1986

Sequences in power residue classes

Duncan A. Buell
University of South Carolina - Columbia, buell@cec.sc.edu

Richard H. Hudson
University of South Carolina - Columbia

Publication Info

Published in *International Journal of Mathematics and Mathematical Sciences*, Volume 9, Issue 2, 1986, pages 261-266.
Buell, D.A. and Hudson, R.H. (1986). Sequences in power residue classes. *International Journal of Mathematics and Mathematical Sciences*, *9*(2), 261-266.

Internat. J. Math. & Math. Sci.
Vol 9 No. 2 (1986) 261-266

SEQUENCES IN POWER RESIDUE CLASSES

DUNCAN A. BUELL

Department of Computer Science
Louisiana State University
Baton Rouge, LA 70803

and

RICHARD H. HUDSON

Department of Mathematics
University of South Carolina
Columbia, SC 29208

(Received June 13, 1985)

ABSTRACT. Using A. Weil's estimates the authors have given bounds for the largest prime P_0 such that all primes $p > P_0$ have sequences of quadratic residues of length m. For $m \leq 8$ the smallest prime having m consecutive quadratic residues is $\equiv 3 \pmod 4$ and $P_0 \equiv 1 \pmod 4$. The reason for this phenomenon is investigated in this paper and the theory developed is used to successfully uncover analogous phenomena for r^{th} power residues, $r \geq 2$, r even.

KEY WORDS AND PHRASES. Sequences of consecutive r^{th} power residues, random sequences of zeros and ones, linear least squares fit.
1980 AMS (MOS) SUBJECT CLASSIFICATIONS. 10A10, 10A15.

1. INTRODUCTION.

In [1] the authors used Weil's estimates [2] to give explicit bounds for the largest prime P_0 such that all primes $p > P_0$ have sequences of quadratic residues of pre-assigned length m. Unexpectedly, the authors discovered that for all $m \leq 8$ the smallest primes having m consecutive quadratic residues are congruent to $3 \pmod r$ and that P_0 is $\equiv 1 \pmod 4$.

In this paper we develop a theory which suggests that primes $\equiv 3 \pmod 4$ can be expected to have a longest sequence of quadratic residues (or non residues) which is, in the mean, approximately one longer that the longest sequence for primes $\equiv 1 \pmod 4$ of comparable size. Data in Table 1 support this theory.

Using our theory we predicted that primes $\equiv 5 \pmod 8$ can be expected to have a longest sequence of quadratic residues which is, in the mean, about 1/2 longer than the longest sequence for primes $\equiv 1 \pmod 8$ of comparable size. This is supported by data in Table 2. In Table 5 we observe that (as a consequence) the smallest primes $\equiv 1 \pmod 4$ having a sequence of $1,2,3,\ldots,10$ consecutive quadratic residues, respectively, are all $\equiv 5 \pmod 8$ rather than $\equiv 1 \pmod 8$.

The data in Tables 3 and 4 support our theory regarding the approximate magnitude of the mean excesses in the lengths of the longest r^{th} power residue sequences, $r \geq 2$ and even, for primes $\equiv r+1 \pmod{2r}$ versus the corresponding mean lengths for prime $\equiv 1 \pmod{2r}$; data is supplied for $r = 6,8$.

Additional supporting material can be obtained from the first author in [3] where data for all cosets formed with respect to the subgroup of r^{th} powers (mod p) is presented and the mean value of the longest sequence in any coset is observed to be closely approximated by $\log_r p$ for all integers $r \geq 2$, $70,000 < p < 300,000$; see Table 6.

2. NOTATION.

For each fixed r let $n(p)$ denote the length of the longest sequence of r^{th} power residues modulo the prime p which, as customary, we take to be $\equiv 1 \pmod{r}$. We let $m(\ell)$ be the smallest prime p such that $n(p) = \ell$ and $m(\ell)$ the largest prime such that $n(p) = \ell$.

3. RANDOM SEQUENCES OF ZEROS AND ONES.

Consider all n-character strings of t zeros and $n-t$ ones. For convenience we shall call a substring of ℓ or more consecutive zeros an ℓ-substring. If X is an event which is a function of a variable x and which happens with probability $P(X)$ we shall say that X happens almost surely if $P(X)$ tends to 1 as x tends to infinity.

Let $R(n,\ell,t)$ denote the number of n-character strings with t zeros and $n-t$ ones which do not contain and ℓ-substring.

THEOREM 3.1 For $n \geq t \geq \ell > 0$, we have

(a) $R(n+1,\ell,t) = R(n,\ell,t) + R(n,\ell,t-1) - R(n-\ell,\ell,t-1)$,

(b) $R(n,\ell,t) = \sum_{i \geq 0} (-1)^i \binom{n-t+1}{i} \binom{n-i\ell}{n-t}$.

PROOF. The recursion for part (a) is easy. If we append a "1" to and n-character string with no ℓ-substring then we get an (n+1)-character string with no ℓ-substring, accounting for the addend $R(n,\ell,t)$. If we append a "0" to an n-character string with no ℓ-substring then we get an (n+1)-character string which has no ℓ-substring unless the original string ended with $\ell-1$ zeros, accounting for the second and thrird addends on the right-hand-side of formula (a).

To prove (b) we use the two variable generating function

$$F(x,y) = \sum R(n,\ell,t)\ (x^{n-t})\ (y^t).$$

Using the recursion in (a) and taking into account the "initial conditions" we get

$$F = xF + yF - xy^{\ell}F + 1 - y^{\ell}.$$

Thus

$$F(x,y) = \frac{1-y^{\ell}}{1-x-y+xy^{\ell}} = \frac{G}{1-xG}$$

where $G = G(y) = (1-y^{\ell})/(1-y)$. The remainder of the proof is easily supplied by the reader using simple algebra to extract coefficients.

Let $s(n,\ell,t)$ denote the number of n-character strings with t zeros and $n-t$ other digits, 0 through $r-1$, with no ℓ-substring. We may omit the proof of the following theorem as its proof is entirely similar to the above.

THEOREM 3.2

(a) For $n \geq t \geq \ell \geq 0$ we have

$$s_r(n+1,\ell,t) = (r-1)s_r(n,\ell,t-1) - s_r(n-\ell,\ell,t-\ell).$$

(b) $$s_r(n,\ell,t) = \sum_{i=0} (-1)^i (r-1)^{n-t+1-i} \binom{n-t+1}{i} \binom{n-\ell i}{n-t}$$

Let $v(n)$ denote the length of the longest ℓ-substring and $w(n)$ denote <u>any</u> function such that $w(n)$ tends to infinity as n tends to infinity.

THEOREM 3.3 Consider an arbitrary n-character string having t zeros.

(a) Let X_1 be the event that there exists at least one ℓ-string. Then

$$P(X_1) < n\left(\frac{t}{n}\right)^{\ell}.$$

(b) If $n = rt$ then $v(n) = \log_r(n)+w(n)$ almost surely does not happen.

(c) Let X_2 be the event that there exists no ℓ-substring. Then

$$P(X_2) < \left(\frac{2}{n-t}\right)\left(\frac{n}{t}\right)^{\ell}\left(1 + \frac{(n-t)}{n(t-\ell)}\right)^{\ell}.$$

(d) If $n = rt$ then $v(n) = \log_r n - w(n)$ almost surely happens.

PROOF.

(a) The probability that at least one ℓ-substrings. Thus

$$P(X_1) < (n-\ell+1)\frac{\binom{n-\ell}{t-\ell}}{\frac{n}{t}} = (n-\ell+1)(a_\ell),$$

where

$$a_\ell = \frac{t(t-1)\ldots(t-\ell+1)}{n(n-1)\ldots(n-\ell+1)}.$$

Henceforth, we assume the easy inequality

$$\frac{t-1}{n-1} < \frac{t}{n} \text{ for } n \geq t \geq i > 0,$$

from which it follows that $a_\ell < (t/n)^\ell$ so that $P(X_1) < n(t/n)^\ell$.

(b) Let $n = rt$ and apply part (a). Then

$$P(X_1) < n\left(\frac{t}{n}\right)^{\ell} = n(r^{-\ell}).$$

If $\ell = \log_r(n) + w(n)$, then $r^{-\ell} = r^{-w(n)}/n$. As n tends to infinity, $P(X_1) = r^{-w(n)}$ tends to zero.

(c) Let X be the number of ℓ-substrings. Using an appropriate version of Chebyshev's inequality we have

$$P(X_2) < \frac{E(X^2)}{E^2(X)} - 1.$$

As before, $E(X) = (n-\ell+1)(a_\ell)$. It is not difficult to see that

$$E(X^2)\binom{n}{t} = 2\binom{n-2\ell+2}{2}\binom{n-2\ell}{t-2\ell} + 2\sum_{i=1}^{\ell-1}(n-2\ell+1+i)\binom{n-2\ell+i}{t-2\ell+i} + (n-\ell+1)\binom{n-\ell}{t-\ell}.$$

Then

$$P(X_2) < \frac{2\binom{n-2\ell+2}{2}a_{2\ell} + 2\sum_{i=1}^{\ell-1}(n-2\ell+1+i)a_{2\ell-i} + (n-\ell+1)(a_\ell)}{(n-\ell)a_\ell^2} - 1.$$

Using the aforementioned inequality we have $a_{2\ell} < a_\ell^2$ so that

$$\frac{(n-2\ell+2)(n-2\ell+1)(a_{2\ell})}{(n-\ell+1)a_\ell^2} < 1, \quad \frac{a_{2\ell-i}}{a_\ell^2} < \left(\frac{n-\ell}{t-\ell}\right)^i.$$

Consequently,

$$P(X_2) < \frac{2\binom{n-2\ell+2}{2}a_{2\ell} + 2\sum_{i=1}^{\ell}(n-2\ell+1+i)a_{2\ell-i}}{(n-\ell+1)^2 a_\ell^2} - 1$$

so that

$$P(X_2) = \frac{2\sum_{i=1}^{\ell}(n-2\ell+1+i)a_{2\ell-i}}{(n-\ell+1)^2 a_\ell^2} < \left(\frac{2}{n-\ell+1}\right)\left(\sum_{i=1}^{\ell}\frac{a_{2\ell-i}}{a_\ell^2}\right)$$

or

$$P(X_2) < \left(\frac{2}{n-\ell+1}\right)\sum_{i=1}^{\ell}\left(\frac{n-\ell}{t-\ell}\right)^i = \left(\frac{2}{n-\ell+1}\right)\left(\frac{n-\ell}{t-\ell}\right)^\ell\left(\sum_{i=1}^{\ell}\left(\frac{t-\ell}{n-\ell}\right)^i\right).$$

Summing the geometric series completes the proof of (c).

(d) Let $n = rt$ so that by part (c)

$$P(X_2) < \left(\frac{2r}{n(r-1)}\right)(r^\ell)\left(1 + \frac{\ell(r-1)}{n-r\ell}\right)^\ell$$

Let $\ell = \log_r n - w(n)$. Then there is a constant m such that $\ell < m \log n$ so that

$$\left(1 + \frac{\ell(r-1)}{n-r\ell}\right)^\ell < \exp\left(\frac{\ell^2(r-1)}{n-r\ell}\right) < \exp\left(\frac{m^2\log^2 n}{n-2m\log n}\right).$$

For large n this is easily bounded by 2 so that

$$P(X_2) < \left(\frac{4r}{n(r-1)}\right)(r^\ell) = \left(\frac{4r}{n(r-1)}\right)(r^{\log_r n})r^{-w(n)}$$

$$= \left(\frac{4r}{r-1}\right)r^{-w(n)} \to 0 \quad \text{as} \quad n \to \infty,$$

completing the proof of Theorem 3.3.

4. CONSEQUENCES OF §3.

We can visualize coset membership formed with respect to the subgroup of r^{th} powers (mod p) as a string of digits, each digit from the range 0 to r-1, with 0 corresponding to the r^{th} powers. These strings are clearly not randomly determined. Nonetheless the theory in §3 suggests that to the extent that n(p) can be thought of as a random variable we should expect its mean value to be on the order of $\log_r p$. Specifically, in Table 6 we give coefficients a and b produced by a linear least squares fit of n(p) to $n(p) = m \ln p + b$.

Tables 1 to 6 illustrate the central feature of this note. If r is even and ≥ 2 then we have $(p-1)/2r$ r^{th} powers (and similarly for the other r-1 cosets formed with respect to the subgroup of r^{th} powers (mod p)) in the interval 1 to (p-1)/2 if $p \equiv 1 \pmod{2r}$ and in the interval 1 to p-1 if $p \equiv r+1 \pmod{2r}$. Data in the following tables suggest that mean lengths of n(p) for primes $\equiv r+1 \pmod{2r}$ exceed those for primes $\equiv 1 \pmod{2r}$ by $\ln 2/\ln r$ for r even and ≥ 2. The mean difference of 1, e.g., for r=2 translates into an expected value for n(p) for $p \equiv 3 \pmod 4$ equal to the expected value for N(q) for a prime $\equiv 1 \pmod 4$ approximately twice the size of p.

The theory which allows us to conjecture approximate mean differences in $n(p)$ between the residue classes produces estimates which are startlingly close to actual data given the obvious differences between r^{th} power residue distributions and random character strings. However, our theory represents only a partial first hypothesis, and a superior explanation for the phenomenon described here may well be developed. Nonetheless statistical tests (see [4] for the standard Z-test) provides better than 99% confidence that primes $\equiv 1 \pmod{2r}$ and primes $\equiv r+1 \pmod{2r}$, $r=2,4,6,8$, constitute two entirely different sample populations.

Of course this note raises a number of questions, many very difficult. Even for $r = 2$ it is not at all obvious for large ℓ whether the probability that $m(\ell) \equiv 3 \pmod 4$ and $m(\ell) \equiv 1 \pmod 4$ increases or decreases or even has a limit as ℓ goes to infinity.

5. COMPUTATION. Originally computations were done in VS FORTRAN (IBM's FORTRAN 77) on the IBM 3033N of the System Network Computer Center at Louisianna State University. The computation was redone, also in FORTRAN, on the VAX 11/780 running VMS of the Department of Computer Science at L.S.U. Most of the statistical results were obtained using SAS on the IBM 3033.

Table 1: $r = 2$

	Primes $\equiv 1 \pmod 4$			Primes $\equiv 3 \pmod 4$			Difference in Mean
Range	# p	Mean	Dev.	# p	Mean	Dev.	$\ell n\ r/\ell n\ 2 = 1$
<70000	3449	12.738	2.496	3485	13.809	2.445	1.071
140000	3029	14.938	1.995	3046	16.007	1.905	1.069
210000	2914	15.731	1.969	2883	16.742	1.907	1.011
280000	2790	16.234	1.992	2835	17.245	1.923	1.011
350000	2762	16.566	2.046	2783	17.572	1.946	1.006
420000	2709	16.886	1.982	2704	17.897	1.941	1.011

Table 2: $r = 4$

	Primes $\equiv 1 \pmod 8$			Primes $\equiv 5 \pmod 8$			Difference in Mean
Range	# p	Mean	Dev.	# p	Mean	Dev.	$\ell r/\ell n\ 2 = 0.5$
<70000	1820	6.359	1.438	1860	6.985	1.302	.626
140000	1606	7.545	1.173	1620	8.078	0.959	.533
210000	1549	7.954	1.170	1535	8.506	1.024	.552
280000	1482	8.172	1.083	1508	8.672	0.967	.500

Table 3: $r = 6$

	Primes $\equiv 1 \pmod{12}$			Primes $\equiv 7 \pmod{12}$			Difference in Mean
Range	# p	Mean	Dev.	# p	Mean	Dev.	$\ell n\ r/\ell n\ 2 = .386\ldots$
<70000	1830	4.892	1.073	1851	5.307	1.019	.415
140000	1601	5.737	0.857	1624	6.206	0.794	.469
210000	1537	6.064	0.864	1548	6.438	0.763	.374
280000	1499	6.253	0.822	1480	6.680	0.766	.427

Table 4: $r = 8$

	Primes $\equiv 1 \pmod{16}$			Primes $\equiv 9 \pmod{16}$			Difference in Mean
Range	# p	Mean	Dev.	# p	Mean	Dev.	$\ell n\ r/\ell n\ 2 = .333\ldots$
<70000	909	4.183	1.011	911	4.535	0.821	.352
140000	803	4.923	0.857	803	5.296	0.693	.373
210000	776	5.173	0.776	773	5.542	0.683	.369
280000	739	5.361	0.872	743	5.681	0.730	.320

Table 5: $r = 4$

ℓ	$m(\ell)$	$m(\ell)$	$m(\ell) \pmod 8$	$m(\ell) \pmod 8$
1	5	41	5	1
2	37	1153	5	1
3	29	2689	5	1
4	101	32233	5	1
5	269	103529	5	1
6	389	?	5	?
7	661	?	5	?
8	1301	?	5	?
9	4621	?	5	?
10	4261	?	5	?

Table 6: Regression $n(p) = m\ \ell np + b$
$70000 < p < 300000$

r	m	b	$1/\ell n\ r$
2	1.436	-1.088	1.443
3	0.910	-0.970	0.910
4	0.726	-0.608	0.721
5	0.612	-0.622	0.621

ACKNOWLEDGMENTS. We wish to express sincere thanks to Andrew Thomason, who has declined to accept co-authorship of this paper, for insight, help and particulary for suggestions regarding the theorems in §3.

REFERENCES

1. BUELL, D. A., and HUDSON, R. H., "On Runs of Consecutive Quadratic Residues and and Quadratic Nonresidues", BIT 24 (1984), 243-247.

2. WEIL, A., "Sur les Courbes Algébriques et les Variétes qui s'en Deduisent", Actualites Math. Sci. No. 1041 (Paris, 1945), deuxiéme partie, Section IV.

3. BUELL, D. A., and HUDSON, R. H., "Sequences in Power Residue Classes", L.S.U. Computer Science Technical Report, Baton Rouge, LA.

4. WALPOLE, R. E., Introduction to Statistics, MacMillian, New York, 1968.