Quadratic Sieve Factoring

October 15, 2019
Quick: Factor 8051

Factor 8051. Looks Hard.

OH- note that $8051 = 90^2 - 7^2 = (90 + 7)(90 - 7) = 97 \times 83$

Key Wrote 8051 as diff of two squares.

But Lucky: we happen to spot two squares that worked.

History Carl Pomerance was on the Math Team in High School and this was a problem he was given. He didn't to solve it in time, but it inspired him to invent the Quadratic Sieve Factoring Algorithm
Quick: Factor 8051

Factor 8051. Looks Hard.

OH- note that

\[ 8051 = 90^2 - 7^2 = (90 + 7)(90 - 7) = 97 \times 83 \]
Quick: Factor 8051

Factor 8051. Looks Hard.

OH- note that

\[ 8051 = 90^2 - 7^2 = (90 + 7)(90 - 7) = 97 \times 83 \]

Key Wrote 8051 as diff of two squares.
Factor 8051. Looks Hard.

**OH- note that**

\[ 8051 = 90^2 - 7^2 = (90 + 7)(90 - 7) = 97 \times 83 \]

**Key** Wrote 8051 as diff of two squares.

**General** If \( N = x^2 - y^2 \) then get \( N = (x - y)(x + y) \).
Quick: Factor 8051

Factor 8051. Looks Hard.

OH- note that

\[ 8051 = 90^2 - 7^2 = (90 + 7)(90 - 7) = 97 \times 83 \]

Key Wrote 8051 as diff of two squares.

General If \( N = x^2 - y^2 \) then get \( N = (x - y)(x + y) \).

But Lucky: we happen to spot two squares that worked.
Quick: Factor 8051

Factor 8051. Looks Hard.

OH- note that

\[ 8051 = 90^2 - 7^2 = (90 + 7)(90 - 7) = 97 \times 83 \]

Key Wrote 8051 as diff of two squares.

General If \( N = x^2 - y^2 \) then get \( N = (x - y)(x + y) \).

But Lucky: we happen to spot two squares that worked.

History Carl Pomerance was on the Math Team in High School and this was a problem he was given. He didn’t to solve it in time, but it inspired him to invent the Quadratic Sieve Factoring Algorithm
Quick: Factor 1261

\[ 1261 = 81^2 - 16^2 = 6305 = 5 \times 1261 \]

Does this help?
Quick: Factor 1261

$$1261 = 81^2 - 16^2 = 6305 = 5 \times 1261$$

Does this help? $$(81 - 16)(81 + 16) = 5 \times 1261$$

$$(65)(97) = 5 \times 1261$$
Quick: Factor 1261

\[ 1261 = 81^2 - 16^2 = 6305 = 5 \times 1261 \]

Does this help? \((81 - 16)(81 + 16) = 5 \times 1261\)

\[(65)(97) = 5 \times 1261\]

Do \(\text{GCD}(65, 1261) = 13\). So 13 divides 1261.
Quick: Factor 1261

\[ 1261 = 81^2 - 16^2 = 6305 = 5 \times 1261 \]

Does this help? \((81 - 16)(81 + 16) = 5 \times 1261\)

\[(65)(97) = 5 \times 1261\]

Do \(\gcd(65, 1261) = 13\). So 13 divides 1261.

**General** If \(x^2 - y^2 = kN\) then

- \(\gcd(x - y, N)\) might be a nontrivial factor
- \(\gcd(x + y, N)\) might be a nontrivial factor.
Quick: Factor 1261

\[ 1261 = 81^2 - 16^2 = 6305 = 5 \times 1261 \]

Does this help? \((81 - 16)(81 + 16) = 5 \times 1261\)

\[(65)(97) = 5 \times 1261\]

Do \(\text{GCD}(65, 1261) = 13\). So 13 divides 1261.

**General** If \((x^2 - y^2) = kN\) then

- \(\text{GCD}(x - y, N)\) might be a nontrivial factor
- \(\text{GCD}(x + y, N)\) might be a nontrivial factor.

Want
\[ x^2 - y^2 = kN \]
\[ x^2 - y^2 \equiv 0 \pmod{N} \]
\[ x^2 \equiv y^2 \pmod{N}. \]
Quick: Factor 1649

Want $x^2 \equiv y^2 \pmod{1649}$. Start at $\lceil \sqrt{1649} \rceil = 41$. 

Does any of this help?

$(41 \times 43)^2 - 80^2 \equiv 0 \pmod{1649}$

$(114 - 80)(114 + 80) \equiv 34 \times 194 \equiv 0 \pmod{1649}$

$\gcd(34, 1649) = 17$ DONE

$\gcd(194, 1649) = 97$ also works
Quick: Factor 1649

Want $x^2 \equiv y^2 \pmod{1649}$. Start at $\lceil \sqrt{1649} \rceil = 41$.

$41^2 \equiv 32 = 2^5 \pmod{1649}$
Quick: Factor 1649

Want $x^2 \equiv y^2 \pmod{1649}$. Start at $\lceil \sqrt{1649} \rceil = 41$.

$41^2 \equiv 32 = 2^5 \pmod{1649}$

$42^2 \equiv 115 = 5 \times 23 \pmod{1649}$
Quick: Factor 1649

Want $x^2 \equiv y^2 \pmod{1649}$. Start at $\lceil \sqrt{1649} \rceil = 41$.

$41^2 \equiv 32 = 2^5 \pmod{1649}$

$42^2 \equiv 115 = 5 \times 23 \pmod{1649}$

$43^2 \equiv 200 = 2^3 \times 5^2 \pmod{1649}$
Quick: Factor 1649

Want \( x^2 \equiv y^2 \pmod{1649} \). Start at \( \lceil \sqrt{1649} \rceil = 41 \).

\[ 41^2 \equiv 32 = 2^5 \pmod{1649} \]

\[ 42^2 \equiv 115 = 5 \times 23 \pmod{1649} \]

\[ 43^2 \equiv 200 = 2^3 \times 5^2 \pmod{1649} \]

Does any of this help?

\[ (41 \times 43)^2 \equiv 2^8 \times 5^2 = 80^2 \pmod{1649} \]

\[ 114^2 \equiv 80^2 \equiv 0 \pmod{1649} \]

\[ (114 - 80)(114 + 80) \equiv 34 \times 194 \equiv 0 \pmod{1649} \]

\[ \text{GCD}(34, 1649) = 17 \]

\[ \text{GCD}(194, 1649) = 97 \] also works
Quick: Factor 1649

Want $x^2 \equiv y^2 \pmod{1649}$. Start at $\lceil \sqrt{1649} \rceil = 41$.

$41^2 \equiv 32 = 2^5 \pmod{1649}$

$42^2 \equiv 115 = 5 \times 23 \pmod{1649}$

$43^2 \equiv 200 = 2^3 \times 5^2 \pmod{1649}$

Does any of this help?

$41^2 \times 43^2 \equiv 2^5 \times 2^3 \times 5^2 = 2^8 \times 5^2 = (2^4 \times 5)^2 = 80^2$

$114^2 - 80^2 \equiv 0 \pmod{1649}$

$(114 - 80)(114 + 80) \equiv 34 \times 194 \equiv 0 \pmod{1649}$

$\text{GCD}(34, 1649) = 17 \text{ DONE}$

$\text{GCD}(194, 1649) = 97$ also works
Quick: Factor 1649

Want $x^2 \equiv y^2 \pmod{1649}$. Start at $\lceil \sqrt{1649} \rceil = 41$.

$41^2 \equiv 32 = 2^5 \pmod{1649}$

$42^2 \equiv 115 = 5 \times 23 \pmod{1649}$

$43^2 \equiv 200 = 2^3 \times 5^2 \pmod{1649}$

Does any of this help?

$41^2 \times 43^2 \equiv 2^5 \times 2^3 \times 5^2 = 2^8 \times 5^2 = (2^4 \times 5)^2 = 80^2$

$(41 \times 43)^2 - 80^2 \equiv 0 \pmod{1649}$
Quick: Factor 1649

Want $x^2 \equiv y^2 \pmod{1649}$. Start at $\lceil \sqrt{1649} \rceil = 41$.

$41^2 \equiv 32 = 2^5 \pmod{1649}$

$42^2 \equiv 115 = 5 \times 23 \pmod{1649}$

$43^2 \equiv 200 = 2^3 \times 5^2 \pmod{1649}$

Does any of this help?

$41^2 \times 43^2 \equiv 2^5 \times 2^3 \times 5^2 = 2^8 \times 5^2 = (2^4 \times 5)^2 = 80^2$

$(41 \times 43)^2 - 80^2 \equiv 0 \pmod{1649}$

$114^2 - 80^2 \equiv 0 \pmod{1649}$
Quick: Factor 1649

Want \( x^2 \equiv y^2 \pmod{1649} \). Start at \( \lceil \sqrt{1649} \rceil = 41 \).

\[ 41^2 \equiv 32 = 2^5 \pmod{1649} \]

\[ 42^2 \equiv 115 = 5 \times 23 \pmod{1649} \]

\[ 43^2 \equiv 200 = 2^3 \times 5^2 \pmod{1649} \]

Does any of this help?

\[ 41^2 \times 43^2 \equiv 2^5 \times 2^3 \times 5^2 = 2^8 \times 5^2 = (2^4 \times 5)^2 = 80^2 \]

\[ (41 \times 43)^2 - 80^2 \equiv 0 \pmod{1649} \]

\[ 114^2 - 80^2 \equiv 0 \pmod{1649} \]

\[ (114 - 80)(114 + 80) \equiv 34 \times 194 \equiv 0 \pmod{1649} \]
Quick: Factor 1649

Want \( x^2 \equiv y^2 \pmod{1649} \). Start at \( \lceil \sqrt{1649} \rceil = 41 \).

\[
41^2 \equiv 32 = 2^5 \pmod{1649}
\]

\[
42^2 \equiv 115 = 5 \times 23 \pmod{1649}
\]

\[
43^2 \equiv 200 = 2^3 \times 5^2 \pmod{1649}
\]

Does any of this help?

\[
41^2 \times 43^2 \equiv 2^5 \times 2^3 \times 5^2 = 2^8 \times 5^2 = (2^4 \times 5)^2 = 80^2
\]

\[
(41 \times 43)^2 - 80^2 \equiv 0 \pmod{1649}
\]

\[
114^2 - 80^2 \equiv 0 \pmod{1649}
\]

\[
(114 - 80)(114 + 80) \equiv 34 \times 194 \equiv 0 \pmod{1649}
\]

\[
\text{GCD}(34, 1649) = 17 \text{ DONE}
\]
Quick: Factor 1649

Want $x^2 \equiv y^2 \pmod{1649}$. Start at $\lceil \sqrt{1649} \rceil = 41$.

$41^2 \equiv 32 = 2^5 \pmod{1649}$

$42^2 \equiv 115 = 5 \times 23 \pmod{1649}$

$43^2 \equiv 200 = 2^3 \times 5^2 \pmod{1649}$

Does any of this help?

$41^2 \times 43^2 \equiv 2^5 \times 2^3 \times 5^2 = 2^8 \times 5^2 = (2^4 \times 5)^2 = 80^2$

$(41 \times 43)^2 - 80^2 \equiv 0 \pmod{1649}$

$114^2 - 80^2 \equiv 0 \pmod{1649}$

$(114 - 80)(114 + 80) \equiv 34 \times 194 \equiv 0 \pmod{1649}$

$\text{GCD}(34, 1649) = 17$ DONE $\text{GCD}(194, 1649) = 97$ also works
How Can We Make This Happen?

Idea Let \( x = \lceil \sqrt{N} \rceil \).

\[
(x + 0)^2 \equiv y_0 \pmod{N}. \quad \text{Factor } y_0
\]

\[
(x + 1)^2 \equiv y_1 \pmod{N}. \quad \text{Factor } y_1
\]

\[\vdots \]

Look for \( I \subseteq \mathbb{N} \) such that:

\[
\prod_{i \in I} y_i = q_1^{2e_1} q_2^{2e_2} \cdots q_k^{2e_k}
\]

and then get

\[
\left( \prod_{i \in I} (x + i) \right)^2 \equiv \left( \prod_{i \in I} q_i^{e_i} \right)^2 \pmod{N}
\]

Let \( X = \prod_{i \in I} \) and \( Y = \prod_{i \in I} q_i^{e_i} \).

\[
X^2 - Y^2 \equiv 0 \pmod{N}.
\]

Is this a good idea? Discuss.
Look at the First Step

$$(x + 0)^2 \equiv y_0 \pmod{N}.$$  Factor $y_0$

$$(x + 1)^2 \equiv y_1 \pmod{N}.$$  Factor $y_1$

$\vdots$  $\vdots$

In order to factor $N$ we needed to factor the $y_i$'s.

Really?  Darn!  Ideas?
Look at the First Step

\[(x + 0)^2 \equiv y_0 \pmod{N}. \quad \text{Factor } y_0\]
\[(x + 1)^2 \equiv y_1 \pmod{N}. \quad \text{Factor } y_1\]
\[\vdots \quad \vdots\]

In order to factor $N$ we needed to factor the $y_i$'s.
Look at the First Step

\[(x + 0)^2 \equiv y_0 \pmod{N}. \quad \text{Factor } y_0\]
\[(x + 1)^2 \equiv y_1 \pmod{N}. \quad \text{Factor } y_1\]
\[\vdots \]

In order to factor \( N \) we needed to factor the \( y_i \)'s. Really?
Look at the First Step

\[(x + 0)^2 \equiv y_0 \pmod{N}. \quad \text{Factor } y_0\]
\[(x + 1)^2 \equiv y_1 \pmod{N}. \quad \text{Factor } y_1\]
\[\vdots \quad \vdots\]

In order to \textbf{factor} \( N \) we needed to \textbf{factor} the \( y_i \)'s. Really? Darn!
Look at the First Step

\[(x + 0)^2 \equiv y_0 \pmod{N}. \quad \text{Factor } y_0\]
\[(x + 1)^2 \equiv y_1 \pmod{N}. \quad \text{Factor } y_1\]
\[\vdots \]

In order to \textbf{factor} \(N\) we needed to \textbf{factor} the \(y_i\)'s. Really? Darn! Ideas?
**B-Factoring**

Idea $B$ be a parameter. $p_1 < p_2 < \cdots < p_B$ are the first $B$ primes.

Def A number is *$B$-factored* if its largest prime factor is $\leq p_B$.
$B$-Factoring

Idea $B$ be a parameter. $p_1 < p_2 < \cdots < p_B$ are the first $B$ primes.

Def A number is $B$-factored if its largest prime factor is $\leq p_B$.

Example $B = 5$. Primes 2,3,5,7,11.
$1000 = 2^3 \times 5^3$. So $B$-factored.
$27378897 = 11 \times 35557$. 35557 is composite. NOT $B$-factored.
**B-Factoring**

Idea $B$ be a parameter. $p_1 < p_2 < \cdots < p_B$ are the first $B$ primes.

Def A number is $B$-factored if its largest prime factor is $\leq p_B$.

Example $B = 5$. Primes 2,3,5,7,11.

$1000 = 2^3 \times 5^3$. So $B$-factored.

$27378897 = 11 \times 35557$. 35557 is composite. NOT $B$-factored.

Is factoring faster than $B$-factoring?
**B-Factoring**

**Idea**  $B$ be a parameter. $p_1 < p_2 < \cdots < p_B$ are the first $B$ primes.

**Def** A number is **$B$-factored** if its largest prime factor is $\leq p_B$.

**Example**  $B = 5$. Primes 2,3,5,7,11.

1000 = $2^3 \times 5^3$. So $B$-factored.

27378897 = $11 \times 35557$. 35557 is composite. NOT $B$-factored.

Is factoring faster than $B$-factoring?

Let's try to $B$-factor 82203.

1. Divide 2 into it. 2 does not divide 82203.
2. Divide 3 into what's left. 82203 = $3 \times 27401$.
3. Divide 5 into what's left. 5 does not divide 27401.
4. Divide 7 into what's left. 7 does not divide 27401.
5. Divide 11 into what's left. 82203 = $3 \times 11 \times 7473$.
6. DONE. NOT $B$-factorable. Only did $B$ divisions.
Example of Algorithm that Uses $B$-Factoring

Want to factor 539873. $B = 7$ so use 2, 3, 5, 7, 11, 13, 17

\[ \left\lfloor \sqrt{539873} \right\rfloor = 735 \]

\[ 735^2 \equiv 352 = 2^5 \times 11 \pmod{539873}. \]

\[ 750^2 \equiv 22627 \equiv 11^3 \times 17 \pmod{539873}. \]

\[ 783^2 \equiv 22627 \equiv 11^3 \times 17 \pmod{539873}. \]

\[ 801^2 \equiv 101728 \equiv 2^5 \times 11 \times 17^2 \pmod{539873}. \]

Notice that

\[ (735 \times 801)^2 \equiv 2^{10} \times 11^2 \times 17^2 \]

\[ (735 \times 801)^2 \equiv (2^5 \times 11 \times 17)^2 \]

\[ 48862^2 - 5984^2 \equiv 0 \pmod{539873} \]

\[ (48862 - 5984) \times (48862 + 5984) \equiv 0 \pmod{539873} \]

\[ (42878) \times (54846) \equiv 0 \pmod{539873} \]

\[ \text{GCD}(42878, 539873) = 1949 \]
Notice That

\[ \left\lceil \sqrt{539873} \right\rceil = 735 \]

\[ 735^2 \equiv 352 \equiv 2^5 \times 11 \pmod{539873} \]

\[ 750^2 \equiv 22627 \equiv 11^3 \times 17 \pmod{539873} \]

\[ 783^2 \equiv 22627 \equiv 11^3 \times 17 \pmod{539873} \]

\[ 801^2 \equiv 101728 \equiv 2^5 \times 11 \times 17^2 \pmod{539873} \]

Notice that

\[ (735 \times 801)^2 \equiv 2^{10} \times 11^2 \times 17^2 \]

How can a program Notice That?
What is a program supposed to notice? Discuss.
\[ \lceil \sqrt{539873} \rceil = 735 \]

\[ 735^2 \equiv 352 \equiv 2^5 \times 11 \pmod{539873}. \]

\[ 750^2 \equiv 22627 \equiv 11^3 \times 17 \pmod{539873}. \]

\[ 783^2 \equiv 22627 \equiv 11^3 \times 17 \pmod{539873}. \]

\[ 801^2 \equiv 101728 \equiv 2^5 \times 11 \times 17^2 \pmod{539873}. \]

Notice that

\[ (735 \times 801)^2 \equiv 2^{10} \times 11^2 \times 17^2 \]

How can a program Notice That?
What is a program supposed to notice? Discuss.

We want a program to notice that some combination of exponents
lead to all being even.
Idea One

\[\lceil \sqrt{539873} \rceil = 735\]

\[
\begin{align*}
735^2 & \equiv 352 \equiv 2^5 \times 11^1 & (5, 0, 0, 0, 11, 0, 0) \\
750^2 & \equiv 22627 \equiv 11^3 \times 17^1 & (0, 0, 0, 0, 3, 0, 1) \\
783^2 & \equiv 73216 \equiv 2^9 \times 11^1 \times 13^1 & (9, 0, 0, 0, 1, 1, 0) \\
801^2 & \equiv 101728 \equiv 2^5 \times 11^1 \times 17^2 & (5, 0, 0, 0, 11, 0, 2)
\end{align*}
\]

Want some combination of the vectors to have all even numbers. Can we use Linear Algebra? Discuss
Idea One


\[ \lceil \sqrt{539873} \rceil = 735 \]

\[
\begin{align*}
735^2 & \equiv 352 \equiv 2^5 \times 11^1 & (5, 0, 0, 0, 11, 0, 0) \\
750^2 & \equiv 22627 \equiv 11^3 \times 17^1 & (0, 0, 0, 0, 3, 0, 1) \\
783^2 & \equiv 73216 \equiv 2^9 \times 11^1 \times 13^1 & (9, 0, 0, 0, 1, 1, 0) \\
801^2 & \equiv 101728 \equiv 2^5 \times 11^1 \times 17^2 & (5, 0, 0, 0, 11, 0, 2)
\end{align*}
\]

Want some combination of the vectors to have all even numbers. Can we use Linear Algebra? Discuss

We do not need the numbers. All we need are the parities!
Idea Two

Store parities of exponents in vector.

\[
\left\lfloor \sqrt{539873} \right\rfloor = 735
\]

\[
\begin{align*}
735^2 &\equiv 352 &\equiv 2^5 \times 11^1 &\equiv (1, 0, 0, 0, 1, 0, 0) \\
750^2 &\equiv 22627 &\equiv 11^3 \times 17^1 &\equiv (0, 0, 0, 0, 1, 0, 1) \\
783^2 &\equiv 73216 &\equiv 2^9 \times 11^1 \times 13^1 &\equiv (1, 0, 0, 0, 1, 1, 0) \\
801^2 &\equiv 101728 &\equiv 2^5 \times 11^1 \times 17^2 &\equiv (1, 0, 0, 0, 1, 0, 0)
\end{align*}
\]
Idea Two

Store parities of exponents in vector.
\[ \lceil \sqrt{539873} \rceil = 735 \]

\[
\begin{align*}
735^2 & \equiv 352 \equiv 2^5 \times 11^1 \quad (1, 0, 0, 0, 1, 0, 0) \\
750^2 & \equiv 22627 \equiv 11^3 \times 17^1 \quad (0, 0, 0, 0, 1, 0, 1) \\
783^2 & \equiv 73216 \equiv 2^9 \times 11^1 \times 13^1 \quad (1, 0, 0, 0, 1, 1, 0) \\
801^2 & \equiv 101728 \equiv 2^5 \times 11^1 \times 17^2 \quad (1, 0, 0, 0, 1, 0, 0)
\end{align*}
\]

Well Defined Math Problem Given a set of 0-1 $B$-vectors over $\mathbb{Z}_2$, does some subset of them sum to $\vec{0}$? Equivalent to asking if some subset is linearly dependent.

- Can solve using Gaussian Elimination.
- If there are $B + 1$ vectors then there will be such a set.
Quad Sieve Alg: First Attempt

Given $N$ let $x = \lceil \sqrt{N} \rceil$. All $\equiv$ are mod $N$. $B, M$ are params.

$$(x + 0)^2 \equiv y_0 \quad \text{Try to } B\text{-Factor } y_0 \text{ to get parity } \vec{v}_0$$

$$\vdots$$

$$(x + M)^2 \equiv y_M \quad \text{Try to } B\text{-Factor } y_M \text{ to get parity } \vec{v}_M$$

Let $I \subseteq \{0, \ldots, M\}$ so that $(\forall i \in I), y_i$ is $B$-factored. Find $J \subseteq I$ such that $\sum_{i \in J} \vec{v}_i = \vec{0}$. Hence $\prod_{i \in J} y_i$ has all even exponents.

$$\prod_{i \in J} y_i = q_1^{2e_1} q_2^{2e_2} \cdots q_k^{2e_k}$$

$$\left(\prod_{i \in J} (x + i)\right)^2 \equiv \left(\prod_{i \in J} q_i^{e_i}\right)^2 \pmod{N}$$

Let $X = \prod_{i \in J} (x + i)$ and $Y = \prod_{i \in J} q_i^{e_i}$.

$$X^2 - Y^2 \equiv 0 \pmod{N}.$$  

GCD$(X - Y, N), \text{ GCD}(X + Y, N)$ should yield factors.
1. Need

I \geq B + 1. So need M big enough so that will likely get \geq B + 1 numbers B-factored.

2. Could get \text{GCD} (X - Y, N) = 1 and \text{GCD} (X + Y, N) = N. Rare.

3. B-factoring all of those numbers, does that take a long time? This we will deal with in a very long aside on sieving.

4. Gaussian Elim will take \( O(B^3) \). This is main time factor.

5. Balancing act: B, M large enough so that you get a lin dep set, small enough for better time analysis.
(1) What Could go Wrong, (2) Missing Steps

1. Need $|l| \geq B + 1$. So need $M$ big enough so that will likely get $\geq B + 1$ numbers $B$-factored.
1. Need $|I| \geq B + 1$. So need $M$ big enough so that will likely get $\geq B + 1$ numbers $B$-factored.

2. Could get $\gcd(X - Y, N) = 1$ and $\gcd(X + Y, N) = N$. Rare.
(1) What Could go Wrong, (2) Missing Steps

1. Need $|l| \geq B + 1$. So need $M$ big enough so that will likely get $\geq B + 1$ numbers $B$-factored.

2. Could get $\text{GCD}(X - Y, N) = 1$ and $\text{GCD}(X + Y, N) = N$. Rare.

3. $B$-factoring all of those numbers, does that take a long time? This we will deal with in a very long aside on sieving.
1. Need $|I| \geq B + 1$. So need $M$ big enough so that will likely get $\geq B + 1$ numbers $B$-factored.

2. Could get $\gcd(X - Y, N) = 1$ and $\gcd(X + Y, N) = N$. Rare.

3. $B$-factoring all of those numbers, does that take a long time? This we will deal with in a very long aside on sieving.

4. Gaussian Elim will take $O(B^3)$. This is main time factor.
(1) What Could go Wrong, (2) Missing Steps

1. Need $|I| \geq B + 1$. So need $M$ big enough so that will likely get $\geq B + 1$ numbers $B$-factored.
2. Could get $\text{GCD}(X - Y, N) = 1$ and $\text{GCD}(X + Y, N) = N$. Rare.
3. $B$-factoring all of those numbers, does that take a long time? This we will deal with in a very long aside on sieving.
4. Gaussian Elim will take $O(B^3)$. This is main time factor.
5. Balancing act: $B, M$ large enough so that you get a lin dep set, small enough for better time analysis.
A LONG Aside on Sieving

October 15, 2019
Finding all Primes $\leq 48$, the Stupid Way

To find all primes $\leq 48$ we could do the following:

$$\text{for } i = 2 \text{ to } 48 \text{ if isprime}(i) = \text{YES} \text{ then output } i.$$ 

Is this a good idea? Discuss.
Finding all Primes $\leq 48$, the Stupid Way

To find all primes $\leq 48$ we could do the following:

$$\text{for } i = 2 \text{ to } 48 \text{ if } \text{isprime}(i) = \text{YES} \text{ then output } i.$$ 

Is this a good idea? Discuss.

No You are testing many numbers that you could have, ahead of time, ruled out.
Finding all Primes \( \leq 48 \), the Smart Way

Write down the numbers \( \leq 48 \)

<table>
<thead>
<tr>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
<th>17</th>
<th>18</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>19</th>
<th>20</th>
<th>21</th>
<th>22</th>
<th>23</th>
<th>24</th>
<th>25</th>
<th>26</th>
<th>27</th>
<th>28</th>
<th>29</th>
<th>30</th>
<th>31</th>
<th>32</th>
<th>33</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>34</th>
<th>35</th>
<th>36</th>
<th>37</th>
<th>38</th>
<th>39</th>
<th>40</th>
<th>41</th>
<th>42</th>
<th>43</th>
<th>44</th>
<th>45</th>
<th>46</th>
<th>47</th>
<th>48</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Output first unmarked—2—and then MARK 2, \( 2 \times 2 \), \( 3 \times 2 \), etc.

**Note** A program could do this quickly by 2’s.

**Very Important** The program does not even look at (say) 3.
Marked the 2, 4, …

|   | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|
| **X** | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |

<table>
<thead>
<tr>
<th></th>
<th>19</th>
<th>20</th>
<th>21</th>
<th>22</th>
<th>23</th>
<th>24</th>
<th>25</th>
<th>26</th>
<th>27</th>
<th>28</th>
<th>29</th>
<th>30</th>
<th>31</th>
<th>32</th>
<th>33</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>X</strong></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>34</th>
<th>35</th>
<th>36</th>
<th>37</th>
<th>38</th>
<th>39</th>
<th>40</th>
<th>41</th>
<th>42</th>
<th>43</th>
<th>44</th>
<th>45</th>
<th>46</th>
<th>47</th>
<th>48</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>X</strong></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Output first unmarked–3–and then MARK 3, 2 × 2, 3 × 3, etc.
Marked the 3, 6, …

<table>
<thead>
<tr>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
<th>17</th>
<th>18</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

| 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| X  | X  | X  | X  | X  | X  | X  | X  | X  | X  | X  | X  | X  | X  | X  | X  |

| 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| X  | X  | X  | X  | X  | X  | X  | X  | X  | X  | X  | X  | X  | X  | X  | X  |

Output first unmarked–5–and then MARK 5, $2 \times 5$, $3 \times 5$, etc.
Marked the 5, 10, ... 

<table>
<thead>
<tr>
<th></th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
<th>17</th>
<th>18</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>19</th>
<th>20</th>
<th>21</th>
<th>22</th>
<th>23</th>
<th>24</th>
<th>25</th>
<th>26</th>
<th>27</th>
<th>28</th>
<th>29</th>
<th>30</th>
<th>31</th>
<th>32</th>
<th>33</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>34</th>
<th>35</th>
<th>36</th>
<th>37</th>
<th>38</th>
<th>39</th>
<th>40</th>
<th>41</th>
<th>42</th>
<th>43</th>
<th>44</th>
<th>45</th>
<th>46</th>
<th>47</th>
<th>48</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Output first unmarked–7–and then MARK 7, 2 × 7, 3 × 7, etc.
Marked the 7, 14, ...  

Output first unmarked–11–and then MARK 11, 2 × 11, 3 × 11, etc. We’ll stop here—you get the idea.
The Sieve of Eratosthenes

1. Input($N$)
2. Write down $2, 3, \ldots, N$. All are unmarked.
3. (MARK STEP) Goto the first unmarked element of the list $p$. Output($p$). Keep pointer there. (When pointer is at $N$ or beyond then stop.)
4. Mark $p$, $2p$, $\ldots$, $\left\lfloor \frac{N}{p} \right\rfloor p$. (This takes $\frac{N}{p}$ steps.)
5. GOTO MARK STEP.

Time:

$$\sum_{p \leq N} \frac{N}{p} = N \sum_{p \leq N} \frac{1}{p}$$

New Question: What is $\sum_{p \leq N} \frac{1}{p}$?
As Aside on $\sum_{p \leq N} \frac{1}{p}$

October 15, 2019
Notation

\[\sum_{n \leq N} \frac{1}{n} = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots + \frac{1}{N}\]

\[\sum_{n} \frac{1}{n} = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots\]

\[\sum_{p \leq N} \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \cdots + \frac{1}{q}\]

where \(q\) is the largest prime \(\leq N\).

\[\sum_{p} \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \cdots\]
Notation

\[\sum_{n \leq N} \frac{1}{n} = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots + \frac{1}{N}\]

\[\sum_{n} \frac{1}{n} = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots\]

\[\sum_{p \leq N} \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \cdots + \frac{1}{q}\]

where \(q\) is the largest prime \(\leq N\).

\[\sum_{p} \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \cdots\]

Example

\[\sum_{p \leq 14} \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13}\]
What is $\sum_{p \leq N} \frac{1}{p}$ Asymptotically? History

If you look up $\sum_{p \leq N} \frac{1}{p}$ on the web you will find

1. Proofs that $\sum_{p \leq N} \frac{1}{p}$ diverges.
2. Some of those proofs show that $\sum_{p \leq N} \frac{1}{p} \geq \ln(\ln(N)) + \mathcal{O}(1)$.
3. Nothing on upper bounds on the sum. But see next point.

A sequence of events:
1. In 2010 Larry W showed Bill G a proof that $\sum_{p \leq N} \frac{1}{p} \leq \ln(\ln(N)) + \mathcal{O}(1)$.
2. Larry says it's a well-known but never written down. Bill suggests they write it down. It is now on arxiv.

Moral of the Story Google is not always enough.
What is $\sum_{p \leq N} \frac{1}{p}$ Asymptotically? History

If you look up $\sum_{p \leq N} \frac{1}{p}$ on the web you will find

1. Proofs that $\sum_p \frac{1}{p}$ diverges.

Moral of the Story Google is not always enough.
What is $\sum_{p \leq N} \frac{1}{p}$ Asymptotically? History

If you look up $\sum_{p \leq N} \frac{1}{p}$ on the web you will find

1. Proofs that $\sum p \frac{1}{p}$ diverges.
2. Some of those proofs show that $\sum_{p \leq N} \frac{1}{p} \geq \ln(\ln(N)) + O(1)$. 
What is \( \sum_{p \leq N} \frac{1}{p} \) Asymptotically? History

If you look up \( \sum_{p \leq N} \frac{1}{p} \) on the web you will find

1. Proofs that \( \sum_{p} \frac{1}{p} \) diverges.
2. Some of those proofs show that \( \sum_{p \leq N} \frac{1}{p} \geq \ln(\ln(N)) + O(1) \).
3. Nothing on upper bounds on the sum. But see next point.
What is $\sum_{p \leq N} \frac{1}{p}$ Asymptotically? History

If you look up $\sum_{p \leq N} \frac{1}{p}$ on the web you will find

1. Proofs that $\sum_{p} \frac{1}{p}$ diverges.

2. Some of those proofs show that $\sum_{p \leq N} \frac{1}{p} \geq \ln(\ln(N)) + O(1)$.

3. Nothing on upper bounds on the sum. But see next point.

A sequence of events:

1. In 2010 Larry W showed Bill G a proof that $\sum_{p \leq N} \frac{1}{p} \leq \ln(\ln(N)) + O(1)$.

2. Larry says its a well known but never written down. Bill suggests they write it down. It is now on arxiv.

Moral of the Story Google is not always enough.
What is $\sum_{p \leq N} \frac{1}{p}$ Asymptotically? History

If you look up $\sum_{p \leq N} \frac{1}{p}$ on the web you will find

1. Proofs that $\sum_{p} \frac{1}{p}$ diverges.
2. Some of those proofs show that $\sum_{p \leq N} \frac{1}{p} \geq \ln(\ln(N)) + O(1)$.
3. Nothing on upper bounds on the sum. But see next point.

A sequence of events:

1. In 2010 Larry W showed Bill G a proof that

$$\sum_{p \leq N} \frac{1}{p} \leq \ln(\ln(N)) + O(1).$$
What is $\sum_{p \leq N} \frac{1}{p}$ Asymptotically? History

If you look up $\sum_{p \leq N} \frac{1}{p}$ on the web you will find

1. Proofs that $\sum p \frac{1}{p}$ diverges.

2. Some of those proofs show that $\sum_{p \leq N} \frac{1}{p} \geq \ln(\ln(N)) + O(1)$.

3. Nothing on upper bounds on the sum. But see next point.

A sequence of events:

1. In 2010 Larry W showed Bill G a proof that

   $$\sum_{p \leq N} \frac{1}{p} \leq \ln(\ln(N)) + O(1).$$

2. Larry says its a well known but never written down. Bill suggests they write it down. It is now on arxiv.
What is $\sum_{p \leq N} \frac{1}{p}$ Asymptotically? History

If you look up $\sum_{p \leq N} \frac{1}{p}$ on the web you will find

1. Proofs that $\sum_{p} \frac{1}{p}$ diverges.

2. Some of those proofs show that $\sum_{p \leq N} \frac{1}{p} \geq \ln(\ln(N)) + O(1)$.

3. Nothing on upper bounds on the sum. But see next point.

A sequence of events:

1. In 2010 Larry W showed Bill G a proof that

   $$\sum_{p \leq N} \frac{1}{p} \leq \ln(\ln(N)) + O(1).$$

2. Larry says its a well known but never written down. Bill suggests they write it down. It is now on arxiv.

**Moral of the Story** Google is not always enough.
More on \( \sum_{p \leq N} \frac{1}{p} \)

1. \( \sum_{n \leq N} \frac{1}{n} \sim \ln(n) \).

2. \( \sum_{p \leq N} \frac{1}{p} \sim \ln(\ln(N)) \)

How good is this approximation?

1) When \( N \geq 286 \),

\[
\ln(\ln N) - \frac{1}{2(\ln N)^2} + C \leq \sum_{p \leq N} \frac{1}{p} \leq \ln(\ln N) + \frac{1}{(2\ln N)^2} + C,
\]

where \( C \sim 0.261497212847643 \).

2)

- \( \sum_{p \leq 10} \frac{1}{p} = 1.176 \)
- \( \sum_{p \leq 10^9} \frac{1}{p} = 3.293 \)
- \( \sum_{p \leq 10^{100}} \frac{1}{p} \sim 5.7 \)
- \( \sum_{p \leq 10^{1000}} \frac{1}{p} \sim 7.8 \)
Take Away

\[ \sum_{p \leq N} \frac{1}{p} \sim \ln(\ln N) \]

▶ This is a very good approximation.
▶ This is very small
▶ (Cheating to make math easier) Current factoring algorithms can factor 170-digit numbers with quite a bit of effort. We assume a limit of 1000 digits. Hence we treat \( \ln(\ln(N)) \) as if it was

\[ \ln \ln(N) \leq \ln(\ln(1000)) \sim 8. \]

(Nobody else does this.)
Back to our Aside on Sieves

October 15, 2019
The Sieve of E can find all primes \( \leq N \) in time

\[
\leq N \sum_{p \leq N} \frac{1}{p} \leq N \ln(\ln(N))
\]
The Sieve of E can find all primes \( \leq N \) in time

\[
\leq N \sum_{p \leq N} \frac{1}{p} \leq N \ln(\ln(N))
\]

How long would finding all primes \( \leq N \) be the stupid way?

\[
\sum_{n \leq N} \log(n) \sim O(N \log(N))
\]
The Sieve of E can find all primes \( \leq N \) in time

\[
\leq N \sum_{p \leq N} \frac{1}{p} \leq N \ln(\ln(N))
\]

How long would finding all primes \( \leq N \) be the stupid way?

\[
\sum_{n \leq N} \log(n) \sim O(N \log(N))
\]

- The Sieve of E is even better than it looks because the constants are much lower.
The Sieve of E can find all primes \( \leq N \) in time

\[
\leq N \sum_{p \leq N} \frac{1}{p} \leq N \ln(\ln(N))
\]

How long would finding all primes \( \leq N \) be the stupid way?

\[
\sum_{n \leq N} \log(n) \sim O(N \log(N))
\]

- The Sieve of E is even better than it looks because the constants are much lower.

- The key to the speed of The Sieve of E is that when it marks it DOES NOT look at (say) 3 and say Oh, thats not even. It literally does not look at all!
The Sieve of E marked all evens. **Better** Divide by 2 knowing it will work. Then divide by 2 again (it might not work) until factor out all powers of 2.

The Sieve of E marked all numbers \( \equiv 0 \pmod{3} \) **Better** Divide by 3 knowing it will work. Then divide by 3 again (it might not work) until factor out all powers of 3.

Do this for the first \( B \) primes and you will have \( B \)-factored many numbers.
B-factoring all $N \leq 48$, the Smart Way

Write down the numbers $\leq 48$. We will 2-factor it, so divide by 2 and 3.

<table>
<thead>
<tr>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
<th>17</th>
<th>18</th>
</tr>
</thead>
</table>

| 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|

| 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|

First unmarked–2, Divide all $\equiv 0 \pmod{2}$ by 2, then 2 again, etc, until get to an odd.

Note A program could do this quickly by 2’s.

Key The program does not even look at (say) 3.
Divide by 2

<p>| | | | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>13</td>
</tr>
<tr>
<td>2 * 1</td>
<td>2 * 2</td>
<td>2 * 3</td>
<td>2^3</td>
<td>2 * 5</td>
<td>2^2 * 3</td>
<td>2 * 7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
<td>26</td>
<td>27</td>
</tr>
<tr>
<td>2^4</td>
<td>2 * 9</td>
<td>2 * 10</td>
<td>2 * 11</td>
<td>2^3 * 3</td>
<td>2 * 13</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>29</td>
<td>30</td>
<td>31</td>
<td>32</td>
<td>33</td>
<td>34</td>
<td>35</td>
<td>36</td>
<td>37</td>
<td>38</td>
<td>39</td>
</tr>
<tr>
<td>2^2 * 7</td>
<td>2 * 15</td>
<td>2^5</td>
<td>2 * 17</td>
<td>2^2 * 9</td>
<td>2 * 19</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>41</td>
<td>42</td>
<td>43</td>
<td>44</td>
<td>45</td>
<td>46</td>
<td>47</td>
<td>48</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2^3 * 5</td>
<td>2 * 21</td>
<td>2^2 * 11</td>
<td>2 * 23</td>
<td>2^4 * 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

First unmarked–3, Divide all \( \equiv 0 \pmod{3} \) by 3, then 3 again, etc, until get to a \( \not\equiv 0 \pmod{3} \).
We only show the last row (for reasons of space).

<p>| | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>40</td>
<td>41</td>
<td>42</td>
<td>43</td>
<td>44</td>
<td>45</td>
<td>46</td>
<td>47</td>
<td>48</td>
</tr>
<tr>
<td>$2^3 \times 5$</td>
<td>$2 \times 3 \times 7$</td>
<td>$3 \times 15$</td>
<td>$2^2 \times 11$</td>
<td>$2 \times 23$</td>
<td>$2^4 \times 3$</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- 48 was 2-factored
- Nothing else was.
Variant of The Sieve of Eratosthenes: Algorithm

1. Input($N, B$)
2. Write down $2, 3, \ldots, N$. All are have blank in box.
3. (BOX STEP) Goto the first blank box, $p$. (When have visited this step $B$ times then stop).
4. Divide what the elements $p, 2p, \ldots, \left\lfloor \frac{N}{p} \right\rfloor p$ by $p$ then $p$ again and again until can’t. (This takes $\sim \frac{N}{p}$ steps.)
5. GOTO BOX STEP.

Time:

\[
\sum_{p \leq B} \frac{N}{p} + \sum_{p \leq B} \frac{N}{p^2} + \sum_{p \leq B} \frac{N}{p^3} + \sum_{p \leq B} \frac{1}{p^4} \cdots
\]

\[
= N \left( \sum_{p \leq B} \frac{1}{p} + \sum_{p \leq B} \frac{1}{p^2} + \sum_{p \leq B} \frac{1}{p^3} + \sum_{p \leq B} \frac{1}{p^4} + \cdots \right)
\]
Variant of The Sieve of Eratosthenes: Analysis

\[ = N \left( \sum_{p \leq B} \frac{1}{p} + \sum_{p \leq B} \frac{1}{p^2} + \sum_{p \leq B} \frac{1}{p^3} + \sum_{p \leq B} \frac{1}{p^4} + \cdots \right) \]

\[ = N \left( \ln(\ln(B)) + \sum_{a=2}^{\infty} \sum_{p \leq B} \frac{1}{p^a} \right) \]

Next slide shows that \( N \sum_{a=2}^{\infty} \sum_{p \leq B} \frac{1}{p^a} \leq (0.5)N \), so time is

\[ \leq N \ln(\ln(B)) + (0.5)N \]

Note: The mult constants really are \( \leq 1 \) and it does matter for real world performance.
Variant of The Sieve of E: That last term is $\leq N$

\[
= N \sum_{a=2}^{\infty} \sum_{p \leq B} \frac{1}{p^a} = N \sum_{p \leq B} \sum_{a=2}^{\infty} \frac{1}{p^a}
\]
Variant of The Sieve of E: That last term is ≤ N

\[= N \sum_{a=2}^{\infty} \sum_{p \leq B} \frac{1}{p^a} = N \sum_{p \leq B} \sum_{a=2}^{\infty} \frac{1}{p^a}\]

\[= N \sum_{p \leq B} \frac{1}{p^2} \frac{1}{1 - (1/p)}\]

\[= N \sum_{p \leq B} \frac{1}{p^2 - 1} \sim N \sum_{p \leq B} \frac{1}{p^2}\]

How big is \(\sum_{p \leq B} \frac{1}{p^2}\)?
Variant of The Sieve of E: That last term is $\leq N$

\[
= N \sum_{a=2}^{\infty} \sum_{p \leq B} \frac{1}{p^a} = N \sum_{p \leq B} \sum_{a=2}^{\infty} \frac{1}{p^a}
\]

\[
= N \sum_{p \leq B} \frac{1/p^2}{1 - (1/p)}
\]

\[
= N \sum_{p \leq B} \frac{1}{p^2 - 1} \sim N \sum_{p \leq B} \frac{1}{p^2}
\]

How big is $\sum_{p \leq B} \frac{1}{p^2}$?

1. $\sum_{n=1}^{\infty} \frac{1}{n^2}$ cvg. Do you know to what?
Variant of The Sieve of E: That last term is \( \leq N \)

\[
= N \sum_{a=2}^{\infty} \sum_{p \leq B} \frac{1}{p^a} = N \sum_{p \leq B} \sum_{a=2}^{\infty} \frac{1}{p^a}
\]

\[
= N \sum_{p \leq B} \frac{1/p^2}{1 - (1/p)}
\]

\[
= N \sum_{p \leq B} \frac{1}{p^2 - 1} \sim N \sum_{p \leq B} \frac{1}{p^2}
\]

How big is \( \sum_{p \leq B} \frac{1}{p^2} \)?

1. \( \sum_{n=1}^{\infty} \frac{1}{n^2} \) cvg. Do you know to what? \( \frac{\pi^2}{6} \sim 1.644 \)
Variant of The Sieve of E: That last term is $\leq N$

\[
= N \sum_{a=2}^{\infty} \sum_{p \leq B} \frac{1}{p^a} = N \sum_{p \leq B} \sum_{a=2}^{\infty} \frac{1}{p^a}
\]

\[
= N \sum_{p \leq B} \frac{1/p^2}{1 - (1/p)}
\]

\[
= N \sum_{p \leq B} \frac{1}{p^2 - 1} \sim N \sum_{p \leq B} \frac{1}{p^2}
\]

How big is $\sum_{p \leq B} \frac{1}{p^2}$?

1. $\sum_{n=1}^{\infty} \frac{1}{n^2}$ cvg. Do you know to what? $\frac{\pi^2}{6} \sim 1.644$

2. $\sum_{p=1}^{\infty} \frac{1}{p^2}$ cvg. Do you know to what?
Variant of The Sieve of E: That last term is $\leq N$

\[
= N \sum_{a=2}^{\infty} \sum_{p \leq B} \frac{1}{p^a} = N \sum_{p \leq B} \sum_{a=2}^{\infty} \frac{1}{p^a}
\]

\[
= N \sum_{p \leq B} \frac{1/p^2}{1 - (1/p)}
\]

\[
= N \sum_{p \leq B} \frac{1}{p^2 - 1} \sim N \sum_{p \leq B} \frac{1}{p^2}
\]

How big is $\sum_{p \leq B} \frac{1}{p^2}$?

1. $\sum_{n=1}^{\infty} \frac{1}{n^2}$ cvg. Do you know to what? $\frac{\pi^2}{6} \sim 1.644$

2. $\sum_{p=1}^{\infty} \frac{1}{p^2}$ cvg. Do you know to what? $\sim 0.45$. 
Recap Variant of The Sieve of Eratosthenes

Given $N, B$ can $B$-factor $\{2, \ldots, N\}$ in time

$$N \leq \ln(\ln(B)) + 0.5N$$

Can easily modify to get a fast algorithm for $B$-factoring $N_1, \ldots, N_1 + N$.

This is not the problem we originally needed to solve, though its close. We now go back to our original problem.
Recall Quad Sieve Alg: First Attempt

Given $N$ let $x = \lceil \sqrt{N} \rceil$. All $\equiv$ are mod $N$. $B, M$ are params.

$(x + 0)^2 \equiv y_0$ Try to $B$-Factor $y_0$ to get parity $\vec{v}_0$

\[ \vdots \]

$(x + M)^2 \equiv y_M$ Try to $B$-Factor $y_M$ to get parity $\vec{v}_M$

Let $I \subseteq \{0, \ldots, M\}$ so that $(\forall i \in I), y_i$ is $B$-factored. Find $J \subseteq I$ such that $\sum_{i \in J} \vec{v}_i = \vec{0}$. Hence $\prod_{i \in J} y_i$ has all even exponents.

$$\prod_{i \in J} y_i = q_1^{2e_1} q_2^{2e_2} \cdots q_k^{2e_k}$$

$$(\prod_{i \in J} (x + i))^2 \equiv (\prod_{i \in J} q_i^{e_i})^2 \pmod{N}$$

Let $X = \prod_{i \in J} (x + i)$ and $Y = \prod_{i \in J} q_i^{e_i}$.

$$X^2 - Y^2 \equiv 0 \pmod{N}.$$

$\text{GCD}(X - Y, N), \text{GCD}(X + Y, N)$ should yield factors.
Recall Quad Sieve Alg: First Attempt, First Step

Given $N$ let $x = \lceil \sqrt{N} \rceil$. All $\equiv$ are mod $N$. $B, M$ are params.

$$(x + 0)^2 \equiv y_0 \quad \text{Try to } B\text{-Factor } y_0 \text{ to get parity } \vec{v}_0$$

$$\vdots$$

$$(x + M)^2 \equiv y_M \quad \text{Try to } B\text{-Factor } y_M \text{ to get parity } \vec{v}_M$$

How do we $B$-factor all of those numbers?
Recall Quad Sieve Alg: First Attempt, First Step

Given $N$ let $x = \left\lceil \sqrt{N} \right\rceil$. All $\equiv$ are mod $N$. $B, M$ are params.

$(x + 0)^2 \equiv y_0$  Try to $B$-Factor $y_0$ to get parity $\vec{v}_0$

\[ \vdots \]

$(x + M)^2 \equiv y_M$  Try to $B$-Factor $y_M$ to get parity $\vec{v}_M$

How do we $B$-factor all of those numbers?
Modified Sieve of E $B$-factored $N_1 + 1, \ldots, N_1 + N$. 
Recall Quad Sieve Alg: First Attempt, First Step

Given $N$ let $x = \left\lceil \sqrt{N} \right\rceil$. All $\equiv$ are mod $N$. $B, M$ are params.

$(x + 0)^2 \equiv y_0$  Try to $B$-Factor $y_0$ to get parity $\vec{v}_0$

$\vdots$

$(x + M)^2 \equiv y_M$  Try to $B$-Factor $y_M$ to get parity $\vec{v}_M$

How do we $B$-factor all of those numbers?
Modified Sieve of E $B$-factored $N_1 + 1, \ldots, N_1 + N$.
We need to $B$-factor $y_0, y_1, \ldots, y_M$. 
Recall Quad Sieve Alg: First Attempt, First Step

Given $N$ let $x = \lceil \sqrt{N} \rceil$. All $\equiv$ are mod $N$. $B, M$ are params.

$(x + 0)^2 \equiv y_0$ Try to $B$-Factor $y_0$ to get parity $\vec{v}_0$

\[ \vdots \]

$(x + M)^2 \equiv y_M$ Try to $B$-Factor $y_M$ to get parity $\vec{v}_M$

How do we $B$-factor all of those numbers?

Modified Sieve of E $B$-factored $N_1 + 1, \ldots, N_1 + N$. We need to $B$-factor $y_0, y_1, \ldots, y_M$.

Plan It was more efficient to $B$-factor $2, \ldots, N$ all at once then one at at time. Same will be true for $y_0, \ldots, y_M$. 

New Problem Given $N$, $B$, $M$, $x$, want to $B$-factor

$(x + 0)^2 \pmod{N}$

$(x + 1)^2 \pmod{N}$

$\vdots$

$(x + M)^2 \pmod{N}$

We do an example on the next slide.
\( N = 1147, \; B = 2, \; M = 10, \; x = 34. \)

Want to 2-factor (so all powers of 2 and 3)

\((34 + 0)^2 \pmod{1147}\)

\[\vdots \]

\((34 + 10)^2 \pmod{1147}\)
The Quadratic Sieve: Example

\[ N = 1147, \ B = 2, \ M = 10, \ x = 34. \]

Want to 2-factor (so all powers of 2 and 3)
\[ (34 + 0)^2 \pmod{1147} \]
\[ : \quad : \quad : \]
\[ (34 + 10)^2 \pmod{1147} \]

For the Sieve of E when we wanted to divide by \( p \) we looked at every \( p \)th element. Is there an analog here?
The Quadratic Sieve: Example

\( N = 1147, \ B = 2, \ M = 10, \ x = 34. \)
Want to 2-factor (so all powers of 2 and 3)
\((34 + 0)^2 \pmod{1147}\)
\(\vdots \quad \vdots \quad \vdots \)
\((34 + 10)^2 \pmod{1147}\)
For the Sieve of E when we wanted to divide by \( p \) we looked at every \( p \)th element. Is there an analog here?
For which \( 0 \leq i \leq 10 \) does 2 divide \((34 + i)^2 \pmod{1147}\)?
The Quadratic Sieve: Example

\[ N = 1147, \ B = 2, \ M = 10, \ x = 34. \]
Want to 2-factor (so all powers of 2 and 3)
\[ (34 + 0)^2 \pmod{1147} \]
\[ \vdots \quad \vdots \quad \vdots \]
\[ (34 + 10)^2 \pmod{1147} \]
For the Sieve of E when we wanted to divide by \( p \) we looked at every \( p \)th element. Is there an analog here?

For which \( 0 \leq i \leq 10 \) does 2 divide \( (34 + i)^2 \pmod{1147} \)?
Next Slide
The Quadratic Sieve: Example of dividing by 2

For which $0 \leq i \leq 10$ does $2$ divide $(34 + i)^2 \pmod{1147}$?
For which $0 \leq i \leq 10$ does $2$ divide $(34 + i)^2 \pmod{1147}$?

Since $0 \leq i \leq 10$, $1147 < (34 + i)^2 < 2 \times 1147$

So $(34 + i)^2 \pmod{1147} = (34 + i)^2 - 1147$. 
For which $0 \leq i \leq 10$ does 2 divide $(34 + i)^2 \pmod{1147}$?

Since $0 \leq i \leq 10$, $1147 < (34 + i)^2 < 2 \times 1147$

So $(34 + i)^2 \pmod{1147} = (34 + i)^2 - 1147$.

Our real question is for which $i$ is

$$(34 + i)^2 - 1147 \equiv 0 \pmod{2}$$

$$i^2 - 1 \equiv 0 \pmod{2}$$

$$i \equiv 1 \pmod{2}.$$ 

Great!- just need to divide the $y_i$ where $i \equiv 1 \pmod{2}$.
The Quadratic Sieve: Example of dividing by 3

For which $0 \leq i \leq 10$ does $3$ divide $(34 + i)^2 \pmod{1147}$?
The Quadratic Sieve: Example of dividing by 3

For which $0 \leq i \leq 10$ does $3$ divide $(34 + i)^2 \pmod{1147}$?

Since $0 \leq i \leq 10$, $1147 < (34 + i)^2 < 2 \times 1147$
For which $0 \leq i \leq 10$ does $3$ divide $(34 + i)^2 \pmod{1147}$?

Since $0 \leq i \leq 10$, $1147 < (34 + i)^2 < 2 \times 1147$

So $(34 + i)^2 \pmod{1147} = (34 + i)^2 - 1147$.

Our real question is for which $i$ is

$$(34 + i)^2 - 1147 \equiv 0 \pmod{3}$$

$$(1 + i)^2 - 1 \equiv 0 \pmod{3}$$

$i \equiv 0, 1 \pmod{3}$.

Great!- just need to divide the $y_i$ where $i \equiv 1, 2 \pmod{2}$. 
The Quad Sieve: Example of dividing by 5, 7, 11, 13

\((34 + i)^2 - 1147 \equiv 0 \pmod{5}\)
\((4 + i)^2 - 2 \equiv 0 \pmod{5}\)
NO SOLUTIONS

\((34 + i)^2 - 1147 \equiv 0 \pmod{7}\)
\((6 + i)^2 \equiv 1 \pmod{7}\)
\(i \equiv 0, 2 \pmod{7}\)

\((34 + i)^2 - 1147 \equiv 0 \pmod{11}\)
\((1 + i)^2 \equiv 3 \pmod{11}\)
\(i \equiv 4, 5 \pmod{11}\)

\((34 + i)^2 - 1147 \equiv 0 \pmod{13}\)
\((8 + i)^2 + 10 \equiv 0 \pmod{13}\)
\(i \equiv 1, 9 \pmod{13}\)
The Quad Sieve: Example of dividing by 17,19,23

\[(34 + i)^2 - 1147 \equiv 0 \pmod{17}\]
\[i^2 + 9 \equiv 0 \pmod{17}\]
\[i \equiv 5, 12 \pmod{17}\]

\[(34 + i)^2 - 1147 \equiv 0 \pmod{19}\]
\[(15 + i)^2 + 12 \equiv 0 \pmod{19}\]
\[i \equiv 8, 15 \pmod{19}\]

\[(34 + i)^2 - 1147 \equiv 0 \pmod{23}\]
\[(11 + i)^2 + 3 \equiv 0 \pmod{23}\]
NO SOLUTIONS
The $B$-Factor Step Using Quad Sieve: Program

**Problem** Given $N$, $B$, $M$, $x$, want to $B$-factor $(x + 0)^2 \pmod{N}$

\[ \vdots \]

$(x + M)^2 \pmod{N}$

**Algorithm**

for all primes $p \leq B$

Find $A \subseteq \{0, \ldots, p - 1\}$: $i \in A$ iff $(x + i)^2 - N \equiv 0 \pmod{p}$

for $a \in A$

for $k = 0$ to $\left\lfloor \frac{M-a}{p} \right\rfloor$

divide $(x + pk + a)^2$ by $p$ (and then $p$ again…)

**Time**

\[ \leq \sum_{p \leq B} (\lg p + 2\frac{M-1}{p}) = \sum_{p \leq B} \lg p + 2M \sum_{p \leq B} \frac{1}{p}. \]

\[ = (\sum_{p \leq B} \lg p) + 2M \ln \ln(B) = 2B + 2M \ln(\ln(B)). \]
Quad Sieve Alg: Second Attempt, Algorithm

Given $N$ let $x = \left \lceil \sqrt{N} \right \rceil$. All $\equiv$ are mod $N$. $B, M$ are params.

$B$-factor $(x + 0)^2 \pmod{N}$, $\ldots$, $(x + M)^2 \pmod{M}$ by Quad S.

Let $I \subseteq \{0, \ldots, M\}$ so that $(\forall i \in I)$, $y_i$ is $B$-factored. Find $J \subseteq I$ such that $\sum_{i \in J} \vec{v}_i = \vec{0}$. Hence $\prod_{i \in J} y_i$ has all even exponents.

$$\prod_{i \in J} y_i = q_1^{2e_1} q_2^{2e_2} \cdots q_k^{2e_k}$$

$$(\prod_{i \in J} (x + i))^2 \equiv (\prod_{i \in J} q_i^{e_i})^2 \pmod{N}$$

Let $X = \prod_{i \in J} (x + i)$ and $Y = \prod_{i \in J} q_i^{e_i}$.

$$X^2 - Y^2 \equiv 0 \pmod{N}.$$ 

$\gcd(X - Y, N)$, $\gcd(X + Y, N)$ should yield factors.
Analysis of Quadratic Sieve Factoring Algorithm

Time to $B$-factor:

$$2B + 2M \ln(\ln(B)).$$

Time to find $J$: $B^3$. 

Total Time:

$$2B + 2M \ln(\ln(B)) + B^3$$

Intuitive but not rigorous arguments yield run time

$$e^{\sqrt{\ln N \ln \ln N}} \sim e^{\sqrt{8 \ln N}} \sim e^{2.8 \sqrt{\ln N}}$$
Speed Up One

Recall:

$(34 + i)^2 - 1147 \equiv 0 \pmod{23}$
$(11 + i)^2 + 3 \equiv 0 \pmod{23}$

NO SOLUTIONS
Recall:
\[(34 + i)^2 - 1147 \equiv 0 \pmod{23}\]
\[(11 + i)^2 + 3 \equiv 0 \pmod{23}\]
NO SOLUTIONS

If there is a prime \( p \) such that \( z^2 \equiv 1147 \pmod{p} \) has NO SOLUTION then we should not ever consider it.
Recall:

\[(34 + i)^2 - 1147 \equiv 0 \pmod{23}\]
\[(11 + i)^2 + 3 \equiv 0 \pmod{23}\]

NO SOLUTIONS

If there is a prime \( p \) such that \( z^2 \equiv 1147 \pmod{p} \) has NO SOLUTION then we should not ever consider it.

There is a fast test to determine just if \( z^2 \equiv 1147 \pmod{p} \) has a solution (and more generally \( z^2 \equiv N \pmod{p} \)). So can eliminate some primes \( p \leq B \) before you start.
Recall:
We started with $x = \lceil \sqrt{N} \rceil$ and did $(x + i)^2$ for $0 \leq i \leq M$. 
Recall:
We started with $x = \left\lceil \sqrt{N} \right\rceil$ and did $(x + i)^2$ for $0 \leq i \leq M$.

We can also (with some care) use $(x + i)^2$ when $i \leq 0$.

**Advantage** Smaller numbers more likely to be $B$-factorable.
Recall:

\[(34 + i)^2 - 1147 \equiv 0 \pmod{19}\]
\[(15 + i)^2 + 12 \equiv 0 \pmod{19}\]
\[i \equiv 8, 15 \pmod{19}\]
Recall:

\[(34 + i)^2 - 1147 \equiv 0 \pmod{19}\]
\[(15 + i)^2 + 12 \equiv 0 \pmod{19}\]
\[i \equiv 8, 15 \pmod{19}\]

We can have one more variable:

\[(34j + i)^2 - 1147 \equiv 0 \pmod{19}\]
\[(15j + i)^2 + 12 \equiv 0 \pmod{19}\]
\[15j + i \equiv 8, 15 \pmod{19}\]

Many values of \((i, j)\) work.
1. Look at all of the non $B$-factored numbers. For each one test if what is left is prime. Let $X$ be the set of all of those primes.

2. Look at all of the non $B$-factored numbers. For each of them try a factoring algorithm (e.g., either of Pollards) for a limited amount of time. Let $Y$ be the set of primes you come across.

3. Do Q. Sieve on all of the non $B$-factored numbers using the primes in $X \cup Y$.

This will increase the number of $B$-factored numbers.
Speed Up Five—Avoid Division

1. Compute $\log((x+i)^2 \mod N) - \log p$. $\log$ is easy on a computer.

2. That's nuts! There will be some error! And . . . to what end.

3. Examples (the numbers are not real):

   ▶ $z = 19807$. $\log z - \log 2 - \log 3 - \log 13 - \log 53 = 2$. Close to 0. $z$ is probably $B$-factorable. Now and only now divide 2, 3, 13, 29, 53 into it, and then powers, until get $B$-factored. In very rare cases not $B$-factorable.

   ▶ $z = 19805$. $\log z - \log 2 - \log 5 - \log 23 = 10$. Not close to 0. Do not bother dividing since probably not $B$-factorable. In some cases it was $B$-factorable and you missed out.
Speed Up Five—Avoid Division

1. Compute $\lg((x + i)^2 \pmod{N}) - \lg p$. \(\lg\) is easy on a computer.
1. Compute $\lg((x + i)^2 \pmod{N}) - \lg p$. $\lg$ is easy on a computer.

2. That's nuts! There will be some error! And ... to what end.
Speed Up Five—Avoid Division

1. Compute $\lg((x + i)^2 \mod N) - \lg p$. $\lg$ is easy on a computer.
2. That's nuts! There will be some error! And ... to what end.
3. Examples (the numbers are not real):
   - $z = 19807$. $\lg z - \lg 2 - \lg 3 - \lg 13 - \lg 53 = 2$. CLOSE to 0. $z$ is prob $B$-factorable. Now and ONLY now divide 2, 3, 13, 29, 53 into it, and then powers, until get $B$-factored. In very rare cases not $B$-factorable.
   - $z = 19805$. $\lg z - \lg 2 - \lg 5 - \lg 23 = 10$. NOT CLOSE to 0. Do not bother dividing since prob not $B$-factorable. In some cases it was $B$-factorable and you missed out.
Speed Up Five—Avoid Division

1. Compute $\lg((x + i)^2 \pmod{N}) - \lg p$. $\lg$ is easy on a computer.

2. That's nuts! There will be some error! And ... to what end.

3. Examples (the numbers are not real):
   - $z = 19807$. $\lg z - \lg 2 - \lg 3 - \lg 13 - \lg 53 = 2$. CLOSE to 0. $z$ is prob $B$-factorable. Now and ONLY now divide 2,3,13,29,53 into it, and then powers, until get $B$-factored. In very rare cases not $B$-factorable.
Speed Up Five—Avoid Division

1. Compute \( \lg((x + i)^2 \mod N)) - \lg p \). \( \lg \) is easy on a computer.

2. That’s nuts! There will be some error! And … to what end.

3. Examples (the numbers are not real):
   - \( z = 19807 \). \( \lg z - \lg 2 - \lg 3 - \lg 13 - \lg 53 = 2 \). CLOSE to 0. \( z \) is prob \( B \)-factorable. Now and ONLY now divide 2,3,13,29,53 into it, and then powers, until get \( B \)-factored. In very rare cases not \( B \)-factorable.
   - \( z = 19805 \). \( \lg z - \lg 2 - \lg 5 - \lg 23 = 10 \). NOT CLOSE to 0. Do not bother dividing since prob not \( B \)-factorable. In some cases it was \( B \)-factorable and you missed out.
Speed Up Five-extra—Avoid Division

Since we are just approximating if
$\log z$ minus some log’s of primes is 0
$\log 2$, $\log 3$, $\log 5$ are so tiny, don’t bother with those.
Since we are just approximating if $\lg z$ minus some log’s of primes is 0 $\lg 2, \lg 3, \lg 5$ are so tiny, don’t bother with those. But will use $2^3, 3^2, \text{ and } 5^2$. 
The Gaussian Elimination is over $\mathbb{Z}_2$ and is for a sparse matrix (most of the entries are 0).

There are special purpose algorithms for this.
Is $z$ $B$-factorable? There is a light for each $p \leq B$ whose intensity is proportional to the $\lg p$. Each light turns on just two times every $p$ cycles, corresponding to the two square roots of $N \mod p$. A sensor senses the combined intensity of all the lights together, and if this is close enough to the $\lg z$ then $z$ is a $B$-factorable number candidate. Can do in parallel.
The Quad Sieve had run time:

$$e^{(\ln N \ln \ln N)^{1/2}} \sim e^{2.8(\ln N)^{1/2}}$$
The Number Field Sieve

The Quad Sieve had run time:

$$e^{(\ln N \ln \ln N)^{1/2}} \sim e^{2.8(\ln N)^{1/2}}$$

The Number Field Sieve which uses some of the same ideas has run time:

$$e^{1.9(\ln N)^{1/3}(\ln \ln N)^{2/3}} \sim e^{14(\ln N)^{1/3}}$$
## Compare Run Times

<table>
<thead>
<tr>
<th>Alg</th>
<th>Run Time in terms of $N$</th>
<th>Run Time in terms of $L$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Naive</td>
<td>$N^{1/2}$</td>
<td>$2^{L/2}$</td>
</tr>
<tr>
<td>Pollard Rho</td>
<td>$N^{1/4}$</td>
<td>$2^{L/4}$</td>
</tr>
<tr>
<td>Linear Sieve</td>
<td>$N^{3.9}/L^{1/2}$</td>
<td>$2^{1.95L^{1/2}}$</td>
</tr>
<tr>
<td>Quad Sieve</td>
<td>$N^{2.8}/L^{1/2}$</td>
<td>$2^{1.4L^{1/2}}$</td>
</tr>
<tr>
<td>N.F. Sieve</td>
<td>$N^{14}/L^{2/3}$</td>
<td>$2^{20L^{1/3}}$</td>
</tr>
</tbody>
</table>

1. Times are more conjectured than proven.
2. Quad S. is better than Prior Method by only a constant in the exponent. Made a big difference IRL.
3. Quad Sieve is better than Pollard-Rho at about $10^{53}$.
Relevance for RSA

History

2. People did not think it would work that well; however, he had friends at Sandia Labs who tried it out. Just for fun.
3. A the same time another group at Sandia Labs was working on a serious RSA project that would use 100-digit $N$.
4. Quad Sieve could factor 100-digit numbers, so the RSA project had to be scrapped.
Relevance for RSA

History

Relevance for RSA

History

2. People did not think it would work that well; however, he had friends at Sandia Labs who tried it out. Just for fun.
Relevance for RSA

History

2. People did not think it would work that well; however, he had friends at Sandia Labs who tried it out. Just for fun.
3. A the same time another group at Sandia Labs was working on a serious RSA project that would use 100-digit $N$
Relevance for RSA

History

2. People did not think it would work that well; however, he had friends at Sandia Labs who tried it out. Just for fun.
3. At the same time another group at Sandia Labs was working on a serious RSA project that would use 100-digit $N$
4. Quad Sieve could factor 100-digit numbers, so the RSA project had to be scrapped.
The Future of Factoring

I paraphrase The Joy of Factoring by Wagstaff:
The best factoring algorithms have time complexity of the form

\[ e^{c \ln N^t (\ln \ln N)^{1-t}} \]

with Q.Sieve using \( c = \frac{1}{2} \) and N.F.Sieve using \( c = \frac{1}{3} \). Moreover, any method that uses \( B \)-factoring must take this long.
The Future of Factoring

I paraphrase The Joy of Factoring by Wagstaff:
The best factoring algorithms have time complexity of the form

$$e^{c (\ln N)^t (\ln \ln N)^{1-t}}$$

with Q.Sieve using $c = \frac{1}{2}$ and N.F.Sieve using $c = \frac{1}{3}$. Moreover, any method that uses $B$-factoring must take this long.
I paraphrase The Joy of Factoring by Wagstaff: The best factoring algorithms have time complexity of the form

$$e^{c(\ln N)^t(\ln \ln N)^{1-t}}$$

with Q.Sieve using $c = \frac{1}{2}$ and N.F.Sieve using $c = \frac{1}{3}$. Moreover, any method that uses $B$-factoring must take this long.

The Future of Factoring

I paraphrase *The Joy of Factoring* by Wagstaff:
The best factoring algorithms have time complexity of the form

\[ e^{c(\ln N)^t(\ln \ln N)^{1-t}} \]

with Q.Sieve using \( c = \frac{1}{2} \) and N.F.Sieve using \( c = \frac{1}{3} \). Moreover, any method that uses \( B \)-factoring must take this long.

▶ My opinion: \( e^{c(\ln N)^t(\ln \ln N)^{1-t}} \) is the best you can do ever, though \( t \) can be improved.
The Future of Factoring

I paraphrase The Joy of Factoring by Wagstaff:
The best factoring algorithms have time complexity of the form

\[ e^{c(\ln N)^t (\ln \ln N)^{1-t}} \]

with Q.Sieve using \( c = \frac{1}{2} \) and N.F.Sieve using \( c = \frac{1}{3} \). Moreover, any method that uses \( B \)-factoring must take this long.

▶ My opinion: \( e^{c(\ln N)^t (\ln \ln N)^{1-t}} \) is the best you can do ever, though \( t \) can be improved.
▶ My opinion: Why hasn’t \( t \) been improved?
I paraphrase The Joy of Factoring by Wagstaff: The best factoring algorithms have time complexity of the form

\[ e^{c(\ln N)^t(\ln \ln N)^{1-t}} \]

with Q.Sieve using \( c = \frac{1}{2} \) and N.F.Sieve using \( c = \frac{1}{3} \). Moreover, any method that uses \( B \)-factoring must take this long.

- My opinion: \( e^{c(\ln N)^t(\ln \ln N)^{1-t}} \) is the best you can do ever, though \( t \) can be improved.
- My opinion: Why hasn’t \( t \) been improved?
  - Wagstaff told me that we’ve run out of parameters to set.
The Future of Factoring

I paraphrase *The Joy of Factoring* by Wagstaff:
The best factoring algorithms have time complexity of the form

\[ e^{c(\ln N)^t(\ln \ln N)^{1-t}} \]

with Q.Sieve using \( c = \frac{1}{2} \) and N.F.Sieve using \( c = \frac{1}{3} \). Moreover, any method that uses \( B \)-factoring must take this long.

- My opinion: \( e^{c(\ln N)^t(\ln \ln N)^{1-t}} \) is the best you can do ever, though \( t \) can be improved.
- My opinion: Why hasn’t \( t \) been improved?
  - Wagstaff told me that we’ve run out of parameters to set.
  - Brandon, Solomon, Mark, and Ivan haven’t worked on it yet.