The Number Field Sieve

Let $f$ be an irreducible monic polynomial in $\mathbb{Z}[x]$. Let $\alpha$ be a root of $f$. Let $m$ be an integer for which $f(m) \equiv 0 \pmod{n}$.

Preliminaries: Let $n$ be a large positive integer, and let $b$ be an integer $\geq 3$ smaller than $n$. Suppose we write $n$ in base $b$, so

$$n = c_db^d + c_{d-1}b^{d-1} + \cdots + c_1b + c_0,$$

for some positive integer $d$ and each $c_j \in \{0, 1, \ldots, b - 1\}$. Set $f(x) = \sum_{j=0}^{d} c_j x^j$. Then one of the following holds:

(i) The polynomial $f(x)$ is irreducible over $\mathbb{Q}[x]$.

(ii) The polynomial $f(x) = g(x)h(x)$ for $g(x)$ and $h(x)$ in $\mathbb{Z}[x]$, and $n = g(b)h(b)$ is a non-trivial factorization of $n$.

Comment: We can use $f(x)$ above and $m = b = \lfloor n^{1/d} \rfloor$. 
Let $f$ be an irreducible monic polynomial in $\mathbb{Z}[x]$. Let $\alpha$ be a root of $f$. Let $m$ be an integer for which $f(m) \equiv 0 \pmod{n}$. The mapping $\phi : \mathbb{Z}[\alpha] \rightarrow \mathbb{Z}_n$ with $\phi(g(\alpha)) = g(m) \pmod{n}$ for all $g(x) \in \mathbb{Z}[x]$ is a homomorphism. (Recall what $\mathbb{Z}[\alpha]$ is.)
The Number Field Sieve

Let \( f \) be an irreducible monic polynomial in \( \mathbb{Z}[x] \). Let \( \alpha \) be a root of \( f \). Let \( m \) be an integer for which \( f(m) \equiv 0 \pmod{n} \). The mapping \( \phi : \mathbb{Z}[\alpha] \to \mathbb{Z}_n \) with \( \phi(g(\alpha)) = g(m) \pmod{n} \) for all \( g(x) \in \mathbb{Z}[x] \) is a homomorphism. (Recall what \( \mathbb{Z}[\alpha] \) is.) The idea is to find a set \( S \) of polynomials \( g(x) \in \mathbb{Z}[x] \) such that both of the following hold:

(i) \( \prod_{g \in S} g(m) = y^2 \) for some \( y \in \mathbb{Z} \)

(ii) \( \prod_{g \in S} g(\alpha) = \beta^2 \) for some \( \beta \in \mathbb{Z}[\alpha] \).

Taking \( x = \phi(\beta) \), we deduce

\[
x^2 \equiv \phi(\beta)^2 \equiv \phi(\beta^2) \equiv \phi \left( \prod_{g \in S} g(\alpha) \right) \equiv \prod_{g \in S} g(m) \equiv y^2 \pmod{n}.
\]

Thus, we can hope to factor \( n \) by computing \( \gcd(x + y, n) \).
The Number Field Sieve

The idea is to find a set $S$ of polynomials $g(x) \in \mathbb{Z}[x]$ such that both of the following hold:

(i) $\prod_{g \in S} g(m) = y^2$ for some $y \in \mathbb{Z}$

(ii) $\prod_{g \in S} g(\alpha) = \beta^2$ for some $\beta \in \mathbb{Z}[\alpha]$.

Taking $x = \phi(\beta)$, we deduce

$$x^2 \equiv \phi(\beta)^2 \equiv \phi(\beta^2) \equiv \phi \left( \prod_{g \in S} g(\alpha) \right) \equiv \prod_{g \in S} g(m) \equiv y^2 \pmod{n}.$$  

What do we choose for the $g(x)$?

Take $g(x)$ of the form $a - bx$ where $|a| \leq D$ and $0 < b \leq D$. 

What do we choose for the $g(x)$?

Take $g(x)$ of the form $a - bx$ where $|a| \leq D$ and $0 < b \leq D$.

We want $g(m)$ to have only small prime factors. This is done by first choosing $b$ and then, with $b$ fixed, letting $a$ vary and sieving to determine the $a$ for which $g(m)$ has only small prime factors.

$$(i) \prod_{g \in S} g(m) = y^2 \text{ for some } y \in \mathbb{Z}$$

$$(ii) \prod_{g \in S} g(\alpha) = \beta^2 \text{ for some } \beta \in \mathbb{Z}[\alpha].$$

How do we obtain the desired square in $\mathbb{Z}[\alpha]$?
What do we choose for the $g(x)$?

Take $g(x)$ of the form $a - bx$ where $|a| \leq D$ and $0 < b \leq D$.

We want $g(m)$ to have only small prime factors. This is done by first choosing $b$ and then, with $b$ fixed, letting $a$ vary and sieving to determine the $a$ for which $g(m)$ has only small prime factors.

How do we obtain the desired square in $\mathbb{Z}[\alpha]$?

Let $\alpha_1, \ldots, \alpha_d$ be the distinct roots of $f(x)$ with $\alpha = \alpha_1$. We consider the norm map $N(g(\alpha)) = g(\alpha_1) \cdots g(\alpha_d)$, where $g(x) \in \mathbb{Z}[x]$. It has the two properties:

- If $g(x)$ and $h(x)$ are in $\mathbb{Z}[x]$, then
  \[ N(g(\alpha)h(\alpha)) = N(g(\alpha))N(h(\alpha)). \]

- If $g(x) \in \mathbb{Z}[x]$, then $N(g(\alpha)) \in \mathbb{Z}$. 
How do we obtain the desired square in \( \mathbb{Z}[\alpha] \)?

Let \( \alpha_1, \ldots, \alpha_d \) be the distinct roots of \( f(x) \) with \( \alpha = \alpha_1 \). We consider the norm map \( N(g(\alpha)) = g(\alpha_1) \cdots g(\alpha_d) \), where \( g(x) \in \mathbb{Z}[x] \). It has the two properties:

- If \( g(x) \) and \( h(x) \) are in \( \mathbb{Z}[x] \), then
  \[
  N( g(\alpha) h(\alpha) ) = N(g(\alpha)) N(h(\alpha)).
  \]
- If \( g(x) \in \mathbb{Z}[x] \), then \( N(g(\alpha)) \in \mathbb{Z} \).

Observe that the norm of a square in \( \mathbb{Z}[\alpha] \) is a square in \( \mathbb{Z} \). On the other hand,

\[
N(a - b\alpha) = b^d \prod_{j=1}^{d} \left( \frac{a_j}{b} - \alpha_j \right) = b^d f(a/b)
\]

\[
= a^d + c_{d-1}a^{d-1}b + \cdots + c_1ab^{d-1} + c_0b^d.
\]

As we force the product \( \pi S \) to be a square.
How do we obtain the desired square in \( \mathbb{Z}[\alpha] \)?

Observe that the norm of a square in \( \mathbb{Z}[\alpha] \) is a square in \( \mathbb{Z} \). On the other hand,

\[
N(a - b\alpha) = b^d \prod_{j=1}^{d} \left( \frac{a}{b} - \alpha_j \right) = b^d f(a/b)
\]

\[
= a^d + c_{d-1} a^{d-1} b + \cdots + c_1 a b^{d-1} + c_0 b^d.
\]

The idea is to try to obtain a set \( S \) of pairs \((a, b)\) as above. As we force the product \( \prod (a - bm) \) to be a square (products over \((a, b) \in S\)), we also force \( \prod (a^d + c_{d-1} a^{d-1} b + \cdots + c_0 b^d) \) to be a square.

This can be done by working with a matrix of exponents, in the prime factorizations of the above, modulo 2 similar to what is done in Dixon’s algorithm.
The Number Field Sieve

Let $f$ be an irreducible monic polynomial in $\mathbb{Z}[x]$. Let $\alpha$ be a root of $f$. Let $m$ be an integer for which $f(m) \equiv 0 \pmod{n}$. The mapping $\phi : \mathbb{Z}[\alpha] \rightarrow \mathbb{Z}_n$ with $\phi(g(\alpha)) = g(m) \pmod{n}$ for all $g(x) \in \mathbb{Z}[x]$ is a homomorphism. (Recall what $\mathbb{Z}[\alpha]$ is.) The idea is to find a set $S$ of polynomials $g(x) \in \mathbb{Z}[x]$ such that both of the following hold:

(i) $\prod_{g \in S} g(m) = y^2$ for some $y \in \mathbb{Z}$

(ii) $\prod_{g \in S} g(\alpha) = \beta^2$ for some $\beta \in \mathbb{Z}[\alpha]$.

Taking $x = \phi(\beta)$, we deduce

$$x^2 \equiv \phi(\beta)^2 \equiv \phi(\beta^2) \equiv \phi\left(\prod_{g \in S} g(\alpha)\right) \equiv \prod_{g \in S} g(m) \equiv y^2 \pmod{n}.$$ 

Thus, we can hope to factor $n$ by computing $\text{gcd}(x + y, n)$. 

Comment 2: What does this mean if $b$ is a prime?
The Number Field Sieve

The idea is to find a set $S$ of polynomials $g(x) \in \mathbb{Z}[x]$ such that both of the following hold:

(i) $\prod_{g \in S} g(m) = y^2$ for some $y \in \mathbb{Z}$

(ii) $\prod_{g \in S} g(\alpha) = \beta^2$ for some $\beta \in \mathbb{Z}[\alpha]$.

Taking $x = \phi(\beta)$, we deduce

$$x^2 \equiv \phi(\beta)^2 \equiv \phi(\beta^2) \equiv \phi \left( \prod_{g \in S} g(\alpha) \right) \equiv \prod_{g \in S} g(m) \equiv y^2 \pmod{n}.$$ 

Note that we have obtained $\prod_{g \in S} g(\alpha)$ having a square norm.

Sadly, this does not mean that it is a square in $\mathbb{Z}[\alpha]$. But it is a start. How do we finish up?
The Number Field Sieve

Comment 1: The running time for the number field sieve is \( \exp \left( c (\log n)^{1/3} (\log \log n)^{2/3} \right) \) where \( c = 4/(3^{2/3}) \) will do.

Comment 2: In 1993, Lenstra, Lenstra, Manasse, and Pollard used the number field sieve to factor \( F_9 = 2^{2^9} + 1 \).
Public-Key Encryption

Problem: How do you communicate with someone you have never met before through the personals without anyone else understanding the private material you are sharing with this stranger.

Initial Idea: Take advantage of something you know that no one else knows. Find two large primes $p$ and $q$. Compute $n = pq$. If you are secretive about your choices for $p$ and $q$ and they are large enough, then you can tell the world what $n$ is and you will know something no one else in the world knows, namely how $n$ factors. You also know what $(n) = (p^{-1})q$ is.
Public-Key Encryption

Problem: How do you communicate with someone you have never met before through the personals without anyone else understanding the private material you are sharing with this stranger.

Initial Idea: Take advantage of something you know that no one else knows. Find two large primes $p$ and $q$. Compute $n = pq$. If you are secretive about your choices for $p$ and $q$ and they are large enough, then you can tell the world what $n$ is and you will know something no one else in the world knows, namely how $n$ factors.
Public-Key Encryption

Problem: How do you communicate with someone you have never met before through the personals without anyone else understanding the private material you are sharing with this stranger.

Initial Idea: Take advantage of something you know that no one else knows. Find two large primes $p$ and $q$. Compute $n = pq$. If you are secretive about your choices for $p$ and $q$ and they are large enough, then you can tell the world what $n$ is and you will know something no one else in the world knows, namely how $n$ factors. You also know what $\phi(n) = (p - 1)(q - 1)$ is.
The Rest:

- Choose \( s \in \mathbb{Z}^+ \) (the “encrypting exponent”) with \( \text{gcd}(s, \phi(n)) = 1 \).

- Publish \( n \) and \( s \) in the personals.

- Tell them that to form a message \( M \), concatenate the symbols 00 for blank, 01 for a, 02 for b, ..., 26 for z, 27 for a comma, 28 for a period, and whatever else you might want.

Example. \( M = 0805121215 \)
The Rest:

- Choose $s \in \mathbb{Z}^+$ (the “encrypting exponent”) with \( \gcd(s, \phi(n)) = 1 \).

- Publish $n$ and $s$ in the personals.

- Tell them that to form a message $M$, concatenate the symbols 00 for blank, 01 for a, 02 for b, ..., 26 for z, 27 for a comma, 28 for a period, and whatever else you might want.

- Tell the person to publish (back in the personals) the value of $E = M^s \mod n$. (The person should be told to make sure that $M^s > n$ by adding extra blanks if necessary and that $M < n$ by breaking up a message into two or more messages if necessary.)
The Rest:

- Choose $s \in \mathbb{Z}^+$ (the “encrypting exponent”) with $\gcd(s, \phi(n)) = 1$.

- Publish $n$ and $s$ in the personals.

- Tell them that to form a message $M$, concatenate the symbols 00 for blank, 01 for a, 02 for b, ..., 26 for z, 27 for a comma, 28 for a period, and whatever else you might want.

- Tell the person to publish (back in the personals) the value of $E = M^s \mod n$. (The person should be told to make sure that $M^s > n$ by adding extra blanks if necessary and that $M < n$ by breaking up a message into two or more messages if necessary.)
The Rest:

- Choose $s \in \mathbb{Z}^+$ (the “encrypting exponent”) with $\gcd(s, \phi(n)) = 1$.
- Publish $n$ and $s$ in the personals.
- Tell them that to form a message $M$, concatenate the symbols 00 for blank, 01 for a, 02 for b, ..., 26 for z, 27 for a comma, 28 for a period, and whatever else you might want.
- Tell the person to publish (back in the personals) the value of $E = M^s$ and the modulus $n$.

What can you do with the encoded message $E$?

An outsider can’t compute $\phi(n)$, and you expect me to compute $\phi(\phi(n))$? mod $n$?

Calculate $t$ with $st \equiv 1 \pmod{\phi(n)}$ (one can use $t \equiv s^{\phi(\phi(n))^{-1}} \pmod{\phi(n)}$). Then compute $E^t \mod n$. This will be the same as $M$ modulo $n$ (unless $p$ or $q$ divides $M$, which isn’t likely).
Certified signatures

Basic Set-Up. Imagine person $A$ has published $n$ and $s$ in the personals, person $B$ is corresponding with person $A$ in the personals, and person $C$ gets jealous. $C$ decides to send $A$ a message in the personals that reads something like, “Dear $A$, I think you are a jerk. Your dear friend, $B$.” This of course would make $A$ very upset with $B$ and would make $C$ very happy. What would be nice is if there were a way for $B$ to sign his messages so that $A$ can see the signature and know whether a message supposedly from $B$ is really from $B$. 
Certified signatures

• $B$ has his very own $n$ and $s$ which he has shared with at least $A$. Call them $n'$ and $s'$, and let the corresponding $t$ be $t'$.

• $B$ informs $A$ of some signature $S$ that $B$ will use.

• At the end of $B$’s encrypted message $E$, he gives $A$ the number $T = S^{t'} \mod n'$. This is part of $E$.

• After $A$ decodes the message, he computes $T^{s'} \mod n'$ (remember $n'$ and $s'$ are public). The result will be $S$.

Comment: Since only $B$ knows $t'$, only $B$ can determine $T$, and $A$ will know that the message really came from $B$. 
Factoring Polynomials

Notation. Let $p$ be a prime, and let $f(x) \in \mathbb{Z}[x]$ with $f(x) \not\equiv 0 \pmod{p}$. We say

$$u(x) \equiv v(x) \pmod{p, f(x)}$$

where $u(x)$ and $v(x)$ are in $\mathbb{Z}[x]$, if there exist $g(x)$ and $h(x)$ in $\mathbb{Z}[x]$ such that $u(x) = v(x) + f(x)g(x) + ph(x)$.

Properties:

- If

$$u(x) \equiv v(x) \pmod{p, f(x)} \text{ and } v(x) \equiv w(x) \pmod{p, f(x)},$$

then $u(x) \equiv w(x) \pmod{p, f(x)}$. 
Properties:

- If
  \[ u(x) \equiv v(x) \pmod{p, f(x)} \quad \text{and} \quad v(x) \equiv w(x) \pmod{p, f(x)}, \]
  then \( u(x) \equiv w(x) \pmod{p, f(x)} \).

- If
  \[ u_1(x) \equiv v_1(x) \pmod{p, f(x)} \quad \text{and} \quad u_2(x) \equiv v_2(x) \pmod{p, f(x)}, \]
  then \( u_1(x) \pm u_2(x) \equiv v_1(x) \pm v_2(x) \pmod{p, f(x)} \).

- If
  \[ u_1(x) \equiv v_1(x) \pmod{p, f(x)} \quad \text{and} \quad u_2(x) \equiv v_2(x) \pmod{p, f(x)}, \]
  then \( u_1(x)u_2(x) \equiv v_1(x)v_2(x) \pmod{p, f(x)} \).

- If \( u(x) \equiv v(x) \pmod{p} \) or \( u(x) \equiv v(x) \pmod{f(x)} \),
  then \( u(x) \equiv v(x) \pmod{p, f(x)} \).
Properties:

- If
  \[ u(x) \equiv v(x) \pmod{(p, f(x))} \quad \text{and} \quad v(x) \equiv w(x) \pmod{(p, f(x))}, \]
  then \[ u(x) \equiv w(x) \pmod{(p, f(x))}. \]

- If
  \[ u_1(x) \equiv v_1(x) \pmod{(p, f(x))} \quad \text{and} \quad u_2(x) \equiv v_2(x) \pmod{(p, f(x))}, \]
  then \[ u_1(x) \pm u_2(x) \equiv v_1(x) \pm v_2(x) \pmod{(p, f(x))}. \]

- If
  \[ u_1(x) \equiv v_1(x) \pmod{(p, f(x))} \quad \text{and} \quad u_2(x) \equiv v_2(x) \pmod{(p, f(x))}, \]
  then \[ u_1(x)u_2(x) \equiv v_1(x)v_2(x) \pmod{(p, f(x))}. \]

- If \[ u(x) \equiv v(x) \pmod{p} \quad \text{or} \quad u(x) \equiv v(x) \pmod{f(x)}, \]
  then \[ u(x) \equiv v(x) \pmod{(p, f(x))}. \]
Properties:

- If \( u(x) \equiv v(x) \pmod{p, f(x)} \) and \( v(x) \equiv w(x) \pmod{p, f(x)} \),
  then \( u(x) \equiv w(x) \pmod{p, f(x)} \).
- If \( u_1(x) \equiv v_1(x) \pmod{p, f(x)} \) and \( u_2(x) \equiv v_2(x) \pmod{p, f(x)} \),
  then \( u_1(x) \pm u_2(x) \equiv v_1(x) \pm v_2(x) \pmod{p, f(x)} \).
- If \( u_1(x) \equiv v_1(x) \pmod{p, f(x)} \) and \( u_2(x) \equiv v_2(x) \pmod{p, f(x)} \),
  then \( u_1(x)u_2(x) \equiv v_1(x)v_2(x) \pmod{p, f(x)} \).
- If \( u(x) \equiv v(x) \pmod{p} \) or \( u(x) \equiv v(x) \pmod{f(x)} \),
  then \( u(x) \equiv v(x) \pmod{p, f(x)} \).
- We have \( u(x) \equiv 0 \pmod{p, f(x)} \) if and only if \( f(x) \) is a factor of \( u(x) \) modulo \( p \).