BILL START RECORDING

Quadratic Sieve Factoring

Notation Reminder

1) $\mathbf{GCD(x, y)}$ is the **Greatest Common Divisor** of x, y.

Notation Reminder

1) $\mathrm{GCD}(\mathbf{x},\mathbf{y})$ is the **Greatest Common Divisor** of x, y.

2) **Sums and Products**

$$\sum_{i=1}^{n} a_i = a_1 + a_2 + \cdots + a_n.$$

$$\prod_{i=1}^{n} a_i = a_1 \times a_2 \times \cdots \times a_n.$$

Notation Reminder

1) $\mathrm{GCD}(\mathbf{x}, \mathbf{y})$ is the **Greatest Common Divisor** of x, y.

2) **Sums and Products**

$$\sum_{i=1}^{n} a_i = a_1 + a_2 + \cdots + a_n.$$

$$\prod_{i=1}^{n} a_i = a_1 \times a_2 \times \cdots \times a_n.$$

3) **More Sums and Products** We **summed** or **producted** over $\{1, \ldots, n\}$. Can use other sets.

Notation Reminder

1) **GCD(x, y)** is the **Greatest Common Divisor** of x, y.

2) **Sums and Products**

$$\sum_{i=1}^{n} a_i = a_1 + a_2 + \cdots + a_n.$$

$$\prod_{i=1}^{n} a_i = a_1 \times a_2 \times \cdots \times a_n.$$

3) **More Sums and Products** We **summed** or **producted** over $\{1, \ldots, n\}$. Can use other sets.
If $A = \{1, 4, 9\}$ then

$$\sum_{i \in A} a_i = a_1 + a_4 + a_9.$$

$$\prod_{i \in A} a_i = a_1 \times a_4 \times a_9.$$

More Notation Reminder

4) $a_1, \ldots, a_n$ could be **vectors.**

$$\sum_{i \in A} \vec{a}_i = \vec{a}_1 + \vec{a}_4 + \vec{a}_9.$$

Addition is **component-wise.**

More Notation Reminder

4) $a_1, \ldots, a_n$ could be **vectors.**

$$\sum_{i \in A} \vec{a}_i = \vec{a}_1 + \vec{a}_4 + \vec{a}_9.$$

Addition is **component-wise.**
We will not be using any notion of a product of vectors.

More Notation Reminder

4) $a_1, \ldots, a_n$ could be **vectors.**

$$\sum_{i \in A} \vec{a}_i = \vec{a}_1 + \vec{a}_4 + \vec{a}_9.$$

Addition is **component-wise.**
We will not be using any notion of a product of vectors.

5) We extend mod notation to vectors of integers. Example:

$$(8, 1, 0, 9) \pmod{2} = (0, 1, 0, 1).$$

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 solve it in time, but it inspired him to (much later) 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 5×1261, 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 5×1261, 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 5×1261, 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 if 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 if 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 $x = \left\lceil \sqrt{N} \right\rceil$.

How Can We Make This Happen?

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

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

How Can We Make This Happen?

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

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

Look for $I \subseteq \mathbb{N}$ such that: $\prod_{i \in I} y_i = q_1^{2e_1} q_2^{2e_2} \cdots q_k^{2e_k}$.

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: $\prod_{i \in I} y_i = q_1^{2e_1} q_2^{2e_2} \cdots q_k^{2e_k}$.
Then we get:

$$\left(\prod_{i \in I} (x+i) \right)^2 \equiv \left(\prod_{i=1}^{k} q_i^{e_i} \right)^2 \pmod{N}$$

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: $\prod_{i \in I} y_i = q_1^{2e_1} q_2^{2e_2} \cdots q_k^{2e_k}$.
Then we get:

$$\left(\prod_{i \in I} (x+i) \right)^2 \equiv \left(\prod_{i=1}^{k} q_i^{e_i} \right)^2 \pmod{N}$$

Let $X = \prod_{i \in I} (x+i) \pmod{N}$ and $Y = \prod_{i=1}^{k} q_i^{e_i} \pmod{N}$.

How Can We Make This Happen?

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

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

Look for $I \subseteq \mathbb{N}$ such that: $\prod_{i \in I} y_i = q_1^{2e_1} q_2^{2e_2} \cdots q_k^{2e_k}$.
Then we get:

$$\left(\prod_{i \in I} (x+i) \right)^2 \equiv \left(\prod_{i=1}^{k} q_i^{e_i} \right)^2 \pmod{N}$$

Let $X = \prod_{i \in I} (x+i) \pmod{N}$ and $Y = \prod_{i=1}^{k} q_i^{e_i} \pmod{N}$.

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

How Can We Make This Happen?

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

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

Look for $I \subseteq \mathbb{N}$ such that: $\prod_{i \in I} y_i = q_1^{2e_1} q_2^{2e_2} \cdots q_k^{2e_k}$.
Then we get:

$$\left(\prod_{i \in I} (x+i) \right)^2 \equiv \left(\prod_{i=1}^{k} q_i^{e_i} \right)^2 \pmod{N}$$

Let $X = \prod_{i \in I} (x+i) \pmod{N}$ and $Y = \prod_{i=1}^{k} q_i^{e_i} \pmod{N}$.

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

Is this a good idea? Discuss.

Look at the First Step

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

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.

Look at the First Step

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

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

Look at the First Step

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

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

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! 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-factorable** if 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*-factorable** if 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-factorable** if 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*-factorable** if 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-factorable** if 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*-factorable** if 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 what's 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*-factorable** if 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 what's left. $82203 = 3 \times 27401$.
3. Divide 5 into what's 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*-factorable** if 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 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.

B-Factoring

Idea B be a parameter. $p_1 < p_2 < \cdots < p_B$ are the first B primes.
Def A number is ***B*-factorable** if 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 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. $82203 = 3 \times 11 \times 2491$.

B-Factoring

Idea B be a parameter. $p_1 < p_2 < \cdots < p_B$ are the first B primes.
Def A number is ***B*-factorable** if 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 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. $82203 = 3 \times 11 \times 2491$.
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,…,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 $2, 3, 5, 7, 11, 13, 17$

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

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

$736^2, \ldots, 749^2$ 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.

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.

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

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.

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

$784^2, \ldots, 800^2$ 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 more nicely.

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

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

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

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

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.

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

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

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 mod 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.

Quad Sieve Alg: First Attempt (Example)

Some of the y_i were B-factored, but some were not:

Quad Sieve Alg: First Attempt (Example)

Some of the y_i were B-factored, but some were not:

$(x+a)^2 \mod N = y_a = 2^{a_1}3^{a_2}\cdots p_B^{a_B}$. $\vec{a} = (a_1,\ldots,a_B) \pmod 2$.

Quad Sieve Alg: First Attempt (Example)

Some of the y_i were B-factored, but some were not:

$(x+a)^2 \mod N = y_a = 2^{a_1}3^{a_2}\cdots p_B^{a_B}$. $\vec{a} = (a_1, \ldots, a_B) \pmod 2$.

$\vdots$

Quad Sieve Alg: First Attempt (Example)

Some of the y_i were B-factored, but some were not:

$(x+a)^2 \mod N = y_a = 2^{a_1}3^{a_2}\cdots p_B^{a_B}$. $\vec{a} = (a_1, \ldots, a_B) \pmod 2$.

$\vdots$

$(x+z)^2 \mod N = y_z = 2^{z_1}3^{z_2}\cdots p_B^{z_B}$, $\vec{b} = (z_1, \ldots, z_B) \pmod 2$.

Quad Sieve Alg: First Attempt (Example)

Some of the y_i were B-factored, but some were not:

$(x+a)^2 \mod N = y_a = 2^{a_1}3^{a_2}\cdots p_B^{a_B}$. $\vec{a} = (a_1, \ldots, a_B) \pmod 2$.

$\vdots$

$(x+z)^2 \mod N = y_z = 2^{z_1}3^{z_2}\cdots p_B^{z_B}$, $\vec{b} = (z_1, \ldots, z_B) \pmod 2$.

Try to find come combination of $\vec{a}$, ..., $\vec{z}$ that sums $\vec{0}$ mod 2.

Quad Sieve Alg: First Attempt (Example)

Some of the y_i were B-factored, but some were not:

$(x+a)^2 \mod N = y_a = 2^{a_1} 3^{a_2} \cdots p_B^{a_B}$. $\vec{a} = (a_1, \ldots, a_B) \pmod 2$.

$\vdots$

$(x+z)^2 \mod N = y_z = 2^{z_1} 3^{z_2} \cdots p_B^{z_B}$, $\vec{b} = (z_1, \ldots, z_B) \pmod 2$.

Try to find come combination of $\vec{a}$, ..., $\vec{z}$ that sums $\vec{0}$ mod 2.

Lets say $\vec{a} + \vec{d} + \vec{q} \equiv \vec{0} \pmod 2$. Then

$$(x+a)^2 (x+d)^2 (x+q)^2 \equiv y_a y_d y_q = Y^2$$

Quad Sieve Alg: First Attempt (Example)

Some of the y_i were B-factored, but some were not:

$(x+a)^2 \mod N = y_a = 2^{a_1}3^{a_2}\cdots p_B^{a_B}$. $\vec{a} = (a_1, \ldots, a_B) \pmod 2$.

$\vdots$

$(x+z)^2 \mod N = y_z = 2^{z_1}3^{z_2}\cdots p_B^{z_B}$, $\vec{b} = (z_1, \ldots, z_B) \pmod 2$.

Try to find come combination of $\vec{a}$, ..., $\vec{z}$ that sums $\vec{0}$ mod 2.

Lets say $\vec{a} + \vec{d} + \vec{q} \equiv \vec{0} \pmod 2$. Then

$$(x+a)^2(x+d)^2(x+q)^2 \equiv y_a y_d y_q = Y^2$$

$$((x+a)(x+d)(x+q))^2 \equiv y_a y_d y_q = Y^2$$

Quad Sieve Alg: First Attempt (Example)

Some of the y_i were B-factored, but some were not:

$(x+a)^2 \mod N = y_a = 2^{a_1}3^{a_2}\cdots p_B^{a_B}$. $\vec{a} = (a_1,\ldots,a_B) \pmod 2$.

$\vdots$

$(x+z)^2 \mod N = y_z = 2^{z_1}3^{z_2}\cdots p_B^{z_B}$, $\vec{b} = (z_1,\ldots,z_B) \pmod 2$.

Try to find come combination of $\vec{a}$, ..., $\vec{z}$ that sums $\vec{0}$ mod 2.

Lets say $\vec{a}+\vec{d}+\vec{q} \equiv \vec{0} \pmod 2$. Then

$$(x+a)^2(x+d)^2(x+q)^2 \equiv y_a y_d y_q = Y^2$$

$$((x+a)(x+d)(x+q))^2 \equiv y_a y_d y_q = Y^2$$

$$X^2 \equiv Y^2 \pmod N$$

Quad Sieve Alg: First Attempt (Example)

Some of the y_i were B-factored, but some were not:

$(x+a)^2 \mod N = y_a = 2^{a_1}3^{a_2}\cdots p_B^{a_B}$. $\vec{a} = (a_1, \ldots, a_B) \pmod 2$.

$\vdots$

$(x+z)^2 \mod N = y_z = 2^{z_1}3^{z_2}\cdots p_B^{z_B}$, $\vec{b} = (z_1, \ldots, z_B) \pmod 2$.

Try to find come combination of $\vec{a}$, ..., $\vec{z}$ that sums $\vec{0}$ mod 2.

Lets say $\vec{a} + \vec{d} + \vec{q} \equiv \vec{0} \pmod 2$. Then

$$(x+a)^2(x+d)^2(x+q)^2 \equiv y_a y_d y_q = Y^2$$

$$((x+a)(x+d)(x+q))^2 \equiv y_a y_d y_q = Y^2$$

$$X^2 \equiv Y^2 \pmod N$$

$$(X-Y)(X+Y) \equiv 0 \pmod N$$

Quad Sieve Alg: First Attempt (Example)

Some of the y_i were B-factored, but some were not:

$(x+a)^2 \mod N = y_a = 2^{a_1}3^{a_2}\cdots p_B^{a_B}$. $\vec{a} = (a_1, \ldots, a_B) \pmod 2$.

$\vdots$

$(x+z)^2 \mod N = y_z = 2^{z_1}3^{z_2}\cdots p_B^{z_B}$, $\vec{b} = (z_1, \ldots, z_B) \pmod 2$.

Try to find come combination of $\vec{a}$, …, $\vec{z}$ that sums $\vec{0}$ mod 2.

Lets say $\vec{a} + \vec{d} + \vec{q} \equiv \vec{0} \pmod 2$. Then

$$(x+a)^2(x+d)^2(x+q)^2 \equiv y_a y_d y_q = Y^2$$

$$((x+a)(x+d)(x+q))^2 \equiv y_a y_d y_q = Y^2$$

$$X^2 \equiv Y^2 \pmod N$$

$$(X-Y)(X+Y) \equiv 0 \pmod N$$

$\mathrm{GCD}(X-Y, N)$ probably a factor of N.

Quad Sieve Alg: Back to First Attempt

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

Quad Sieve Alg: Back to First Attempt

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

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

Let I be the set of all i such that y_i was B-factored.

Quad Sieve Alg: Back to First Attempt

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

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

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: Back to First Attempt

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

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

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.

A Tip for Learning This Material

We will revisit the above algorithm later when we get it to really work.

A Tip for Learning This Material

We will revisit the above algorithm later when we get it to really work.

When we do we are not going to redo the $y_a y_d y_q$ example.

A Tip for Learning This Material

We will revisit the above algorithm later when we get it to really work.

When we do we are not going to redo the $y_a y_d y_q$ example.

SO – Make sure you understand the algorithm before the next lecture (and the one after that).

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 $X^2 \equiv Y^2 \pmod N$ 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.