# Quadratic Sieve Factoring

November 13, 2019

# Quick: Factor 8051

Factor 8051. Looks Hard.

# 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.

# 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 $N = (x-y)(x+y)$.

## 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

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

Does this help?

# Quick: Factor 1261

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

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

$$65 \times 97 = 5 \times 1261$$

# Quick: Factor 1261

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

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

$$65 \times 97 = 5 \times 1261$$

(Could divide both sides by 5, please ignore that.)

# Quick: Factor 1261

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

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

$$65 \times 97 = 5 \times 1261$$

(Could divide both sides by 5, please ignore that.)
65 divides $5 \times 1261$, so 65 might share a factor with 1261. Take GCD: $\mathrm{GCD}(65, 1261) = 13$. So 13 divides 1261.

# Quick: Factor 1261

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

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

$$65 \times 97 = 5 \times 1261$$

(Could divide both sides by 5, please ignore that.)
65 divides $5 \times 1261$, so 65 might share a factor with 1261. Take GCD: $\mathrm{GCD}(65, 1261) = 13$. So 13 divides 1261.
General If $(x^2 - y^2) = kN$ then

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

# Quick: Factor 1261

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

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

$$65 \times 97 = 5 \times 1261$$

(Could divide both sides by 5, please ignore that.)
65 divides $5 \times 1261$, so 65 might share a factor with 1261. Take GCD: $\mathrm{GCD}(65, 1261) = 13$. So 13 divides 1261.
General If $(x^2 - y^2) = kN$ then

- $\mathrm{GCD}(x-y, N)$ might be a nontrivial factor
- $\mathrm{GCD}(x+y, N)$ 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 $\lceil \sqrt{1649} \rceil = 41$.

# 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?

# 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?

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

# 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?

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

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

$$1763^2 - 80^2 \equiv 0 \pmod{1649}$$

# 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?

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

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

$$1763^2 - 80^2 \equiv 0 \pmod{1649}$$

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

# 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?

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

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

$$1763^2 - 80^2 \equiv 0 \pmod{1649}$$

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

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

# 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?

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

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

$$1763^2 - 80^2 \equiv 0 \pmod{1649}$$

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

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

$\mathrm{GCD}(34, 1649) = 17$ Found a Factor!

# Factoring 1649: 194 Also Works?

Recall:

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

# Factoring 1649: 194 Also Works?

Recall:

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

$\mathrm{GCD}(34, 1649) = 17$ Found a Factor!

# Factoring 1649: 194 Also Works?

Recall:

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

$\mathrm{GCD}(34, 1649) = 17$ Found a Factor!

What is we used 194 instead of 34?

# Factoring 1649: 194 Also Works?

Recall:

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

$\mathrm{GCD}(34, 1649) = 17$ Found a Factor!

What is we used 194 instead of 34?
$\mathrm{GCD}(194, 1649) = 97$ Found a Factor!
So 194 also works.

# How Can We Make This Happen?

Idea Let $x = \left\lceil \sqrt{N} \right\rceil$.

$$\begin{array}{llll} (x+0)^2 \equiv y_0 & \pmod{N}. & \text{Factor } y_0 \\ (x+1)^2 \equiv y_1 & \pmod{N}. & \text{Factor } y_1 \\ & \vdots & \vdots \end{array}$$

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 $X = \prod_{i \in I}(x+i) \pmod{N}$ and $Y = \prod_{i \in I} q_i^{e_i} \pmod{N}$.

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

Is this a good idea? Discuss.

# MANDATORY

READ THE SOLUTIONS TO THE MIDTERM

On some of the solutions we say

Okay, We accepted this answer on the midterm, but we WILL NOT on the final

So you really need to read the midterm solutions even for problems you got right.

# Look at the First Step

$$
\begin{aligned}
(x+0)^2 &\equiv y_0 \pmod{N}. \quad \text{Factor } y_0 \\
(x+1)^2 &\equiv y_1 \pmod{N}. \quad \text{Factor } y_1 \\
&\qquad\qquad\quad \vdots \qquad \vdots
\end{aligned}
$$

# Look at the First Step

$$
\begin{aligned}
(x+0)^2 &\equiv y_0 \pmod{N}. \quad \text{Factor } y_0 \\
(x+1)^2 &\equiv y_1 \pmod{N}. \quad \text{Factor } y_1 \\
&\vdots \qquad \vdots
\end{aligned}
$$

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

# Look at the First Step

$$\begin{array}{lll}(x+0)^2 \equiv y_0 & \pmod{N}. & \text{Factor } y_0 \\ (x+1)^2 \equiv y_1 & \pmod{N}. & \text{Factor } y_1 \\ & \vdots & \vdots\end{array}$$

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

# Look at the First Step

$$
\begin{aligned}
(x+0)^2 &\equiv y_0 \pmod{N}. \quad \text{Factor } y_0 \\
(x+1)^2 &\equiv y_1 \pmod{N}. \quad \text{Factor } y_1 \\
&\vdots \quad \vdots
\end{aligned}
$$

In order to factor $N$ we needed to factor the $y_i$'s. Really? Darn!

# Look at the First Step

$$\begin{array}{llll} (x+0)^2 \equiv y_0 & \pmod{N}. & \text{Factor } y_0 \\ (x+1)^2 \equiv y_1 & \pmod{N}. & \text{Factor } y_1 \\ & \vdots & \vdots \end{array}$$

In order to factor $N$ we needed to 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.
$27378897 = 11 \times 31^2 \times 37$. 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.
$27378897 = 11 \times 31^2 \times 37$. NOT $B$-factored.
Is $B$-factoring faster than 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.
$27378897 = 11 \times 31^2 \times 37$. NOT $B$-factored.
Is $B$-factoring faster than factoring?
Lets try to $B$-factor 82203.

# $B$-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.
$27378897 = 11 \times 31^2 \times 37$. NOT $B$-factored.
Is $B$-factoring faster than factoring?
Lets try to $B$-factor 82203.

1. Divide 2 into it. 2 does not divide 82203.

# $B$-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.
$27378897 = 11 \times 31^2 \times 37$. NOT $B$-factored.
Is $B$-factoring faster than factoring?
Lets try to $B$-factor 82203.

1. Divide 2 into it. 2 does not divide 82203.
2. Divide 3 into whats left. $82203 = 3 \times 27401$.

# $B$-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.
$27378897 = 11 \times 31^2 \times 37$. NOT $B$-factored.
Is $B$-factoring faster than factoring?
Lets try to $B$-factor 82203.

1. Divide 2 into it. 2 does not divide 82203.
2. Divide 3 into whats left. $82203 = 3 \times 27401$.
3. Divide 5 into whats left. 5 does not divide 27401.

# $B$-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 $\le p_B$.

Example $B = 5$. Primes 2,3,5,7,11.
$1000 = 2^3 \times 5^3$. So $B$-factored.
$27378897 = 11 \times 31^2 \times 37$. NOT $B$-factored.
Is $B$-factoring faster than factoring?
Lets try to $B$-factor 82203.

1. Divide 2 into it. 2 does not divide 82203.
2. Divide 3 into whats left. $82203 = 3 \times 27401$.
3. Divide 5 into whats left. 5 does not divide 27401.
4. Divide 7 into whats left. 7 does not divide 27401.

# $B$-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.
$27378897 = 11 \times 31^2 \times 37$. NOT $B$-factored.
Is $B$-factoring faster than factoring?
Lets try to $B$-factor 82203.

1. Divide 2 into it. 2 does not divide 82203.
2. Divide 3 into whats left. $82203 = 3 \times 27401$.
3. Divide 5 into whats left. 5 does not divide 27401.
4. Divide 7 into whats left. 7 does not divide 27401.
5. Divide 11 into whats left. $82203 = 3 \times 11 \times 2491$.

# $B$-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.
$27378897 = 11 \times 31^2 \times 37$. NOT $B$-factored.
Is $B$-factoring faster than factoring?
Lets try to $B$-factor 82203.

1. Divide 2 into it. 2 does not divide 82203.
2. Divide 3 into whats left. $82203 = 3 \times 27401$.
3. Divide 5 into whats left. 5 does not divide 27401.
4. Divide 7 into whats left. 7 does not divide 27401.
5. Divide 11 into whats left. $82203 = 3 \times 11 \times 2491$.
6. DONE. NOT $B$-factorable. Only did $B$ divisions.

# Abbreviation

We use $B$-fact for $B$-factorable.

Why?

# Abbreviation

We use $B$-fact for $B$-factorable.

Why?

Space on slides!

# Example of Algorithm that Uses $B$-Factoring

Want to factor 539873. $B = 7$ so use $2, 3, 5, 7, 11, 13, 17$
$\lceil \sqrt{539873} \, \rceil = 735$

# Example of Algorithm that Uses $B$-Factoring

Want to factor 539873. $B = 7$ so use $2, 3, 5, 7, 11, 13, 17$
$\lceil \sqrt{539873}\ \rceil = 735$
$735^2 \equiv 352 = 2^5 \times 11^1 \pmod{539873}$.

$736^2, \ldots, 749^2$ did not 7-factor.

# Example of Algorithm that Uses $B$-Factoring

Want to factor 539873. $B = 7$ so use $2, 3, 5, 7, 11, 13, 17$
$\lceil \sqrt{539873}\, \rceil = 735$
$735^2 \equiv 352 = 2^5 \times 11^1 \pmod{539873}$.

$736^2, \ldots, 749^2$ did not 7-factor.

$750^2 \equiv 22627 \equiv 11^3 \times 17^1 \pmod{539873}$.

# Example of Algorithm that Uses $B$-Factoring

Want to factor 539873. $B = 7$ so use $2, 3, 5, 7, 11, 13, 17$
$\lceil \sqrt{539873} \rceil = 735$
$735^2 \equiv 352 = 2^5 \times 11^1 \pmod{539873}$.

$736^2$,...,$749^2$ did not 7-factor.

$750^2 \equiv 22627 \equiv 11^3 \times 17^1 \pmod{539873}$.

$751^2$,..., $782^2$ did not 7-factor.

# Example of Algorithm that Uses $B$-Factoring

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

$\lceil \sqrt{539873} \rceil = 735$

$735^2 \equiv 352 = 2^5 \times 11^1 \pmod{539873}$.

$736^2, \ldots, 749^2$ did not 7-factor.

$750^2 \equiv 22627 \equiv 11^3 \times 17^1 \pmod{539873}$.

$751^2, \ldots, 782^2$ did not 7-factor.

$783^2 \equiv 73216 \equiv 2^9 \times 11^1 \times 13^1 \pmod{539873}$.

# Example of Algorithm that Uses $B$-Factoring

Want to factor 539873. $B = 7$ so use $2, 3, 5, 7, 11, 13, 17$
$\lceil \sqrt{539873}\ \rceil = 735$
$735^2 \equiv 352 = 2^5 \times 11^1 \pmod{539873}$.

$736^2$,...,$749^2$ did not 7-factor.

$750^2 \equiv 22627 \equiv 11^3 \times 17^1 \pmod{539873}$.

$751^2$,..., $782^2$ did not 7-factor.

$783^2 \equiv 73216 \equiv 2^9 \times 11^1 \times 13^1 \pmod{539873}$.

$784^2$,...,$800^2$ did not 7-factor.

$801^2 \equiv 101728 \equiv 2^5 \times 11^1 \times 17^2 \pmod{539873}$.
Can we use this? Next Slide I write it nicer.

# Example Continued: Trying to factor 539873

$735^2 \equiv 352 = 2^5 \times 11^1 \pmod{539873}$.
$750^2 \equiv 22627 \equiv 11^3 \times 17^1 \pmod{539873}$.
$783^2 \equiv 73216 \equiv 2^9 \times 11^1 \times 13^1 \pmod{539873}$.
$801^2 \equiv 101728 \equiv 2^5 \times 11^1 \times 17^2 \pmod{539873}$.

Can you find a way to multiple some of these to get $X^2 \equiv Y^2$?

# Example Continued: Trying to factor 539873

$735^2 \equiv 352 = 2^5 \times 11^1 \pmod{539873}$.
$750^2 \equiv 22627 \equiv 11^3 \times 17^1 \pmod{539873}$.
$783^2 \equiv 73216 \equiv 2^9 \times 11^1 \times 13^1 \pmod{539873}$.
$801^2 \equiv 101728 \equiv 2^5 \times 11^1 \times 17^2 \pmod{539873}$.

Can you find a way to multiple some of these to get $X^2 \equiv Y^2$?

$$(735 \times 801)^2 \equiv 2^{10} \times 11^2 \times 17^2 \pmod{539873}$$
$$(735 \times 801)^2 \equiv (2^5 \times 11 \times 17)^2 \pmod{539873}$$

$$588735^2 \equiv 5984^2 \pmod{539873}$$

$$48862^2 \equiv 5984^2 \pmod{539873}$$

# Example Finished: Trying to factor 539873

We have found:

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

Now we use it to find a factor:

# Example Finished: Trying to factor 539873

We have found:

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

Now we use it to find a factor:

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

# Example Finished: Trying to factor 539873

We have found:

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

Now we use it to find a factor:

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

$$42878 \times 54846 \equiv 0 \pmod{539873}$$

# Example Finished: Trying to factor 539873

We have found:

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

Now we use it to find a factor:

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

$$42878 \times 54846 \equiv 0 \pmod{539873}$$

$$\mathrm{GCD}(42878, 539873) = 1949$$

1949 divides 539873. Found a Factor!

# We Noticed That... Can a Program?

$\lceil \sqrt{539873} \rceil = 735$
$735^2 \equiv 352 = 2^5 \times 11^1 \pmod{539873}$.
$750^2 \equiv 22627 \equiv 11^3 \times 17^1 \pmod{539873}$.
$783^2 \equiv 73216 \equiv 2^9 \times 11^1 \times 13^1 \pmod{539873}$.
$801^2 \equiv 101728 \equiv 2^5 \times 11^1 \times 17^2 \pmod{539873}$.

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 Noticed That... Can a Program? Cont

$\lceil \sqrt{539873} \rceil = 735$
$735^2 \equiv 352 = 2^5 \times 11^1 \pmod{539873}$.
$750^2 \equiv 22627 \equiv 11^3 \times 17^1 \pmod{539873}$.
$783^2 \equiv 73216 \equiv 2^9 \times 11^1 \times 13^1 \pmod{539873}$.
$801^2 \equiv 101728 \equiv 2^5 \times 11^1 \times 17^2 \pmod{539873}$.

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

All of the exponents on the right-hand-side are even.

# We Noticed That... Can a Program? Cont

$\lceil \sqrt{539873} \rceil = 735$
$735^2 \equiv 352 = 2^5 \times 11^1 \pmod{539873}$.
$750^2 \equiv 22627 \equiv 11^3 \times 17^1 \pmod{539873}$.
$783^2 \equiv 73216 \equiv 2^9 \times 11^1 \times 13^1 \pmod{539873}$.
$801^2 \equiv 101728 \equiv 2^5 \times 11^1 \times 17^2 \pmod{539873}$.

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

All of the exponents on the right-hand-side are even.

We want to find a set of right-hand-sides so that when multiplied together all of the exponents are even.

# Idea One

Store exponents in vector. Power-of-2, Power-of-3,...,Power-of-17.
$\lceil \sqrt{539873}\, \rceil = 735$

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

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

# Idea One

Store exponents in vector. Power-of-2, Power-of-3,...,Power-of-17.
$\lceil \sqrt{539873} \rceil = 735$

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

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.

$\lceil \sqrt{539873}\ \rceil = 735$

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

# Idea Two

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

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

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

# Quad Sieve Alg: First Attempt

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

$$\begin{array}{rl} (x+0)^2 \equiv y_0 & \text{Try to } B\text{-Factor } y_0 \text{ to get parity } \vec{v}_0 \\ \vdots & \vdots \\ (x+M)^2 \equiv y_M & \text{Try to } B\text{-Factor } y_M \text{ to get parity } \vec{v}_M \end{array}$$

# Quad Sieve Alg: First Attempt

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

$$\begin{array}{rl} (x+0)^2 \equiv y_0 & \text{Try to } B\text{-Factor } y_0 \text{ to get parity } \vec{v}_0 \\ \vdots & \vdots \\ (x+M)^2 \equiv y_M & \text{Try to } B\text{-Factor } y_M \text{ to get parity } \vec{v}_M \end{array}$$

Some of the $y_i$ were $B$-factored, but some were not.
Let $I$ be the set of all $i$ such that $y_i$ was $B$-factored.

# Quad Sieve Alg: First Attempt

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

$$\begin{array}{rl} (x+0)^2 \equiv y_0 & \text{Try to } B\text{-Factor } y_0 \text{ to get parity } \vec{v}_0 \\ \vdots & \vdots \\ (x+M)^2 \equiv y_M & \text{Try to } B\text{-Factor } y_M \text{ to get parity } \vec{v}_M \end{array}$$

Some of the $y_i$ were $B$-factored, but some were not.
Let $I$ be the set of all $i$ such that $y_i$ was $B$-factored.

Find $J \subseteq I$ such that $\sum_{i \in J} \vec{v}_i = \vec{0}$.

# Quad Sieve Alg: First Attempt

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

$$\begin{array}{rl} (x+0)^2 \equiv y_0 & \text{Try to } B\text{-Factor } y_0 \text{ to get parity } \vec{v}_0 \\ \vdots & \vdots \\ (x+M)^2 \equiv y_M & \text{Try to } B\text{-Factor } y_M \text{ to get parity } \vec{v}_M \end{array}$$

Some of the $y_i$ were $B$-factored, but some were not.
Let $I$ be the set of all $i$ such that $y_i$ was $B$-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.
Important! Since $\prod_{i \in J} y_i$ has all even exponents, there exists $Y$

$$\prod_{i \in J} y_i = Y^2$$

# Quad Sieve Alg: First Attempt, Cont

$$\left(\prod_{i\in J}(x+i)\right)^2 \equiv \prod_{i\in J} y_i = Y^2 \pmod{N}$$

Let $X = \prod_{i\in J}(x+i) \pmod{N}$ and $Y = \prod_{i\in J} y_i \pmod{N}$.

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

$$(X-Y)(X+Y) = kN \text{ for some } k$$

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

# What Could go Wrong

# What Could go Wrong

1. There is no set of rows that is linearly dependent.

# What Could go Wrong

1. There is no set of rows that is linearly dependent.
2. You find $X, Y$ such that $X^2 \equiv Y^2 \mod N$ but then $\mathrm{GCD}(X - Y, N) = 1$ and $\mathrm{GCD}(X + Y, N) = N$. This is very rare so we will not worry about it.

# Balancing Act

# Balancing Act

1. Run time will depend on $B$ and $M$. Gaussian Elimination is $O(B^3)$ which will be the main time sink. So want $B$ small.

# Balancing Act

1. Run time will depend on $B$ and $M$. Gaussian Elimination is $O(B^3)$ which will be the main time sink. So want $B$ small.
2. If $B$ is large then more numbers are $B$-fact, so have to go through less numbers to get $B+1$ $B$-fact numbers (hence $B+1$ vectors of dim $B$) so guaranteed to have a linear dependency. Hence want $B$ large.

# Balancing Act

1. Run time will depend on $B$ and $M$. Gaussian Elimination is $O(B^3)$ which will be the main time sink. So want $B$ small.
2. If $B$ is large then more numbers are $B$-fact, so have to go through less numbers to get $B+1$ $B$-fact numbers (hence $B+1$ vectors of dim $B$) so guaranteed to have a linear dependency. Hence want $B$ large.
3. In practice $B$ is chosen carefully based on computation and conjectures in Number Theory.

# Most Important Step to Speed Up

An earlier slide said

Gaussian Elimination is $O(B^3)$ which will be the main time sink.

# Most Important Step to Speed Up

An earlier slide said

Gaussian Elimination is $O(B^3)$ which will be the main time sink.

What about $B$ factoring $M$ numbers. That would seem to also be a time sink.

# Most Important Step to Speed Up

An earlier slide said

Gaussian Elimination is $O(B^3)$ which will be the main time sink.

What about $B$ factoring $M$ numbers. That would seem to also be a time sink.

The key to making the algorithm practical is Carl Pomerance's insight which is the how to do all that $B$-factoring fast. To do this we need a LOOOOOONG aside on Sieving.

# A LONG Aside on Sieving

November 13, 2019

# Finding all Primes $\leq 48$, the Stupid Way

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

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

Is this a good idea? Discuss.

# Finding all Primes $\le 48$, the Stupid Way

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

for $i = 2$ to 48 if $\mathrm{isprime}(i)$=YES 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 $\leq 48$.

| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | |

| 16 | 17 | 18 | 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 |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |

# Finding all primes $\leq 48$ the Smart Way

Write down the numbers $\leq 48$.

| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | |

| 16 | 17 | 18 | 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 |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |

Now output first unmarked—2—and MARK all multiples of 2.

# We Have Marked Multiples of 2

Now Have:

| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $X$ | | $X$ | | $X$ | | $X$ | | $X$ | | $X$ | | $X$ | |

| 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $X$ | | $X$ | | $X$ | | $X$ | | $X$ | | $X$ | |

| 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $X$ | | $X$ | | $X$ | | $X$ | | $X$ | | $X$ | |

| 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 |
|---|---|---|---|---|---|---|---|---|
| $X$ | | $X$ | | $X$ | | $X$ | | $X$ |

# We Have Marked Multiples of 2

Now Have:

| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $X$ | | $X$ | | $X$ | | $X$ | | $X$ | | $X$ | | $X$ | |

| 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $X$ | | $X$ | | $X$ | | $X$ | | $X$ | | $X$ | |

| 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $X$ | | $X$ | | $X$ | | $X$ | | $X$ | | $X$ | |

| 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 |
|---|---|---|---|---|---|---|---|---|
| $X$ | | $X$ | | $X$ | | $X$ | | $X$ |

Now output first unmarked—3—and MARK all multiples of 3.

# We Have Marked Multiples of 2 and 3

Now Have:

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

| 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| X | | X | | X | X | X | | X | | X | X |

| 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| X | | X | | X | X | X | | X | | X | X |

| 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 |
|---|---|---|---|---|---|---|---|---|
| X | | X | | X | X | X | | X |

# We Have Marked Multiples of 2 and 3

Now Have:

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

| 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| X | | X | | X | X | X | | X | | X | X |

| 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| X | | X | | X | X | X | | X | | X | X |

| 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 |
|---|---|---|---|---|---|---|---|---|
| X | | X | | X | X | X | | X |

Now output first unmarked—5—and MARK all multiples of 5.

# We Have Marked Multiples of 2,3 and 5

Now Have:

| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $X$ | $X$ | $X$ | $X$ | $X$ | | $X$ | $X$ | $X$ | | $X$ | | $X$ | $X$ |

| 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $X$ | | $X$ | | $X$ | $X$ | $X$ | | $X$ | $X$ | $X$ | $X$ |

| 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $X$ | | $X$ | | $X$ | $X$ | $X$ | $X$ | $X$ | | $X$ | $X$ |

| 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 |
|---|---|---|---|---|---|---|---|---|
| $X$ | | $X$ | | $X$ | $X$ | $X$ | | $X$ |

# We Have Marked Multiples of 2,3 and 5

Now Have:

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

| 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| X | | X | | X | X | X | | X | X | X | X |

| 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| X | | X | | X | X | X | X | X | | X | X |

| 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 |
|---|---|---|---|---|---|---|---|---|
| X | | X | | X | X | X | | X |

Now output first unmarked—7—and MARK all multiples of 7. You get the idea so we stop here.

# A Few Points About this Process

Speed

1. This process is really fast since when (say) MARKING mults of 3: We DO NOT look at (say) 23 and say no. WE DO NOT look at (say) 23 at all.
2. The KEY to many Number Theory Algorithms is not looking
3. Good number theory algs act on a need-to-know basis.

# A Few Points About this Process

Speed

1. This process is really fast since when (say) MARKING mults of 3: We DO NOT look at (say) 23 and say no. WE DO NOT look at (say) 23 at all.
2. The KEY to many Number Theory Algorithms is not looking
3. Good number theory algs act on a need-to-know basis.

Could we make it faster?

1. When MARKING mults of 3 we could mark 3, 3+6, $3 + 2 \times 6$ since mults of 2 are already MARKED.
2. When MARKING mults of 5 we could mark 5, 5+10, $5 + 2 \times 10$ since mults of 2 are already MARKED. Hard to also avoid mults of 3: $5, 25, 35$ not equally spaced.
3. When MARKING mults of BLAH we could BLAHBLAH.
4. If our goal was to JUST get a list of primes, we might do this.
5. Our goal will be to FACTOR these numbers. As such we cannot use this shortcut. (Clear later.)

# 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 all multiples of $p$ up to $\left\lfloor \frac{N}{p} \right\rfloor p$. (This takes $\frac{N}{p}$ steps.)
5. GOTO MARK STEP.

Time:

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

New Question: What is $\sum_{p \le N} \frac{1}{p}$?

# As Aside on $\sum_{p \leq N} \frac{1}{p}$

November 13, 2019

# Notation

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

$$\sum_{n < \infty} \frac{1}{n} = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots$$

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

where $q$ is the largest prime $\leq N$.

$$\sum_{p < \infty} \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \cdots$$

# Notation

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

$$\sum_{n<\infty}\frac{1}{n}=\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\cdots$$

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

where $q$ is the largest prime $\leq N$.

$$\sum_{p<\infty}\frac{1}{p}=\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\cdots$$

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

When I looked up $\sum_{p \leq N} \frac{1}{p}$ on the web I found:

# What is $\sum_{p \le N} \frac{1}{p}$ Asymptotically? History

When I looked up $\sum_{p \le N} \frac{1}{p}$ on the web I found:

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

## What is $\sum_{p \le N} \frac{1}{p}$ Asymptotically? History

When I looked up $\sum_{p \le N} \frac{1}{p}$ on the web I found:

1. Proofs that $\sum_{p < \infty} \frac{1}{p}$ diverges.
2. Some of those proofs show that $\sum_{p \le N} \frac{1}{p} \ge \ln(\ln(N)) + O(1)$.

# What is $\sum_{p \le N} \frac{1}{p}$ Asymptotically? History

When I looked up $\sum_{p \le N} \frac{1}{p}$ on the web I found:

1. Proofs that $\sum_{p < \infty} \frac{1}{p}$ diverges.
2. Some of those proofs show that $\sum_{p \le N} \frac{1}{p} \ge \ln(\ln(N)) + O(1)$.
3. Nothing on upper bounds on the sum.
4. TA Erik, when proofreading these slides, was able to find the theorem, though it was difficult. It's Merten's Second Thm.

## What is $\sum_{p \le N} \frac{1}{p}$ Asymptotically? History

When I looked up $\sum_{p \le N} \frac{1}{p}$ on the web I found:

1. Proofs that $\sum_{p < \infty} \frac{1}{p}$ diverges.
2. Some of those proofs show that $\sum_{p \le N} \frac{1}{p} \ge \ln(\ln(N)) + O(1)$.
3. Nothing on upper bounds on the sum.
4. TA Erik, when proofreading these slides, was able to find the theorem, though it was difficult. It's Merten's Second Thm.

A sequence of events:

# What is $\sum_{p \le N} \frac{1}{p}$ Asymptotically? History

When I looked up $\sum_{p \le N} \frac{1}{p}$ on the web I found:

1. Proofs that $\sum_{p < \infty} \frac{1}{p}$ diverges.
2. Some of those proofs show that $\sum_{p \le N} \frac{1}{p} \ge \ln(\ln(N)) + O(1)$.
3. Nothing on upper bounds on the sum.
4. TA Erik, when proofreading these slides, was able to find the theorem, though it was difficult. It's Merten's Second Thm.

A sequence of events:

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

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

# What is $\sum_{p \le N} \frac{1}{p}$ Asymptotically? History

When I looked up $\sum_{p \le N} \frac{1}{p}$ on the web I found:

1. Proofs that $\sum_{p < \infty} \frac{1}{p}$ diverges.
2. Some of those proofs show that $\sum_{p \le N} \frac{1}{p} \ge \ln(\ln(N)) + O(1)$.
3. Nothing on upper bounds on the sum.
4. TA Erik, when proofreading these slides, was able to find the theorem, though it was difficult. It's Merten's Second Thm.

A sequence of events:

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

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

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

# What is $\sum_{p \le N} \frac{1}{p}$ Asymptotically? History

When I looked up $\sum_{p \le N} \frac{1}{p}$ on the web I found:

1. Proofs that $\sum_{p<\infty} \frac{1}{p}$ diverges.
2. Some of those proofs show that $\sum_{p \le N} \frac{1}{p} \ge \ln(\ln(N)) + O(1)$.
3. Nothing on upper bounds on the sum.
4. TA Erik, when proofreading these slides, was able to find the theorem, though it was difficult. It's Merten's Second Thm.

A sequence of events:

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

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

2. Larry says its a well known theorem 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 $\sum_{p \le N} \frac{1}{p}$

1. $\sum_{n \le N} \frac{1}{n} \sim \ln(n)$.
2. $\sum_{p \le N} \frac{1}{p} \sim \ln(\ln(N))$

How good is this approximation?

1) When $N \ge 286$,

$$\ln(\ln N) - \frac{1}{2(\ln N)^2} + C \le \sum_{p \le N} \frac{1}{p} \le \ln(\ln N) + \frac{1}{(2 \ln N)^2} + C,$$

where $C \sim 0.261497212847643$.

2)

- $\sum_{p \le 10} \frac{1}{p} = 1.176$
- $\sum_{p \le 10^9} \frac{1}{p} = 3.293$
- $\sum_{p \le 10^{100}} \frac{1}{p} \sim 5.7$
- $\sum_{p \le 10^{1000}} \frac{1}{p} \sim 7.8$

# 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) The largest $pq$ factored is around 170-digits. 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

November 13, 2019

# Time Analysis of Sieve of E

The Sieve of E can find all primes $\leq N$ in time

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

# Time Analysis of Sieve of E

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?

Testing if a number is prime takes $(\log n)^3$ steps (we did not do this in class; however, it involves taking what we did do an adding to it to avoid false positives).

So testing all numbers $n \leq N$ for primality takes time:

$$\sum_{n \leq N} (\log n)^3 \sim N(\log N)^3$$

# Time Analysis of Sieve of E

The Sieve of E can find all primes $\le N$ in time

$$\le N \sum_{p \le N} \frac{1}{p} \le N \ln(\ln(N))$$

How long would finding all primes $\le N$ be the stupid way?

Testing if a number is prime takes $(\log n)^3$ steps (we did not do this in class; however, it involves taking what we did do an adding to it to avoid false positives).

So testing all numbers $n \le N$ for primality takes time:

$$\sum_{n \le N} (\log n)^3 \sim N(\log N)^3$$

- The time difference here is not that impressive. When we modify the Sieve to actually factor, it will be much more impressive.

# Time Analysis of Sieve of E

The Sieve of E can find all primes $\le N$ in time

$$\le N \sum_{p \le N} \frac{1}{p} \le N \ln(\ln(N))$$

How long would finding all primes $\le N$ be the stupid way?

Testing if a number is prime takes $(\log n)^3$ steps (we did not do this in class; however, it involves taking what we did do an adding to it to avoid false positives).

So testing all numbers $n \le N$ for primality takes time:

$$\sum_{n \le N} (\log n)^3 \sim N(\log N)^3$$

- The time difference here is not that impressive. When we modify the Sieve to actually factor, it will be much more impressive.
- The key to the speed of The Sieve of E is that when it marks

# $B$-Factoring-Variant on Sieve of E: Example

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 numbers $\leq 48$. We 2-factor them, so divide by 2,3.

| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | |

| 16 | 17 | 18 | 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 |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |

# B-factoring all $N \leq 48$, the Smart Way

Write down numbers $\leq 48$. We 2-factor them, so divide by 2,3.

| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | |

| 16 | 17 | 18 | 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 is 2. DIVIDE mults of 2 by 2.

# Divide by 2

| 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $2*1$ | | $2*2$ | | $2*3$ | | $2^3$ | | $2*5$ | | $2^2*3$ | | $2*7$ | |

| 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $2^4$ | | $2*9$ | | $2*10$ | | $2*11$ | | $2^3*3$ | | $2*13$ | |

| 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $2^2*7$ | | $2*15$ | | $2^5$ | | $2*17$ | | $2^2*9$ | | $2*19$ | |

| 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 |
|---|---|---|---|---|---|---|---|---|
| $2^3*5$ | | $2*21$ | | $2^2*11$ | | $2*23$ | | $2^4*3$ |

First unmarked is 2. DIVIDE mults of 3 by 3.

# Divide by 3

We only show the last row (for reasons of space).

| 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 |
|---|---|---|---|---|---|---|---|---|
| $2^3 * 5$ | | $2 * 3 * 7$ | | $2^2 * 11$ | $3^2 * 5$ | $2 * 23$ | | $2^4 * 3$ |

- 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:

$$\sum_{p \le B} \frac{N}{p} + \sum_{p \le B} \frac{N}{p^2} + \sum_{p \le B} \frac{N}{p^3} + \sum_{p \le B} \frac{N}{p^4} \cdots$$

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

# Variant of The Sieve of Eratosthenes: Analysis

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

$$N\sum_{p\le B}\frac{1}{p}+N\sum_{p\le B}\frac{1}{p^2}+N\sum_{p\le B}\frac{1}{p^3}+N\sum_{p\le B}\frac{1}{p^4}+\cdots$$

$$= N\ln(\ln(B))+N\sum_{a=2}^{\infty}\sum_{p\le B}\frac{1}{p^a}$$

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

# Variant of The Sieve of Eratosthenes: Analysis

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

$$N\sum_{p\le B}\frac{1}{p} + N\sum_{p\le B}\frac{1}{p^2} + N\sum_{p\le B}\frac{1}{p^3} + N\sum_{p\le B}\frac{1}{p^4} + \cdots$$

$$= N\ln(\ln(B)) + N\sum_{a=2}^{\infty}\sum_{p\le B}\frac{1}{p^a}$$

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

$$\le N\ln(\ln(B)) + (0.5)N.$$

Note: The mult constants really are $\le 1$ 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 $\leq N$

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

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

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

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

# Variant of The Sieve of E: That last term is $\leq N$

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

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

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

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 $\le N$

$$= N \sum_{a=2}^{\infty} \sum_{p \le B} \frac{1}{p^a} = N \sum_{p \le B} \sum_{a=2}^{\infty} \frac{1}{p^a}$$

$$= N \sum_{p \le B} \frac{1/p^2}{1 - (1/p)}$$

$$= N \sum_{p \le B} \frac{1}{p^2 - p} \sim N \sum_{p \le B} \frac{1}{p^2}$$

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

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 $\le N$

$$= N \sum_{a=2}^{\infty} \sum_{p \le B} \frac{1}{p^a} = N \sum_{p \le B} \sum_{a=2}^{\infty} \frac{1}{p^a}$$

$$= N \sum_{p \le B} \frac{1/p^2}{1-(1/p)}$$

$$= N \sum_{p \le B} \frac{1}{p^2 - p} \sim N \sum_{p \le B} \frac{1}{p^2}$$

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

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 $\le N$

$$= N \sum_{a=2}^{\infty} \sum_{p \le B} \frac{1}{p^a} = N \sum_{p \le B} \sum_{a=2}^{\infty} \frac{1}{p^a}$$

$$= N \sum_{p \le B} \frac{1/p^2}{1 - (1/p)}$$

$$= N \sum_{p \le B} \frac{1}{p^2 - p} \sim N \sum_{p \le B} \frac{1}{p^2}$$

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

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

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

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.

# Back to Quadratic Sieve Factoring Algorithm

November 13, 2019

# Recall Quad Sieve Alg: First Attempt

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

$$\begin{array}{ll} (x+0)^2 \equiv y_0 & \text{Try to } B\text{-Factor } y_0 \text{ to get parity } \vec{v}_0 \\ \vdots & \vdots \\ (x+M)^2 \equiv y_M & \text{Try to } B\text{-Factor } y_M \text{ to get parity } \vec{v}_M \end{array}$$

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, so exists $Y$:

$$\prod_{i \in J} y_i = Y^2$$

$$(\prod_{i \in J}(x+i))^2 \equiv \prod_{i \in J} y_i = Y^2 \pmod{N}$$

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

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

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

# 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.

$$\begin{aligned}
(x+0)^2 &\equiv y_0 & &\text{Try to } B\text{-Factor } y_0 \text{ to get parity } \vec{v}_0 \\
&\vdots & &\vdots \\
(x+M)^2 &\equiv y_M & &\text{Try to } B\text{-Factor } y_M \text{ to get parity } \vec{v}_M
\end{aligned}$$

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.

$$\begin{array}{rl} (x+0)^2 \equiv y_0 & \text{Try to } B\text{-Factor } y_0 \text{ to get parity } \vec{v}_0 \\ \vdots & \vdots \\ (x+M)^2 \equiv y_M & \text{Try to } B\text{-Factor } y_M \text{ to get parity } \vec{v}_M \end{array}$$

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.

$$\begin{array}{rl} (x+0)^2 \equiv y_0 & \text{Try to } B\text{-Factor } y_0 \text{ to get parity } \vec{v}_0 \\ \vdots & \vdots \\ (x+M)^2 \equiv y_M & \text{Try to } B\text{-Factor } y_M \text{ to get parity } \vec{v}_M \end{array}$$

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

$$\begin{array}{rl} (x+0)^2 \equiv y_0 & \text{Try to } B\text{-Factor } y_0 \text{ to get parity } \vec{v}_0 \\ \vdots & \vdots \\ (x+M)^2 \equiv y_M & \text{Try to } B\text{-Factor } y_M \text{ to get parity } \vec{v}_M \end{array}$$

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 $y_0, \ldots, y_M$.

# The Quadratic Sieve: The Problem

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

$$
\begin{array}{l}
(x+0)^2 \pmod{N} \\
(x+1)^2 \pmod{N} \\
\quad\vdots \qquad \vdots \\
(x+M)^2 \pmod{N}
\end{array}
$$

We do an example on the next slide.

# The Quadratic Sieve: Example

$N = 1147$, $B = 2$, $M = 10$, $x = 34$.
Want to 2-factor (so all powers of 2 and 3)

$$\begin{array}{l}(34+0)^2 \pmod{1147}\\ \quad\vdots \qquad \vdots \qquad \vdots\\ (34+10)^2 \pmod{1147}\end{array}$$

# 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?

# The Quadratic Sieve: Example

$N = 1147$, $B = 2$, $M = 10$, $x = 34$.
Want to 2-factor (so all powers of 2 and 3)

$$
\begin{array}{lll}
(34+0)^2 & \pmod{1147} \\
\vdots & \vdots & \vdots \\
(34+10)^2 & \pmod{1147}
\end{array}
$$

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 $0 \le i \le 10$ 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)
$(34 + 0)^2 \pmod{1147}$
$$\vdots \qquad \vdots \qquad \vdots$$
$(34 + 10)^2 \pmod{1147}$
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

Need to know the set of $0 \leq i \leq 10$ such that 2 divides

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

# The Quadratic Sieve: Example of dividing by 2

Need to know the set of $0 \leq i \leq 10$ such that 2 divides

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

What is $(34+i)^2 \pmod{1147}$?

# The Quadratic Sieve: Example of dividing by 2

Need to know the set of $0 \leq i \leq 10$ such that 2 divides

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

What is $(34 + i)^2 \pmod{1147}$? Since $0 \leq i \leq 10$,

# The Quadratic Sieve: Example of dividing by 2

Need to know the set of $0 \leq i \leq 10$ such that 2 divides

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

What is $(34+i)^2 \pmod{1147}$? Since $0 \leq i \leq 10$,

$$(34+0)^2 < (34+i)^2 < (34+10)^2$$

# The Quadratic Sieve: Example of dividing by 2

Need to know the set of $0 \le i \le 10$ such that 2 divides

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

What is $(34+i)^2 \pmod{1147}$? Since $0 \le i \le 10$,

$$(34+0)^2 < (34+i)^2 < (34+10)^2$$

$$1156 < (34+i)^2 < 1936$$

# The Quadratic Sieve: Example of dividing by 2

Need to know the set of $0 \leq i \leq 10$ such that 2 divides

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

What is $(34+i)^2 \pmod{1147}$? Since $0 \leq i \leq 10$,

$$(34+0)^2 < (34+i)^2 < (34+10)^2$$

$$1156 < (34+i)^2 < 1936$$

$$1147+9 < (34+i)^2 < 1147+789$$

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

# The Quadratic Sieve: Example of dividing by 2

Need to know the set of $0 \leq i \leq 10$ such that 2 divides

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

What is $(34+i)^2 \pmod{1147}$? Since $0 \leq i \leq 10$,

$$(34+0)^2 < (34+i)^2 < (34+10)^2$$

$$1156 < (34+i)^2 < 1936$$

$$1147 + 9 < (34+i)^2 < 1147 + 789$$

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

Our question is, for which $i$ does:

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

# The Quadratic Sieve: Example of dividing by 2, cont

Need to know the set of $0 \le i \le 10$ such that 2 divides

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

# The Quadratic Sieve: Example of dividing by 2, cont

Need to know the set of $0 \leq i \leq 10$ such that 2 divides

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

We know that

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

# The Quadratic Sieve: Example of dividing by 2, cont

Need to know the set of $0 \le i \le 10$ such that 2 divides

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

We know that

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

Our question is, for which $i$ does:

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

## The Quadratic Sieve: Example of dividing by 2, cont

Need to know the set of $0 \le i \le 10$ such that 2 divides

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

We know that

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

Our question is, for which $i$ does:

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

Take mod 2 to both sides to get

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

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

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 $(34+i)^2 \pmod{1147}$?

# The Quadratic Sieve: Example of dividing by 3

For which $0 \leq i \leq 10$ does 3 divide $(34+i)^2 \pmod{1147}$?
We know that $(34+i)^2 \pmod{1147} = (34+i)^2 - 1147$.

Our question is, for which $i$ does

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

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

$$i \equiv 1, 2 \pmod{3}.$$

Great!- just need to divide the $y_i$ where $i \equiv 0, 1 \pmod{3}$.

# 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

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

$\vdots \quad \vdots$

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

Algorithm

As $p$ goes through the first $B$ primes.

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 $\left\lceil \frac{M-a}{p} \right\rceil$

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

Time $\le \sum_{p \le B} (\lg p + 2\frac{M-1}{p}) = \sum_{p \le B} \lg p + 2M \sum_{p \le B} \frac{1}{p}$.

$$= (\sum_{p \le B} \lg p) + 2M \ln\ln(B) = 2B + 2M \ln(\ln(B)).$$

# Names of Sieves

1. The *Sieve of E* is the Sieve that, given $N$, finds all of the primes $\leq N$. We may also use the name for finding all primes between $N_1$ and $N_2$.
2. The *B-Factoring Sieve of E* is the Sieve that, given $N$, tries to $B$-factors all of the numbers from 2 to $N$. We may also use the name for $B$-factoring all numbers between $N_1$ and $N_2$.
3. The *Quadratic Sieve* is from the last slide. Given $N, B, M, x$ it tries to $B$-factor $(x+0)^2 \pmod N$, ..., $(x+M)^2 \pmod N$. Note that it is quite fast.

# 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 $(x+0)^2 \pmod{N}$, …, $(x+M)^2 \pmod{N}$ 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, so there exists $Y$

$$\prod_{i \in J} y_i = Y^2$$

$$\left(\prod_{i \in J}(x+i)\right)^2 \equiv \prod_{i \in J} y_i = Y^2 \pmod{N}$$

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

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

$\mathrm{GCD}(X - Y, N)$, $\mathrm{GCD}(X + Y, N)$ 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

# Speed Up One

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.

# Speed Up One

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.

# Speed Up Two

Recall:
We started with $x = \left\lceil \sqrt{N} \right\rceil$ and did $(x+i)^2$ for $0 \le i \le M$.

# Speed Up Two

Recall:
We started with $x = \left\lceil \sqrt{N} \right\rceil$ and did $(x+i)^2$ for $0 \le i \le M$.

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

Advantage Smaller numbers more likely to be $B$-fact.

# Speed Up Three

Recall:

$(34+i)^2 - 1147 \equiv 0 \pmod{19}$

$(15+i)^2 + 12 \equiv 0 \pmod{19}$

$i \equiv 8, 15 \pmod{19}$

# Speed Up Three

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.

# Speed Up Four—Use some primes $> B$

1. Look at all of the non $B$-factored numbers. For each one test if what is left is prime. Let $Z_1$ 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, Pollards rho) for a limited amount of time. Let $Z_2$ be the set of primes you come across.
3. Do Q. Sieve on all of the non $B$-factored numbers using the primes in $Z_1 \cup Z_2$.

This will increase the number of $B$-factored numbers.

# Speed Up Five—Avoid Division

For this slide lg means $\lceil \lg \rceil$ which is very fast on a computer.

Using Divisions Primes $q_1, \ldots, q_m < B$ divide $x$. Divide $x$ by all the $q_i$. Also $q_i^2$, $q_i^3$, etc until does not work. When you are done you've $B$-factored the number or not.

# Speed Up Five—Avoid Division

For this slide lg means $\lceil \lg \rceil$ which is very fast on a computer.

Using Divisions Primes $q_1, \ldots, q_m < B$ divide $x$. Divide $x$ by all the $q_i$. Also $q_i^2$, $q_i^3$, etc until does not work. When you are done you've $B$-factored the number or not.

Using Subtraction Primes $q_1, \ldots, q_m < B$ divide $x$. Do

$$d = \lg(x) - \lg(q_1) - \lg(q_2) - \cdots - \lg(q_m)$$

# Speed Up Five—Avoid Division

For this slide lg means $\lceil \lg \rceil$ which is very fast on a computer.

Using Divisions Primes $q_1, \ldots, q_m < B$ divide $x$. Divide $x$ by all the $q_i$. Also $q_i^2$, $q_i^3$, etc until does not work. When you are done you've $B$-factored the number or not.

Using Subtraction Primes $q_1, \ldots, q_m < B$ divide $x$. Do

$$d = \lg(x) - \lg(q_1) - \lg(q_2) - \cdots - \lg(q_m)$$

If $d \sim 0$ then we think $x$ IS $B$-fact, so $B$-factor $x$.
If far from 0 then DO NOT DIVIDE!

# Speed Up Five—Avoid Division, Why Works

Why Does This Work? If $x = q_1 q_2 q_3$ then

$$\lg(x) = \lg(q_1) + \lg(q_2) + \lg(q_3)$$

$$\lg(x) - \lg(q_1) - \lg(q_2) - \lg(q_3) = 0$$

# Speed Up Five—Avoid Division, Why Works

Why Does This Work? If $x = q_1 q_2 q_3$ then

$$\lg(x) = \lg(q_1) + \lg(q_2) + \lg(q_3)$$

$$\lg(x) - \lg(q_1) - \lg(q_2) - \lg(q_3) = 0$$

So why not insist that

$$\lg(x) - \lg(q_1) - \lg(q_2) - \cdots - \lg(q_m) = 0$$

1. Using $\lceil \lg \rceil$ may introduce approximations so you don't get 0.
2. If $x = q_1^2 q_2 q_3$ then

$$\lg(x) = \lg(q_1^2) + \lg(q_2) + \lg(q_3) = 2\lg(q_1) + \lg(q_2) + \lg(q_3)$$

$$\lg(x) - \lg(q_1) + \lg(q_2) + \lg(q_3) = \lg(q_1) \neq 0$$

3. We need to define small carefully. Will still err.

# Speed Up Five—Avoid Division, Why Fast

Why is this fast?

1. Subtraction is much faster than division.
2. Most numbers are not $B$-fact, so don't do divisions that won't help.

# Speed Up Five—Avoid Division, Example One

$B = 7$ so we are looking at $2, 3, 5, 7, 11, 13, 17$. Small is $\leq 10$.

## Speed Up Five—Avoid Division, Example One

$B = 7$ so we are looking at $2, 3, 5, 7, 11, 13, 17$. Small is $\leq 10$.

108290 7-fact? We find that 2,5,7,13,17 all divide it.

# Speed Up Five—Avoid Division, Example One

$B = 7$ so we are looking at $2, 3, 5, 7, 11, 13, 17$. Small is $\leq 10$.

108290 7-fact? We find that 2,5,7,13,17 all divide it.

$$\lg(108290) - \lg(2) - \lg(5) - \lg(7) - \lg(13) - \lg(17) = 4 \leq 10$$

# Speed Up Five—Avoid Division, Example One

$B = 7$ so we are looking at $2, 3, 5, 7, 11, 13, 17$. Small is $\leq 10$.

108290 7-fact? We find that 2,5,7,13,17 all divide it.

$$\lg(108290) - \lg(2) - \lg(5) - \lg(7) - \lg(13) - \lg(17) = 4 \leq 10$$

So we think 108290 IS 7-fact. Is this correct? Yes:

# Speed Up Five—Avoid Division, Example One

$B = 7$ so we are looking at $2, 3, 5, 7, 11, 13, 17$. Small is $\leq 10$.

108290 7-fact? We find that 2,5,7,13,17 all divide it.

$$\lg(108290) - \lg(2) - \lg(5) - \lg(7) - \lg(13) - \lg(17) = 4 \leq 10$$

So we think 108290 IS 7-fact. Is this correct? Yes:

$$108290 = 2 \times 5 \times 7^2 \times 13 \times 17$$

# Speed Up Five—Avoid Division, Examples Two

Is 78975897 7-fact? We find that 3,7,11,13,17 all divide it.

# Speed Up Five—Avoid Division, Examples Two

Is 78975897 7-fact? We find that 3,7,11,13,17 all divide it.

$$\lg(78975897) - \lg(3) - \lg(7) - \lg(11) - \lg(13) - \lg(17) = 11 > 10$$

## Speed Up Five—Avoid Division, Examples Two

Is 78975897 7-fact? We find that 3,7,11,13,17 all divide it.

$$\lg(78975897) - \lg(3) - \lg(7) - \lg(11) - \lg(13) - \lg(17) = 11 > 10$$

So we think 78975897 is NOT 7-fact. Is this correct? No!

$$78975897 = 3 \times 7^2 \times 11 \times 13^2 \times 17^4.$$

# Speed Up Five—Avoid Division, Examples Two

Is 78975897 7-fact? We find that 3,7,11,13,17 all divide it.

$$\lg(78975897) - \lg(3) - \lg(7) - \lg(11) - \lg(13) - \lg(17) = 11 > 10$$

So we think 78975897 is NOT 7-fact. Is this correct? No!

$$78975897 = 3 \times 7^2 \times 11 \times 13^2 \times 17^4.$$

**Cautionary Note**

$78975897 = 3 \times 7^2 \times 11 \times 13^2 \times 17^4$. was thought to NOT be 7-fact. Erred because primes had large exponents. The large exponents made

$$\lg(78975897)$$

LARGER than

$$\lg(3) + \lg(7) + \lg(11) + \lg(13) + \lg(17)$$

# Speed Up Five—Avoid Division, Examples Three

Is 9699690 7-fact? We find that 2,3,5,7,11,13,17 all divide it.

# Speed Up Five—Avoid Division, Examples Three

Is 9699690 7-fact? We find that 2,3,5,7,11,13,17 all divide it.

$$\lg(9699690) - \lg(2) - \lg(3) - \lg(5) - \lg(7) - \lg(11) - \lg(13) - \lg(17) = 1 \leq 10$$

# Speed Up Five—Avoid Division, Examples Three

Is 9699690 7-fact? We find that 2,3,5,7,11,13,17 all divide it.

$\lg(9699690) - \lg(2) - \lg(3) - \lg(5) - \lg(7) - \lg(11) - \lg(13) - \lg(17) = 1 \le 10$

So we think 9699690 is 7-fact. Is this correct? No!

$\lg(9699690) - \lg(2) - \lg(3) - \lg(5) - \lg(7) - \lg(11) - \lg(13) - \lg(17) = 1 \le 10$

Cautionary Note $78975897 = 2 \times 3 \times 5 \times 7 \times 11 \times 13 \times 17 \times 19$. was thought to NOT be 7-fact. Erred because it had low exponents and only one a small prime over $B$.

# Speed Up Five—Avoid Division, Examples Three

Is 9699690 7-fact? We find that 2,3,5,7,11,13,17 all divide it.

$$\lg(9699690) - \lg(2) - \lg(3) - \lg(5) - \lg(7) - \lg(11) - \lg(13) - \lg(17) = 1 \leq 10$$

So we think 9699690 is 7-fact. Is this correct? No!

$$\lg(9699690) - \lg(2) - \lg(3) - \lg(5) - \lg(7) - \lg(11) - \lg(13) - \lg(17) = 1 \leq 10$$

Cautionary Note $78975897 = 2 \times 3 \times 5 \times 7 \times 11 \times 13 \times 17 \times 19$. was thought to NOT be 7-fact. Erred because it had low exponents and only one a small prime over $B$.
Lemon to Lemonade Not $B$-fact, but still useful. Speedup 4.

# Speed Up Five-extra—Avoid Division, One More Trick

We are just approximating if

$$\lg x - \lg(q_1) - \cdots - \lg(q_m)$$

is small.

# Speed Up Five-extra—Avoid Division, One More Trick

We are just approximating if

$$\lg x - \lg(q_1) - \cdots - \lg(q_m)$$

is small.

$\lg 2$, $\lg 3$, $\lg 5$ are so tiny, don't bother with those.

# Speed Up Five-extra—Avoid Division, One More Trick

We are just approximating if

$$\lg x - \lg(q_1) - \cdots - \lg(q_m)$$

is small.

$\lg 2$, $\lg 3$, $\lg 5$ are so tiny, don't bother with those.

If $B = 7$ then use:

$$2^3, 3^2, 5^2, 7, 11, 13, 17, 19$$

# Speed Up Six

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.

1. Can be done in $O(B^{2+\epsilon})$ steps rather than $O(B^3)$.
2. Can't store the entire matrix—to big.

# Speed Up Seven

(This is a paragraph from a blog post about Quad Sieve
`https://blogs.msdn.microsoft.com/devdev/2006/06/19/factoring-large-numbers-with-quadratic-sieve/`)

Is $z$ $B$-fact? There is a light for each $p \le B$ 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 $B$-fact number candidate. Can do in parallel.

# 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

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

| Alg | Run Time as $N^{a/L^{\delta}}$ | Run Time in terms of $L$ |
|---|---|---|
| Naive | $N^{1/2}$ | $2^{L/2}$ |
| Pollard Rho | $N^{1/4}$ | $2^{L/4}$ |
| Linear Sieve | $N^{3.9/L^{1/2}}$ | $2^{1.95L^{1/2}}$ |
| Quad Sieve | $N^{2.8/L^{1/2}}$ | $2^{1.4L^{1/2}}$ |
| N.F. Sieve | $N^{14/L^{2/3}}$ | $2^{20L^{1/3}}$ |

1. Times are more conjectured than proven.
2. Quad S. is better than Linear Sieve by only a constant in the exponent. Made a big difference IRL.
3. Quad Sieve is better than Pollard-Rho at about $10^{50}$.

# Relevance for RSA

# Relevance for RSA

1. Carl Pomerance devised the Quad S. algorithm in 1982.

# Relevance for RSA

1. Carl Pomerance devised the Quad S. algorithm in 1982.
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

1. Carl Pomerance devised the Quad S. algorithm in 1982.
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 $N$

# Relevance for RSA

1. Carl Pomerance devised the Quad S. algorithm in 1982.
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 $t=\frac{1}{2}$ and N.F.Sieve using $t=\frac{1}{3}$. 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 $t = \frac{1}{2}$ and N.F.Sieve using $t = \frac{1}{3}$. Moreover, any method that uses $B$-factoring must take this long.

- No progress since N.F.Sieve in 1988.

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

- No progress since N.F.Sieve in 1988.
- 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 $t = \frac{1}{2}$ and N.F.Sieve using $t = \frac{1}{3}$. Moreover, any method that uses $B$-factoring must take this long.

- No progress since N.F.Sieve in 1988.
- My opinion: $e^{c(\ln N)^t(\ln\ln N)^{1-t}}$ is the best you can do ever, though $t$ can be improved.
- Why hasn't $t$ been improved? Wagstaff told me:

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

- No progress since N.F.Sieve in 1988.
- My opinion: $e^{c(\ln N)^t(\ln \ln N)^{1-t}}$ is the best you can do ever, though $t$ can be improved.
- Why hasn't $t$ been improved? Wagstaff told me:
  - We've run out of parameters to optimize.

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

- No progress since N.F.Sieve in 1988.
- My opinion: $e^{c(\ln N)^t(\ln \ln N)^{1-t}}$ is the best you can do ever, though $t$ can be improved.
- Why hasn't $t$ been improved? Wagstaff told me:
  - We've run out of parameters to optimize.
  - Brandon, Solomon, Mark, and Ivan haven't worked on it yet.