

A Factorization Scheme with Gaussian Sums and Fourier Transforms

Seenu S. Reddi
Signal Research Laboratory
15091 Clemons Circle
Irvine, CA 92604

March 7, 1998

Abstract.

A factorization scheme is presented using Gaussian sums and Fourier transforms. This scheme acts as a sieve as well as a factor splitter. Proofs are presented to justify the scheme.

1 Introduction

We present a simple scheme to factorize integers and test their primality using Gaussian sums and Fourier transforms. Proofs are given to substantiate the scheme and a criterion is derived for factorability of integers. Given an integer p , define the following sequence of partial Gaussian sums:

$$G_k = \sum_{j=0}^k e^{i2\pi j^2/p}, k = 0, 1, \dots, p-1 \quad (1)$$

Define the Fourier transform of the above sequence:

$$H_k = \sum_{j=0}^{p-1} G_j e^{i2\pi jk/p}, k = 0, 1, \dots, p-1 \quad (2)$$

We note G_{p-1} is the classical definition of the Gauss sum. For a given p (assumed to be odd throughout this note), we evaluate the series $\{H_k\}$ and retain only those indices k which satisfy:

$$|H_k|^2 = 0 \pmod{p} \quad (3)$$

By examining these indices one can judge the primality or factorability of p . These indices will be referred to as *interesting* hereafter. Index k is said to be

primed or unprimed if $|H_k|^2$ is 0 or p. Table 1 shows these indices for odd $p = 11$ to 49.

Table 1. Interesting Indices

p	Indices
11	4 7
13	4 9
15	4 5 6 9 10 11
17	4 13
19	4 15
21	3 4 7 14 17 18
23	4 19
25	4 5' 10' 15' 20' 21
27	4 9' 18' 23
29	4 25
31	4 27
33	4 11 15 18 22 29
35	4 10 14 21 25 31
37	4 33
39	4 9 13 26 30 35
41	4 37
43	4 39
45	4 5 9 15' 30' 36 40 41
47	4 43
49	4 7' 14' 21' 28' 35' 42' 45

The primed indices are marked with single quotes in the table. A cursory examination of the table reveals that the primes have only two entries (4 and $p-4$) and factorability is indicated by the presence of more than 2 indices. If an integer contains a repeated factor (e.g., 25), primed indices will appear. Since 4 and $p-4$ always appear as interesting indices, we refer to them as *primary*. Other indices will be designated as *non-primary*. We state the following theorem.

Theorem 1 For any odd p , the number of interesting indices will be 2 if and only if it is a prime. For a factorable p , the number will be greater than 2. If p contains a repeated factor, it will have primed indices.

2 Proof of the Main Theorem

Before we proceed to the proof of the main theorem, we need the following lemmas. Define $\alpha = e^{i2\pi/n}$, $G_{p-1,k} = \sum_{t=0}^{p-1} \alpha^{tk} \alpha^{t^2}$ and $2k' = k - 4 \pmod{p}$.

Lemma 1

$$G_{p-1} = \sum_{t=0}^{p-1} \alpha^{t^2} = \sqrt{p} \quad \text{for } p \equiv 1 \pmod{4}$$

$$= i\sqrt{p} \text{ for } p = 3 \pmod{4}$$

For a proof see Rose[1].

Lemma 2 $G_{p-1,k} = \alpha^{-\widehat{k}^2} G_{p-1}$ where $2 * \widehat{k} = k \pmod{p}$.

Lemma 3

$$H_k = G_{p-1}(1 - \alpha^{-(k'+2)^2}) / (\alpha^k - 1) \text{ for } k \neq 0 \quad (4)$$

$$= p(G_{p-1} + 1)/2 \text{ for } k = 0 \quad (5)$$

Lemma 4 An index k is interesting index if and only if any of the following three criteria holds:

=

$$(k' + 2)^2 = k \pmod{p} \iff k'(k' + 2) = 0 \pmod{p} \quad (6)$$

$$(k' + 2)^2 = -k \pmod{p} \iff (k' + 2)(k' + 4) = 0 \pmod{p} \quad (7)$$

$$(k' + 2)^2 = 0 \pmod{p} \iff (k' + 2)(k' + 2) = 0 \pmod{p} \quad (8)$$

Proof: From Equation (4), one can deduce if the exponent of α in the numerator is $\pm k$, the magnitude of H_k will be \sqrt{p} , i.e., k will be interesting. If the exponent is zero, the magnitude will be 0 and k will be a primed index.

Lemma 5 If p is composite and can be written as a product of two relatively prime numbers, say $p = r * s$ where $(r, s) = 1$, then an interesting, non-primary index k can always be found.

Proof: The following constructive process can be used to find k . Select k' and $k' + 2$ such that Equation (6) is satisfied. Choose $k' = t * r$ where $1 \leq t < s$ such that $k' + 2 = 0 \pmod{s}$, i.e., $tr + 2 = 0 \pmod{s}$. Since $(r, s) = 1$, there always exists a multiplicative inverse for r , say r^* , and a solution for t is $t = -2 * r^* \pmod{s}$. As $k' = 0 \pmod{r}$ and $k' + 2 = 0 \pmod{s}$, Equation (6) is satisfied. Now we find k such that $k - 4 = 2 * k' \pmod{p}$.

Example: For $p = 21 = 3 * 7$, let $k' = t * 3$. We can compute t such that $t * 3 + 2 = 0 \pmod{7}$, i.e., $t = 4$. Thus $k' = 12$ and $k = 7$.

Lemma 6 If p is a power of prime, say $p = r^l$, then an interesting, non-primary, primed index k can always be found.

Proof: Select k' such that $k' + 2 = r^{t/2}$ for even t and $k' + 2 = r^{(t+1)/2}$ for odd t . Equation (8) will be satisfied. Now we find k such that $k - 4 = 2 * k' \pmod{p}$ which gives the required non-primary, primed index.

Now we present the proof of the main theorem. Equation (6) always holds for $k = 4$ since $k' = 0$ and (8) holds for $k = p-4$ since $k' = -4$. If p is a prime, there cannot exist integers k_1 and k_2 such that their product or square is $0 \pmod{p}$. Hence for prime p , the only interesting indices are 4 and $p-4$.

On the other hand, assume only interesting indices to be 4 and $p-4$. We now show that if p is composite, there will be a contradiction. If p is factorable as a

product of two relatively prime numbers, Lemma 5 asserts that a non-primary index can be found leading to a contradiction that not all indices are primary. If p is composite and not factorable as a product of two relatively prime numbers, p is a power of some prime q . In this case Lemma 6 dictates the presence of non-primary primed indices leading to a contradiction.

The above arguments imply that a factorable p will have non-primary, primed or unprimed indices, and thus always more than 2 primary indices. If p has a repeated factor, say $p = r^t * s$, choose k' such that $k' + 2 = r^{t/2} * s$ for even t or $k' + 2 = r^{(t+1)/2} * s$ for odd t . Equation (8) will be satisfied thus giving a primed k . Hence repeated factors in p give primed indices.

Equations (6) - (8) imply that one need not compute the Fourier transforms to check primality or factorability. For a given odd p , we compute indices k' :

$$2k' = k - 1 \pmod{p} \quad \text{for } k = 1 \dots (p-1)/2 \quad (9)$$

If the number of indices satisfying (6) - (8) exceeds 1, we conclude p is not a prime number. We have the following interesting corollary to the theorem.

Corollary 1 *If an odd integer p is factorable, there exists a non-zero $k < p$ and $k \neq p - 2$ such that one of the following equations are satisfied:*

$$k * (k + 2) = 0 \pmod{p} \quad (10)$$

$$k * k = 0 \pmod{p} \quad (11)$$

Combining Theorem 1 and Lemma 4 the following simple procedure may be used to check if a given odd integer p is prime or not.

Procedure to check for Primality:

- (i) $k = 1, m = 0$. // k - index, m - number of interesting indices
- (ii) Compute k' such that $2 * k' = k - 1 \pmod{p}$.
- (iii) If k' satisfies any of Equations (6) - (8), $m = m + 1$.
- (iv) If $m > 1$, jump to (vii).
- (v) Increment k . If $k < p/2$, go to (ii); otherwise go to (vi).
- (vi) p is prime. Stop.
- (vii) p is composite. Stop.

Condition (10) can be recast as follows. Noting that $k * (k + 2) = c * p$ for some nonzero p , we have $k^2 + 2 * k - c * p = 0 \iff k = -1 \pm \sqrt{1 + c * p}$ and hence:

$$\sqrt{1 + c * p} \text{ is an integer for some nonzero } c < p/2 \quad (12)$$

or equivalently:

$$x^2 = 1 \pmod{p} \text{ has solutions other than } 1 \text{ and } p-1 \quad (13)$$

It has been found numerically that c can always be found which is a multiple of 8 for composite numbers and this reduces computation by a factor of 4. As an example for $p = 39$, $c = 5$ and 16 ($= 8 * 2$) and $p = 45$, $c = 8$ and 15.

It may be noted (11) and (13) constitute elegant conditions for odd factorable p .

Reference

- [1] Rose, H. E., 1988. *A Course in Number Theory*, Clarendon Press, Oxford.

Simple Primality Testing and Factorization with Near Polynomial Bounds

Seenu S. Reddi
Signal Research Laboratory
15091 Clemons Circle
Irvine, CA 92604
ReddiSS@AOL.COM

March 7, 1998

Abstract

Simple algorithms are presented for primality checking and factorization with near polynomial complexity bounds. The algorithms require concepts that are elementary as compared to others that require deep number theoretic knowledge. The primality checking algorithm, though does not possess the best known theoretical bound, has the advantage of finding at least one factor if the number under question is factorable.

1 Introduction

Simple algorithms are presented for primality checking and factorization with upper computational bounds of $O(\log^k p)$ and $O(\log^{k+1} p)$ respectively where $k = \log p / \log \log p + 2$ and p is the number under consideration. Though the proposed primality scheme does not stack up favorably with the bound $O(\log^{C \log \log \log p})$ established by Adelman, et al with the aid of Pomerance [1, 2], it does possess simplicity and does not require concepts beyond modulo arithmetic and Chinese Remainder Theorem, and has the advantage of finding out at least one factor if the number is factorable. Also it should be emphasized that these bounds, though near polynomial, are crude and can be hopefully improved over time. The algorithms are based upon the work presented in [3].

2 Foundations for a Procedure for Primality

The following proposition is basic for the algorithms.

Proposition 1 *A given odd integer p is factorable iff there exists a non-zero $k < p$ such that either $k * k = 1 \pmod{p}$, $k \neq 1, -1 \pmod{p}$ or $k * k = 0 \pmod{p}$.*

The proposition was presented as a corollary in [3] but can be proved independently.

Proposition 2 *A given odd integer p is factorable iff there exists an integer k such that one of the following conditions hold:*

$$k^2 = 1 + n * p \quad \text{for} \quad 1 \leq n < p - 2 \quad (1)$$

$$k^2 = n * p \quad \text{for} \quad 1 \leq n < p \quad (2)$$

Proof: Follows from Proposition 1.

Equation (1) implies:

$$(k - 1) * (k + 1) = 0 \pmod{p} \quad (3)$$

and Equation (2) shows the presence of a repeated factor in p . We refer to these k as *key indices*, *key* to unlock factorization and primality. Table 1 shows these indices if they satisfy (1) or (2) along with $(k \pm 1)$ when relevant for odd $p = 101$ to 139. The indices are primed when they satisfy (2).

Table 1. Key Indices for odd $p = 101 - 139$

p	Indices
101	None - Prime
103	None - Prime
105	$8^*1(28, 30)$ $11(33, 35)$ $8^*2(40, 42)$ $39(63, 65)$ $8^*6(70, 72)$ $55(75, 77)$ - Composite
107	None - Prime
109	None - Prime
111	$13(37, 39)$ $8^*6(72, 74)$ - Composite
113	None - Prime
115	$5(23, 25)$ $8^*9(90, 92)$ - Composite
117	$13'(39)$ $8^*3(52, 54)$ $35(63, 65)$ $52'(78)$ - Repeated Factor
119	$21(49, 51)$ $8^*5(68, 70)$ - Composite
121	$1'(11)$ $4'(22)$ $9'(33)$ $16'(44)$ $25'(55)$ $36'(66)$ $49'(77)$ $64'(88)$ $81'(99)$ $100'(110)$ - Repeated Factor
123	$13(39, 41)$ $8^*7(82, 84)$ - Composite
125	$5'(25)$ $20'(50)$ $45'(75)$ $80'(100)$ - Repeated Factor
127	None - Prime
129	$15(43, 45)$ $8^*7(84, 86)$ - Composite
131	None - Prime
133	$3(19, 21)$ $8^*12(112, 114)$ - Composite
135	$5(25, 27)$ $15'(45)$ $60'(90)$ $8^*11(108, 110)$ - Composite
137	None - Prime
139	None - Prime

As an illustration of the underlying principles for the factorization to come, consider the number 123. We find the number 13 which satisfies Equation (1),

i.e., $40^2 = 1 + 13 * 123$ and conclude 123 is composite. Then we look at 39 and 41 associated with 40, and compute $\gcd(123, 39) = 3$ and $\gcd(123, 41) = 41$ as possible factors of 123 ($= 41 * 3$). In this instance the number is completely factored but sometimes the procedure may have to be iterated. Note for the number 117, the key index 13 is primed indicating a repeated factor, i.e., $117 = 3 * 3 * 13$. When we stipulate an algorithm based along these lines, we find the computational complexity of $O(p * \log^2 p)$ since n can range from 1 to $p-2$ and the square root operation to check Equations (1) and (2) requires $\log^2 p$ operations.

3 Complexity Determination

To reduce the complexity to polynomial bounds, choose the first Q primes starting from 3 to Q_{Hi} such that their product is greater than or equal to p , i.e., $3 * 5 * 7 * \dots * Q_{Hi} \geq p$ and represent n as a Q -tuple $\langle n_3, n_5, \dots, n_{Q_{Hi}} \rangle$, $n_i = n \pmod{i}$. By the Chinese Remainder Theorem n can be recovered from these residues. Assume that none of these primes divides p as if any does, we are done factoring p . If n satisfies Equations (1) or (2), its residues should satisfy the conditions set forth in the following proposition. We assume 0 to be a quadratic residue (unlike in [4]) for notational and expositional convenience (otherwise we have to state zero or a quadratic residue in our results) and hence there will be $(q+1)/2$ quadratic residues (as compared to $(q-1)/2$ in [4]) modulo q .

Proposition 3 *Let q be a prime, $(p, q) = 1$, and $n_q = n \pmod{p}$ and $p_q = p \pmod{q}$. If n satisfies Equations (1) or (2), there exists a quadratic residue $k_q \pmod{q}$ such that one of the following equations hold:*

$$n_q = p_q^{-1} * (k_q - 1) \pmod{q} \quad (4)$$

$$n_q = p_q^{-1} * k_q \pmod{q} \quad (5)$$

Proof: If there exists a solution to Equation (1), taking modulo q on both sides one gets for some quadratic residue k_q :

$$k_q = 1 + n_q * p_q \pmod{q} \quad (6)$$

from which Equation (4) follows. Since q is prime, p_q^{-1} exists. By a similar argument Equation (5) follows.

Proposition 3 reduces the complexity from $O(p \log^2 p)$ to $O((p \log^2 p)/2^Q)$ for checking primality. Before proceeding further let us consider an example. Let $n = 103$ and $Q = 3$ (since $3 * 5 * 7 \geq 103$) and the quadratic residues are $\{0, 1\}$, $\{0, 1, 4\}$, and $\{0, 1, 2, 4\}$ for modulo 3, modulo 5 and modulo 7 respectively. Represent n as $\langle n_3, n_5, n_7 \rangle$ and to check whether Equation (4) holds, choose $n_3, n_5,$ and n_7 from the sets $\{0, 2\}$, $\{0, 1, 3\}$ and $\{0, 2, 3, 4\}$ respectively. Convert from $\langle n_3, n_5, n_7 \rangle$ to n by using $(70 * n_3 + 21 * n_5 + 15 * n_7) \pmod{105}$ and check whether $1 + n * 105$ is a perfect square by taking its square root.

Perform the same procedure using Equation (5). Since none of these eligible numbers will satisfy Equations (1) or (2), we conclude 103 is a prime.

In view of Proposition 3 one need to consider only $O(p/2^Q)$ integers between 1 and p to see if Equations (1) or (2) are satisfied and this leads to a $O((p \log^2 p)/2^Q)$ primality checking algorithm. If it is demonstrated that $p/2^Q$ is $O(\log^k p)$ where $k = \log p / \log \log p$, we will have a primality checking algorithm with near polynomial complexity.

Proposition 4 $Q \geq (\log_2 p)/(3 \log_2 \log_2 p)$ for $Q \geq 3$.

Proof: Note $3 * 5 * \dots * Q_{Hi} \leq Q! * 3^Q * \log 2 * \log 3 * \dots * \log Q$ by modifying Rosser's inequality on n th prime number [5] to $p_n < 3 * n * \log n$ for $n \geq 2$. Hence $Q^Q * 3^Q * \log^Q 2 * \log_2^Q p \geq p \Rightarrow Q * \log_2 Q + Q * \log_2 3 + Q * \log_2 \log 2 + Q * \log_2 \log_2 p \geq \log_2 p$. Since $\log_2 p \geq Q$, we get $Q \geq (\log_2 p)/(2 * \log_2 \log_2 p + 1.057)$. The proposition follows as $\log_2 \log_2 p > 1.057$ for $Q \geq 3$.

Table 2 shows the number of factors Q and the lower bound $(\log_2 p)/(3 \log_2 \log_2 p)$ and as can be seen the bound is not tight. This does not hamper our proof of polynomial complexity but it is of interest to know whether tighter bounds exist (for instance it was observed numerically $Q \geq \log p / \log \log p$ but cannot be easily proved).

Table 2. Lower Bounds for Factors up to 100

p	Bound	Factor
105	0.81	3
1155	1.01	4
15015	1.22	5
255255	1.44	6
4.84985e+006	1.66	7
1.11546e+008	1.88	8
3.23485e+009	2.11	9
1.00280e+011	2.35	10
2.03648e+028	4.78	20
2.00724e+048	7.30	30
1.49098e+070	9.88	40
2.22262e+093	12.49	50
3.48768e+117	15.12	60
4.61630e+142	17.77	70
3.49481e+168	20.44	80
1.09219e+195	23.12	90
1.28871e+222	25.82	100

Proposition 5 $p/2^Q$ is $O(\log_2^k p)$, $k = \log_2 p / \log_2 \log_2 p$.

Proof: By Proposition 4, one obtains:

$$p/2^Q \leq p/2^{\log_2 p / (3 \log_2 \log_2 p)} \quad (7)$$

We find a k such that the following equation holds:

$$\log_2 p / (3 \log_2 \log_2 p) = \log_2 (p / \log_2^k p) \quad (8)$$

Expanding the RHS of Equation (8) and solving for k one gets:

$$k = \frac{\log_2 p}{\log_2 \log_2 p} - \frac{\log_2 p}{(3 \log_2 \log_2 p)^2} \quad (9)$$

Substituting the RHS of (8) in the RHS of (7) and using $2^{\log_2 X} = X$, Equation (7) becomes:

$$p/2^Q \leq \log_2^k p \quad (10)$$

where k is defined as in Equation (9). The proposition follows by taking the leading term of k and ignoring the negative second order term.

By changing logarithmic bases and using the properties of $O(\cdot)$, we get

Proposition 6 $p/2^Q$ is $O(\log^k p)$, $k = \log p / \log \log p$.

4 A Procedure for Primality and Factorization

The following procedure checks for primality and factorizes.

Procedure to check for Primality:

- (i) For a given odd p , find Q such that the product of the primes $3*5*\dots*p_{Q+1} \geq p$ where p_n is the n th prime. These primes are referred to as the base factors.
- (ii) If any of the base factors divide p , reduce p by dividing with this base factor. If $p = 1$, stop; otherwise jump to (i).
- (iii) Use the base factors to represent integers from 1 to $(p-1)/2$ in terms of residues and choose only those integers $\{q\}$ ($\{r\}$) whose residues satisfy Equation (4) (Equation (5)).
- (iv) If any integer n in this set $\{q\}$ ($\{r\}$) satisfies Equation (1) (Equation (2)), jump to (vi).
- (v) p is prime. Stop.
- (vi) p is composite. If Equation (1) is satisfied for a particular n , compute $k+1$ and $k-1$ where k is defined by this equation. Compute the gcd's of these integers with respect to p . Reduce p by dividing with these gcd's. Jump to (vii). If Equation (2) is satisfied, compute k . Compute the $\text{gcd}(k, p)$ and reduce p by this factor. Jump to (vii).
- (vii) If p is reduced to 1, stop; otherwise jump to (i).

In view of Proposition 6, the above primality checking algorithm has a complexity of $O(\log^{k+2} p)$ where k is defined as in this proposition. The reason for the extra factor 2 is that the integer square root operation needed to check Equations (1) and (2) requires $\log^2 p$ operations. For factorization, the algorithm may have to be iterated as many times as there are factors in the given number p . Since there can be at most $\log p$ factors, we get a complexity of $O(\log^{k+3} p)$.

5 Future Research

It appears that the upper bounds can be reduced by taking advantage of quadratic residue relationships (Equations (4) and (5)) obtainable using primes other than the base factors. For instance, when p is 103 and base factors 3, 5, and 7 are used, further relations can be obtained using other primes such as 11, 13, and 17. Though these relations cut down the solution space to be explored, it is not clear how to accomplish this. There is an intimate connection between the key index n and p the number to be factored. For instance it is easy to prove that if $p = q * (q \pm 2)$, $n = 1$ implying a relatively easy factorization. There are several relations of this sort exist, and it would be desirable to characterize the key indices (as to their size and number) for a given p with known factors. As can be noted from Table 1, all even key indices are multiples of 8 (a fact that can be used for reducing solution space) and we cannot find a proof for this.

References

- [1] Pomerance, C., 1981. "Recent Developments in Primality Testing," Mathematical Intelligencer, Vol. 3, pp. 97 - 105.
- [2] Adelman, L. M., et al., 1983. "On Distinguishing Primes from Composite Numbers," Annals of Math., Vol. 2, pp. 173 - 206.
- [3] Reddi, S. S., 1998. "A Factorization Scheme with Gaussian Sums and Fourier Transforms," Submitted for publication.
- [4] Ireland, K. and M. Rosen, 1991. *A Classical Introduction to Modern Number Theory*, Springer-Verlag, NY.
- [5] Rosser, Barkley and L. Schoenfeld, 1962. "Approximate Formulas for Some Functions of Prime Numbers," Illinois Journal of Mathematics, Vol. 6, pp. 64-94.