Linear Factors and the Pollard Rho Method

Brian Nixon

July 15, 2009

Abstract

This paper examines the Pollard Rho factorization method and the associated polynomial $x^2 + 1$. Then it examines the family of polynomial pairs that differ by a constant and split into linear factors.

1 Introduction

The fast factorization of integers is a significant problem. In this paper, we take a look at a common factorization method in the hopes that we achieve a better average time complexity. To do so, we will examine the Galois groups of a family of polynomials. Then, we will focus on a family of polynomials that will also result in greater factorization speed if members of the family can be easily generated.

2 Analysis of Pollard-Rho Polynomials

The Pollard Rho algorithm is a common method used for factoring smaller integers. A good description is given by Rosen[2]. While it is not a deterministic algorithm, it offers better complexity in the average case than the more heavy duty factoring algorithms such as the quadratic sieve or use of elliptic curves. Given an integer $n$ and a prime $p$ that divides $n$, the Rho method looks for two integers that are congruent modulo $p$ but not modulo $n$. Given such $x_i, x_j$, we have $y = (x_i - x_j) \mod n$ with $p \mid y$ and $y \neq 0$. Thus $\gcd(y, n)$ yields a nontrivial factor of $n$. There is no way to know in advance what values of $x_i$ will work so a pseudo-random sequence is generated and the terms compared. Commonly, the sequence used is $x_{i+1} = f(x_i) \mod n$ with $f(x) = x^2 + 1$. This has produced good results and offers the additional property that $x_i = x_j \mod p \Rightarrow f(x_i) = f(x_j) \mod p \Rightarrow x_{i+k} = x_{j+k} \mod p \forall k$. We will examine this function with the aim of possibly replacing it.

Our focus will be on the Galois groups generated from this family. We know that a Galois group of a field extension over a finite field must be cyclic. From Dummit and Foote[1], we get the following theorem about the generating element of the group.
**Theorem 1.** Let $G \in \text{Sym}_n$ be the Galois group of $f(x)$ over $\mathbb{Q}$. Let $n_T$ be the number of elements of cycle type $T$ in $G$. The density of primes $p$ for which the Galois group of $f(x)$ over $\mathbb{F}_p$ is generated by an element of type $T$ is $n_T/|G|$.

As we are looking for roots of $f(x)$ in the base field $\mathbb{F}_p$, we need the linear factors of $f(x)$ in $\mathbb{F}_p[x]$. The Galois group over $\mathbb{F}_p$ acts transitively on the roots of each factor so the number of linear factors of $f(x)$ is exactly the number of elements fixed by the group. Using the above theorem, we can compute the statistical likelihood of finding a root for a random prime $p$.

### 2.1 Analysis of $f_n - x$

Let $f(x) = x^2 + 1$ and define a sequence of functions $f_i$ with $f_0(x) = x$ and $f_{i+1}(x) = f(f_i(x))$. By this definition, we also see that $f_{i+1}(x) = f_i(f(x))$. Now we ask what the Galois group of the splitting field of $f_i - f_j$ over $\mathbb{Q}$ looks like.

As the roots of these polynomials will span the field extension, the following lemma is important.

**Theorem 2.** Let $\alpha$ satisfy some $f_i(\alpha) - f_j(\alpha) = 0$ with $i > j$. Then $\exists n > m$ that $f_n(\alpha) - f_m(\alpha) = 0$ and $\forall i > j$, $f_i(\alpha) - f_j(\alpha) = 0$ if and only if $j \geq m$ and $(n - m)$ divides $(i - j)$. Consequently, $f_n - f_m$ divides such $f_i - f_j$.

**Proof.** First, we should construct such $n, m$. Let $I_\alpha = \{(i, j) | i > j, f_i(\alpha) - f_j(\alpha) = 0\}$. We can take $(n, m) \in I_\alpha$ such that $\forall (i, j) \in I_\alpha$, $n \leq i$ and $\forall (n, j) \in I_\alpha$, $m \leq j$. Similarly, take $(n', m') \in I_\alpha$ such that $\forall (i, j) \in I_\alpha$, $m' \leq j$ and $\forall (i, m') \in I_\alpha$, $n' \leq i$. Then as $n' \geq n$ we get $f_{n'}(\alpha) = f_{n+(n'-m)}(\alpha) = f_{n+0}(\alpha)$. If $m + n' - n \neq m'$ then by the minimality of $n'$ we have $m + n' - n \geq n' \geq m$ and $m \geq n$. This is a contradiction so $m + n' - n = m' = m$ and $n' - n = m' - m$. As $n' - n \geq 0 \geq m' - m$, we get $n' = n$ and $m' = m$ and $f_n - f_m$ is the minimal polynomial we are seeking.

($\leftarrow$) Let $k = (n - m)$. We know $(m + k, m) \in I_\alpha$. Suppose, $(m + lk, m) \in I_\alpha$. Then $f_{m+(i+1)k}(\alpha) = f_k(f_{m+lk}(\alpha)) = f_k(f_m(\alpha)) = f_m(\alpha) = f_{m+k}(\alpha)$ so $(m + (l + 1)k, m) \in I_\alpha$. Inductively, $(m + lk, m) \in I_\alpha \forall l$. Now given $(i, j) \in I_\alpha$, $f_{i+k}(\alpha) = f_k(f_i(\alpha)) = f_k(f_j(\alpha)) = f_{j+i}(\alpha)$ so $(i + l, j + l) \in I_\alpha$.

($\rightarrow$) Take $(i, j) \in I_\alpha$. With $k$ as above, we get $(i - j) = lk + r$, $0 < r < k$. If $l \neq 0$, we know from the above that $(j + lk, j) \in I_\alpha$ so $f_{j+k}(\alpha) = f_{l+k+(r+1)(l+k)}(\alpha) = f_{l+k}(\alpha) = f_{l+k}(\alpha)$ and $(j + r, j) \in I_\alpha$. If $l = 0$, then we get $(r + j, j) \in I_\alpha$ directly.

Let us start our analysis with the class of polynomials $f_n - f_0$. Let $\alpha$ be a root of $f_n - f_0$. The above theorem tells us $f_i - f_j$ divides $f_n - f_0$ if and only if $i/n$ and $j = 0$. Also, $f_n(\alpha) = \alpha$ and $f_n(f(\alpha)) = f(\alpha)$ so $f(\alpha)$ is a root of $f_n - f_0$.

Every root has a minimal $f_d - f_0$ that it satisfies so we can symbolize the roots of $f_n - f_0$ by copies of cycle graphs with $d$ nodes where $d|n$. The arrows of the graphs correspond to the action of $f$ and the nodes are the roots.
The question arises, how many copies of a particular graph are there? We can denote this as $g(n)$ defined by the equation $\text{deg}(f_n - f_0) = 2^n = \sum_{d|n} dg(d)$.

Applying Möbius Inversion, this becomes $ng(n) = \sum_{d|n} 2^d \mu(n/d)$ with $\mu$ the Möbius function.

Given an automorphism $\sigma$ in the Galois group of the splitting field, $\sigma$ permutes the roots of each irreducible factor of $f_n - f_0$ so it preserves the minimal $n, m$ that a root satisfies. We also have $f(\sigma(\alpha)) = \sigma(f(\alpha))$ so the action on the roots from one cycle of the graph are determined by the action on a single root in that cycle. The Galois group must therefore be a subgroup of the group $\prod_{d|n}(\mathbb{Z}/d\mathbb{Z})^{g(d)} \rtimes \text{Sym}_{g(d)}$ where the action of the symmetry group is to permute the copies of the cyclic groups.

### 2.2 Analysis of $f_n - f_m$

We note that $(f_n - f_0)(f_n + f_0) = f_n^2 - f_0^2 + 1 - 1 = f_{n+1} - f_1$. Further, $f$ is an even function so $f_n(\alpha) = \alpha \Rightarrow f_n(-\alpha) = -\alpha$ so the roots of $f_n + f_0$ are the additive inverses of the roots of $f_n - f_0$. Thus the splitting field of $f_{n+1} - f_1$ is the same as the splitting field of $f_n - f_0$ so the Galois groups are the same. This becomes apparent if we return to the graph idea we had above. The nodes outside the cycles are the roots of $f_n + f_0$. The action on them determines the action on the nodes inside the cycles as the values on the two nodes preceding arrows leading into a given node are additively inverse. One node is on the outside of the cycle and one is on the inside.

We can use the graph of the roots of a polynomial to talk about the Galois group. As previously stated, an automorphism of the Galois group permutes the roots of the irreducible factors of $f_n - f_m$. Thus it preserves the minimal $n, m$ that a root satisfies. The action on the nodes of the graph will similarly preserve this property by sending the roots of a node to a node that occupies a symmetric position. The graph of $f_{m+k} - f_m$ will be made of the cycles as in the earlier graph of $f_k - f_0$ with each central node connected to a root of a complete binary tree with depth $m - 1$ (it is a binary tree as $f^{-1}(\alpha)$ has two solutions). We note that the group of all permutations on a complete binary
Figure 2: Roots of $f_5 - f_1$

tree of depth $k$ that preserves the depth of each node is $Syl_2(Sym_{2k})$. The maximal possible Galois group of $f_{m+k} - f_m$ must be $Syl_2(Sym_{2m-1})^{G_k} \times G_k$, with $G_k \cong \prod_{d|n}(\mathbb{Z}/d\mathbb{Z})^{g(d)} \times Sym_{g(d)}$ the Galois group of $f_k - f_0$. The action of $G_k$ on the Sylow groups is to exchange the corresponding elements as in the internal action of $G_k$.

2.3 An Alternative

One possible contender is the polynomial series $f_n(x) = x^n - t$ with $t$ a constant. Then $f_n - f_m = x^n - x^m = x^m(x^n - m! - 1)$. The Galois group is the multiplicative group of $\mathbb{Z}/(n! - m!)\mathbb{Z}$. Letting $n! - m! = 2^{a_0} \prod_{i>0} p_i^{a_i}$ be the prime factorization and $A \cong \prod_{i>0} \mathbb{Z}/p_i^{a_i-1}(p_i - 1)\mathbb{Z}$, if $a_0 \leq 1$ then the group is isomorphic to $A$ and isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{a_0-2}\mathbb{Z} \times A$ otherwise. We cannot use $x = 0$ in the Pollard Rho method as it will be equal to 0 modulo any integer. Therefore with this family, we only consider the action of the automorphisms on the $n! - m!$ roots of unity. As stated above, these correspond to the multiplicative group $\mathbb{Z}/(n! - m!)\mathbb{Z}^\times$. For $a \in \mathbb{Z}/(n! - m!)\mathbb{Z}^\times$ and $d|n! - m!$, we fix the $d$th roots of unity if $a \mod d = 1$. This should provide a method for determining if this family is more effective than the family derived from $x^2 + 1$.

3 Maximizing Linear Factors

Using the Pollard Rho method, one hopes to find a root of a polynomial over a finite field. The object is to maximize the odds of finding a root while minimizing the effort required to generate the polynomial. To accomplish the first, we are going to focus on polynomials that separate into linear factors over $\mathbb{Q}$. These will have the maximum number of linear factors possible over any finite field, excepting for the moment multiplicity of roots. As multiplication is an expensive operation, to minimize the effort the focus is on finding new roots
using only addition. For this reason, we’re studying pairs of polynomials \( f(x) = \prod_i (x - a_i) = c + \prod_i (x - b_i) = c + g(x) \) with \( a_i, b_i, c \in \mathbb{Z} \). This allows us to compare against \( \deg(f) \) new roots with only a single addition. We can build high degree polynomials by alternately multiplying and adding as in straight line programs. Using this method and given an integer \( n \), one hopes to find a root over \( p|n \) that does not evaluate to \( 0 \mod n \).

### 3.1 Comparison over Finite Fields

The first question is how to find these pairs. Given such \( f \) and \( g \) in \( \mathbb{Z}[x] \) and a prime \( p \) we get a corresponding pair of polynomials \( \bar{f}, \bar{g} \in \mathbb{F}_p[x] \) that likewise split into linear factors over \( \mathbb{F}_p \) and which differ by a constant. This being true for all primes, it is to be hoped that the possible roots over the finite fields will tell us more about the possible roots in the integers. First, note that \( p|c \Rightarrow \bar{f} = \bar{g} \) so their split into linear factors is identical. That is really all that can be said about that case so our focus will be on the cases where \( p \) does not divide \( c \). We note that given \( c \neq 0 \mod p \) and \( \bar{f}(a) = 0 \) implies \( \bar{g}(a) \neq 0 \) so roots of \( \bar{f} \) are distinct from the roots of \( \bar{g} \). Also, \( f(x) = \bar{g}(x)+c \) implies \( f(x-a) = \bar{g}(x-a)+c \) and we can always make \( 0 \) a root of \( f \). So for \( p = 2 \) and \( c \) odd, we have that \( \bar{f}(x) = x^n = \bar{g}(x)+ = (x+1)^n \). This forces \( n \) to be a power of 2. We can provide so motivation for the following conjecture.

**Conjecture 1.** Given \( p \) prime, \( f, g \in \mathbb{F}_p[x] \) that split into linear factors and \( c \in \mathbb{F}_p \) such that \( f(x) = g(x) + c \), then either \( c = 0 \) or \( \deg(f) = \deg(g) = r \cdot p^n \) where \( 0 < r < p \).

We have already shown this for \( p = 2 \) and can further show it for \( p = 3 \). Let \( f, g \in \mathbb{F}_3[x], c \in \mathbb{F}_3 \) match our conditions and \( c \neq 0 \) with \( \deg(f) = n > 2 \). The two polynomials don’t share any roots so at least one of these polynomials has the form \((x-a)^n\). Using the substitution, \( x \mapsto x+a \) without loss of generality, we can let \( f(x) = x^n \) and \( g(x) = (x+1)^n(x-1)^b \). The coefficient on \( x^{n-2} \) must be the same for both so \( a-b = 0 \mod 3 \). Our condition that \( n > 2 \) means that the coefficient on \( x^{n-2} \) is not the constant term so \( \binom{n}{2} (1)^2 + \binom{n}{1} (-1)^2 + (1+1)ab = 0 \mod 3 \) and \( a(a-1) - a^2 = 0 \mod 3 \). Thus \( b = a = 0 \mod 3 \) and we can alter our polynomials to read \( f(x) = (x^3)^m, g(x) = (x^3+1)^d(x^3-1)^b \). If \( m > 3 \), we can replace \( x^3 \) with \( y \) and the same fact will show we can reduce to a polynomial on \( y^3 \).

An interesting thing occurs if \( f(x) = g(x) + 2 \mod 4 \). Without loss of generality, let the constant term of \( g(x) \) be nonzero. \((x+2)^2 = x^2 \mod 4 \) so \( g(x) = (x+2)^r(x+1)^u(x-1)^v \) with \( r \leq 1 \). We know \( f(x) = g(x) \mod 2 \) which means \( f(x) = x^r(x+1)^u(x-1)^v \) with \( a' + b' = a + b \). Note \((x-1)^2 = x^2 -2x+1 = x^2+2x+1 = (x+1)^2 \mod 4 \) so we can let \( f(x) = x^t(x+c)^t(x+1)^k \) and \( g(x) = (x+2)^r(x+c+d)^r(x+1)^k \) with \( r, t \leq 1, c = 1, 3, \) and \( d = 0, 2 \). If \( r = 0 \) we look at the constant terms to get \( c^t1^k = (c+d)^t1^k + 2 \mod 4 \) so \( d = 2 \) and \( t = 1 \). If \( k > 0 \), look at the coefficient on \( x^{n-1} \) and see \( c+k = c+2+k \mod 4 \) which leads to a contradiction. Thus \( r = 0 \Rightarrow f(x) = (x+c), g(x) = (x+c+2) \).
If \( r = 1 \) and \( n = \deg(f) > 2 \) we can again look at the coefficient of \( x^{n-1} \) to see \( ct + k = 2 + (c + d)t + k \mod 4 \) and \( dt = 2 \mod 4 \) so \( d = 2, t = 1 \). The coefficient on \( x^{n-2} \) tells us \( kc + \binom{k}{2} = 2(c + 2) + 2k + (c + 2)k + \binom{k}{2} \mod 4 \) which implies \( 2c + 4 + 4k = 2c = 0 \mod 4 \). This contradicts our specification that \( c = 1, 3 \). Thus \( f(x) = g(x) + 2 \mod 4 \Rightarrow \deg(f) \leq 2 \).

## 3.2 Examples up to degree 8

The information about pairs over finite fields tell us about the relative structure of the roots and the constant but it does not help us find such pairs. Now letting the roots have absolute value no greater than \( n \) and taking the degree of the polynomials to be \( d \) we get a loose upper bound on the possible coefficient of \( x^{d-i} \) of \( \binom{d}{i} n^i \). There are \( O(n^{d(d-1)/2}) \) polynomials in this range. Only \( (2n+1)^d \) will correspond to polynomials that split into linear factors so heuristically we expect the odds of finding pairs within a bounded root range to decrease rapidly as the degree of the polynomials increase. However, there seems to be more at play here as numerous examples of such pairs have been computed up to degree 8.

In hopes of finding a method of finding pairs we examine pairs of small degree. A number of methods were used. Calculating all polynomials generated by roots in a given range, storing them, and comparing them pairwise would have been extremely costly in both time and space. Instead, each polynomial is computed in turn and the various roots are evaluated on it. If \( d-1 \) of the values match it is easy to compute a potential last root subtracting the sum of the matching integers from the coefficient on \( x^{d-1} \). If this last integer evaluates to the same value as the rest then the product of linear factors of these integers differs from the polynomial by the constant the integers evaluated to. This drops search complexity from quadratic to linear on the number of polynomials so \( O(n^d) \). The search can be further refined and duplicate matches due to reordering of roots can be avoided by requiring the iteration on the roots of the polynomial examined to maintain a decreasing order. If we know a pattern in the pairs of a certain degree, the search can be further refined to match it.

All degree one polynomials are related in the desired fashion. Degree two polynomials will be related if the sum of their roots equal. From there it gets harder to find pairs.

Looking at odd degree polynomials, one refinement on the search is to look at those whose roots \( \{a_i\} \) sum to zero and compare \( \prod_i (x - a_i) \) with \( \prod_i (x + a_i) \).

The coefficients on odd monomials will have to match as they are sums of even products on the roots and the sum of the roots will have to match. Our program discovered 183 such pairs of polynomials of degree five with roots whose absolute values were less than 100. \((87 - 1 - 5 - 9), (-8 - 7159)\) is one such pair. Only two pairs were found for polynomials of degree seven with roots of magnitude less than 60. They are \((5038137 - 24 - 33 - 51), (-50 - 38 - 13 - 724351)\) and \((5149196 - 30 - 40 - 55), (-51 - 49 - 19 - 6304055)\). Notably, each 7-tuple contains a subset of 4 whose terms sum to zero (and therefore a subset of 3
whose terms sum to zero). It is unclear if this is necessary or not. No other pattern has been found. No pairs of degree 9 were found but the search was terminated before completion as it was taking too long.

Allowing for multiplicity of roots, over a 100 degree six polynomial pairs were found with root magnitude less than 22. Almost all pairs could be translated so that each polynomial had roots $a, -a$ with $a \in \mathbb{Z}$. An example is $((-6 - 55611 - 11), (1091 - 1 - 9 - 10))$. Those that could not had roots $a + \frac{b}{2}, -(a + \frac{b}{2})a, b \in \mathbb{Z}$. Again, no reason nor other pattern could be found.

Using this as a model we computed the degree 8 polynomial pairs where a root implies $-a$ is a root and found 20 matches with root magnitude less than 100. One example is $((-5 - 14 - 23 - 25142324), (-2 - 16 - 21 - 252162125))$. No pattern has been found among these pairs.

One example of the original desired building process is given by the following sequence.

\[
\begin{align*}
(x - 237) + 474 &= (x + 237) \\
(x - 237) \cdot (x + 237) + 44933 &= (x - 106) \cdot (x + 106) \\
(x^2 - 237^2) \cdot (x^2 - 106^2) + 500669280 &= (x^2 - 178^2) \cdot (x^2 - 189^2) \\
(x^2 - 237^2) \cdot (x^2 - 106^2) \cdot (x^2 - 178^2) \cdot (x^2 - 189^2) + 58651026148915200 &= (x^2 - 126^2) \cdot (x^2 - 227^2) \cdot (x^2 - 141^2) \cdot (x^2 - 218^2)
\end{align*}
\]

Only two other such pairs have been found with roots less than 1000 (up to rearrangement or scaling). They correspond to the polynomial pairs with roots $(\pm 11, \pm 131, \pm 343 \pm 367), (\pm 77, \pm 101, \pm 353, \pm 359)$ and $(\pm 54, \pm 474, \pm 613, \pm 773), (\pm 206, \pm 366, \pm 683, \pm 747)$. So far no relationship between the pairs has been found that would make it easier to generate such pairs. Interestingly enough, each of these display another property. Of course, all pairs $(x + c)(x - c)$ will differ by a constant but each of these degree 8 pairs also split into a 4-tuple of degree 4 polynomials that differ pairwise by constants. The degree 8 pairs were generated by finding degree 4 pairs and looking for a matching degree 8 polynomial from the resulting product. There does seem to be any reason from the search method for the resulting degree 8 match to split into such degree 4 pairs. Whether this property is necessary is still unknown.

4 Conclusion

We have a wealth of polynomial pairs that demonstrate the required properties but still no knowledge as to why the roots are related in this fashion. Without that, we have no method for generating pairs and our factorization idea won’t work. Pairs are much more prevalent than predicted so there is reason to believe that a pattern exists. More work will have to be done in analysis.

We also have a method of analyzing the predicted results of the Pollard Rho method with different generating functions. If one can be found that offers better performance than $x^2 + 1$, it can increase the usefulness of the algorithm.
References
