On the stochasticity parameter of quadratic residues

Mikhail Gabdullin

Quebec, 12th of July

The main definition

Let U be a subset of $\mathbb{Z}_M$ and

$$U = \{0 \le u_1 < u_2 < \ldots < u_k < M\}.$$

Let also $u_{k+1} = M + u_1$. V.I.Arnold defined ***the stochaticity parameter*** of the set U to be the quantity

$$S(U) = \sum_{i=1}^{k} (u_{i+1} - u_i)^2.$$

The stochasticity parameter of a random set

Too small or too large values of $S(U)$ indicate that U is «far» from a random set: $S(A)$ is minimal when the points of U are equidistributed and $S(U)$ is maximal when U is an interval.

One can find the mean value $s(k)$ of $S(U)$ over all k-element subsets of $\mathbb{Z}_M$.

Proposition 1. *We have*

$$s(k) = M\frac{2M-k+1}{k+1} .$$

$M = p$

Let R be the set of quadratic residues modulo p. A special case of result of M.Z.Garaev, S.V.Konyagin and Yu.V.Malykhin is the following.

Theorem A. *Let $M = p$ be a prime. Then*

$$S(R) = s(|R|)(1 + o(1)), \quad p \to \infty.$$

So we can say that the set of quadratic residues behave like a random set (of the same size) with respect to the stochasticity parameter.

$M = Ap_1 \dots p_t$

We study the stochasticity parameter of the set R of quadratic residues modulo M of the form

$$M = Am, \tag{1}$$

where $(A, m) = 1$, $m = p_1 \dots p_t$ and p_j are prime numbers such that $p_t > \dots > p_1 \gg_{A,t} 1$.

The main result

Our main result is the following.

Theorem 1. *Let M be of the form (1), where $A \geq 2$. Then*

$$S(R) = m2^{t+1}A^2|R_A|^{-1} - A^2|R_A|^{-1}m + O_A(m2^{-t}).$$

The main result

Our main result is the following.

Theorem 1. *Let M be of the form (1), where $A \geq 2$. Then*

$$S(R) = m2^{t+1}A^2|R_A|^{-1} - A^2|R_A|^{-1}m + O_A(m2^{-t}).$$

On the other hand, for these modulus M Proposition 1 gives us

$$s(|R|) = m2^{t+1}A^2|R_A|^{-1} - Am + O_A(mp_1^{-0.98})$$

and we see that $S(R) < s(|R|)$ for $A \geq 2$ and large t.

Another result: $M = Ap$

Also we can write the asymptotic of $S(R)$ for the case where $t = 1$.

Theorem 2. *Let $M = Ap$. Then*

$$S(R) = 2f_A(0.5)p + O_A(p^{1-1/18})$$

where f_A is a function determined by the number A.

Another result: $M = Ap$

Also we can write the asymptotic of $S(R)$ for the case where $t = 1$.

Theorem 2. *Let $M = Ap$. Then*

$$S(R) = 2f_A(0.5)p + O_A(p^{1-1/18}),$$

where f_A is a function determined by the number A.

On the other hand, for these modulus M Proposition 1 gives us

$$s(|R|) = \left(\frac{4A^2}{|R_A|} - A\right)p + O_A(p^{0.02}).$$

First values of A for which $S(R) > s(|R|)$ are
$89, 109, 178, 197, 218, 233.$

Corollaries

Corollary 1. *For the modulus M of the form (1) with $A \geq 2$ and large t we have*

$$S(R) < s(|R|).$$

Corollary 2. *We have*

$$\underline{\lim}_{M\to\infty} \frac{S(R)}{s(|R|)} < 1 < \overline{\lim}_{M\to\infty} \frac{S(R)}{s(|R|)}.$$

Hypothesis

Hypothesis. *For almost all modulus M we have*

$$S(R) < s(|R|).$$

Theorems 1 and 2: method of the proof

We can write

$$S(R) = \sum_{l \geq 1} N_l l^2,$$

where

$$N_l = \#\{x \in \mathbb{Z}_M : x, x+l \in R, x+1, \ldots, x+l-1 \notin R\}.$$

For small l we can find the asymptotics for N_l using a simple version of sieve method and estimates of character sums. Large values of l give negligible contribution to the sum $\sum_l N_l l^2$.

In fact

In fact, we prove that

$$S(R) = m2^t f_A(y) + O(m2^{-t}),$$

where $y = 1 - 2^{-t}$ and f_A is a function determined by the number A.

Let us have a look on the functions f_A for small A.

f_A

$$f_1(y) = 1 + y$$

$$f_3(y) = \frac{5y^2 + 8y + 5}{1 + y}$$

$$f_4(y) = \frac{10y^2 + 12y + 10}{1 + y}$$

$$f_5(y) = \frac{11y^3 + 14y^2 + 14y + 11}{1 + y + y^2}$$

$$f_7(y) = \frac{15y^4 + 24y^3 + 20y^2 + 24y + 15}{1 + y + y^2 + y^3}$$

$$f_8(y) = \frac{26y^3 + 38y^2 + 38y + 26}{1 + y + y^2}$$

f_A

$$f_{11}(y) = \frac{27y^6 + 38y^5 + 34y^4 + 44y^3 + 34y^2 + 38y + 27}{1 + y + y^2 + y^3 + y^4 + y^5}$$

$$f_{13}(y) = \frac{37y^7 + 38y^6 + 54y^5 + 40y^4 + 40y^3 + 54y^2 + 38y + 37}{1 + y + y^2 + y^3 + y^4 + y^5 + y^6}$$

The bottom line

We found an algorithm for calculating the function f_A and proved that

$$f_A(1) = \frac{2A^2}{|R_A|}, \quad f_A'(1) = \frac{A^2}{|R_A|}.$$

Hence

$$m2^t f_A(y) = m2^{t+1} A^2 |R_A|^{-1} - mA^2 |R_A|^{-1} + \frac{1}{2} f_A''(\theta_t) m2^{-t}.$$

To prove Theorem 1 it remains to show that $f_A''(y) \ll A^{O(1)}$.

THANK YOU FOR YOUR ATTENTION !