NTIA-Report-82-104

# An Experimental Study of Monte Carlo Factoring Techniques

W.J. Hartman

**U.S. DEPARTMENT OF COMMERCE**
**Malcolm Baldrige, Secretary**

Bernard J. Wunder, Jr., Assistant Secretary
for Communications and Information

July 1982

TABLE OF CONTENTS

## LIST OF FIGURES



## LIST OF TABLES

# AN EXPERIMENTAL STUDY OF MONTE CARLO FACTORING TECHNIQUES

W. J. Hartman*

Pollard (1975) describes a "Monte Carlo" factoring algorithm based on iterating some specific quadratic polynomials. In this paper different polynomials are tested in the algorithm to see if a more efficient factoring can be obtained. The results are inconclusive.

Key words: Monte Carlo factoring

## 1. INTRODUCTION

Pollard (1975) has suggested using the functions $X_n \equiv f(X_{n-1}) \pmod N$, with $f(X) = X^2 + 1$ or $f(X) = X^2 - 1$ and $X_0 = 2$, as a method of factoring N, assuming N is known to be composite. ($X \equiv Y \pmod N$ means $0 < X \leq N$ and N divides Y - X, abbreviated $N|Y - X$). Here we consider N to be of the form $p \cdot q = N$ where p and q are primes, where $p = 2p' + 1$, $q = 2q' + 1$ where p' and q' are primes. In this paper, we examine two questions: (1) Is there an a, b, $X_0$ such that $f(X) = (X-a)(X-b)$ produces a faster factoring than Pollard's function and (2) is there a way of selecting a polynomial form of f(X) which produces faster factoring.

The results obtained here are negative in the sense that no substantial improvement in Pollard's original method is obtained. However, these results do not imply that such improvement is impossible.

## 2. BACKGROUND

Pollard (1975) notes that since the equation is reduced (mod N) at most N values of X will be generated. Similarly, if p is a prime divisor of N, at most p values (mod p) will be generated. Therefore, the recursion will become periodic eventually. If we begin with $X_0$ and plot the successive points

*The author is with the Institute for Telecommunication Sciences, National Telecommunications and Information Administration, U.S. Department of Commerce, Boulder, CO 80303

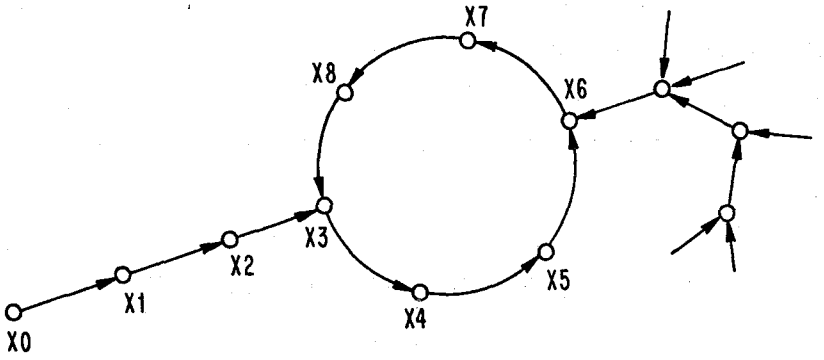


Figure 1. A directed graph showing two tails and a periodic part.

we obtain a directed graph as in fig. 1. The portion from $X_0$ to $X_3$ we call the/a tail and the portion including the points from $X_3$ to $X_{3+6}$ the periodic part. There may be more than one tail as shown going to the right in fig. 1, and some points may have more than one predecessor. We will call the graph including all of the connected points a section. A given function f and a given prime p may produce several sections.

A section may have a periodic part consisting of a single point as illustrated in fig. 2 (a) and (b).

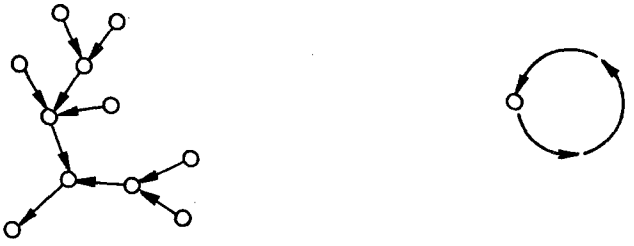


Figure 2. Two directed graphs with one-cycles (a), with tails (b) without tails.

We define the epact E, for a specific function f, a starting value $X_0$ and a prime p as the number of points, n, between X and the first $X_n$ which is a repetition of a previous $X_i$, i.e., n is the number of points in the tail plus the number of points in the periodic part starting at $X_0$.

We are interested in finding functions f and starting values $X_0$ which have small epacts.

## 3. POLLARD'S METHOD FOR DIFFERENT QUADRATIC f(X)

Rather than look at the factoring problem directly we consider instead the substantially equivalent form of the problem as follows.

For p prime, and

$$X_n \equiv f(X_{n-1}) \pmod{p}$$

find the smallest j and k such that

$$X_{j+k} \equiv X_j \pmod{p}.$$

The number j+k is called the epact. This is guaranteed to occur since this recursion generates at most p - 1 distinct numbers. The algorithm used for determining j and k is that of Brent (1980).

If, for some j and k, the greatest common divisor of $(X_{j+k} - X_j)$ and N is different from 1 and N, $(1 < \text{g.c.d.}\ (X_{j+k} - X_j, N) < N)$ then a divisor of N has been found.

For the two functional forms

$$f(X) = X^2 + a \text{ and } f(X) = X^2 - a,$$

I investigated a large number of a's with the following properties.

(1) a is an $\ell^{th}$ power, $\ell$ = 2, 3, 4, 7, 11
(2) a is square free and highly composite
(3) a is prime.

Since the largest epacts for

$$f(X) = X^2 - 1,\ f(X) = X^2 + 1,\ X_0 = 2$$

are known for primes less than $10^6$ (Guy, 1975), a set of 10 primes p of the form p = 2p' + 1, p' a prime were used to eliminate those combinations of a's and $X_0$'s which had epacts on the order of the maximum epacts for $X^2$ -1, $X^2$ + 1, $X_0$ = 2.

For those $(a, X_0)$ pairs not eliminated by this original screening 50 primes less than $10^6$ were used for an additional screening. The first screening eliminated approximately 50 percent of the approximately 10,000 $(X_0, a)$ pairs, and the second screening eliminated approximately 75 percent of the remainder leaving 1239 $(X_0, a)$ pairs. These were tested on the primes just larger than $10^6$ until each was eliminated. All were eliminated before 1000 primes were used.

It is concluded that no choice of $(X_0, a)$ pairs is consistently better than the (2, 1) or (2, -1) pairs.

Since it was not feasible to print most of the results, a few $(X_0, a)$ pairs were selected to see if the average epacts were smaller than those for the (2, 1) and (2, -1) pairs. These pairs were chosen at random from the original set. Two pairs showed a better average when averaged over the first 50 primes greater than $10^6$, but were approximately the same when averaged over the first 1000 primes $> 10^6$.

Although it is known that the epacts for (2, 1) and, (2, -1) can both be large for some primes, it is not known whether there are two $(X_0, a)$ pairs such that when one is large the other is "small." Also, it is not known how small these "small" epacts might be.

## 4. OTHER POLYNOMIALS

The quadratics used for f(X) in the previous section require only one multiplication and reduction (mod N) at each step. Therefore, in order that polynomial forms requiring more multiplication and reductions produce an improved factoring method, they must result in substantially smaller epacts for most starting values. It should be noted that a function requiring k multiplications that results in epacts $\frac{1}{k}$ as long as the simple quadratics would show a significant advantage over the quadratic because of the reduction in the number of g.c.d. calculations required. In the following, the statements with Roman numerals are proven, those with an asterisk are not proven, but appear to be amenable to proof, while those with an exclamation mark are only supported by some empirical evidence and may not be true.

We first investigate the sets and the size of the sets which are the range of a given (polynomial) function when the argument is taken over a

complete residue system (mod p). The epact will be no larger than the size of this set.

Throughout the rest of the paper, we will assume primes of the form $p = 2p' + 1$ where $p'$ is a prime.

Thus, $p \equiv 3 \pmod 4$ and also $p \equiv 2 \bmod 3$.

(I) The set $\{a X+b \pmod p, X=0, 1, 2, \ldots p-1, 0<a<p\}$ is the complete set of residues. Hereafter we will call a complete residue set generated by a function P(X) a permutation, or call such a function a permutation.

(II) If k is odd and the greatest common divisor of k and p-1 is 1, [(k, p-1) = 1], then the set $X^k \pmod p$ X=0, 1,2, ... p-1, is a permutation (Small, 1977).

(III) If P(X) (mod p) is a permutation, P(ax+b) (mod p) is a permutation for rational a and b, with a and b defined (mod p) and $a \not\equiv 0 \pmod p$.

(IV) If $P_1(X) \pmod p$ and $P_2(X) \pmod p$ are permutations, $P_1(X) \cdot P_2(X) \pmod p$ is not a permutation (Chowla, et al., 1948). That is, $P_1(X) \cdot P_2(X) \pmod p$ does not generate a complete residue system. Unfortunately, little is known about the size of the set generated.

(V) If P(X) (mod p) is a permutation so is (a P(X) + b) (mod p) for integer a, b, with $a \not\equiv 0 \pmod p$.

(VI) If P(X) (mod p) generates a set of size n, then so does (a P(X) + b) (mod p) and P(a X + b) (mod p). (These are usually not the same sets.) We shall call these sets "size equivalent."

(VII) $P(X) = X^2 \pmod p$ generates a set of size $\frac{p+1}{2}$. (Therefore using VI, so do all quadratics.)

Comments: Although IV gives a method for reducing a permutation to a smaller set, these same operations may not reduce smaller sets. For example, take $P_1(X) = X^2 \pmod p$ $P_2(X) = X \pmod p$. Then, $P_1(X) \cdot P_2(X) = X^3 \pmod p$ which, for the primes considered, is a permutation. However, see IX.

(VIII) The cubic polynomials $P(X) = \alpha X^3 + 3\beta X^2 + 3\,\delta X + \gamma$ separate into two size equivalent sets corresponding to the transformations of the following.

(1) $X^3$ of size p ($\beta^2 = \alpha\delta$)

(2) $X^3 + X$, $X^3 - X$ of size $2\left(\frac{p+1}{3}\right) - 1$ ($\beta^2 \neq \alpha\delta$)(Dickson, 1952).

(IX) $P_1\,(P_2(X))$ generates a set of size less than or equal to the minimum of the sets generated by either $P_1(X)$ or $P_2(X)$.

By iterating a function P(X) until, for some n, the size of $P^{(n)}(X)$ equals the size of $P^{(n-1)}(X)$, one obtains the number of elements in the cycles of P(X). However, the number of elements in the cycles gives only a crude measure of the size of the epact. For example $P(X) = X^p$ has size p, but has an epact of 1 for every starting element, while the function $P(X) = X^2$ has size $\frac{p+1}{2}$ and an epact of $\frac{p-1}{2}$ or $\frac{p+1}{2}$ for most starting elements. Nonetheless, for larger numbers it is easier to examine the size of the (possibly iterated) function than to obtain the graph of the function. Thus, numerical results tend to support the following conjectures.

(I*) Let $P_1(X) = X^3 \pm X$ and $P_2(X) = X^2$. Then the size of $P_2(P_1(X)) \leq$ the size of $P_1(P_2(X))$.

(I!) For $P_1$ and $P_2$ as in (I*), the average epacts for $P_1(P_2(X))$ are smaller than for $P_2(P_1(X))$.

(II!) For $P_1(X)$ a polynomial of odd degree, not a permutation, and $P_2(X) = X^2$, the size of $P_2(P_1(X)) \leq$ size of $P_1(P_2(X))$. Also, the average epact for $P_1(P_2(X))$ is less than the average epact for $P_2(P_1(X))$.

Note†: Although the size of $P(X) = X^2 + X$ and every transformation of P(X) as in V and/or VI is the same, the average epacts may differ. Table 1 gives the values of several polynomials for p = 47. The interested reader may easily construct the graphs for various polynomial iterations from this table in order to obtain support for the above conjectures. For example, using the notation of the table, $P_3(P_1(5)) = P_3(25) = 46$, and $P_1(P_3(5)) = P_1(36) = 27$.

Table 1. Values of Various Polynomials (mod 47).

| x | $P_1(x)$ $x^2$ | $P_2(x)$ $x^3$ | $P_3(x)$ $x^3+x$ | $P_4(x)$ $x^3-x$ | $P_5(x)$ $x^5+x$ | $P_3(P_3(x))$ | $P_4(P_4(x))$ | $P_4(P_3(x))$ |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 2 | 0 | 2 | 10 | 0 | 6 |
| 2 | 4 | 8 | 10 | 6 | 34 | 23 | 22 | 3 |
| 3 | 9 | 27 | 30 | 24 | 11 | 5 | 29 | 39 |
| 4 | 16 | 17 | 21 | 13 | 41 | 23 | 22 | 28 |
| 5 | 25 | 31 | 36 | 26 | 28 | 21 | 19 | 43 |
| 6 | 36 | 28 | 34 | 22 | 27 | 46 | 4 | 25 |
| 7 | 2 | 14 | 21 | 7 | 35 | 23 | 7 | 28 |
| 8 | 17 | 42 | 3 | 34 | 17 | 30 | 25 | 24 |
| 9 | 34 | 24 | 33 | 15 | 26 | 15 | 23 | 43 |
| 10 | 6 | 13 | 23 | 3 | 41 | 17 | 24 | 18 |
| 11 | 27 | 15 | 26 | 4 | 40 | 24 | 13 | 19 |
| 12 | 3 | 36 | 1 | 24 | 26 | 2 | 29 | 0 |
| 13 | 28 | 35 | 1 | 22 | 6 | 2 | 4 | 0 |
| 14 | 8 | 18 | 32 | 4 | 17 | 41 | 13 | 24 |
| 15 | 37 | 38 | 6 | 23 | 11 | 34 | 18 | 22 |
| 16 | 21 | 7 | 23 | 38 | 22 | 17 | 32 | 18 |
| 17 | 7 | 25 | 42 | 8 | 4 | 11 | 34 | 21 |
| 18 | 42 | 4 | 22 | 33 | 45 | 1 | 43 | 4 |
| 19 | 32 | 44 | 16 | 25 | 17 | 23 | 43 | 38 |
| 20 | 24 | 10 | 30 | 37 | 25 | 5 | 44 | 39 |
| 21 | 18 | 2 | 23 | 28 | 10 | 17 | 22 | 18 |
| 22 | 14 | 26 | 1 | 4 | 10 | 2 | 13 | 0 |
| 23 | 12 | 41 | 17 | 18 | 45 | 42 | 33 | 8 |
| 24 | 12 | 6 | 30 | 29 | 2 | 5 | 14 | 39 |
| 25 | 14 | 21 | 46 | 43 | 37 | 45 | 34 | 0 |
| 26 | 18 | 45 | 24 | 19 | 37 | 30 | 25 | 29 |
| 27 | 24 | 37 | 17 | 10 | 22 | 42 | 3 | 8 |
| 28 | 32 | 3 | 31 | 22 | 30 | 24 | 4 | 9 |
| 29 | 42 | 43 | 25 | 14 | 2 | 46 | 4 | 43 |
| 30 | 7 | 22 | 5 | 39 | 43 | 36 | 13 | 26 |
| 31 | 21 | 40 | 24 | 9 | 25 | 30 | 15 | 29 |
| 32 | 37 | 9 | 41 | 24 | 36 | 13 | 29 | 25 |
| 33 | 8 | 29 | 15 | 43 | 30 | 6 | 34 | 23 |
| 34 | 28 | 12 | 46 | 25 | 41 | 45 | 43 | 0 |
| 35 | 3 | 11 | 46 | 23 | 21 | 45 | 18 | 0 |
| 36 | 27 | 32 | 21 | 43 | 7 | 23 | 34 | 28 |
| 37 | 6 | 34 | 24 | 44 | 6 | 30 | 23 | 29 |
| 38 | 34 | 23 | 14 | 32 | 21 | 32 | 24 | 4 |
| 39 | 17 | 5 | 44 | 13 | 30 | 17 | 22 | 23 |
| 40 | 2 | 33 | 26 | 40 | 12 | 24 | 40 | 19 |
| 41 | 36 | 19 | 13 | 25 | 20 | 1 | 43 | 22 |
| 42 | 25 | 16 | 11 | 21 | 19 | 26 | 28 | 4 |
| 43 | 16 | 30 | 26 | 34 | 6 | 24 | 25 | 19 |
| 44 | 9 | 20 | 17 | 23 | 36 | 42 | 18 | 8 |
| 45 | 4 | 39 | 37 | 41 | 13 | 24 | 25 | 44 |
| 46 | 1 | 46 | 45 | 0 | 45 | 37 | 0 | 41 |

(X) Given the sets $\{X_i\}$, $\{y_i\}$ $i = 0, 1, 2, \ldots k$ such that $P(X_i) = y_i$ $i = 0, 1, 2, \ldots k$, one may determine a polynomial of degree k by using an interpolation formula (Newton's formula is recommended if the degree of the polynomial is not predetermined; see Kopal, 1955). Thus one may set up cycles of arbitrary lengths.

One such function which was tried was $P_7(X)$, obtained from the points

$$X_i = (i + 1)^2 \quad i = 0,1, \ldots 7,$$

$$\{y_i\} = \{X_1, X_2, X_0, X_4, X_5, X_6, X_7, X_3\}$$

and the polynomial to be iterated was $P_7(X^2)$ which contains one cycle of length 3 and one cycle of length 5. The evaluation of this polynomial at each point requires at most 21 multiplications. A program was written for a desk top calculator for counting cycles. Unfortunately, due to storage limitations, no more than 5 cycles could be counted. For primes near 1000, $P_7(X^2)$ produced a minimum of 5 cycles. And for several primes near $10^6$, $P_7(X^2)$ produced a minimum of 5 cycles. For two 12 digit primes, 8 different starting values gave a maximum epact of $3.8 \times 10^5$. (The minimum epact was 7).

A second polynomial similar to $P_7(X)$ was constructed with three cycles of length 3. The numerical results were similar to those for $P_7$, except that the maximum epact for the two 12 digit primes and 8 starting values was 1827.

The evidence is too weak to support any conclusion or even conjectures regarding the merits of polynomials constructed to produce cycles. Because of the unreliability of numerical results for small primes as predictors for results for large primes, and the cost of obtaining results for large primes, this portion of the work was terminated.

## 5. PROGNOSIS

A very desirable function would be one which produced binary trees for the primes. However, such a function is highly unlikely. Therefore, an alternative might be a function which has many small cycles, no long cycles and no long tails. This also appears difficult to attain. If the function has one large cycle, the probability that a starting value leads to this cycle is also large, so the hope of obtaining a good function and a good starting value is small.

## 6. CONCLUSIONS

The conclusion of this study is that we did not find any functions demonstrably better than Pollard's functions. This does not imply that none are available, only that their discovery is difficult.

## 7. REFERENCES


Brent, R.P. (1980), An improved Monte Carlo factorization algorithm BIT 20, pp. 176-184.

Chowla, S., and T. Vijayaraghavan (1948), On complete residue systems, Quart. J. Math., 19, pp. 193-194.

Dickson, L.E. (1952), History of the theory of numbers, Vol. II, Chelsea Publishing Co., New York, NY.

Guy, R.K. (1975), How to factor a number, Congressus Numerantium XVI, Proceedings Fifth Manitoba Conference on Numerical Mathematics, Winnipeg, pp. 49-89.

Kopal, Z. (1955), Numerical Analysis, John Wiley & Sons Inc., New York, NY.

Pollard, J.M. (1975), A monte Carlo method for factorization, Nordisk Tidski Informationsbehandling (BIT), 15, pp. 331-334.

Small, C. (1977), Powers Mod n, Mathematics Magazine, 50, #2, pp. 84-86.

FORM **NTIA-29**
(4-80)

U.S. DEPARTMENT OF COMMERCE
NAT'L. TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

# BIBLIOGRAPHIC DATA SHEET

| | 1. PUBLICATION NO. | 2. Gov't Accession No. | 3. Recipient's Accession No. |
|---|---|---|---|
| | NTIA Report 82-104 | | |

4. TITLE AND SUBTITLE

AN EXPERIMENTAL STUDY OF MONTE CARLO FACTORING TECHNIQUES

5. Publication Date
July 1982

6. Performing Organization Code

7. AUTHOR(S)
W. J. Hartman

9. Project/Task/Work Unit No.

8. PERFORMING ORGANIZATION NAME AND ADDRESS
U.S. Department of Commerce
National Telecommunications and Information Admin.
Institute for Telecommunication Sciences
325 Broadway, Boulder, Colorado 80303

10. Contract/Grant No.

11. Sponsoring Organization Name and Address
NTIA/ITS
325 Broadway
Boulder, CO 80303

12. Type of Report and Period Covered

13.

14. SUPPLEMENTARY NOTES

15. ABSTRACT *(A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here.)*

Pollard (1975) describes a "Monte Carlo" factoring algorithm based on iterating some specific quadratic polynomials. In this paper different polynomials are tested in the algorithm to see if a more efficient factoring can be obtained. The results are inconclusive.

16. Key Words *(Alphabetical order, separated by semicolons)*

Monte Carlo factoring

17. AVAILABILITY STATEMENT

☒ UNLIMITED.

☐ FOR OFFICIAL DISTRIBUTION.

18. Security Class. *(This report)*
Unclassified

20. Number of pages
12

19. Security Class. *(This page)*
Unclassified

21. Price:

☆ U.S. GOVERNMENT PRINTING OFFICE: 1982—579-711/337 REGION No. 8