisible by a square of a prime.

Definition

*$M(p) =$ the smallest integer M such that any residue class $\bmod p$ contains a p-**smooth square-free** positive $s \le M$ (set $M(p) = \infty$ if no such representative exists).*

Booker & Pomerance (2017)

- *Theorem: We have $M(p) < \infty$ for every $p \ge 11$ and $M(p) = p^{O(\log p)}$*
- *Conjecture: We have $M(p) = p^{O(1)}$*

Motivation: Euclidean Prime Generator ($\sim$ 300 BC)

Definition (Classical Generator)

Set $p_1 = 2$ *and the for* $k = 1, 2, \ldots$ *define* p_{k+1} *as the smallest prime divisor of* $n + 1$, *where* $n = p_1 \cdots p_k$.

Definition (Modified Generator of Crandall & Pomerance (2005))

Set $p_1 = 2$ *and the for* $k = 1, 2, \ldots$ *define*

$$p_{k+1} = \min\{p : p \nmid n,\ p \mid (d+1) \text{ for some } d \mid n\},$$

where $n = p_1 \cdots p_k$.

Booker & Pomerance (2017)

The above procedure produces 2, 3, 7, 5, and then **all** *primes in order.*

The **proof** is based on an existence result for *small smooth square-free* numbers in arithmetic progressions.

Booker & Pomerance (2017)

- *Theorem:* We have $M(p) < \infty$ for every $p \geq 11$ and $M(p) = p^{O(\log p)}$
- *Conjecture:* We have $M(p) = p^{O(1)}$

Munsch & Shparlinski (2017)

- *Theorem:* We have $M(p) \leq p^{3/2+o(1)}$.
- *Conjecture:* We have $M(p) = p^{1+o(1)}$.

Remark

- *This improves a special case of Balog and Pomerance (1992) about the existence (without the additional condition of square-freeness) of a p-smooth integer $n \leq p^{7/4+\varepsilon}$ in arithmetic progressions modulo p.*
- *Our method can be used to obtain a more general improvement of the lower bound of Balog and Pomerance (1992) for the number y-smooth integer $n \leq x$ in arithmetic progressions modulo p (with or without the square-freeness condition).*

Generalisation

Booker and Pomerance (**2017**) also introduced a generalisation of $M(p)$:

Definition

For $\alpha > 0$, $M^*_\alpha(q) =$ the smallest integer M such that any reduced residue class modulo a positive integer q contains a q^α-smooth square-free positive $s \le M$, and set, formally, $M^*_\alpha(q) = \infty$ if no such representative exists.

So $M(q)$ is essentially $M^*_1(q)$ (if one forgets about non-reduced classes).

Munsch & Shparlinski (2017)

We have $M^*_\alpha(q) \le q^{2+o(1)}$ *for any fixed*

$$\alpha > \begin{cases} 1/(4e^{1/2}), & \text{if } q \text{ is cube-free,} \\ 1/(3e^{1/2}), & \text{otherwise.} \end{cases}$$

Remark

*This improves a result of Harman (**1999**): for any* $\varepsilon > 0$, *and sufficiently large* q, *in all reduced residue classes* $\bmod q$, *there exists*

- *a* $q^{1/(3e^{1/2})+\varepsilon}$*-smooth* $s \le q^{7/3+\varepsilon}$ *for any* q;
- *a* $q^{1/(4e^{1/2})+\varepsilon}$*-smooth* $s \le q^{9/4+\varepsilon}$ *for a cube-free* q;

*(this is **without** the additional **square-freeness** condition). Note that* $7/3 > 9/4 > 2$.

Remark

For $\alpha < 1/(4e^{1/2})$, *proving that* $M^*_\alpha(p) < \infty$ *for large* p *is impossible until the Burgess bound on the smallest quadratic non-residue is improved.*

Typical case

For *almost all* primes p, we obtain stronger results:

Munsch & Shparlinski (2017)

As $Q \to \infty$, for any fixed $\alpha > 0$ for all but $Q^{o(1)}$ primes $p \in [Q, 2Q]$, we have

$$M^*_\alpha(p) \le p^{2+o(1)} \quad \text{and} \quad M(p) \le p^{4/3+o(1)}.$$

Ideas Behind our Bounds on $M^*_\alpha(q)$

We estimate $M^*_\alpha(q)$ by getting an asymptotic formula for the number of solutions $N^\sharp_{a,q}(L,h)$ to the congruence

$$\ell_1\ell_2 u \equiv a \bmod q,$$

- primes $\ell_1, \ell_2 \in [L/2, L]$
- square-free positive integer $u \le h$

We need to maintain $h, L \le q^\alpha$ to enforce smoothness and optimise L^2h.

- We control the square–freeness of u via standard inclusion/exclusion.
- We then control the square–freeness of $\ell_1\ell_2 u$ observing that if it is not square–free than it is divisible by a square of a large prime $\ell \ge L/2$.

Remark

Generating smooth square-free integers in the form $\ell_1\ell_2 u$ does **not** *produce an asymptotic formula for y-smooth square-free positive integers $n \le x$ in an arithmetic progression, — an interesting open question.*

What stops us from doing better?

Methods and tools

- Sieve as in *Harman & Shparlinski* (**2014**) to control the smoothness.
- *Garaev* (**2010**): bounds on double Kloosterman sums with reciprocals $\overline{\ell}_1$ and $\overline{\ell}_2$ modulo p of primes ℓ_1 and ℓ_2:

$$\sum_{\ell_1,\ell_2 \in [L/2,L], \text{ primes}} \mathbf{e}_p\left(a\overline{\ell}_1\overline{\ell}_2\right),$$

  where $\mathbf{e}_p(z) = \exp\left(2\pi i z/p\right)$.
- A version of the *Burgess* bound over square-free numbers due to *Munsch and Trudgian* (**2017**).
- A bound on the number of solutions to congruences

$$u^2 v \equiv a \bmod p, \qquad 1 \le u \le U,\ 1 \le v \le V.$$

Improving on any of these results will propagate in better bounds on $M(p)$ and $M_\alpha(p)$.

Methods: Small α; e.g., $\alpha = 1/(4e^{1/2})$

- Sieve as in *Harman & Shparlinski* (**2014**) to control the smoothness of u in $\ell_1\ell_2 u$ modified to accomodate the square-freeness condition;
- Some error terms in the sieve depend on character sums

$$\sum_{\chi\neq\chi_0}\left|\sum_{\ell_1,\ell_2\in[L/2,L]}\sum_{u\le h}^{\#}\chi(\ell_1\ell_2 u)\right| = \sum_{\chi\neq\chi_0}\left|\sum_{\ell\in[L/2,L]}\chi(\ell)\right|^2\left|\sum_{u\le h}^{\#}\chi(u)\right|$$

  where $\Sigma^{\sharp}$ indicates that the summation over square-free numbers.
- Use a version of the *Burgess* bound over square-free numbers due to *Munsch and Trudgian* (**2017**) to estimate the sum over u.
- Use the orthogonality of characters to bound the remaining sum $\sum_{\chi\neq\chi_0}\left|\sum_{\ell\in[L/2,L]}\chi(\ell)\right|^2 \le \sum_{\chi}\left|\sum_{\ell\in[L/2,L]}\chi(\ell)\right|^2 \le pL.$

Methods: Large α; e.g., $\alpha = 1$

I. Preliminary transformations

- Use inclusion/exclusion to reduce $\ell_1\ell_2 u \equiv a \bmod p$ with a square-free $u \le h$ to several congruences

$$\ell_1\ell_2 u d^2 \equiv a \bmod p, \quad \ell_1, \ell_2 \in [L/2, L],\ 1 \le u \le h/d^2,$$

  where u is arbitrary, and $d = 1, 2, \ldots$.
- Fix parameters $D < E$ and split the value of d into three ranges

  Small $d < D$, *Medium* $D \le d < E$, *Large* $d \ge E$,
- We want
  - An asymptotic formula for the contribution from *small* $d < D$.
  - Upper bounds for the contributions from *medium* $D \le d < E$ and *large* $d \ge E$.

II. We treat *small* $d < D$ "individually":

- fix d and treat this congruence as a question about reciprocals $\overline{d}^2\overline{\ell}_1\overline{\ell}_2$ in a short interval $[1, h/d^2]$, $\Longleftrightarrow$ *A uniformity of distribution question.*
- To control the distribution, use bounds of double Kloosterman sums

$$\sum_{\ell_1,\ell_2 \in [L/2,L], \text{ primes}} \mathbf{e}_p\left(k\overline{\ell}_1\overline{\ell}_2\right), \qquad k = 1, 2, \ldots,$$

with products of reciprocals of two primes ℓ_1, ℓ_2 due to

- *Garaev* (**2010**) (for all primes p)
- *Irving* (**2014**) (for almost all primes $p \in [Q, 2Q]$);

- Combine this with the *Erdős–Turàn* inequality linking the uniformity of distribution to exponential sums.

III. We bundle *medium* $D \le d < E$ together in dyadic intervals $[F, 2F]$:

- We need to estimate

$$T = \#\{d \in [F, 2F] : \ \overline{d}^2 \equiv bv \bmod p, \ 1 \le v \le V\},$$

where $V = L^2 h/F^2$ (coming from the bound on $\ell_1 \ell_2 u$ with $\ell_1, \ell_2 \in [L/2, L]$, $1 \le u \le h/d^2$) and $b = \overline{a}$.

- Observe that

$$T^2 \le \#\{d_1, d_2 \in [F, 2F] : \ \overline{d}_1^2 + \overline{d}_2^2 \equiv bv \bmod p, \ 1 \le v \le 2V\}.$$

- By the Cauchy inequality, we deduce

$$T^4 \ll V \# \left\{ d_1, d_2, d_3, d_4 \in [F, 2F] : \ \overline{d}_1^2 + \overline{d}_2^2 \equiv \overline{d}_3^2 + \overline{d}_4^2 \bmod p \right\}.$$

- The above congruence was studied by
  - by *Nunes* (**2017**), "individually' for every p,
  - by *Fouvry & Shparlinski* (**2010**), "on average" over $p \in [Q, 2Q]$.

IV. We treat *large* $d \ge E$ 'individually" again:

- We write

$$\ell_1\ell_2 u d^2 \equiv a \bmod p \quad \text{as} \qquad \ell_1\ell_2 u \equiv a\overline{d}^2 \bmod p.$$

- Since $1 \le \ell_1\ell_2 u \le L^2 h/d^2$ we see that $\ell_1\ell_2 u = b + kp$ for some fixed $b \in [1, p-1]$ (when d is fixed) and non-negative

$$k \le \frac{L^2 h}{d^2 p}.$$

- When k is fixed (in at most $L^2 h d^{-2} p^{-1} + 1$ ways) for each of them ℓ_1 and ℓ_2 can take at most $O(\log p)$ possible values among the divisors of $b + kp \ge 1$, and then u is uniquely defined.

V. Put everything together and optimise D and E.

Where are we?

Booker & Pomerance (2017)

- *Theorem:* *We have* $M(p) = p^{O(\log p)}$.
- *Conjecture:* *We have* $M(p) = p^{O(1)}$.

Munsch & Shparlinski (2017)

- *Theorem:* *We have* $M(p) \le p^{3/2+o(1)}$.
- *Conjecture:* *We have* $M(p) = p^{1+o(1)}$.

Booker (2017)

Lower bound: *We have*

$$M(p) \gg p\frac{\log p}{\log\log p}.$$

Booker's argument:

For an integer parameter K we choose a prime p such that

$$kp + 4 \equiv 0 \bmod p_{k+1}^2, \qquad k = 1, ..., K,$$

where p_k denotes the kth prime.

Clearly, the smallest positive square-free $s \equiv 4 \bmod p$ satisfies

$$s > Kp.$$

By the Chinese Remainder Theorem and *Linnik's* theorem

$$p = \left(\prod_{k=2}^{K} p_{k+1}^2 \right)^{O(1)} = \exp\left(O(K \log K)\right) \quad \Longrightarrow \quad K \gg \frac{\log p}{\log \log p}$$

Can we do better?

Further Applications

Munsch, Shparlinski & Yau (**2019**): Extending the above methods to get tight lower bounds of the form

$$\psi^\sharp(x, y; p, a) \geq x/p^{1+o(1)}$$

for $x = p^{\alpha+o(1)}$ and $y = p^{\beta+o(1)}$ in some ranges of α and β, where

$$\psi^\sharp(x, y; p, a) = \#\{n \leq x : n \equiv a \bmod p, \text{ square-free \& } y\text{-smooth}\}.$$

This improves *Balog & Pomerance* (**1992**) in some ranges

Square-full numbers in arithmetic progressions

Let $F(a,p)$ be the smallest positive squarefull number $n \equiv a \bmod p$ (i.e. $\ell \,|\, n \Longrightarrow \ell^2 \,|\, n$ for any prime ℓ). Clearly

- $F(a,p) \le (p-1)^2/4$ if a is a quadratic residue modulo p.
- $F(a,p) \le n_p^3(p-1)^2/4$ if a is a quadratic non-residue modulo p, where n_p denotes the least quadratic non-residue modulo p.

Munsch & Shparlinski & Yau (2018)

For all but $o(p)$ quadratic non-residues $a \in [0, p-1]$, we have

$$p^2 n_p f(p) \ll F(a,p) \le p^{2+1/(4e^{1/2})+o(1)}$$

for any function $f(p)$ such that $f(p) \to 0$ as $p \to \infty$.

Remark

We do not know how to substitute $p^{1/(4e^{1/2})}$ with n_p

The **proof** is based on

- *Banks & Garaev & Heath-Brown & Shparlinski* (**2008**):
  There is a positive proportion of quadratic non-residues in the *Burgess* interval $[1, p^{1/(4e^{1/2})+\varepsilon}]$.
- *Ayyad & Cochrane & Zheng* (**1996**):
  A tight bound on the 4th moment of short character sums

$$\sum_{\substack{\chi \bmod p \\ \chi \neq \chi_0}} \left| \sum_{1 \le n \le K} \chi(n) \right|^4 \le K^2 p^{1+o(1)}.$$

Question: What is the true order of $F(a,p)$? Is it $p^{2+o(1)}$?

. . . perhaps, but we have no nontrivial upper bounds, besides the obvious $F(a,p) \le n_p^3 (p-1)^2/4$

Thank you!!