MATHEMATICS OF COMPUTATION, VOLUME 25, NUMBER 114, APRIL, 1971

Chains of Quadratic Residues

By Hansraj Gupta

Abstract. The problem considered in this paper is that of finding longest chains of the type: $r_1, r_2, r_3, \cdots, r_m$, for which the $m(m+1)/2$ sums $r_i + r_{i+1} + r_{i+2} + \cdots + r_j$, $1 \leqq i \leqq j \leqq m$, will be distinct quadratic residues of a given prime p.

1. Let p be a fixed prime and R the set of its $(p-1)/2$ quadratic residues. In what follows, r's are elements of R and all sums are reduced modulo p. The problem is to find longest chains of the type:

$$r_1, r_2, r_3, \cdots, r_m, \tag{1}$$

for which the $m(m+1)/2$ sums:

$$\sum_{k=i}^{j} r_k, \qquad 1 \leqq i \leqq j \leqq m, \tag{2}$$

will all be distinct quadratic residues of p. Trivially,

$$(2m+1)^2 \leqq (4p-3). \tag{3}$$

Since for (1) to be a quadratic residue chain, it is necessary and sufficient that

$$rr_1, rr_2, rr_3, \cdots, rr_m, \tag{4}$$

be a quadratic residue chain, we can take $r_1 = 1$ in (1) and this we shall do.

2. A Configuration. Write the quadratic residues of p round the circumference of a circle in order of magnitude. Join r_i and r_j if $r_i + r_j$ is in R.

It is well known that for any r_i, according to whether p is or is not of the form $8t \pm 1$, there are exactly $[(p-7)/4]$ or $[(p-3)/4]$ quadratic residues r of p, for which

$$r_i + r \in R, \qquad r_i \neq r.$$

Hence, each of the residues gets joined to exactly the same number of quadratic residues as any other.

The configuration obtained appears to be of interest. For $p = 19$, we get Figure 1. Here each point gets joined to four of the remaining eight.

It might be noted that for $p = 13$, the configuration consists of two disjoint triangles and one cannot travel from one point to every other by moving along the straight lines joining the points. This situation does not seem to arise for any other value of p.

Received April 16, 1970, revised August 17, 1970.

AMS 1970 *subject classifications.* Primary 10-04, 10A15.

Key words and phrases. Chains of quadratic residues, cycles of quadratic residues, configurations, lengths of chains, reciprocation.

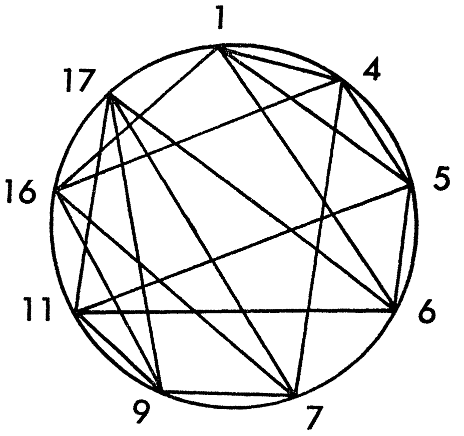

FIGURE 1

3. If r_1, r_2 are taken at random, the probability that $r_1 + r_2$ will belong to R is, in view of the statement in Section 2, about 1/2. If r_1, $r_1 + r_2$, $r_1 + r_2 + r_3$, $r_2 + r_3$ all belong to R, then, since r_1 will have to be joined to r_2 and both $r_1 + r_2$ and r_2 to r_3, I felt that the probability of r_1, r_2, r_3 forming a quadratic residue chain, would be about 1/4. This made me conjecture that the length of the longest chain, for any prime p, might not exceed $\log_2 p$.

I further thought that if $m(p)$ denotes the length of the longest chain for any prime p, then

$$m(p_1) \leqq m(p_2), \quad \text{if } p_1 < p_2. \tag{5}$$

4. Numerical Results. The problem was put on the computer by Professor D. H. Lehmer and his team and the following two sets of chains were obtained, the first when the elements of the chains are increasing in magnitude and the second when there is no such restriction. The results belie my first conjecture.

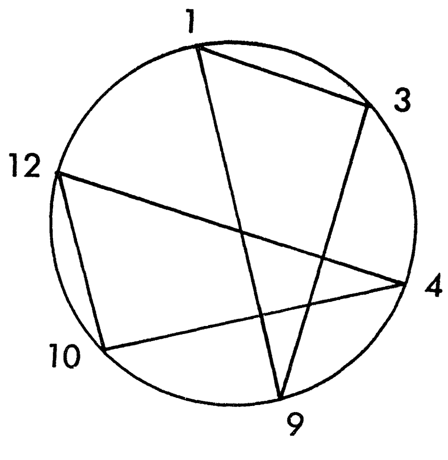

FIGURE 2

First Set

Least p with longest chain of length m

m	p	*chain*
2	11	1, 3
3	19	1, 5, 11
4	41	1, 20, 25, 32
5	59	1, 3, 17, 28, 36
6	83	1, 11, 16, 21, 44, 77
7	131	1, 27, 53, 55, 58, 117, 121
8	191	1, 24, 26, 46, 98, 125, 130, 163
9	251	1, 48, 66, 83, 118, 131, 156, 219, 221
10	467	1, 27, 47, 48, 66, 173, 250, 413, 417, 421
11	631	1, 4, 45, 94, 261, 310, 344, 387, 393, 394, 456

For $m = 12$, the least p exceeds 829.

Chains for which p is not necessarily least

12	2551	1, 4, 9, 32, 36, 44, 116, 164, 327, 603, 919, 1144
13	4663	1, 8, 13, 16, 35, 49, 204, 345, 546, 1497, 2426, 2954, 3961
14	5077	1, 3, 22, 36, 46, 81, 151, 451, 519, 744, 1192, 1450, 2072, 2165

Second Set

Least p with longest chain of length m

m	p	*chain*	$n(p)$
2	11	1, 3	2
3	19	1, 5, 11	4
4	41	1, 4, 32, 25	6
5	43	1, 9, 14, 35, 25	4
6	59	1, 21, 41, 25, 20, 26	4
7	103	1, 25, 91, 50, 55, 17, 49	2
8	131	1, 11, 9, 39, 5, 112, 55, 58	12
9	179	1, 14, 168, 169, 19, 126, 129, 151, 20	6
10	239	1, 80, 121, 40, 26, 66, 160, 113, 132, 127	2
11	331	1, 5, 121, 144, 53, 266, 31, 165, 296, 191, 224	

It was noted that except for 41, the least p for any m is of the form $4t - 1$.

Counting the number $n(p)$ of longest chains for each of the primes p less than 331, the Lehmer team further noticed that there are more such chains for primes of the form $4t + 1$ than for those of the form $4t - 1$.

For $239 \leqq p < 331$, the results are:

p	$n(p)$
239	2
241	36472
251	50
257	25762
263	10

p	$n(p)$
269	54080
271	2
277	53888
281	115650
283	136
293	143488
307	1024
311	230
313	438144
317	273120

Since to any chain (1) for p, there corresponds another obtained by multiplying the elements of the chain:

$$r_m, r_{m-1}, r_{m-2}, \cdots, r_2, 1 \tag{6}$$

by the reciprocal of r_m modulo p, $n(p)$ is necessarily even.

For primes of the form $4t + 1$, provided $r_2 \neq p - 2$, we have still another chain corresponding to (1) viz.

$$1, p - 1 - r_2, p - r_3, p - r_4, \cdots, p - r_m. \tag{7}$$

Another chain would be obtained from this by the reciprocation technique. For certain primes of the form $4t + 1$, therefore, the chains come in groups of four. For certain primes of the form $8t + 5$, $m > 3$, they even appear in groups of eight.

5. Cycles of Residues. Calling (1) a cycle of residues if

$$r_i, r_{i+1}, \cdots, r_m, r_1, r_2, \cdots, r_{i-1} \tag{8}$$

is a quadratic residue chain for each positive $i \leqq m$, the Lehmer team obtained the following cycles:

m	p	*cycle*	*number of cycles*
3	41	1, 4, 32	6
4	67	1, 9, 16, 39	8
5	131	1, 4, 11, 28, 20	10
6	227	1, 9, 53, 133, 141, 112	12

A cycle of length m leads to $2m$ cycles. Thus, the cycle 1, 9, 16, 39 for $p = 67$ gives the cycles

1, 9, 16, 39	1, 9, 26, 55
1, 39, 49, 15	1, 55, 21, 15
1, 15, 21, 55	1, 15, 49, 39
1, 55, 26, 9	1, 39, 16, 9

University of Allahabad
402 Mumfordganj
Allahabad, India