Quadratic Sieve Factoring Method - part 2

How it works

Define $Q(x) = x^2 - n$.

Pick integers $x_1, x_2, ..., x_k$ such that $Q(x_1), Q(x_2), ..., Q(x_k)$ factors over a chosen set of small primes.

From the set $\{x_1, x_2, ..., x_k\}$, pick a subset such that $Q(x_{i_1})Q(x_{i_2})...Q(x_{i_r})$ is a perfect square, say $A^2$.

Check if $x_{i_1}^2 x_{i_2}^2 ... x_{i_r}^2 = A^2 \mod n$ gives the factorization of $n$.

Since $Q(x_i) = x_i^2 \mod n$ we have that $Q(x_{i_1})Q(x_{i_2})...Q(x_{i_r}) = A^2 = (x_{i_1} x_{i_2} ... x_{i_r})^2 \mod n$.

Then, by Fermat's theorem we have that either $\gcd(x_{i_1} x_{i_2} ... x_{i_r} - A, n)$ or $\gcd(x_{i_1} x_{i_2} ... x_{i_r} + A, n)$ is a factor of $n$. 

Quadratic Sieve Factoring Method - part 2
How it works

- Define $Q(x) = x^2 - n$
How it works

- Define $Q(x) = x^2 - n$
- Pick integers $x_1, x_2, ..., x_k$ such that $Q(x_1), Q(x_2), ..., Q(x_k)$ factors over a chosen set of small primes.
How it works

- Define $Q(x) = x^2 - n$
- Pick integers $x_1, x_2, ..., x_k$ such that $Q(x_1), Q(x_2), ..., Q(x_k)$ factors over a chosen set of small primes.
- From the set $\{x_1, x_2, ..., x_k\}$, pick a subset such that $Q(x_{i_1})Q(x_{i_2})...Q(x_{i_r})$ is a perfect square, say $A^2$. 
How it works

- Define $Q(x) = x^2 - n$
- Pick integers $x_1, x_2, ..., x_k$ such that $Q(x_1), Q(x_2), ..., Q(x_k)$ factors over a chosen set of small primes.
- From the set $\{x_1, x_2, ..., x_k\}$, pick a subset such that $Q(x_{i_1})Q(x_{i_2})...Q(x_{i_r})$ is a perfect square, say $A^2$.
- Check if $x_{i_1}^2x_{i_2}^2, ..., x_{i_r}^2 = A^2 \mod n$ gives the factorization of $n$. 
How it works

- Define $Q(x) = x^2 - n$
- Pick integers $x_1, x_2, ..., x_k$ such that $Q(x_1), Q(x_2), ..., Q(x_k)$ factors over a chosen set of small primes.
- From the set $\{x_1, x_2, ..., x_k\}$, pick a subset such that $Q(x_{i_1})Q(x_{i_2})...Q(x_{i_r})$ is a perfect square, say $A^2$.
- Check if $x_1^2x_2^2, ..., x_{i_r}^2 = A^2 \mod n$ gives the factorization of $n$. 
How it works

- Define \( Q(x) = x^2 - n \)
- Pick integers \( x_1, x_2, ..., x_k \) such that \( Q(x_1), Q(x_2), ..., Q(x_k) \) factors over a chosen set of small primes.
- From the set \( \{x_1, x_2, ..., x_k\} \), pick a subset such that \( Q(x_{i_1})Q(x_{i_2})...Q(x_{i_r}) \) is a perfect square, say \( A^2 \).
- Check if \( x_1^2x_2^2, ..., x_{i_r}^2 = A^2 \ mod \ n \) gives the factorization of \( n \).

Since \( Q(x_i) = x_i^2 \ mod \ n \) we have that

\[
Q(x_{i_1})Q(x_{i_2})...Q(x_{i_r})
\]
How it works

- Define $Q(x) = x^2 - n$
- Pick integers $x_1, x_2, ..., x_k$ such that $Q(x_1), Q(x_2), ..., Q(x_k)$ factors over a chosen set of small primes.
- From the set $\{x_1, x_2, ..., x_k\}$, pick a subset such that $Q(x_{i_1})Q(x_{i_2})...Q(x_{i_r})$ is a perfect square, say $A^2$.
- Check if $x_{i_1}^2x_{i_2}^2, ..., x_{i_r}^2 = A^2 \mod n$ gives the factorization of $n$.

Since $Q(x_i) = x_i^2 \mod n$ we have that

$$Q(x_{i_1})Q(x_{i_2})...Q(x_{i_r}) = A^2 =$$
How it works

- Define $Q(x) = x^2 - n$
- Pick integers $x_1, x_2, ..., x_k$ such that $Q(x_1), Q(x_2), ..., Q(x_k)$ factors over a chosen set of small primes.
- From the set $\{x_1, x_2, ..., x_k\}$, pick a subset such that $Q(x_{i_1})Q(x_{i_2})...Q(x_{i_r})$ is a perfect square, say $A^2$.
- Check if $x_1^2x_2^2, ..., x_{i_r}^2 = A^2 \mod n$ gives the factorization of $n$.

Since $Q(x_i) = x_i^2 \mod n$ we have that

$$Q(x_{i_1})Q(x_{i_2})...Q(x_{i_r}) = A^2 = (x_{i_1}x_{i_2}...x_{i_r})^2 \mod n.$$
How it works

- Define $Q(x) = x^2 - n$
- Pick integers $x_1, x_2, ..., x_k$ such that $Q(x_1), Q(x_2), ..., Q(x_k)$ factors over a chosen set of small primes.
- From the set $\{x_1, x_2, ..., x_k\}$, pick a subset such that $Q(x_{i_1})Q(x_{i_2})...Q(x_{i_r})$ is a perfect square, say $A^2$.
- Check if $x_1^2x_2^2, ..., x_r^2 = A^2 \mod n$ gives the factorization of $n$.

Since $Q(x_i) = x_i^2 \mod n$ we have that

$$Q(x_{i_1})Q(x_{i_2})...Q(x_{i_r}) = A^2 = (x_{i_1}x_{i_2}...x_{i_r})^2 \mod n.$$  

Then, by Fermat's theorem we have that either $gcd(x_{i_1}x_{i_2}...x_{i_r} - A, n)$ or $gcd(x_{i_1}x_{i_2}...x_{i_r} + A, n)$ is a factor of $n$.  

Defining a sieving interval and constructing a factor base

Define a sieving interval $\left\lceil \frac{n}{2} \right\rceil - M, \left\lceil \frac{n}{2} \right\rceil + M$ with optimal value for $M = \exp\left(\frac{\ln(n)}{\ln(\ln(n))} \right) \frac{3}{4}$.

The integers $x_i$ will be chosen from this interval.

Define a factor base to be the set of all primes $p$ with $\text{legendre}(n, p) = 1$ and less than $B$ and the number $(-1)$.

The number $B$ effects the number of primes in the factor base and depends on the size of $n$.

The optimal value for $B$ is $\exp\left(\frac{1}{2} + o(1) \right) \left(\log n \log \log n \right)^{1/2}$.

For example, a factor base of 524,339 primes was used to factor RSA - 129.
Defining a sieving interval and constructing a factor base

Define a sieving interval \([\lceil n^{1/2} \rceil - M, \lceil n^{1/2} \rceil + M]\) with optimal value for \(M = \exp(\ln n \ln(\ln n))^{3\sqrt{2}/4}\).

The integers \(x_i\) will be chosen from this interval. Define a factor base to be the set of all primes \(p\) with \(\text{legendre}(n, p) = 1\) and less than \(B\) and the number \((-1)\). The number \(B\) effects the number of primes in the factor base and depends on the size of \(n\). The optimal value for \(B\) is \(\exp((1/2 + o(1))(\log n \log \log n))^{1/2}\). For example, a factor base of 524,339 primes was used to factor RSA - 129.
Defining a sieving interval and constructing a factor base

- Define a sieving interval $[\lceil n^{1/2} \rceil - M, \lceil n^{1/2} \rceil + M]$ with optimal value for $M = \exp(\ln n \ln(\ln n))^{3\sqrt{2}/4}$. The integers $x_i$ will be chosen from this interval.
Defining a sieving interval and constructing a factor base

- Define a sieving interval \([\lceil n^{1/2} \rceil - M, \lceil n^{1/2} \rceil + M]\) with optimal value for \(M = \exp(\ln n \ln(\ln n))^{3\sqrt{2}/4}\). The integers \(x_i\) will be chosen from this interval.
- Define a factor base to be the set of all primes \(p\) with \(\text{legendre}(n, p) = 1\) and less than \(B\) and the number \((-1)\).
Define a sieving interval $\lceil n^{1/2} \rceil - M, \lceil n^{1/2} \rceil + M$ with optimal value for $M = \exp(lnnln(lnn))^{3\sqrt(2)/4}$. The integers $x_i$ will be chosen from this interval.

Define a factor base to be the set of all primes $p$ with $\text{legendre}(n, p) = 1$ and less than $B$ and the number $(-1)$. The number $B$ effects the number of primes in the factor base and depends on the size of $n$. 
Defining a sieving interval and constructing a factor base

- Define a sieving interval \([\lceil n^{1/2} \rceil - M, \lceil n^{1/2} \rceil + M]\) with optimal value for \(M = \exp(ln n \ln(n))^{3\sqrt(2)/4}\). The integers \(x_i\) will be chosen from this interval.

- Define a factor base to be the set of all primes \(p\) with \(\text{legendre}(n, p) = 1\) and less than \(B\) and the number \((-1)\). The number \(B\) effects the number of primes in the factor base and depends on the size of \(n\). The optimal value for \(B\) is \(\exp((1/2 + o(1))(\log n \log \log n)^{1/2})\).
Define a sieving interval \([\lceil n^{1/2} \rceil - M, \lceil n^{1/2} \rceil + M]\) with optimal value for \(M = \exp(\ln n \ln(\ln n))^{3\sqrt{2}/4}\). The integers \(x_i\) will be chosen from this interval.

Define a factor base to be the set of all primes \(p\) with \(\text{legendre}(n, p) = 1\) and less than \(B\) and the number \((-1)\). The number \(B\) effects the number of primes in the factor base and depends on the size of \(n\). The optimal value for \(B\) is \(\exp((1/2 + o(1))(\log n \log \log n)^{1/2})\).

For example, a factor base of 524,339 primes was used to factor RSA - 129.
Sieving

Suppose \( p \) is in the factor base for \( n \). For each \( p \) in the factor base use Tonelli-Shanks Algorithm to solve \( r^2 = n \mod p \) to find the roots \( r = \pm a_p \mod p \).

If \( p | Q(x) \), then \( x^2 = n = a_p^2 \mod p \), then \( x = \pm a_p \mod p \).

This means that if \( p | Q(x) \), then \( x = kp \pm a_p \).

This way we able to eliminate many \( Q(x) \)'s that do not factor over the factor base without obtaining a factorization of every \( Q(x) \) by trial division.

We are able to select \( Q(x) \)'s that are likely to be factored over the factorized base.
Suppose \( p \) is in the factor base for \( n \).
Suppose $p$ is in the factor base for $n$.

- For each $p$ in the factor base use Tonelli-Shanks Algorithm to solve $r^2 = n \mod p$ to find the roots $r = \pm a_p \mod p$. 

This way we can eliminate many $Q(x)$'s that do not factor over the factor base without obtaining a factorization of every $Q(x)$ by trial division. We are able to select $Q(x)$'s that are likely to be factored over the factor base.
Suppose $p$ is in the factor base for $n$.

- For each $p$ in the factor base use Tonelli-Shanks Algorithm to solve $r^2 = n \mod p$ to find the roots $r = \pm a_p \mod p$.
- If $p | Q(x)$, then $x^2 = n = a_p^2 \mod p$, then $x = \pm a_p \mod p$. 

This way we are able to eliminate many $Q(x)$'s that do not factor over the factor base without obtaining a factorization of every $Q(x)$ by trial division. We are able to select $Q(x)$'s that are likely to be factored over the factorized base.
Suppose \( p \) is in the factor base for \( n \).

- For each \( p \) in the factor base use Tonelli-Shanks Algorithm to solve \( r^2 = n \mod p \) to find the roots \( r = \pm a_p \mod p \).
- If \( p \mid Q(x) \), then \( x^2 = n = a_p^2 \mod p \), then \( x = \pm a_p \mod p \).
- This means that if \( p \mid Q(x) \), then \( x = kp \pm a_p \).
Suppose $p$ is in the factor base for $n$.

- For each $p$ in the factor base use Tonelli-Shanks Algorithm to solve $r^2 = n \mod p$ to find the roots $r = \pm a_p \mod p$.
- If $p | Q(x)$, then $x^2 = n = a_p^2 \mod p$, then $x = \pm a_p \mod p$.
- This means that if $p | Q(x)$, then $x = kp \pm a_p$.
- This way we able to eliminate many $Q(x)$’s that do not factor over the factor base without obtaining a factorization of every $Q(x)$ by trial division.
Suppose $p$ is in the factor base for $n$.

- For each $p$ in the factor base use Tonelli-Shanks Algorithm to solve $r^2 = n \mod p$ to find the roots $r = \pm a_p \mod p$.
- If $p | Q(x)$, then $x^2 = n = a_p^2 \mod p$, then $x = \pm a_p \mod p$.
- This means that if $p | Q(x)$, then $x = kp \pm a_p$.
- This way we able to eliminate many $Q(x)$’s that do not factor over the factor base without obtaining a factorization of every $Q(x)$ by trial division. We are able to select $Q(x)$’s that are likely to be factored over the factored base.
Let's $n = 17819$. 

Let $\{2, 5, 7\}$ be the factor base and $[128, 138]$ be the sieving interval. Let $x \in [128, 138]$. Since $n = 1 \pmod{2}$, $Q(x)$ is divisible by 2 for $x$ odd. Since $n = 4 \pmod{5}$, $Q(x)$ is divisible by 5 when $x = 2, 3 \pmod{5}$. Since $n = 4 \pmod{7}$, $Q(x)$ is divisible by 7 when $x = 2, 5 \pmod{7}$. We can eliminate $x = 130, 134, 136$ since $Q(x)$ for these values of $x$ don't have factors from the factor base. The values of $Q(x)$ for $x = 128, 131, 133, 135, 137, 138$ are likely to factor over the primes in the factor base. It is easy to see that $Q(138) = 5^2 \cdot 7^2$. This term is a perfect square, so yields the congruence $138^2 = 35^2 \pmod{n}$. From here we get that $\gcd(138 - 35, n) = 103$ is one of the factors of $n$. 

Quadratic Sieve Factoring Method - part 2
Let's $n = 17819$. Let $\{2, 5, 7\}$ be the factor base and
Let’s \( n = 17819 \). Let \( \{2, 5, 7\} \) be the factor base and \( [128, 138] \) be the sieving interval.
Let's $n = 17819$. Let $\{2, 5, 7\}$ be the factor base and $[128, 138]$ be the sieving interval. Let $x \in [128, 138]$. Since $n = 1 \mod 2$, 

Since $n = 4 \mod 5$, $Q(x)$ is divisible by 5 when $x = 2, 3 \mod 5$. 

Since $n = 4 \mod 7$, $Q(x)$ is divisible by 7 when $x = 2, 5 \mod 7$. We can eliminate $x = 130, 134, 136$ since $Q(x)$ for these values of $x$ don't have factors from the factor base. 

The values of $Q(x)$ for $x = 128, 131, 133, 135, 137, 138$ are likely to factor over the primes in the factor base. It is easy to see that $Q(138) = 5^2 \cdot 7^2$. This term is a perfect square, so yields the congruence $138^2 \equiv 35^2 \mod n$. From here we get that $\gcd(138 - 35, n) = 103$ is one of the factors of $n$. 

Quadratic Sieve Factoring Method - part 2
Let’s $n = 17819$. Let \{2, 5, 7\} be the factor base and [128, 138] be the sieving interval. Let $x \in [128, 138]$. Since $n = 1 \mod 2$, $Q(x)$ is divisible by 2 for $x$ odd.
Let's \( n = 17819 \). Let \( \{2, 5, 7\} \) be the factor base and \([128, 138]\) be the sieving interval. Let \( x \in [128, 138] \). Since \( n = 1 \mod 2 \), \( Q(x) \) is divisible by 2 for \( x \) odd. Since \( n = 4 \mod 5 \),
Let's $n = 17819$. Let $\{2, 5, 7\}$ be the factor base and $[128, 138]$ be the sieving interval. Let $x \in [128, 138]$. Since $n = 1 \mod 2$, $Q(x)$ is divisible by 2 for $x$ odd. Since $n = 4 \mod 5$, $Q(x)$ is divisible by 5 when $x = 2, 3 \mod 5$. We can eliminate $x = 130, 134, 136$ since $Q(x)$ for these values don't have factors from the factor base.

The values of $Q(x)$ for $x = 128, 131, 133, 135, 137, 138$ are likely to factor over the primes in the factor base. It is easy to see that $Q(138) = 5^2 \cdot 7^2$. This term is a perfect square, so yields the congruence $138^2 \equiv 35^2 \mod n$. From here we get that $\gcd(138 - 35, n) = 103$ is one of the factors of $n$. 
Let's $n = 17819$. Let $\{2, 5, 7\}$ be the factor base and $[128, 138]$ be the sieving interval. Let $x \in [128, 138]$. Since $n = 1 \mod 2$, $Q(x)$ is divisible by 2 for $x$ odd. Since $n = 4 \mod 5$, $Q(x)$ is divisible by 5 when $x = 2, 3 \mod 5$. Since $n = 4 \mod 7$, $Q(x)$ is divisible by 7 when $x = 2, 5 \mod 7$. We can eliminate $x = 130, 134, 136$ since $Q(x)$ for these values of $x$ don't have factors from the factor base. The values of $Q(x)$ for $x = 128, 131, 133, 135, 137, 138$ are likely to factor over the primes in the factor base. It is easy to see that $Q(138) = 5^2 \cdot 7^2$. This term is a perfect square, so yields the congruence $138^2 \equiv 35^2 \mod n$. From here we get that $\gcd(138 - 35, n) = 103$ is one of the factors of $n$. 
Let’s $n = 17819$. Let $\{2, 5, 7\}$ be the factor base and $[128, 138]$ be the sieving interval. Let $x \in [128, 138]$. Since $n = 1 \mod 2, Q(x)$ is divisible by 2 for $x$ odd. Since $n = 4 \mod 5, Q(x)$ is divisible by 5 when $x = 2, 3 \mod 5$. Since $n = 4 \mod 7, Q(x)$ is divisible by 7 when $x = 2, 5 \mod 7$. We can eliminate
Let’s $n = 17819$. Let $\{2, 5, 7\}$ be the factor base and $[128, 138]$ be the sieving interval. Let $x \in [128, 138]$. Since $n = 1 \mod 2$, $Q(x)$ is divisible by 2 for $x$ odd. Since $n = 4 \mod 5$, $Q(x)$ is divisible by 5 when $x = 2, 3 \mod 5$. Since $n = 4 \mod 7$, $Q(x)$ is divisible by 7 when $x = 2, 5 \mod 7$. We can eliminate $x = 130, 134, \text{ and } 136$.\[Q(138) = 5^2 \cdot 7^2\]This term is a perfect square, so yields the congruence $138^2 = 35^2 \mod n$. From here we get that $\gcd(138 - 35, n) = 103$ is one of the factors of $n$.\[103\]
Let’s $n = 17819$. Let \{2, 5, 7\} be the factor base and [128, 138] be the sieving interval. Let $x \in [128, 138]$. Since $n = 1 \mod 2$, $Q(x)$ is divisible by 2 for $x$ odd. Since $n = 4 \mod 5$, $Q(x)$ is divisible by 5 when $x = 2, 3 \mod 5$. Since $n = 4 \mod 7$, $Q(x)$ is divisible by 7 when $x = 2, 5 \mod 7$. We can eliminate $x = 130, 134, \text{ and } 136$ since $Q(x)$ for these values of $x$ don’t have factors from the factor base.

The values of $Q(x)$ for $x = 128, 131, 133, 135, 137, \text{ and } 138$ are likely to factor over the primes in the factor base. It is easy to see that $Q(138) = 5^2 \cdot 7^2$. This term is a perfect square, so yields the congruence $138^2 = 35^2 \mod n$. From here we get that $\gcd(138 - 35, n) = 103$ is one of the factors of $n$. 

Quadratic Sieve Factoring Method - part 2

Sieving - example
Let’s $n = 17819$. Let $\{2, 5, 7\}$ be the factor base and $[128, 138]$ be the sieving interval. Let $x \in [128, 138]$. Since $n = 1 \mod 2, Q(x)$ is divisible by 2 for $x$ odd. Since $n = 4 \mod 5, Q(x)$ is divisible by 5 when $x = 2, 3 \mod 5$. Since $n = 4 \mod 7, Q(x)$ is divisible by 7 when $x = 2, 5 \mod 7$. We can eliminate $x = 130, 134, \text{ and } 136$ since $Q(x)$ for these values of $x$ don’t have factors from the factor base. The values of $Q(x)$ for $x = 128, 131, 133, 135, 137 \text{ and } 138$ are likely to factor over the primes in the factor base.
Let’s \( n = 17819 \). Let \( \{2, 5, 7\} \) be the factor base and \([128, 138]\) be the sieving interval. Let \( x \in [128, 138] \). Since \( n = 1 \mod 2 \), \( Q(x) \) is divisible by 2 for \( x \) odd. Since \( n = 4 \mod 5 \), \( Q(x) \) is divisible by 5 when \( x = 2, 3 \mod 5 \). Since \( n = 4 \mod 7 \), \( Q(x) \) is divisible by 7 when \( x = 2, 5 \mod 7 \). We can eliminate \( x = 130, 134, \) and 136 since \( Q(x) \) for these values of \( x \) don’t have factors from the factor base. The values of \( Q(x) \) for \( x = 128, 131, 133, 135, 137 \) and 138 are likely to factor over the primes in the factor base. It is easy to see that \( Q(138) = 5^2 \cdot 7^2 \). This term is a perfect square, so yields the congruence \( 138^2 = 35^2 \mod n \). From here we get that \( \gcd(138 - 35, n) = 103 \) is one of the factors of \( n \).
Define $S(x) = \log(|Q(x)|) = \sum_{i=1}^{r} \log(p_i)$.

For each prime $p$ in the factor base check if $p$ divides $Q(x)$. If yes, subtract $\log(p)$ from $S(x)$. If not, eliminate that $Q(x)$ and go to the next $Q(x)$.
Speeding up the sieving

Define \( S(x) = \log(|Q(x)|) \)

For each prime \( p \) in the factor base check if \( p \) divides \( Q(x) \). If yes, subtract \( \log p \) from \( S(x) \). If not, eliminate that \( Q(x) \) and go to the next \( Q(x) \).
Speeding up the sieving

- Define $S(x) = \log(|Q(x)|) = \sum_{i=1}^{r} \log(p_i)$.
Define $S(x) = \log(|Q(x)|) = \sum_{i=1}^{r} \log(p_i)$.

For each prime $p$ in the factor base check if $p$ divides $Q(x)$.
Speeding up the sieving

- Define $S(x) = \log(|Q(x)|) = \sum_{i=1}^{r} \log(p_i)$. 
- For each prime $p$ in the factor base check if $p$ divides $Q(x)$. 
- If yes, subtract $\log p$ from $S(x)$. If not, eliminate that $Q(x)$ and go to the next $Q(x)$. 

Quadratic Sieve Factoring Method - part 2
Speeding up the sieving

- Define $S(x) = \log(|Q(x)|) = \sum_{i=1}^{r} \log(p_i)$.
- For each prime $p$ in the factor base check if $p$ divides $Q(x)$.
- If yes, subtract $\log p$ from $S(x)$. If not, eliminate that $Q(x)$ and go to the next $Q(x)$. 
Speeding up the sieving-Example

Let's $n = 87463$. 

Let the set $\{2, 3, 13, 17, 19, 29\}$ be the factor base and $[195, 395]$ be the sieving interval. Then $S(x) = \log(|Q(x)|) < \log(p_{\text{max}}) = \log(29) = 3.36$. The only values of $x$ for which $S(x) < 3.36$ are $x = 265, 278, 296, 307$ and $347$. Here is the prime factorization of $Q(x)$'s:

- $x = 265$: $Q(x) = -1 \cdot 2 \cdot 3 \cdot 13^2 \cdot 17$
- $x = 278$: $Q(x) = -1 \cdot 3^3 \cdot 13 \cdot 29$
- $x = 296$: $Q(x) = 3^2 \cdot 17$
- $x = 299$: $Q(x) = 2 \cdot 3 \cdot 17 \cdot 19$
- $x = 307$: $Q(x) = 2 \cdot 3^2 \cdot 13 \cdot 19$
- $x = 347$: $Q(x) = 2 \cdot 3 \cdot 17^2 \cdot 19$
Speeding up the sieving - Example

Let's $n = 87463$. Let the set $\{2, 3, 13, 17, 19, 29\}$ be the factor base.
Speeding up the sieving - Example

Let's \( n = 87463 \). Let the set \( \{2, 3, 13, 17, 19, 29\} \) be the factor base and \([195, 395]\) be the sieving interval.

The only values of \( x \) for which \( S(x) < 3.36 \) are \( x = 265, 278, 296, 307 \) and \( 347 \). Here is the prime factorization of \( Q(x) \):

- \( x = 265 \):
  \( Q(x) = -1 \cdot 2 \cdot 3 \cdot 13 \cdot 17^2 \cdot 19 \)

- \( x = 278 \):
  \( Q(x) = -1 \cdot 3^3 \cdot 13 \cdot 29 \)

- \( x = 296 \):
  \( Q(x) = 3^2 \cdot 17 \)

- \( x = 299 \):
  \( Q(x) = 2 \cdot 3 \cdot 17 \cdot 19 \)

- \( x = 307 \):
  \( Q(x) = 2 \cdot 3^2 \cdot 13 \cdot 19 \)

- \( x = 347 \):
  \( Q(x) = 2 \cdot 3 \cdot 17^2 \cdot 19 \)
Speeding up the sieving—Example

Let's $n = 87463$. Let the set $\{2, 3, 13, 17, 19, 29\}$ be the factor base and $[195, 395]$ be the sieving interval. Then

$$S(x) = \log(|Q(x)|) < \log(p_{max}) = \log(29) = 3.36.$$
Speeding up the sieving-Example

Let's \( n = 87463 \). Let the set \( \{2, 3, 13, 17, 19, 29\} \) be the factor base and \([195, 395]\) be the sieving interval. Then

\[
S(x) = \log(|Q(x)|) < \log(p_{max}) = \log(29) = 3.36.
\]

The only values of \( x \) for which \( S(x) < 3.36 \) are
Let's $n = 87463$. Let the set $\{2, 3, 13, 17, 19, 29\}$ be the factor base and $[195, 395]$ be the sieving interval. Then

$$S(x) = \log(|Q(x)|) < \log(p_{\text{max}}) = \log(29) = 3.36.$$ 

The only values of $x$ for which $S(x) < 3.36$ are $x = 265, 278, 296, 307$ and $347$. 

Here is the prime factorization of $Q(x)$'s:

$x = 265$: $Q(x) = -1 \cdot 2 \cdot 3 \cdot 13^2 \cdot 17$

$x = 278$: $Q(x) = -1 \cdot 3^3 \cdot 13 \cdot 29$

$x = 296$: $Q(x) = 3^2 \cdot 17$

$x = 307$: $Q(x) = 2 \cdot 3 \cdot 17 \cdot 19$

$x = 347$: $Q(x) = 2 \cdot 3 \cdot 17^2 \cdot 19$
Speeding up the sieving - Example

Let's \( n = 87463 \). Let the set \( \{2, 3, 13, 17, 19, 29\} \) be the factor base and \([195, 395]\) be the sieving interval. Then

\[
S(x) = \log(|Q(x)|) < \log(p_{\text{max}}) = \log(29) = 3.36.
\]

The only values of \( x \) for which \( S(x) < 3.36 \) are \( x = 265, 278, 296, 307 \) and 347.

Here is the prime factorization of \( Q(x) \)'s:
Speeding up the sieving—Example

Let's $n = 87463$. Let the set $\{2, 3, 13, 17, 19, 29\}$ be the factor base and $[195, 395]$ be the sieving interval. Then

$$S(x) = \log(|Q(x)|) < \log(p_{max}) = \log(29) = 3.36.$$ 

The only values of $x$ for which $S(x) < 3.36$ are $x=265, 278, 296, 307$ and 347.

Here is the prime factorization of $Q(x)$'s:

$x=265$: $Q(x) = -1 \cdot 2 \cdot 3 \cdot 13^2 \cdot 17$

$x=278$: $Q(x) = -1 \cdot 3^3 \cdot 13 \cdot 29$

$x=296$: $Q(x) = 3^2 \cdot 17$

$x=299$: $Q(x) = 2 \cdot 3 \cdot 17 \cdot 19$

$x=307$: $Q(x) = 2 \cdot 3^2 \cdot 13 \cdot 19$

$x=347$: $Q(x) = 2 \cdot 3 \cdot 17^2 \cdot 19$
Gaussian elimination

Assume the following factorization of the $Q(x)$ that are selected after the sieving process:

\[
Q(x_1) = p^{a_{11}} \cdot p^{a_{12}} \cdot \ldots \cdot p^{a_{1r}}
\]

\[
Q(x_k) = p^{a_{k1}} \cdot p^{a_{k2}} \cdot \ldots \cdot p^{a_{kr}}
\]

where $p_1, p_2, \ldots, p_r$ are the primes from the factor base including $-1$. We have to find $e_1, e_2, \ldots, e_k$ such that $Q(x_1)^{e_1} Q(x_2)^{e_2} \ldots Q(x_k)^{e_k}$ is a perfect square.

Using the prime factorization of $Q(x)$ we find the numbers $e_1, e_2, \ldots, e_k$ such that $e_{a_{1i}} + e_{a_{2i}} + \ldots + e_{a_{ki}}$ is even for all $i = 1, 2, \ldots, r$.

We have to solve the equation $eA \equiv 0 \pmod{2}$ where $e = (e_1, e_2, \ldots, e_k)$ and $A$ is the matrix whose $ij$th entry is $a_{ij}$. 
Gaussian elimination

Assume the following factorization of the $Q(x)$ that are selected after the sieving process:
Gaussian elimination

Assume the following factorization of the $Q(x)$ that are selected after the sieving process:

$$Q(x_1) = p_1^{a_{11}} \cdot p_2^{a_{12}} \cdot \ldots \cdot p_r^{a_{1r}}$$

.............

$$Q(x_k) = p_1^{a_{k1}} \cdot p_2^{a_{k2}} \cdot \ldots \cdot p_r^{a_{kr}}$$
Gaussian elimination

Assume the following factorization of the $Q(x)$ that are selected after the sieving process:

$$Q(x_1) = p_1^{a_1} \cdot p_2^{a_2} \cdot ... \cdot p_r^{a_r}$$

............... 

$$Q(x_k) = p_1^{a_{k1}} \cdot p_2^{a_{k2}} \cdot ... \cdot p_r^{a_{kr}}$$

where $p_1, p_2, ..., p_r$ are the primes from the factor base including $(-1)$. 
Gaussian elimination

Assume the following factorization of the $Q(x)$ that are selected after the sieving process:

$$Q(x_1) = p_1^{a_{11}} \cdot p_2^{a_{12}} \cdot \ldots \cdot p_r^{a_{1r}}$$

.............

$$Q(x_k) = p_1^{a_{k1}} \cdot p_2^{a_{k2}} \cdot \ldots \cdot p_r^{a_{kr}}$$

where $p_1, p_2, \ldots, p_r$ are the primes from the factor base including $(-1)$. We have to find $e_1, e_2, \ldots, e_k$ such that
Gaussian elimination

Assume the following factorization of the $Q(x)$ that are selected after the sieving process:

$$Q(x_1) = p_1^{a_{11}} \cdot p_2^{a_{12}} \cdot \ldots \cdot p_r^{a_{1r}}$$

```

```

$$Q(x_k) = p_1^{a_{k1}} \cdot p_2^{a_{k2}} \cdot \ldots \cdot p_r^{a_{kr}}$$

where $p_1, p_2, \ldots, p_r$ are the primes from the factor base including ($-1$). We have to find $e_1, e_2, \ldots, e_k$ such that $Q(x_1)^{e_1} Q(x_2)^{e_2} \ldots Q(x_k)^{e_k}$ is a perfect square.
Gaussian elimination

Assume the following factorization of the $Q(x)$ that are selected after the sieving process:

$$Q(x_1) = p_1^{a_{11}} \cdot p_2^{a_{12}} \cdot \ldots \cdot p_r^{a_{1r}}$$

............

$$Q(x_k) = p_1^{a_{k1}} \cdot p_2^{a_{k2}} \cdot \ldots \cdot p_r^{a_{kr}}$$

where $p_1, p_2, \ldots, p_r$ are the primes from the factor base including $(-1)$. We have to find $e_1, e_2, \ldots, e_k$ such that $Q(x_1)^{e_1}Q(x_2)^{e_2}\ldots Q(x_k)^{e_k}$ is a perfect square.

Using the prime factorization of $Q(x)$ we find the numbers $e_1, e_2, \ldots, e_k$ such that
Gaussian elimination

Assume the following factorization of the $Q(x)$ that are selected after the sieving process:

\[ Q(x_1) = p_1^{a_{11}} \cdot p_2^{a_{12}} \cdot \ldots \cdot p_r^{a_{1r}} \]

\[
\ldots \\
\]

\[ Q(x_k) = p_1^{a_k1} \cdot p_2^{a_k2} \cdot \ldots \cdot p_r^{a_{kr}} \]

where $p_1, p_2, \ldots, p_r$ are the primes from the factor base including ($-1$). We have to find $e_1, e_2, \ldots, e_k$ such that $Q(x_1)^{e_1} Q(x_2)^{e_2} \ldots Q(x_k)^{e_k}$ is a perfect square.

Using the prime factorization of $Q(x)$ we find the numbers $e_1, e_2, \ldots, e_k$ such that $e_1^{a_{1i}} + e_2^{a_{2i}} + \ldots + e_k^{a_{ki}}$ is even for all $i = 1, 2, \ldots, r.$
Gaussian elimination

Assume the following factorization of the $Q(x)$ that are selected after the sieving process:

$$Q(x_1) = p_1^{a_{11}} \cdot p_2^{a_{12}} \cdot \ldots \cdot p_r^{a_{1r}}$$

.............

$$Q(x_k) = p_1^{a_{k1}} \cdot p_2^{a_{k2}} \cdot \ldots \cdot p_r^{a_{kr}}$$

where $p_1, p_2, \ldots, p_r$ are the primes from the factor base including $(-1)$. We have to find $e_1, e_2, \ldots, e_k$ such that $Q(x_1)^{e_1} Q(x_2)^{e_2} \ldots Q(x_k)^{e_k}$ is a perfect square.

Using the prime factorization of $Q(x)$ we find the numbers $e_1, e_2, \ldots, e_k$ such that $e_1^{a_{1i}} + e_2^{a_{2i}} + \ldots + e_k^{a_{ki}}$ is even for all $i = 1, 2, \ldots, r$.

We have to solve the equation $eA = 0 \ mod \ 2$ where
Gaussian elimination

Assume the following factorization of the $Q(x)$ that are selected after the sieving process:

$$Q(x_1) = p_1^{a_{11}} \cdot p_2^{a_{12}} \cdot \ldots \cdot p_r^{a_{1r}}$$

..............

$$Q(x_k) = p_1^{a_{k1}} \cdot p_2^{a_{k2}} \cdot \ldots \cdot p_r^{a_{kr}}$$

where $p_1, p_2, \ldots, p_r$ are the primes from the factor base including $(-1)$. We have to find $e_1, e_2, \ldots, e_k$ such that $Q(x_1)^{e_1} Q(x_2)^{e_2} \ldots Q(x_k)^{e_k}$ is a perfect square.

Using the prime factorization of $Q(x)$ we find the numbers $e_1, e_2, \ldots, e_k$ such that $e_1^{a_{1i}} + e_2^{a_{2i}} + \ldots + e_k^{a_{ki}}$ is even for all $i = 1, 2, \ldots, r$.

We have to solve the equation $eA = 0 \mod 2$ where $e = (e_1, e_2, \ldots, e_k)$ and
Gaussian elimination

Assume the following factorization of the $Q(x)$ that are selected after the sieving process:

$$Q(x_1) = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_r^{a_r}$$

$$\ldots \ldots$$

$$Q(x_k) = p_1^{a_{k1}} \cdot p_2^{a_{k2}} \cdot \ldots \cdot p_r^{a_{kr}}$$

where $p_1, p_2, \ldots, p_r$ are the primes from the factor base including $(-1)$. We have to find $e_1, e_2, \ldots, e_k$ such that $Q(x_1)^{e_1} Q(x_2)^{e_2} \ldots Q(x_k)^{e_k}$ is a perfect square.

Using the prime factorization of $Q(x)$ we find the numbers $e_1, e_2, \ldots, e_k$ such that $e_1^{a_{1i}} + e_2^{a_{2i}} + \ldots + e_k^{a_{ki}}$ is even for all $i = 1, 2, \ldots, r$.

We have to solve the equation $eA = 0 \ mod \ 2$ where $e = (e_1, e_2, \ldots, e_k)$ and $A$ is the matrix whose $ij$th entry is $a_{ij}$. 
Gaussian elimination-Example

For $n = 87643$ we have the following matrix
Gaussian elimination-Example

For $n = 87643$ we have the following matrix:

$$
\begin{pmatrix}
1 & 1 & 1 & 0 & 1 & 0 & 0 \\
1 & 0 & 1 & 1 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 0 \\
0 & 1 & 1 & 0 & 0 & 1 & 0
\end{pmatrix}
$$
Gaussian elimination-Example

One solution of the equation $eA = 0 \mod 2$ is $e_1 = (0, 0, 1, 1, 0, 1)$.

From $e_1$ we have that $Q(x_3)Q(x_4)Q(x_6)$ is a perfect square.

We compute $d = \gcd((296 \cdot 299 \cdot 347 - 2 \cdot 3^2 \cdot 17 \cdot 19), n)$. Since $d = 1$ the first solution fails to yield a factor of $n$.

Another solution of $eA = 0 \mod 2$ is $e_2 = (1, 1, 1, 0, 1, 0)$.

From $e_2$ we have that $Q(x_1)Q(x_2)Q(x_3)Q(x_5)$ is a perfect square.

We compute $d = \gcd((265 \cdot 278 \cdot 296 \cdot 307 - 2 \cdot 3^4 \cdot 13 \cdot 17 \cdot 29), n)$. Since $d = 149$ we have a factor of $n$. 
Gaussian elimination - Example

- One solution of the equation $eA = 0 \mod 2$ is $e_1 = (0, 0, 1, 1, 0, 1)$. 

We compute $d = \gcd((296 \cdot 299 \cdot 347 - 2 \cdot 3^2 \cdot 17^2 \cdot 19), n)$. Since $d = 1$, the first solution fails to yield a factor of $n$.

Another solution of $eA = 0 \mod 2$ is $e_2 = (1, 1, 1, 0, 1, 0)$. From $e_2$ we have that $Q(x_1)Q(x_2)Q(x_3)Q(x_5)$ is a perfect square.

We compute $d = \gcd((265 \cdot 278 \cdot 296 \cdot 307 - 2 \cdot 3^4 \cdot 13 \cdot 17 \cdot 29), n)$. Since $d = 149$, we have a factor of $n$. 

Quadratic Sieve Factoring Method - part 2
One solution of the equation $eA = 0 \mod 2$ is 
$e_1 = (0, 0, 1, 1, 0, 1)$. From $e_1$ we have that 
$Q(x_3)Q(x_4)Q(x_6)$ is a perfect square.
One solution of the equation $eA = 0 \mod 2$ is $e_1 = (0, 0, 1, 1, 0, 1)$. From $e_1$ we have that $Q(x_3)Q(x_4)Q(x_6)$ is a perfect square. We compute $d = \gcd((296 \cdot 299 \cdot 347 - 2 \cdot 3^2 \cdot 17^2 \cdot 19), n)$. 
One solution of the equation $eA = 0 \text{ mod } 2$ is $e_1 = (0, 0, 1, 1, 0, 1)$. From $e_1$ we have that $Q(x_3)Q(x_4)Q(x_6)$ is a perfect square. We compute $d = \gcd((296 \cdot 299 \cdot 347 - 2 \cdot 3^2 \cdot 17^2 \cdot 19), n)$. Since $d = 1$ the first solution fails to yield a factor of $n$. 
One solution of the equation $eA = 0 \mod 2$ is $e_1 = (0, 0, 1, 1, 0, 1)$. From $e_1$ we have that $Q(x_3)Q(x_4)Q(x_6)$ is a perfect square. We compute $d = \gcd((296 \cdot 299 \cdot 347 - 2 \cdot 3^2 \cdot 17^2 \cdot 19), n)$. Since $d = 1$ the first solution fails to yield a factor of $n$.

Another solution of $eA = 0 \mod 2$ is $e_2 = (1, 1, 1, 0, 1, 0)$. 
Gaussian elimination—Example

- One solution of the equation $eA = 0 \mod 2$ is $e_1 = (0, 0, 1, 1, 0, 1)$. From $e_1$ we have that $Q(x_3)Q(x_4)Q(x_6)$ is a perfect square. We compute
  $$d = \gcd((296 \cdot 299 \cdot 347 - 2 \cdot 3^2 \cdot 17^2 \cdot 19), n)$$
  Since $d = 1$ the first solution fails to yield a factor of $n$.

- Another solution of $eA = 0 \mod 2$ is $e_2 = (1, 1, 1, 0, 1, 0)$. From $e_2$ we have that $Q(x_1)Q(x_2)Q(x_3)Q(x_5)$ is a perfect square.
One solution of the equation $eA = 0 \mod 2$ is $e_1 = (0, 0, 1, 1, 0, 1)$. From $e_1$ we have that $Q(x_3)Q(x_4)Q(x_6)$ is a perfect square. We compute $d = \gcd((296 \cdot 299 \cdot 347 - 2 \cdot 3^2 \cdot 17^2 \cdot 19), n)$. Since $d = 1$ the first solution fails to yield a factor of $n$.

Another solution of $eA = 0 \mod 2$ is $e_2 = (1, 1, 1, 0, 1, 0)$. From $e_2$ we have that $Q(x_1)Q(x_2)Q(x_3)Q(x_5)$ is a perfect square. We compute $d = \gcd((265 \cdot 278 \cdot 296 \cdot 307 - 2 \cdot 3^4 \cdot 13^2 \cdot 17 \cdot 29), n)$. Since $d = 149$ we have a factor of $n$. 