THE SEQUENCE OF LARGEST QUADRATIC RESIDUES MODULO THE PRIMES

(Last revision: November 2004)

Ferenc Adorján
Zápor u. 2.
H-2040 Budaörs, HUNGARY
(Email: fadorjan@freemail.hu)

Abstract. A numerical exploration of the behavior of the sequence of largest quadratic residues (and also of the largest quadratic non-residues) modulo the primes has revealed some unexpected findings. Some of the findings are proven but several intriguing and surprising observations, conjectures are also presented. These features shed light on the intricate relation between the primes and the quadratic residues.

2000 Mathematics Subject Classification: 11A15, 11A41, 11B05, 11B99

1. Introduction

The realm of quadratic residues is famous of offering special attractions and now the author is trying to escort the reader to a niche in the neighborhood of the quadratic reciprocity low, which is seemingly unexplored so far though it is hiding a few remarkable gems. Let us see first a sequence having a simple definition and showing – by a superficial inspection – not too many interesting peculiarities. The sequence of largest (in the sense of not exceeding the moduli) quadratic residues modulo the subsequent primes (see A88190 in [2]) starts as (100 terms):

$\mathbf{A}$ =[1, 1, 4, 4, 9, 12, 16, 17, 18, 28, 28, 36, 40, 41, 42, 52, 57, 60, 65, 64, 72, 76, 81, 88, 96, 100, 100, 105, 108, 112, 124, 129, 136, 137, 148, 148, 156, 161, 162, 172, 177, 180, 184, 192, 196, 196, 209, 220, 225, 228, 232, 232, 240, 249, 256, 258, 268, 268, 276, 280, 281, 292, 305, 300, 312, 316, 329, 336, 345, 348, 352, 352, 364, 372, 377, 378, 388, 396, 400, 408, 417, 420, 424, 432, 436, 441, 448, 456, 460, 460, 465, 466, 484, 489, 497, 498, 508, 520, 521, 540,...]

At a first glance it looks semi-monotonic (in the $a_i \leq a_{i+1}$ sense) but around the 20^{th} term one can notice that the members ...65,64,72,... violate also the semi-monotonic behavior. Later on there occur similar "glitches" (e. g. ...305,300,312,...). If we regard all the cases where $a_{i+1} \leq a_i$ (i. e. $\mathbf{A}$ is non monotonic), then we can find quite a few such places. We will see below that these non monotonic places do not occur completely at random, characteristic behavior with specific features can be observed at these indices.

In the first sub-chapter of Chapter 3 the characteristics of $\mathbf{A}$ and some related sequences are described, in the second sub-chapter we deal with the sequence of largest quadratic non-residues of $\mathbf{P}$ – which is denoted by $\widetilde{\mathbf{A}}$

–, where several specific consequences of the quadratic reciprocity theorem are demonstrated. In the third sub-chapter we show that $\mathbf{A}$ and $\widetilde{\mathbf{A}}$ can be merged in a logical way into a single sequence which maintains most of the features of its parents, though also exhibits some original features.

2. Notations, definitions

Bold capitals, e. g. $\mathbf{X}$, are used to denote an infinite integer sequence. The corresponding lower case symbol with a lower index x_i, denotes the i-th member of $\mathbf{X}$.

$\mathbf{P}$ denotes the sequence of primes.

In general, any lower case symbol stands for an integer.

The notation $|a|_q$ is used for *the least absolute residue class* congruent $a (\mathrm{mod}\, q)$, i. e. $-q+1 \leq |a|_q \leq q-1$.

$\mathbf{C} = \mathbf{A} \star \mathbf{B}$ is a sequence with members $c_i = a_i \star b_i$, where $\star \in \{+, -, \cdot\}$. Clearly, by these operations the set of integer sequences form a ring.

$\mathbf{X}_k$ (where $k > 0$) is the "k-th truncation" of sequence $\mathbf{X}$, i. e. $x_{k,i} = x_{i+k}$.

The operator $\widehat{\mathbf{Q}}(q) = z$ is the "*largest true quadratic residue modulo q*", i. e. $z = \max\{r < q \,|\, (r/q) = 1\}$, where (r/q) is the Jacobi symbol.

Thus formally the sequence $\mathbf{A}$ above is defined by its members as $a_i = \widehat{\mathbf{Q}}(p_i)$, or we may also use the $\mathbf{A} = \widehat{\mathbf{Q}}(\mathbf{P})$ notation. Note that this way we introduced a well defined transformation for an arbitrary positive sequence.

3. Looking deeper into...

Since, due to the Gauss's criterion (see e. g. [4] at p. 285), it is rather easy to calculate the sequence $\mathbf{A}$ above (e. g. by a program similar to what is given in the Appendix), the author calculated the sequence (as well as all the other related sequences, we discuss later) up to the index of 10^5. This size is quite enough to make serious *inspections* which yielded a few interesting *observations*, as well as it is enough to regard most of the observations as *conjectures*, proposing the observed properties being generally valid.

3.1. The sequence of largest quadratic residues of the primes.

Let us concentrate first at the "glitches" of $\mathbf{A}$, i. e. where it is non-monotonic. The sequence of those primes p_i for which $\widehat{\mathbf{Q}}(p_i) \leq \widehat{\mathbf{Q}}(p_{i-1})$ ($\mathbf{A}$ is non-monotonic) can be found at A88193 in [2].

Observation 1. One can notice that the relative density of the indices where the "glitches" occur, is almost constant. It is seemingly decreasing rather slowly, perhaps converging asymptotically to some positive value (somewhere below 0.05), though one can not exclude that it converges to zero, or even that the number of non-monotonic positions in $\mathbf{A}$ is finite. The observed behavior within the explored range is demonstrated in Table 1.

Index range	No. of non-monotonic positions
1- 10000	605
10001- 20000	541
20001- 30000	504
30001- 40000	481
40001- 50000	500
50001- 60000	471
60001- 70000	463
70001- 80000	491
80001- 90000	491
90001-100000	470

TABLE 1. The number of non-monotonic points in the sequence $\mathbf{A}$ per 10^4 terms

Observation 2. If we denote the i-th element of the sequence of primes $\mathbf{P}$ by p_i and denote the corresponding element in $\mathbf{A}$ by a_i, then for $i > 3$, whenever $a_i \leq a_{i-1}$then $p_i \equiv 7 \pmod 8$ (or $|p_i|_8 = -1$). Additionally, it is also observable that if $i > 4$ then $p_i \not\equiv 2 \pmod 5$. Note that the reverse of these combined modal conditions does not hold!

Observation 3. It is related to the difference sequence $\mathbf{B} = \mathbf{P} - \mathbf{A}$, i. e. the sequence of $b_i = p_i - a_i$. The initial one-hundred members of $\mathbf{B}$ (see also A88192 in [2]) are as follows:

$\mathbf{B}$ =[1, 2, 1, 3, 2, 1, 1, 2, 5, 1, 3, 1, 1, 2, 5, 1, 2, 1, 2, 7, 1, 3, 2, 1, 1, 1, 3, 2, 1, 1, 3, 2, 1, 2, 1, 3, 1, 2, 5, 1, 2, 1, 7, 1, 1, 3, 2, 3, 2, 1, 1, 7, 1, 2, 1, 5, 1, 3, 1, 1, 2, 1, 2, 11, 1, 1, 2, 1, 2, 1, 1, 7, 3, 1, 2, 5, 1, 1, 1, 1, 2, 1, 7, 1, 3, 2, 1, 1, 1, 3, 2, 13, 3, 2, 2, 5, 1, 1, 2, 1,...]

One can notice immediately that the members of this sequence are *either* 1 *or a prime number* (which is also proven below). Also note, that in the *ring of integer sequences* (corresponding to the definition of operations in Chapter 2) the sequences, which are built from primes and 1, are analogues of the "primes" among the naturals, thus $\mathbf{B}$ is a "prime" sequence.

Observation 4. For $i > 1$, $b_i = 1$ if and only if $|p_i|_4 = 1$. This is actually a fact, since it is identical to the well known $(-1/p) = (-1)^{(p-1)/2}$ quadratic reciprocity relation [1] (where (x/p) is the Legendre symbol). This also means that asymptotically one half of the terms of $\mathbf{B} = \mathbf{P} - \mathbf{A}$ are units. We will call later these *trivial members*.

Observation 5. Concerning the *non-trivial members* b_i of $\mathbf{B} = \mathbf{P} - \mathbf{A}$, $b_i \in \mathbf{P}$ *if and only if* $p_i \equiv 3 \pmod 4$. The "only if" follows from the fact presented at Observation 4, while the "if" side is also a provable fact:

Lemma 3.1. *For every* $p \in \mathbf{P}$ *such that* $p \equiv 3 \pmod 4$, $\exists\, m$ *prime,* $m < p$, *such that* $(-m/p) = 1$, *while* $\forall r$ *such that* $0 < r < m$, $(-r/p) = -1$.

Proof. Since $p \equiv 3 \pmod 4$, therefore due to the Euler's criterion $(-1/p) = (-1)^{(p-1)/2} = -1$. Obviously, there exists such $0 < m < p$, that $(-m/p) = 1$,

Index	prime	p in $\mathbf{B}$
2	3	2
4	7	3
9	23	5
20	71	7
64	311	11
92	479	13
246	1559	17
752	5711	19
1289	10559	23
2084	18191	29
3383	31391	31
31284	366791	43
35558	422231	37
56644	701399	41

TABLE 2. The first occurrence of different primes in the sequence $\mathbf{B}$

therefore let us assume that m is the least such value. We need to see that m is prime. Since $(-m/p) = (-1/p) \cdot (m/p) = 1$, hence $(m/p) = -1$.

Let us assume now that m is composite. Since $(m/p) = -1$, therefore $\exists p' \in \mathbf{P}$ factor of m, such that $(p'/p) = -1$. Obviously $p' < m$, therefore m is not the least quadratic non-residue of p, i. e. $q = p - m$ is not the largest quadratic residue. Hence, m must be prime. □

Note that in the 10^5 terms, every prime number $p \leq 43$ turns up in $\mathbf{B}$, though not in a monotonic order. The first occurrence of different primes in $\mathbf{B}$ according to the index of primes is shown in Table 2.

Observation 6. A strange correlation can be observed between the members of the sequence $\mathbf{B}$ and of $\mathbf{D} = \mathbf{A}_1 - \mathbf{A}$, the first difference sequence of $\mathbf{A}$, where the members of $\mathbf{D}$ are $d_i = a_{i+1} - a_i$ (see also A88191 in [2]). The observation is that when i is such that $d_i \leq 0$ (i. e. $\mathbf{A}$ is non-monotonic) then if $b_{i+1} = 3 \Rightarrow d_i = 0$, whereas if $d_i = -1 \Rightarrow b_{i+1} = 7$ (cf. sequences A88194 and A88195 in [2]).

Observation 7. This also relates to the indices where $\mathbf{A}$ is non-monotonic (i. e. at index i, such that $d_i \leq 0$). For every such an i, it holds that $b_{i+1} > -d_i$. This can be proven easily:

Lemma 3.2. *If $a_i \leq a_{i-1}$ then $b_i > -d_{i-1}$, where $\mathbf{A} = \widehat{\mathbf{Q}}(\mathbf{P})$, $\mathbf{B} = \mathbf{P} - \mathbf{A}$ and $\mathbf{D} = \mathbf{A}_1 - \mathbf{A}$.*

Proof. Since $\forall i > 1, a_i < p_i$ and also $p_i > p_{i-1}+1$, now $a_i < a_{i-1} < p_{i-1}$ and also $p_i - a_i > p_{i-1} - a_{i-1} + 1$, i. e.: $b_i > b_{i-1} + 1$. Hence $-d_{i-1} = a_{i-1} - a_i = p_{i-1} - b_{i-1} - p_i + b_i < p_i - 1 - b_{i-1} - p_i + b_i = b_i - (b_{i-1} + 1) < b_i$. □

Corollary 3.3. *When $d_{i-1} < 0$ then $-d_{i-1} < b_i - (b_{i-1} + 1)$ and also $b_i > b_{i-1} + 1$.*

Index i		p_i ($\lvert p_i \rvert_4$)	a_i
1	15196	166301 (1)	166300
	15197	166303 (-1)	166300
	15198	166319 (-1)	166296
	15199	166349 (1)	166348
2	28215	327581 (1)	327580
	28216	327583 (-1)	327580
	28217	327599 (-1)	327580
	28218	327619 (-1)	327617
3	34084	403061 (1)	403060
	34085	403063 (-1)	403060
	34086	403079 (-1)	403056
	34087	403097 (1)	403096
4	45373	550661 (1)	550660
	45374	550663 (-1)	550660
	45375	550679 (-1)	550656
	45376	550691 (-1)	550689
5	48868	596861 (1)	596860
	48869	596863 (-1)	596860
	48870	596879 (-1)	596856
	48871	596899 (-1)	596897
6	66945	840821 (1)	840820
	66946	840823 (-1)	840820
	66947	840839 (-1)	840802
	66948	840841 (1)	840840
7	79004	1006781 (1)	1006780
	79005	1006783 (-1)	1006780
	79006	1006799 (-1)	1006762
	79007	1006847 (-1)	1006842

TABLE 3. The first 7 "twin" non-monotonic locations in the sequence **A**

Observation 8. At a first glance, the indices where **A** is non-monotonic seem to be "apart" from each other, i. e. if $a_i \leq a_{i-1} \Rightarrow a_{i+1} > a_i$. However, by checking this illusion, it was found that the indices $i = 15197$ and $i+1 = 15198$ are the first two consecutive ones where the d_i members of **D** (the difference sequence of **A**) are non-positive $(...0, -4, ...)$. It is also notable that in every case ($i \leq 10^5$) when such "twin glitches" were observed, the lower member of the two consecutive non-positive members of **D** is 0 and the element in **B** prior to the 0 element in **D** is a trivial (unit) element. By mathematical notations: if $a_i \leq a_{i-1} \leq a_{i-2}$ then $d_{i-1} = 0$ (i. e. $a_{i-1} = a_{i-2}$) and also $p_{i-2} - a_{i-2} = b_{i-2} = 1$.

Remark. The density of these "twin glitches" is fairly low: up to the index of 10^5 one can find only 7 such positions (see Table 3) and there is only a single case (at $i = 28215$) where there are two consecutive 0-s in the sequence **D** (corresponding to 3 identical terms in **A**).

Observation 9. The most remarkable fact which can be noticed in the middle column of Table 3 is that the first three subsequent primes in each of the 7 groups are such that taken them modulo 120, we get $\{101, 103, 119\}$. By mathematical notation: if i is such that $\widehat{\mathbf{Q}}(p_{i+2}) \leq \widehat{\mathbf{Q}}(p_{i+1}) \leq \widehat{\mathbf{Q}}(p_i)$ (i. e.: $a_{i+2} \leq a_{i+1} \leq a_i$) then $\{p_i, p_{i+1}, p_{i+2}\} \equiv \{101, 103, 119\} \pmod{120}$. Note that there exist 76 triplets with such modular property (mod 120) among the first 10^5 primes but only 7 of them have this particular property. Though the number of observed cases is fairly low, still this observation can be proposed as a conjecture, due to its beauty.

3.2. **Sequence of largest quadratic non-residues of primes.** By exploring the behavior of *largest quadratic non-residues* (the numbers which are not quadratic residues) of the sequence of primes $\mathbf{P}$ (A88196 in [2]), one can see a qualitatively very similar behavior as presented for the largest quadratic residues, hence the following observations are rather symmetric to the preceeding ones:

Observation 10. The sequence of *largest quadratic non-residues* of primes is also "almost" monotonic:

$\widetilde{\mathbf{A}}$ =[1, 2, 3, 6, 10, 11, 14, 18, 22, 27, 30, 35, 38, 42, 46, 51, 58, 59, 66, 70, 68, 78, 82, 86, 92, 99, 102, 106, 107, 110, 126, 130, 134, 138, 147, 150, 155, 162, 166, 171, 178, 179, 190, 188, 195, 198, 210, 222, 226, 227, 230, 238, 234, 250, 254, 262, 267, 270, 275, 278, 282, 291, 306, 310, 308, 315, 330, 332, 346, 347, 350, 358, 366, 371, 378, 382, 387, 395, 398, 402, 418, 419, 430, 428, 438, 442, 446, 452, 459, 462, 466, 478, 486, 490, 498, 502, 507, 518, 522, 539,...]

Calculating the terms of the sequence $\widetilde{\mathbf{A}}$ up to 10^5 terms, it was possible to determine how the density of non-monotonic "glitches" varies (see table 4).

Range	Occurrence of non-monotonic positions
1- 10000	442
10001- 20000	398
20001- 30000	393
30001- 40000	360
40001- 50000	375
50001- 60000	384
60001- 70000	382
70001- 80000	350
80001- 90000	369
90001-100000	344

TABLE 4. The number of non-monotonic positions in the sequence $\widetilde{\mathbf{A}}$

Observation 11. Denoting the i-th element of the sequence of primes $\mathbf{P}$ by p_i and the corresponding element in $\widetilde{\mathbf{A}}$ by $\widetilde{a}_i$ then if $\widetilde{a}_i \leq \widetilde{a}_{i-1}$then $p_i \equiv 1 \pmod 8$. This is a neat *mirror relation* to Observation 2 (see also A88199 in[2]).

Observation 12. This relates to the difference sequence $\widetilde{\mathbf{B}} = \mathbf{P} - \widetilde{\mathbf{A}}$, having the members $\widetilde{b}_i = p_i - \widetilde{a}_i$ (A88297 in [2]). The first hundred members of $\widetilde{\mathbf{B}}$ are as follows:

$\widetilde{\mathbf{B}}$ =[1, 1, 2, 1, 1, 2, 3, 1, 1, 2, 1, 2, 3, 1, 1, 2, 1, 2, 1, 1, 5, 1, 1, 3, 5, 2, 1, 1, 2, 3, 1, 1, 3, 1, 2, 1, 2, 1, 1, 2, 1, 2, 1, 5, 2, 1, 1, 1, 1, 2, 3, 1, 7, 1, 3, 1, 2, 1, 2, 3, 1, 2, 1, 1, 5, 2, 1, 5, 1, 2, 3, 1, 1, 2, 1, 1, 2, 2, 3, 7, 1, 2, 1, 5, 1, 1, 3, 5, 2, 1, 1, 1, 1, 1, 1, 1, 2, 3, 1, 2,...]

One can notice immediately that the members of this sequence seem to be either one or a prime number.

Observation 13. It is well noticeable that for $i > 1$, $\widetilde{b}_i = 1$ if and only if $p_i \equiv 3 \pmod 4$. Analogously to Observation 4, this fact is also well known, hence it is identical to the $(-1/p) = (-1)^{(p-1)/2}$ quadratic reciprocity relation (where (x/p) is the Legendre symbol). This also means that asymptotically one half of the terms of $\widetilde{\mathbf{B}} = \mathbf{P} - \widetilde{\mathbf{A}}$ are units.

Observation 14. This is also symmetric to Observation 5, i. e. for the members $\widetilde{b}_i$ of $\widetilde{\mathbf{B}} = \mathbf{P} - \widetilde{\mathbf{A}}$, $\widetilde{b}_i \in \mathbf{P}$ if and only if $p_i \equiv 1 \pmod 4$. This is also a provable fact, the proof is quite symmetrical to the proof of Lemma 3.1 and it follows easily from the quadratic reciprocity theorem:

Lemma 3.4. *For every $p \in \mathbf{P}$ such that $p \equiv 1 \pmod 4$, $\exists\, m$ prime, $m < p$, such that $(-m/p) = -1$, while $\forall\, 0 < r < m$, $(-r/p) = 1$.*

Proof. Since $p \equiv 1 \pmod 4$, therefore $(-1/p) = (-1)^{(p-1)/2} = 1$. Obviously, there exists such $m < p$, that $(-m/p) = -1$, therefore let us assume that m is the least such value. We need to see that it is prime. Since $(-m/p) = (-1/p) \cdot (m/p) = -1$, hence $(m/p) = -1$.

Let us assume now that m is composite. Since $(m/p) = -1$, therefore $\exists p' \in \mathbf{P}$ factor of m, such that $(p'/p) = -1$. Obviously $p' < m$, therefore m is not the *least* quadratic non-residue of p, i. e. $q = p - m$ is not the largest quadratic non-residue of p. Hence, m must be prime. □

Observation 15. This relates to a strange correlation between the members of the sequence $\widetilde{\mathbf{B}}$ and of $\widetilde{\mathbf{D}} = \widetilde{\mathbf{A}}_1 - \widetilde{\mathbf{A}}$, the difference sequence of $\widetilde{\mathbf{A}}$, having the members $\widetilde{d}_i = \widetilde{a}_{i+1} - \widetilde{a}_i$ (A88198 in [2]). The observation is that where $\widetilde{d}_i \leq 0$ (i. e. $\widetilde{\mathbf{A}}$ is non-monotonic) then $\widetilde{b}_{i+1} = 5 \Leftrightarrow \widetilde{d}_i = -2$ (cf. sequences A88200 and A88201 in [2]). Note, that unlike Observation 6, this a symmetric (if and only if) relation.

Observation 16. This also relates to the indices where $\widetilde{\mathbf{A}}$ is non-monotonic (i. e. $\widetilde{d}_i \leq 0$). Thus if $\widetilde{d}_i \leq 0$ then $\widetilde{b}_{i+1} > -\widetilde{d}_i$. The an easy proof can be constructed analogously to the one given at Observation 7.

Observation 17. Concerning the sequence $\widetilde{\mathbf{A}}$, it is surprising that – in contrary to what was found for the sequence $\mathbf{A}$ (see Observation 8) – there are *no subsequent indices* below 10^5 where $\widetilde{\mathbf{A}}$ is non-monotonic, i. e. if $\widetilde{a}_i \leq \widetilde{a}_{i-1} \Rightarrow \widetilde{a}_{i+1} > \widetilde{a}_i$ if $i < 10^5$. It is a challenging question whether there exist any "twin glitches" in $\widetilde{\mathbf{A}}$.

Observation 18. This one has no pair in relation to the largest quadratic residues. It was found that at the indices *where* $\widetilde{\mathbf{A}}$ *is non-monotonic the members of the difference sequence* $\widetilde{\mathbf{D}}$ *are always even*, i. e. if $\widetilde{a}_i < \widetilde{a}_{i-1} \Rightarrow \widetilde{a}_{i-1} - \widetilde{a}_i = -\widetilde{d}_{i-1} = 2k$ for some $k \geq 0$.

3.3. **The mixed sequence.** The next twist is based on the fact that about half of the members of both $\mathbf{A}$ and $\widetilde{\mathbf{A}}$ are trivially units (see observations 4 & 13). Also note that where a_i is trivial, there $\widetilde{a}_i$ is non-trivial, and vice-versa. Thus, one can *merge the two sequences* by omitting the trivial unit terms from $\mathbf{A}$ (corresponding to the indices i where $|p_i|_4 = -1$) and substitute them from $\widetilde{\mathbf{A}}$. In other words: if $|p_i|_4 = 1$ then we take the largest quadratic non-residue modulo p_i, otherwise we take the largest quadratic residue modulo p_i. In this manner, we obtain the sequence as follows (A91380 in [2]):

$\overline{\mathbf{A}}$ =[1, 1, 3, 4, 9, 11, 14, 17, 18, 27, 28, 35, 38, 41, 42, 51, 57, 59, 65, 64, 68, 76, 81, 86, 92, 99, 100, 105, 107, 110, 124, 129, 134, 137, 147, 148, 155, 161, 162, 171, 177, 179, 184, 188, 195, 196, 209, 220, 225, 227, 230, 232, 234, 249, 254, 258, 267, 268, 275, 278, 281, 291, 305, 300, 308, 315, 329, 332, 345, 347, 350, 352, 364, 371, 377, 378, 387, 395, 398, 402, 417, 419, 424, 428, 436, 441, 446, 452, 459, 460, 465, 466, 484, 489, 497, 498, 507, 518, 521, 539,...]

Observation 19. We can see that this sequence is qualitatively similar to both $\mathbf{A}$ and $\widetilde{\mathbf{A}}$, hence this is also "almost" monotonic. See Table 5.

Observation 20. Correspondingly to Observations 2 and 11, a very compact form can be written for $i > 1$ members of $\overline{\mathbf{A}}$: if $\overline{a}_i \leq \overline{a}_{i-1}$then $|p_i|_8 = |p_i|_4$.

Analogously to the above, we can define $\overline{\mathbf{B}} = \mathbf{P} - \overline{\mathbf{A}}$ (A91382 in [2]):

$\overline{\mathbf{B}}$ =[1, 2, 2, 3, 2, 2, 3, 2, 5, 2, 3, 2, 3, 2, 5, 2, 2, 2, 2, 7, 5, 3, 2, 3, 5, 2, 3, 2, 2, 3, 3, 2, 3, 2, 2, 3, 2, 2, 5, 2, 2, 2, 7, 5, 2, 3, 2, 3, 2, 2, 3, 7, 7, 2, 3, 5, 2, 3, 2, 3, 2, 2, 2, 11, 5, 2, 2, 5, 2, 2, 3, 7, 3, 2, 2, 5, 2, 2, 3, 7, 2, 2, 7, 5, 3, 2, 3, 5, 2, 3, 2, 13, 3, 2, 2, 5, 2, 3, 2, 2, ...]

Apart from the first term, it is obvious due to the way $\overline{\mathbf{A}}$ was constructed, that $\overline{\mathbf{B}}$ consists of prime numbers only (for $i > 1$). Since $\overline{\mathbf{B}}$ can be created from $\mathbf{B}$ and $\widetilde{\mathbf{B}}$ by merging these two, such a way that if $b_i > 1$, the i-th member of $\overline{\mathbf{B}}$ is b_i, otherwise it is $\widetilde{b}_i$. Therefore, the Lemmas 3.1 and 3.4 are automatically valid for $\overline{\mathbf{B}}$. This is formulated in a very compact way in Theorem 3.5. Note, that the sequence $\overline{\mathbf{B}}$ is identical (apart from its first term) to the sequence which is defined as "the smallest positive quadratic non-residue modulo p_i" which can be found at [3]. This identity is obvious from the proofs given for the Lemmas 3.1 and 3.4.

Theorem 3.5. *For every odd* $p \in \mathbf{P}$, $\exists\, m \in \mathbf{P}$, $m < p$, *such that* $(-m/p) = -|p|_4$ *while* $\forall\, 0 < r < m$, $(-r/p) = |p|_4$.

A basically equivalent form: *For every* $p \in \mathbf{P}$, $\exists\, m \in \mathbf{P}$, $m < p$, *such that* $(m/p) = -1$ *while* $\forall\, 0 < r < m$, $(r/p) = 1$.

Proof. It follows from Lemmas 3.1 and 3.4 and as such, it is a consequence of the Quadratic Reciprocity Theorem. □

Range	No. of non-monotonic positions		
	at LQR	at LQnR	overall
1- 10000	180	237	417
10001- 20000	182	223	405
20001- 30000	170	214	384
30001- 40000	165	204	369
40001- 50000	157	200	357
50001- 60000	155	200	355
60001- 70000	139	213	352
70001- 80000	152	196	348
80001- 90000	142	195	327
90001-100000	133	192	325

TABLE 5. The number of non-monotonic positions in the sequence $\overline{\mathbf{A}}$

Remark 3.6. Thus, if $x \in \overline{\mathbf{B}}_1$ then $x \in \mathbf{P}$. But is it also true that if $x \in \mathbf{P}$ then $x \in \overline{\mathbf{B}}$? It seems a very hard question, whether every prime is present in $\overline{\mathbf{B}}$ or some of them never show up. However, it is a great temptation to conjecture that every prime is present in $\overline{\mathbf{B}}$.

The distribution of non-monotonic positions in the mixed sequence is demonstrated in Table 5. It is surprising that the number of non-monotonic points at largest quadratic residues (LQR) seems to be systematically lower compared to the number of non-monotonic points at largest quadratic non-residues (LQnR). This is even more surprising if one compares this finding with the data in Tables 1 and 4, showing larger number of non-monotonic points in the sequence $\mathbf{A}$ than in $\widetilde{\mathbf{A}}$. This effect may easily be caused only by the relatively small number of observed terms, since it is known that there are several other features related to the sequence of primes which show a slight asymmetry by observing several millions of terms, though the symmetry is proven asymptotically. Note that most of the non-monotonic positions both in $\mathbf{A}$ and in $\widetilde{\mathbf{A}}$ are such that either a_i or $a_{i+1}$is trivial, therefore not present in $\overline{\mathbf{A}}$; hence the majority of the non-monotonic positions in $\overline{\mathbf{A}}$ are at different indices than in $\mathbf{A}$ and in $\widetilde{\mathbf{A}}$.

Also note, that the relation proved in Lemma 3.2 (given after Observation 7) is also easily provable for the mixed sequence $\overline{\mathbf{A}}$, hence the corollary also holds.

It is also worthwhile to look at the "twin" non-monotonic positions in $\overline{\mathbf{A}}$. Up to the index of 10^5 there exist 7 such locations (by accident exactly the same as in $\mathbf{A}$, though at completely different locations).

The qualitative observables are also different (cf. Observation 8 and see Table 6):

- the 0 difference has seemingly no specific role,
- one of the members of each of the twins in $\overline{\mathbf{A}}$ is LQR while the other is LQnR, i. e. if $\overline{a}_i \leq \overline{a}_{i+1} \leq \overline{a}_{i+2}$ then $|p_{i+1}|_4 \cdot |p_{i+2}|_4 = -1$.

Index i		p_i ($\lvert p_i \rvert_4$)	$\overline{a}_i$
1	16877	186469 (1)	186467
	16878	186479 (-1)	186466
	16879	186481 (1)	186462
	16880	186551 (-1)	186544
2	19897	223429 (1)	223427
	19898	223439 (-1)	223426
	19899	223441 (1)	223424
	19900	223463 (-1)	223458
3	35556	422203 (-1)	422201
	35557	422209 (1)	422198
	35558	422231 (-1)	422194
	35559	422239 (1)	422236
4	37082	441829 (1)	441827
	37083	441839 (-1)	441826
	37084	441841 (1)	441824
	37085	441877 (-1)	441875
5	43577	526667 (-1)	526665
	43578	526679 (-1)	526656
	43579	526681 (1)	546652
	43580	526703 (-1)	526698
6	62743	783707 (-1)	783705
	62744	783719 (-1)	783700
	62745	783721 (1)	783698
	62746	783733 (1)	783731
7	74910	950029 (1)	950027
	74911	950039 (-1)	950022
	74912	950041 (1)	950022
	74913	950071 (-1)	950068

TABLE 6. The first 7 "twin" non-monotonic locations in $\overline{\mathbf{A}}$, the "mixed" sequence

- the primes with the same index where $\overline{\mathbf{A}}$ has twin non-monotonic positions are such that in decimal representation the first ends always by 9 while the second by 1,
- the element d_i at the first member of the twins is always larger in absolute value than the at the second member.

4. Conclusion

The behavior of the largest quadratic residues of primes seems to be a relatively unexplored range in the field of elementary number theory. However, as it is illustrated above, there are some unexpected jewels within this range. The author assumes that some of the unproved, presented observations are provable quite easily, though a few seem to be quite hard or are not generally valid. Naturally, the reader could ask many more questions related to the

behavior of the sequences $\mathbf{A}$, $\widetilde{\mathbf{A}}$ and $\overline{\mathbf{A}}$, as well as of their relatives, which may be challenging and intriguing.

A possible way further is to study the general behavior of the transformation $\mathbf{Y} = \widehat{\mathbf{Q}}(\mathbf{X})$. Certainly, it is related to the "density" of $\mathbf{X}$ whether $\mathbf{Y} = \widehat{\mathbf{Q}}(\mathbf{X})$ is monotonic or not. It is rather easy to construct the "densest" sequence having a monotonic $\widehat{\mathbf{Q}}$-transform (it is left to the reader). It is also clear that by skipping a small fraction of the members (though probably an infinite number!?) from the sequence of primes, the remaining sequence will have a monotonic $\widehat{\mathbf{Q}}$-transform.

Appendix:

A PARI/GP [5] code to generate the sequences $\mathbf{A}$, $\widetilde{\mathbf{A}}$ and $\overline{\mathbf{A}}$:

```
{/* Function: mixqr(fl,fr,to).
   If fl=1 then it calculates the largest quadratic residues of primes,
   if fl=-1 then the largest quadratic non-residues, while
   if fl=0 then the largest "mixed" quadratic residues of the sequence of primes
   for the index range of [fr,to].
   If the range (to-fr) < 500, it generates a detailed output,
   otherwise only the non-monotonic points are accounted,
   and the "twin" non-monotonic places are listed. */
   mixqr(fl,fr,to)=local(v=[],d=[],l=[],mp=[],mv=[],md=[],ml=[],j=0,nm=0,nmm=0,nnr=0,nqr=0,n=0);
   for(i=fr,to,k=prime(i)-1;r=-1*(prime(i)%4-2);
   if(fl==0,if(r==1,
   q=kronecker(k,prime(i));while(q>-1,k-=1;q=kronecker(k,prime(i))),
   q=kronecker(k,prime(i));while(q<1,k-=1;q=kronecker(k,prime(i)))),
   q=kronecker(k,prime(i));while(q<>fl,k-=1;q=kronecker(k,prime(i))));
   if((to-fr)<500,print(i" "prime(i)," "k" "prime(i)-k" "k-j" "r" "prime(i)%8);
   v=concat(v,k);l=concat(l,prime(i)-k);if(n>0,d=concat(d,k-j)));n+=1;
   if(k-j<=0, mp=concat(mp,prime(i);if((i-nm)<2,print(i" "prime(i)" "n));nm=i);
   mv=concat(mv,k);ml=concat(ml,prime(i)-k);if(n>1,md=concat(md,k-j));nmm+=1;
   if(r==1,nnr+=1,nqr+=1));
   j=k);
   if((to-fr)<500,print(v);print(d);print(l));
   print(nmm" ",nqr" ",nnr);print(mp);print(mv);print(md);print(ml);
   v=[nmm,nqr,nnr];return(v) }
```

References

[1] H. Cohn: *Advanced number theory*, p. 19, Dover Publishing (1962)

[2] N. J. A. Sloane: *The On-Line Encyclopedia of Integer Sequences* The sequences A88190-A88201 and A91380-A91385 submitted by F. Adorjan, 2003, 2004. http://www.research.att.com/~njas/sequences/index.html

[3] N. J. A. Sloane: *The On-Line Encyclopedia of Integer Sequences* The sequence A53760 submitted by S. Finch, 2000. http://www.research.att.com/~njas/sequences/index.html

[4] I. Stewart, D. Tall: *Algebraic Number Theory and Fermat's Last Theorem* (Third edition) A. K. Peters, Ltd. (2002)

[5] C. Batut et al.: *User's guide to PARI/GP*, http://www.parigp-home.de *and also* ftp://megrez.math.u-bordeaux.fr/pub/pari