

A DESCRIPTION OF THE NUMBER FIELD SIEVE

JOSHUA BARON

ABSTRACT. The number field sieve is a relatively new method to factor large integers. Its most notable success is the factorization of the ninth Fermat number. It is significantly faster than all known existing integer factoring algorithms. We examine the theoretical underpinnings of the sieve; after understanding how it works, we state the algorithm. We look mostly to the algebraic number theory aspects of the sieve while leaving the question of the sieve's computational efficiency to other discussions.

1. INTRODUCTION

The question of how to best factor large numbers has significance in both theoretical and applied mathematics. Mathematicians have long attempted to locate all Mersenne primes (prime numbers of the form $2^n - 1$) as well as factor Fermat numbers (numbers of the form $2^{2^n} - 1$). In more applied areas of mathematics, one of the dominant methods of cryptographic encryption, RSA-based public key cryptography, revolves around the infeasibility of factoring large numbers into two large primes.

In 1988 John Pollard attempted in [?] to give a method of factoring large numbers (at least over 100 digits) of the form $a^b - c$, $a, b, c \in \mathbf{Z}$, for a and c small. This method has been generalized by [?] to work for integers of any form. In the meantime, Pollard's method, dubbed the number field sieve for its intermediate sieving steps and for the number field constructed for each n to be factored, yielded the solution to the 9th Fermat number, a 155 digit number. We present a version of the number field sieve that is able to factor $n \in \mathbf{Z}$ of any form, not just in Pollard's special case. In doing so, we closely follow [?]; when otherwise uncited, all proofs are based on theirs. We will not worry about the details relating to computational efficiency. Instead, we will examine the theoretical machinery that makes the sieve work in order to give the algorithm in all its glory as quickly as possible.

2. GENERAL IDEA

In order to factor a number n , what we will attempt to do is find a solution to the equation

$$(2.1) \quad x^2 \equiv y^2 \pmod{n}.$$

We can then factorize n by finding $\gcd(x - y, n)$. This idea relies on the fact that for at least half of those x and $y \pmod{n}$ that are coprime and satisfy (2.1), we have that $1 < \gcd(x - y, n) < n$. We accomplish this by dealing mostly with $\mathbf{Z}[\alpha]$ rather than \mathbf{Z} , where α is the root of some monic irreducible polynomial $f \in \mathbf{Z}[x]$ of degree $d > 1$.

Suppose that for some $m \in \mathbf{Z}$, $f(m) \equiv 0 \pmod n$. We have a natural homomorphism $\phi : \mathbf{Z}[\alpha] \rightarrow \mathbf{Z}/n\mathbf{Z}$ which is induced by $\phi(\alpha) \equiv m \pmod n$. Since for any $a \in \mathbf{Z}[\alpha]$, we can think of a as $(a_1, a_2, \dots, a_{d-1})$, we have that $\phi(a) = \phi(\sum_i a_i \alpha^i) = \sum_i a_i m^i \pmod n$. What we are going to be looking for is a set S of pairs of relatively prime integers (a, b) such that we have two equations:

$$(2.2) \quad \prod_{(a,b) \in S} (a + bm) \quad \text{is a square in } \mathbf{Z}$$

$$(2.3) \quad \prod_{(a,b) \in S} (a + b\alpha) \quad \text{is a square in } \mathbf{Z}[\alpha].$$

From these equations, we get that $x \in \mathbf{Z}$ is a square root of the first equation while $\beta \in \mathbf{Z}[\alpha]$ is a square root of the second one. Under the homomorphism ϕ , we get that $\phi(\beta^2) = x^2 \pmod n$. We then have that $\phi(\beta) = y \pmod n$, and thus having our $x^2 \equiv y^2 \pmod n$, we can factor n at least one out of every two times.

We then see that achieving the actual sieve will require us to answer three questions: how do we find f and m , how do we find the set S , and given β^2 , how do we find β ? The answers to these three questions will comprise the rest of the paper.

3. THE SEARCH FOR THE RIGHT POLYNOMIAL

We just saw that the first thing that we need to do is find some monic irreducible polynomial $f \in \mathbf{Z}[x]$ and some m such that $f(m) \equiv 0 \pmod n$. We do this by setting $m = \lceil n^{1/d} \rceil$ and writing n base m , i.e. $n = c_d m^d + \dots + c_0$, $0 \leq c_i < m$. To ensure the proper size, we make sure to take $n > 2^{d^2}$. This immediately yields

$$(3.1) \quad f(x) = c_0 + c_1 x + \dots + c_d x^d$$

Lemma 3.1. $c_d = 1$, and $c_{d-1} \leq d$.

Proof. Since we took $n > 2^{d^2}$, we get that $\binom{d}{i} \leq 2^d - 2 \leq n^{\frac{1}{d}} - 2 \leq m - 1$. Since the coefficients of $(m+1)^d$ base m are the binomial coefficients, the Lemma follows from $m^d \leq n < (m+1)^d$. \square

We note that f may indeed be reducible; in that case, it turns out that the non-trivial factorization of f yields a partial factorization of n , which would reduce us to a new and easier case [?]. So we'll continue with the assumption that f is in fact irreducible.

4. FINDING S

We want to find a set S of coprime integer pairs such that

$$(4.1) \quad \prod_{(a,b) \in S} (a + bm) \quad \text{is a square in } \mathbf{Z}$$

$$(4.2) \quad \prod_{(a,b) \in S} (a + b\alpha) \quad \text{is a square in } \mathbf{Z}[\alpha].$$

We first need to find a set T of coprime integers pairs (a, b) such that we have $a + bm$ is a product of small primes, hence called smooth, and that $a + b\alpha$ is "smooth" as well, as we'll define later. We then find $S \subset T$.

In choosing S and T , define a set U , $S \subset T \subset U$. This U is basically a bound for S and T , and we'll define it as $\{(a, b) : a, b \in \mathbf{Z}, \gcd(a, b) = 1, |a| \leq u, 0 < b \leq u\}$. In this way, we see that u bounds S and T for some large enough choice of u .

We now proceed on two fronts. The first is to examine (2.2) within \mathbf{Z} , which is a relatively simple task, and the second is to examine (2.3) within $\mathbf{Z}[\alpha]$, which is not such a simple task.

5. FINDING A SQUARE IN \mathbf{Z}

Take some parameter y specific to n , and we find a subset $T_1 = \{(a, b) \in U : a + bm \text{ is } y\text{-smooth}\}$. Here, a number is y -smooth if all its prime divisors are less than or equal to y . We sieve by fixing an integer b , $0 < b \leq u$, and along this line in the array we have the integers $a + bm$ for $|a| \leq u$. Then, for every prime $p \leq y$, we find the numbers in the array where $a \equiv -bm \pmod{p}$, and divide out by all the powers of p and replace that new number back in the same place where we took the old one from. We will then have at the a th place the largest divisor of $a + bm$ that is prime to y . Look for ± 1 - these will be the places where $a + bm$ is y -smooth. Where $\gcd(a, b) = 1$, we have then found our elements of T_1 .

Say that $\#T_1 > \pi(y) + 1$, where $\#T_1$ is the cardinality of T_1 and $\pi(y)$ is the number of primes less than or equal to y . Take $B = \pi(y)$, and let p_j be the j th prime (by convention, we set $p_0 = -1$). Then, for a y -smooth integer w , we have

$$(5.1) \quad w = \prod_{j=0}^B p_j^{e_j}.$$

Set $e(w) = (e_0 \pmod{2}, \dots, e_B \pmod{2}) \in \mathbf{F}_2^{B+1}$. Since $\#T_1 > \dim \mathbf{F}_2^{B+1} / \mathbf{F}_2$, we have that the set of $e(a + bm)$ as (a, b) runs through T_1 is linearly dependent in the vector space \mathbf{F}_2^{B+1} . We then take S such that

$$\sum_{(a,b) \in S} e(a + bm) = 0 \in \mathbf{F}_2^{B+1}.$$

This immediately yields (2.2).

6. FINDING A SQUARE IN $\mathbf{Z}[\alpha]$

We basically want to mimic the sieving technique that we used in the previous section; the problem is that $\mathbf{Z}[\alpha]$ is rarely a unique factorization domain, so we'll have to delve deeper into the structure of $\mathbf{Z}[\alpha]$. Buhler notes in [?] that in their searches, when $\mathbf{Z}[\alpha]$ hasn't been a U.F.D., \mathcal{O} , its ring of integers, has been.

In any event, we define $\beta \in \mathbf{Z}[\alpha]$ to be y -smooth if its norm, $N(\beta)$, is. Note that for $a, b \in \mathbf{Z}$, $N(a + b\alpha) = a^d - c_{d-1}a^{d-1}b + \dots + (-1)^d c_0 b^d$. We take a set similar to T_1 ; namely, we take a set $T_2 = \{(a, b) \in U : a + b\alpha \text{ is } y\text{-smooth}\}$. We want to look at the zeros of $f \pmod{p}$, and we denote that set as $R(p)$.

Like in the last section, we make an array; this time, instead of $a + bm$ in each place, for $|a| \leq u$, we have $N(a + b\alpha)$. For each b , then, we run through all primes relatively prime to b and less than or equal to y and all $r \in R(p)$, and find all such $(a + b\alpha)$ where $N(a + b\alpha) = 0$, which is precisely when $a \equiv -br \pmod{p}$. We then divide a by its highest power of p and put the new number in the old one's place. We continue this process just like in the above section, looking for the places that end up with value ± 1 ; these are our y -smooth values of $(a + b\alpha)$, and so for $\gcd(a, b) = 1$ we've found our members of T_2 .

The problem is that here, we don't have that

$$\prod_{(a,b) \in S} (a + b\alpha) \text{ is a square in } \mathbf{Z}[\alpha];$$

rather, we have that its norm is. To deal with this this problem we define

$$e_{p,r}(a + b\alpha) = \begin{cases} \text{ord}_p(N(a + b\alpha)) & \text{if } a + br \equiv 0 \pmod{p} \\ 0 & \text{otherwise,} \end{cases}$$

where $\text{ord}_p(k)$ is the highest power of p that divides k . This yields

$$N(a + b\alpha) = \pm \prod_{p,r} p^{e_{p,r}(a+b\alpha)}.$$

In order to proceed further, we need to recall some definitions. The norm $\mathfrak{N}\mathfrak{p}$ of a prime ideal \mathfrak{p} of $\mathbf{Z}[\alpha]$ is $\#\mathbf{Z}[\alpha]/\mathfrak{p}$; the degree of \mathfrak{p} is k , where $\mathbf{Z}[\alpha]/\mathfrak{p} \cong \mathbf{F}_{p^k}$. \mathfrak{p} is called a first degree prime if $k = 1$. If \mathfrak{p} is first degree, then we have the canonical map $\mathbf{Z}[\alpha] \rightarrow \mathbf{Z}_p$ with kernel \mathfrak{p} , and it sends α to some zero of $f \pmod{p}$, which we'll call r . In this manner, every first degree prime \mathfrak{p} is naturally associated to some pair of integers p, r . This correspondence is a bijection because the map $\mathbf{Z}[\alpha] \rightarrow \mathbf{F}_p$ is completely determined by the choice of r . We note that \mathfrak{p} is generated by p and $\alpha - r$.

If we examine what $e_{p,r}(a + b\alpha)$ is, it's a generalization of the valuation of the ideal generated by $a + b\alpha$ from \mathcal{O} to $\mathbf{Z}[\alpha]$. In order to prove this generalization, we need, for K^* the field of fractions of $\mathbf{Z}[\alpha]$, a

Proposition 6.1. *There is, for each prime \mathfrak{p} of $\mathbf{Z}[\alpha]$, a group homomorphism $\iota_{\mathfrak{p}} : K^* \rightarrow \mathbf{Z}$, such that the following hold:*

- (a) $\iota_{\mathfrak{p}}(\beta) \geq 0$ for all nonzero $\beta \in \mathbf{Z}[\alpha]$
- (b) if $\beta \in \mathbf{Z}[\alpha]$, β nonzero, then $\iota_{\mathfrak{p}}(\beta) > 0$ if and only if $\beta \in \mathfrak{p}$
- (c) for each $\beta \in K^*$, we have $\iota_{\mathfrak{p}}(\beta) = 0$ for all but finitely many \mathfrak{p} , and

$$\prod_{\mathfrak{p}} (\mathfrak{N}\mathfrak{p})^{\iota_{\mathfrak{p}}(\beta)} = |N(\beta)|$$

where \mathfrak{p} ranges over the prime ideals of $\mathbf{Z}[\alpha]$.

We defer the proof of this until later, but note that it is hardly a large jump from the work we have done in lecture.

We further want a

Corollary 6.2. *Take coprime integers a and b . If \mathfrak{p} is not a first degree prime, then $\iota_{\mathfrak{p}}(a + b\alpha) = 0$. If \mathfrak{p} is a first degree prime corresponding to p, r , then $\iota_{\mathfrak{p}}(a + b\alpha) = e_{p,r}(a + b\alpha)$.*

Proof. Take \mathfrak{p} a prime ideal with $\mathfrak{N}\mathfrak{p} = p^n$, $\iota_{\mathfrak{p}}(a + b\alpha) > 0$. By Proposition 6.4(b), under the map induced upon $\mathbf{Z}[\alpha] \rightarrow \mathbf{Z}[\alpha]/\mathfrak{p}$, $a + b\alpha$ maps to zero. But b can't map to zero, or we'll violate $\gcd(a, b) = 1$; hence, it maps to some element whose inverse is in \mathbf{F}_p . Thus, since $a + b\alpha$ maps to 0, we have that α in fact belongs to \mathbf{F}_p as well, which means that all of $\mathbf{Z}[\alpha]$ maps to \mathbf{F}_p . This implies that \mathfrak{p} is first degree and thus gives us part one of the Corollary. From our bijection of \mathfrak{p} and pair p, r , we have that \mathfrak{p} is the unique prime ideal that contains p and $a + b\alpha$. The last part of the Corollary follows immediately from examining the exponent in part (c) of the above Proposition. \square

To complete our initial examination, we give a proposition whose converse we will need.

Proposition 6.3. *Suppose we have our set S such that $\prod_{(a,b) \in S} (a + b\alpha)$ is some square in K . Then, for each prime p and each $r \in R(p)$, we have*

$$\sum_{(a,b) \in S} e_{p,r}(a + b\alpha) \equiv 0 \pmod{2}.$$

Proof. We take $\prod_{(a,b) \in S} (a + b\alpha) = \gamma^2$, and let the first degree prime \mathfrak{p} correspond to p, r . We get that

$$\sum_{(a,b) \in S} e_{p,r}(a + b\alpha) = \sum_{(a,b) \in S} \iota_{\mathfrak{p}}(a + b\alpha) = \iota_{\mathfrak{p}}\left(\prod_{(a,b) \in S} (a + b\alpha)\right) = \iota_{\mathfrak{p}}(\gamma^2) = 2\iota_{\mathfrak{p}}(\gamma) \equiv 0 \pmod{2}$$

and we're done. \square

7. IN SEARCH OF A CONVERSE

We will now set out to find a way to construct a set that gives us the converse of Proposition 6.3. Consider the set H of first degree primes \mathfrak{p} with $\mathfrak{N}\mathfrak{p} \leq y$; let $\#H = B'$. When $\#T_2 > B'$, we can do the same thing we did in section 5 by finding a set $S \subset T_2$ such that

$$(7.1) \quad \sum_{(a,b) \in S} \iota_{\mathfrak{p}}(a + b\alpha) \equiv 0 \pmod{2} \quad \text{for all } \mathfrak{p}.$$

There are four obstructions to saying that this S is exactly what we want, and they are:

- 1) The ideal generated by $\prod_{(a,b) \in S} (a + b\alpha)$ in \mathcal{O} might not be the square of an ideal.
- 2) Even if the ideal is a square, the square root ideal might not be principal.
- 3) Even if the the ideal generated in \mathcal{O} is the square of an ideal generated by some $\gamma \in \mathcal{Q}$, it might not be that $\prod_{(a,b) \in S} (a + b\alpha) = \gamma^2$.
- 4) Even if we have $\prod_{(a,b) \in S} (a + b\alpha) = \gamma^2$, we don't know that $\gamma \in \mathbf{Z}[\alpha]$.

Let's tackle the last problem first. It turns out to have a simple answer, namely if we have that

$$\prod_{(a,b) \in S} (a + b\alpha) = \gamma^2$$

with $\gamma \in K$, then we have that $\gamma \in \mathcal{O}$ and $\gamma f'(\alpha) \in \mathbf{Z}[\alpha]$ (see [?, Proposition 3-7-14]). What this means is we have to multiply everything by $f'(m)^2$ in order to factor, but the bottom line is that

$$(7.2) \quad f'(\alpha)^2 \cdot \prod_{(a,b) \in S} (a + b\alpha) \quad \text{is a square of something in } \mathbf{Z}[\alpha].$$

That we have to multiply by $f'(\alpha)^2$ above and by $f'(m)^2$ in equation (7.2) won't hinder our factorization efforts. We note that by assumption, $\gcd(f'(m), n) = 1$; otherwise n splits and we restart our algorithm.

Solving the first three obstructions, however, is more complicated. We will appeal to quadratic characters to do so. For this, we'll need to assume that $n > d^{2d^2}$. First, consider a finite set $X \subset \mathbf{Z}$ of primes. For motivation, suppose for some nonzero integer l that it factors completely into primes p_i such that $\text{ord}_{p_i}(l)$ is odd if $p_i \notin X$. Can we then say that l is a square? The answer clearly requires our knowledge of the sign of l as well as the exponents of the $p_i \in X$. But even if we didn't have that information, we could still test l for squareness. We do so as follows: for $p \notin X$, p not dividing $2l$, we take $(\frac{l}{p})$, the Legendre character. If $(\frac{l}{p}) = -1$ then l is not a square. If we run this for significantly more primes than $\#X$ and it yields 1 every time, we can be pretty certain that l is a square. We'll make this idea more concrete below.

To being ourselves back to the task at hand, we have the

Proposition 7.1. *Let S be a finite set of coprime integer pairs such that $\text{prod}_{(a,b) \in S} (a+b\alpha)$ is a square in K . Take an odd prime q and $s \in R(q)$ such that $a+bs \not\equiv 0 \pmod q$ as (a,b) runs through S and $f'(s) \not\equiv 0 \pmod q$. Then we have*

$$\prod_{(a,b) \in S} \left(\frac{a+bs}{q} \right) = 1.$$

Proof. We take the first degree prime ideal \mathfrak{q} that corresponds to q, s . This induces a map $\mathbf{Z}[\alpha] \rightarrow \mathbf{F}_q$ such that $\alpha \mapsto s \pmod q$ with kernel \mathfrak{q} . From this, we define $\chi_{\mathfrak{q}} \mathbf{Z}[\alpha] - \mathfrak{q} \rightarrow \{\pm 1\}$ as the composition of $\mathbf{Z}[\alpha] - \mathfrak{q} \rightarrow \mathbf{F}_q - \{0\}$ with the Legendre symbol mod q . This immediately yields $\chi_{\mathfrak{q}}(a+b\alpha) = (\frac{a+bs}{q})$. The Proposition follows by applying $\chi_{\mathfrak{q}}$ to equation (7.2). \square

We note that what we really want is the converse of the above Proposition, and here we can get it. If some $\beta \in \mathbf{Z}[\alpha]$ satisfies $\chi_{\mathfrak{q}}(\beta) = 1$ for all primes \mathfrak{p} that are first degree, $2\beta \notin \mathfrak{q}$, then β is a square in K .

Moving on, we set $T = T_1 \cap T_2$ and define:

$$B = \pi(y)$$

$$B' = \# \text{ of first degree primes with norm } \leq y$$

$$B'' = \lceil 3(\log n) / \log 2 \rceil.$$

We create 3 orderings. The first is a list p_1, p_2, \dots, p_B . The second is the list of pairs $(p_1, r_1), \dots, (p_{B'}, r_{B'})$ corresponding to the B' y -smooth first degree prime ideals. The third list takes B'' ordered pairs of primes q_i and $s_i \in R(p)$ such that $f'(s_i) \not\equiv 0 \pmod{q_i}$, and order them by increasing q_i . Define $e : T \rightarrow \mathbf{F}_2^{1+B+B'+B''}$. The first coordinate is the sign of $a+bm$; it's 1 if it's positive and 0 if it's not. The next B coordinates are $\text{ord}_{p_i}(a+bm)$ as we run through the p_i . The next B' coordinates are $e_{p_i, r_i}(a+b\alpha) \pmod 2$. Finally, the last B'' coordinates are the Legendre symbol $(\frac{a+bs}{q})$ with $e : 1 \mapsto 0, -1 \mapsto 1$.

The idea is that since we have (or want to have) $\#T > 1+B+B'+B''$, then the $e(a,b)$ as (a,b) run over T are linearly dependent over $\mathbf{F}_2^{1+B+B'+B''}$. The set S is then the subset of T such that $\sum_{(a,b) \in S} e(a,b) = 0 \in \mathbf{F}_2^{1+B+B'+B''}$. This gives us (2.3) immediately.

The claim is that we also have equation (7.1). This involves a rather elaborate explanation which can only be proven with an as yet unproven strong version of the Chebotarev density theorem. What happens is one can consider the density of prime ideals \mathfrak{q} in $\mathbf{Z}[\alpha]$ such that $f'(\alpha) \notin \mathfrak{q}$ and order them by increasing norms. Then

a strong version of the density theorem will imply that the $\chi_{\mathfrak{q}}$ are asymptotically equally distributed over $\text{Hom}(V/K^{*2}, \{\pm 1\})$, where $V \subset K^*$ is the subgroup of all β such that $\iota_{\mathfrak{p}}(\beta) \equiv 0 \pmod{2}$ for all primes \mathfrak{p} of $\mathbf{Z}[\alpha]$. This combined with the high odds that the $\chi_{\mathfrak{q}}$ span $\text{Hom}(V/K^{*2}, \{\pm 1\})$ would give us (7.1).

8. SQUARE ROOTS IN $\mathbf{Z}[\alpha]$

Finding the square root of $f'(\alpha)^2 \cdot \prod_{(a,b) \in S} (a + bm)$ is easy, especially because all the work is done mod n . On the other hand, given some $\gamma^2 \in \mathbf{Z}[\alpha]$, finding γ is by no means trivial.

The first problem is that we really can't work mod n like in the \mathbf{Z} case, so we may be dealing with huge numbers. It turns out that the bulk of the run time for the number field sieve will actually be taken up by this problem. In fact, the method suggested in [?] is to set $\delta = f'(\alpha)^2 \cdot \prod_{(a,b) \in S} (a + b\alpha)$. The way to solve for the square is to consider the polynomial $x^2 - \delta \in K[x]$ and solve it using one of many existing algorithms that solve polynomials over number fields. The question of what algorithm to choose, while interesting, speaks more to the computational complexity of the question rather than the number theoretic underpinnings that are more the province of this paper, so we won't get into them here (a lengthy discussion is contained in [?]). No matter which algorithm is chosen, the question of solving the polynomial is by no means a quick one, and so the time taken to run the sieve will depend rather directly on this run time.

9. THE NUMBER FIELD SIEVE

For completion, we now state the algorithm in its entirety. We are given some integer n to factor and then choose parameters d , u , and y such that $d > 1$, $n > d^{2d^2}$, and y and u are sufficiently large. This algorithm will either find a nontrivial factor of n or prove that it's prime, although it will halt eventually regardless of its success achieving this.

Step 1. See whether n is either a prime power or divisible by a prime that is less than or equal to y . If so, output the prime and stop.

Step 2. Set $m = \lceil n^{1/d} \rceil$ and let f be as in (3.1). Then $f(m) \equiv 0 \pmod{n}$. Factor f into irreducible factors by the algorithm given in [?]. If $g \in \mathbf{Z}[x]$ is a nontrivial factor of f , output $g(m)$ and stop. Otherwise, f is irreducible and let α be a zero of f . Take $\gcd(f'(m), n)$; if it's a nontrivial factor of n , output the number and stop.

Step 3. As we showed above, use a sieve to find the set

$$T = \{(a, b) \in \mathbf{Z}^2 : \gcd(a, b) = 1, |a| \leq u, 0 < b \leq u, (a+bm)N(a+b\alpha) \text{ is } y \text{ smooth}\}.$$

Step 4. Let A be the matrix with $\#T$ columns and whose rows are the \mathbf{F}_2 -vectors $e(a, b)$ as the (a, b) run over T . Try to find a non-trivial linear dependence relation on the rows in the matrix. One can use the Wiederman coordinate recurrence algorithm to accomplish this [?]. If it doesn't work, stop. Otherwise, let S be the set of (a, b) such that $e(a, b)$ occurs in the dependence relation.

Step 5. Set $\delta = f'(\alpha)^2 \cdot \prod_{(a,b) \in S} (a + b\alpha)$ as a polynomial over α . Using a polynomial solving algorithm, try to find the square root, γ , of δ . If unsuccessful, stop.

Step 6. Find the square root, c , of $f'(\alpha)^2 \cdot \prod_{(a,b) \in S} (a + bm) \pmod n$.

Step 7. Compute $\gcd(c, h)$, where h is $\phi(\delta)$, ϕ being defined in Section 2 (recall $\phi(\alpha) = m \pmod n$). If this is a nontrivial factor of n , output the number and stop. Otherwise, remove an element of S from T and go to Step 4.

10. THE PROOF OF PROPOSITION 6.1

As promised, we will now give the proof of Proposition 6.1. Actually, we will prove a more general case. We first recall some facts from algebraic number theory. Set K to be an algebraic number field with K^* its group of units. Let A be an order in K , an order being a subring of the ring of integers, $\mathcal{O} \subset K$, such that $(\mathcal{O} : A) < \infty$ considered as additive groups. Note that $\mathbf{Z}[\alpha]$ is an order in $\mathbf{Q}(\alpha)$. As we saw in lecture, we have a well defined norm map $\mathfrak{N}\mathfrak{a} = \#A/\mathfrak{a}$, for \mathfrak{a} an ideal of A ; this builds on the norm map $N(a) = \#A/aA$ for $a \in A$. Further, if \mathfrak{p} is a prime ideal of A , then $\mathfrak{N}\mathfrak{p} = p^k$ for some prime integer p . We state our Proposition bearing in mind that this proves Proposition 6.1 for the case where $A = \mathbf{Z}[\alpha]$.

Proposition 10.1. *For each prime ideal $\mathfrak{p} \subset A$, there exists a group homomorphism $\iota_{\mathfrak{p}} : K^* \rightarrow \mathbf{Z}$ such that we have the following:*

- (a) $\iota_{\mathfrak{p}}(x) \geq 0$ for all nonzero $x \in A$;
- (b) for nonzero $x \in A$, $\iota_{\mathfrak{p}}(x) = 0$ if and only if $x \in \mathfrak{p}$;
- (c) for each $x \in K^*$, $\iota_{\mathfrak{p}}(x) = 0$ for all but finitely many \mathfrak{p} , and

$$\prod_{\mathfrak{p}} (\mathfrak{N}\mathfrak{p})^{\iota_{\mathfrak{p}}(x)} = |N(x)|,$$

where \mathfrak{p} ranges over the primes of A .

Proof. We explicitly construct $\iota_{\mathfrak{p}}$. Let \mathfrak{p} be prime and take a nonzero $x \in A$. Since A is finite over xA , we have some finite chain of ideals

$$A = \mathfrak{a}_0 \supset \mathfrak{a}_1 \supset \dots \supset \mathfrak{a}_t = xA$$

such that the tower can't be further refined. We take $\iota_{\mathfrak{p}}(x)$ to be the i such that $\mathfrak{a}_{i-1}/\mathfrak{a}_i \cong A/\mathfrak{p}$. From the Jordan-Holder theorem (see [?, p. 156]), we see that $\iota_{\mathfrak{p}}$ doesn't depend on the choice of \mathfrak{a}_i 's for the tower. For $x, y \in A$ nonzero, we can associate the towers $\mathfrak{a}_0 \supset \mathfrak{a}_1 \supset \dots \supset \mathfrak{a}_t$ and $\mathfrak{b}_0 \supset \mathfrak{b}_1 \supset \dots \supset \mathfrak{b}_u$ for x and y , respectively. For the element xy , we then have the tower $y\mathfrak{a}_0 \supset y\mathfrak{a}_1 \supset \dots \supset y\mathfrak{a}_t = \mathfrak{a}_0 \supset \mathfrak{a}_1 \supset \dots \supset \mathfrak{a}_t$. This shows us that we have $\iota_{\mathfrak{p}}(xy) = \iota_{\mathfrak{p}}(x) + \iota_{\mathfrak{p}}(y)$. We can extend $\iota_{\mathfrak{p}}$ to K^* by setting $\iota_{\mathfrak{p}}(x/y) = \iota_{\mathfrak{p}}(x) - \iota_{\mathfrak{p}}(y)$. From this construction, it is immediate that (a) holds.

For (b), we note the "if" part holds when we take $\mathfrak{a}_1 = \mathfrak{p}$ if $x \in \mathfrak{p}$. For the "only if" part, assume $x \notin \mathfrak{p}$. We get that the ideal $xA + \mathfrak{p}$ equals A since \mathfrak{p} is maximal, so for some $y \in A$ and $z \in \mathfrak{p}$, we have that $xy + z = 1$. Since this means that $z \equiv 1 \pmod{xA}$, we get that multiplication by z induces the identity map on A/xA . This gives us $z(\mathfrak{a}_{i-1}/\mathfrak{a}_i) = \mathfrak{a}_{i-1}/\mathfrak{a}_i$, which implies that $\mathfrak{a}_{i-1}/\mathfrak{a}_i$ isn't isomorphic to A/\mathfrak{p} since $z \in \mathfrak{p}$.

To prove (c), we just need to show it holds for $x \in A$. We then have that $|N(x)| = \#A/xA = \prod_{i=1}^t \#\mathfrak{a}_{i-1}/\mathfrak{a}_i$. We then only need to show that for each i there is a unique prime \mathfrak{p} such that $\mathfrak{a}_{i-1}/\mathfrak{a}_i \cong A/\mathfrak{p}$. Since our tower of ideals couldn't be refined, we have that for $y \in \mathfrak{a}_{i-1} - \mathfrak{a}_i$, $yA + \mathfrak{a}_i = \mathfrak{a}_{i-1}$, so multiplication by y induces the surjective map $A \rightarrow \mathfrak{a}_{i-1}/\mathfrak{a}_i$. This gives us that $\mathfrak{a}_{i-1}/\mathfrak{a}_i \cong A/\mathfrak{p}$ for some prime \mathfrak{p} ; since we have no trivial submodules, \mathfrak{p} is maximal. Additionally, since \mathfrak{p} is the annihilator of the A -module $\mathfrak{a}_{i-1}/\mathfrak{a}_i$, the ideal is uniquely determined. \square

REFERENCES

- [1] J. Brillhart, M. Filaseta, A. Odlyzko, *On an irreducibility theorem of A. Cohn*, Can. J. Math, **33** (1981), pp. 1055-1059.
- [2] J. P. Buhler, H. W. Lenstra, C. Pomerance, *Factoring integers with the number field sieve*, The development of the number field sieve, Springer Verlag, Berlin, Germany, 1993, pp. 50-94.
- [3] S. Lang, *Algebra*, Springer Verlag, New York, 2002.
- [4] A. K. Lenstra, H. W. Lenstra, Jr., L. Lovasz, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), pp. 515-534.
- [5] A. K. Lenstra, H. W. Lenstra, Jr., M. S. Manasse, J. M. Pollard, *Factoring integers with the number field sieve*, The development of the number field sieve, Springer Verlag, Berlin, Germany, 1993, pp. 11-42.
- [6] J. M. Pollard, *Factoring with cubic integers*, The development of the number field sieve, Springer Verlag, Berlin, Germany, 1993, pp. 4-10.
- [7] E. Weiss, *Algebraic number theory*, Chelsea, New York, 1976.
- [8] D. Wiedermann, *Solving sparse linear equations over finite fields*, IEEE Trans. Inform. Theory **32** (1986), pp. 54-62.