BILL START RECORDING

Bill vs Student; Theory vs Practice

Bill: Alice should not use the same value of e all the time. If she does then that e becomes an object of study. Zan finds a Ramsey-Theory-connection to that e! Eric finds an Automata-Theory-connection to that e! Josh finds an Algebraic-Geomtry-connection to that e! etc.

Bill vs Student; Theory vs Practice

Bill: Alice should not use the same value of e all the time. If she does then that e becomes an object of study. Zan finds a Ramsey-Theory-connection to that e! Eric finds an Automata-Theory-connection to that e! Josh finds an Algebraic-Geomtry-connection to that e! etc.

Student: I've read on the web that you should use $e = 2^{2^4} + 1$, the fourth Fermat Prime. And the article *20 years of attacks on RSA* (on the course website now) says so. The article was written by a theorist like you, Dan Boneh.

Bill vs Student; Theory vs Practice

Bill: Alice should not use the same value of e all the time. If she does then that e becomes an object of study. Zan finds a Ramsey-Theory-connection to that e! Eric finds an Automata-Theory-connection to that e! Josh finds an Algebraic-Geomtry-connection to that e! etc.

Student: I've read on the web that you should use $e = 2^{2^4} + 1$, the fourth Fermat Prime. And the article *20 years of attacks on RSA* (on the course website now) says so. The article was written by a theorist like you, Dan Boneh.

Bill: Dan Boneh is a **much better theorist** than me. Email me the website and paper and I'll see whats up.

Bill vs Student; Theory vs Practice

Bill: Alice should not use the same value of e all the time. If she does then that e becomes an object of study. Zan finds a Ramsey-Theory-connection to that e! Eric finds an Automata-Theory-connection to that e! Josh finds an Algebraic-Geomtry-connection to that e! etc.

Student: I've read on the web that you should use $e = 2^{2^4} + 1$, the fourth Fermat Prime. And the article *20 years of attacks on RSA* (on the course website now) says so. The article was written by a theorist like you, Dan Boneh.

Bill: Dan Boneh is a **much better theorist** than me. Email me the website and paper and I'll see whats up.
Well pierce my ears and call me drafty! In practice you SHOULD use $e = 2^{2^4} + 1$.

Why $e = 2^{2^4} + 1$ is good to use

Recall that in RSA Bob must compute m^e.

Bill: Can do m^e with repeated squaring in **roughly** $\lg_2(m)$ steps.

Practioner: **roughly** $\lg_2(m)$ steps? Lets see:

$e = 2^{2^4} + 1$: You do the usual repeated squaring

$m^2, m^{2^2}, m^{2^3}, \ldots, m^{2^{2^4}}$ in 16 steps. Total: 17 steps.

$e = 2^{2^4} - 1$: You do the usual repeated squaring

$m^2, m^{2^2}, m^{2^3}, \ldots, m^{2^{2^4-1}}$ in 15 steps. Then 15 MORE mults. so **roughly** 30 steps.

Why $e = 2^{2^4} + 1$ is good to use

Recall that in RSA Bob must compute m^e.

Bill: Can do m^e with repeated squaring in **roughly** $\lg_2(m)$ steps.

Practioner: **roughly** $\lg_2(m)$ steps? Lets see:

$e = 2^{2^4} + 1$: You do the usual repeated squaring

$m^2, m^{2^2}, m^{2^3}, \ldots, m^{2^{2^4}}$ in 16 steps. Total: 17 steps.

$e = 2^{2^4} - 1$: You do the usual repeated squaring

$m^2, m^{2^2}, m^{2^3}, \ldots, m^{2^{2^4-1}}$ in 15 steps. Then 15 MORE mults. so **roughly** 30 steps.

Bill: Does 16 vs 30 steps matter?

Why $e = 2^{2^4} + 1$ is good to use

Recall that in RSA Bob must compute m^e.

Bill: Can do m^e with repeated squaring in **roughly** $\lg_2(m)$ steps.

Practioner: **roughly** $\lg_2(m)$ steps? Lets see:

$e = 2^{2^4} + 1$: You do the usual repeated squaring

$m^2, m^{2^2}, m^{2^3}, \ldots, m^{2^{2^4}}$ in 16 steps. Total: 17 steps.

$e = 2^{2^4} - 1$: You do the usual repeated squaring

$m^2, m^{2^2}, m^{2^3}, \ldots, m^{2^{2^4-1}}$ in 15 steps. Then 15 MORE mults. so **roughly** 30 steps.

Bill: Does 16 vs 30 steps matter?

Practioner: YES you moron.

Why $e = 2^{2^4} + 1$ is good to use

Recall that in RSA Bob must compute m^e.
Bill: Can do m^e with repeated squaring in **roughly** $\lg_2(m)$ steps.

Practioner: **roughly** $\lg_2(m)$ steps? Lets see:
$e = 2^{2^4} + 1$: You do the usual repeated squaring
$m^2, m^{2^2}, m^{2^3}, \ldots, m^{2^{2^4}}$ in 16 steps. Total: 17 steps.

$e = 2^{2^4} - 1$: You do the usual repeated squaring
$m^2, m^{2^2}, m^{2^3}, \ldots, m^{2^{2^4-1}}$ in 15 steps. Then 15 MORE mults. so **roughly** 30 steps.

Bill: Does 16 vs 30 steps matter?

Practioner: YES you moron.

Bill: Only Cheyenne is allowed to call me a moron.

$e = 2^{2^4} + 1$ vs my fears

In Practice: Want to use $e = 2^{2^4} + 1$ since:

1. Only 15 mults.
2. $2^{2^4} + 1$ is big enough to ward off the low-e attackes
3. $2^{2^4} + 1$ is prime, so only way it fails to be rel prime to $R = (p-1)(q-1)$. is if it divides R. Unlikely and easily tested.

In Theory: Do not want to use **the same** e over and over again for fear of this being exploited.

Who is Right: $e = 2^{16} + 1$ is right.

$e = 2^{2^4} + 1$ vs my fears

In Practice: Want to use $e = 2^{2^4} + 1$ since:

1. Only 15 mults.
2. $2^{2^4} + 1$ is big enough to ward off the low-e attackes
3. $2^{2^4} + 1$ is prime, so only way it fails to be rel prime to $R = (p-1)(q-1)$. is if it divides R. Unlikely and easily tested.

In Theory: Do not want to use **the same** e over and over again for fear of this being exploited.

Who is Right: $e = 2^{16} + 1$ is right. For now

An Early Idea on Factoring: Jevons' Number

Jevons' Number

In the 1870s William Stanley Jevons wrote of the difficulty of factoring. We paraphrase Solomon Golomb's paraphrase:

> **Jevons observed that there are many cases where an operation is easy but it's inverse is hard. He mentioned encryption and decryption. He mentioned multiplication and factoring. He anticipated RSA!**

Jevons' Number

In the 1870s William Stanley Jevons wrote of the difficulty of factoring. We paraphrase Solomon Golomb's paraphrase:

> **Jevons observed that there are many cases where an operation is easy but it's inverse is hard. He mentioned encryption and decryption. He mentioned multiplication and factoring. He anticipated RSA!**

Jevons thought factoring was hard (prob correct!) and that a certain number would **never** be factored (wrong!). Here is a quote:

Jevons' Number

In the 1870s William Stanley Jevons wrote of the difficulty of factoring. We paraphrase Solomon Golomb's paraphrase:

> **Jevons observed that there are many cases where an operation is easy but it's inverse is hard. He mentioned encryption and decryption. He mentioned multiplication and factoring. He anticipated RSA!**

Jevons thought factoring was hard (prob correct!) and that a certain number would **never** be factored (wrong!). Here is a quote:

> **Can the reader say what two numbers multiplied together will produce**
>
> $$\mathbf{8,616,460,799}$$
>
> **I think it is unlikely that anyone aside from myself will ever know.**

Jevons' Number

$$J = 8,616,460,799$$

We can now factor J easily. Was Jevons' comment stupid?

Discuss

Jevons' Number

$$J = 8,616,460,799$$

We can now factor J easily. Was Jevons' comment stupid?

Discuss

1. Jevons lived 1835–1882 (He died at the age of 46.

Jevons' Number

$$J = 8,616,460,799$$

We can now factor J easily. Was Jevons' comment stupid?

Discuss

1. Jevons lived 1835–1882 (He died at the age of 46. Cause of death: Drowned while swimming.)

Jevons' Number

$$J = 8,616,460,799$$

We can now factor J easily. Was Jevons' comment stupid?

Discuss

1. Jevons lived 1835–1882 (He died at the age of 46. Cause of death: Drowned while swimming.)
2. Jevons did not predict computers.

Jevons' Number

$$J = 8,616,460,799$$

We can now factor J easily. Was Jevons' comment stupid?

Discuss

1. Jevons lived 1835–1882 (He died at the age of 46. Cause of death: Drowned while swimming.)
2. Jevons did not predict computers. Should he have?

Jevons' Number

$$J = 8,616,460,799$$

We can now factor J easily. Was Jevons' comment stupid?

Discuss

1. Jevons lived 1835–1882 (He died at the age of 46. Cause of death: Drowned while swimming.)
2. Jevons did not predict computers. Should he have?
3. Jevons did not predict math would help.

Jevons' Number

$$J = 8,616,460,799$$

We can now factor J easily. Was Jevons' comment stupid?
Discuss

1. Jevons lived 1835–1882 (He died at the age of 46. Cause of death: Drowned while swimming.)
2. Jevons did not predict computers. Should he have?
3. Jevons did not predict math would help. Should he have?

Jevons' Number

$$J = 8,616,460,799$$

We can now factor J easily. Was Jevons' comment stupid?

Discuss

1. Jevons lived 1835–1882 (He died at the age of 46. Cause of death: Drowned while swimming.)
2. Jevons did not predict computers. Should he have?
3. Jevons did not predict math would help. Should he have?
4. Lehmer factored J in 1903 using math and computation.

Jevons' Number

$$J = 8,616,460,799$$

We can now factor J easily. Was Jevons' comment stupid?
Discuss

1. Jevons lived 1835–1882 (He died at the age of 46. Cause of death: Drowned while swimming.)
2. Jevons did not predict computers. Should he have?
3. Jevons did not predict math would help. Should he have?
4. Lehmer factored J in 1903 using math and computation.
5. Golomb in 1996 showed that, given the math **of his day,** Jevons' number could be factored by hand.

Jevons' Number

$$J = 8,616,460,799$$

We can now factor J easily. Was Jevons' comment stupid?
Discuss

1. Jevons lived 1835–1882 (He died at the age of 46. Cause of death: Drowned while swimming.)
2. Jevons did not predict computers. Should he have?
3. Jevons did not predict math would help. Should he have?
4. Lehmer factored J in 1903 using math and computation.
5. Golomb in 1996 showed that, given the math **of his day,** Jevons' number could be factored by hand.
6. **Student:** Why didn't Jevons just Google **Factoring Quickly**

Jevons' Number

$$J = 8,616,460,799$$

We can now factor J easily. Was Jevons' comment stupid?
Discuss

1. Jevons lived 1835–1882 (He died at the age of 46. Cause of death: Drowned while swimming.)
2. Jevons did not predict computers. Should he have?
3. Jevons did not predict math would help. Should he have?
4. Lehmer factored J in 1903 using math and computation.
5. Golomb in 1996 showed that, given the math **of his day,** Jevons' number could be factored by hand.
6. **Student:** Why didn't Jevons just Google **Factoring Quickly**
   Bill: They didn't have the Web back then. Or Google.

Jevons' Number

$$J = 8,616,460,799$$

We can now factor J easily. Was Jevons' comment stupid?
Discuss

1. Jevons lived 1835–1882 (He died at the age of 46. Cause of death: Drowned while swimming.)
2. Jevons did not predict computers. Should he have?
3. Jevons did not predict math would help. Should he have?
4. Lehmer factored J in 1903 using math and computation.
5. Golomb in 1996 showed that, given the math **of his day,** Jevons' number could be factored by hand.
6. **Student:** Why didn't Jevons just Google **Factoring Quickly**
   Bill: They didn't have the Web back then. Or Google.
   Student: How did they live?

Jevons' Number

$$J = 8,616,460,799$$

We can now factor J easily. Was Jevons' comment stupid?
Discuss

1. Jevons lived 1835–1882 (He died at the age of 46. Cause of death: Drowned while swimming.)
2. Jevons did not predict computers. Should he have?
3. Jevons did not predict math would help. Should he have?
4. Lehmer factored J in 1903 using math and computation.
5. Golomb in 1996 showed that, given the math **of his day,** Jevons' number could be factored by hand.
6. **Student:** Why didn't Jevons just Google **Factoring Quickly**
   Bill: They didn't have the Web back then. Or Google.
   Student: How did they live?
   Bill: How indeed!

Golomb's Method to Factor Jevons' Number

$$J = 8,616,460,799$$

We apply a method of Fermat (in the 1600's) to the problem of factoring J.

To factor J find x, y such that

$$J = x^2 - y^2 = (x - y)(x + y)$$

So we must narrow our search for x, y.

Use Mods. Which Mod?

$$J = 8,616,460,799$$

J ends in 99. Hence

$$J \equiv 99 \equiv -1 \pmod{100}.$$

Use Mods. Which Mod?

$$J = 8,616,460,799$$

J ends in 99. Hence

$$J \equiv 99 \equiv -1 \pmod{100}.$$

Ah-ha. -1 is small! Mod 100 might be useful.

Golomb's Method to Factor Jevons' Number

$$J = 8,616,460,799$$
$$J = x^2 - y^2$$

$$J \equiv x^2 - y^2 \pmod{100}$$

$$99 \equiv x^2 - y^2 \pmod{100}$$

$$y^2 + 99 \equiv x^2 \pmod{100}$$

$$y^2 \equiv x^2 - 99 \pmod{100}$$

$$y^2 \equiv x^2 + 1 \pmod{100}$$

Golomb's Method to Factor Jevons' Number

$$J = 8,616,460,799$$

$$J = x^2 - y^2$$

$$J \equiv x^2 - y^2 \pmod{100}$$

$$99 \equiv x^2 - y^2 \pmod{100}$$

$$y^2 + 99 \equiv x^2 \pmod{100}$$

$$y^2 \equiv x^2 - 99 \pmod{100}$$

$$y^2 \equiv x^2 + 1 \pmod{100}$$

$$x^2 + 1 \equiv y^2 \pmod{100}$$

Golomb's Works Mod 100

$$x^2 + 1 \equiv y^2 \pmod{100}$$

All squares mod 100:

$$\{00, 01, 04, 09, 16, 21, 24, 25, 29, 36, 41, 44, 49\} \cup$$

$$\{56, 61, 64, 69, 76, 81, 84, 89, 96\}$$

The only pairs which differ by 1 are $(00, 01)$ and $(24, 25)$. So either:

1. $x^2 \equiv 0$, so $x \bmod 100 \in \{10, 20, 30, 40, 50, 60, 70, 80, 90\}$, OR
2. $x^2 \equiv 24$, so $x \bmod 100 \in \{18, 32, 68, 82\}$.

Golomb Works Mod 1000

$$x^2 - J \equiv y^2 \pmod{1000}, \text{ hence}$$

$$x^2 + 201 \equiv y^2 \pmod{1000}$$

If $x \pmod{100} \in \{10, 20, 30, 40, 50, 60, 70, 80, 90\}$ then
$x = 100a + 10b$
where $a \in \mathbb{N}$ and $b \in \{0, \ldots, 9\}$.
Easy but tedious to show that $b \equiv 0 \pmod{2}$. Hence

1. $x^2 \equiv 0$, so x mod $100 \in \{20, 40, 60, 80\}$
2. $x^2 \equiv 24$, so x mod $100 \in \{18, 32, 68, 82\}$

Recap

Combine the two sets for $x \pmod{100}$ to get

$$x \pmod{100} \in \{18, 20, 32, 40, 60, 68, 80, 82\}$$

Since $J = x^2 - y^2$, $x^2 = J + y^2$, so

$$x \geq \left\lceil \sqrt{J} \right\rceil = 92824$$

Since $J = x^2 - y^2$, $x^2 - J = y^2$, hence

$$x^2 - J = y^2 \text{ a square}$$

Welcome BACK

After those tedious slides we have the next slide.

Golomb's Method to Factor Jevons' Number: $x^2 \geq J$

1. $x \pmod{100} \in \{18, 20, 32, 40, 60, 68, 80, 82\}$.
2. $x \geq \left\lceil \sqrt{J} \right\rceil = 92824$.
3. $x^2 - J = y^2$, a square.

x	$y = (x^2 - J)^{1/2}$
92832	1148.6 ...
92840	1674.7 ...
92860	2553.1 ...
92868	2829.2 ...
92880	3199

AH-HA! We take $x = 92880$, $y = 3199$.

$$92880^2 - 3199^2 = 8,616,460,799$$

$$(92880 - 3199)(92880 + 3199) = 8,616,460,799$$

$$(89681)(96079) = 8,616,460,799$$

What Math or CS Did Jevons Know or Know of?

Did Jevons ask any mathematicians about this?

What Math or CS Did Jevons Know or Know of?

Did Jevons ask any mathematicians about this?

1. Jevons worked in logic and knew De Morgan.

What Math or CS Did Jevons Know or Know of?

Did Jevons ask any mathematicians about this?

1. Jevons worked in logic and knew De Morgan.
2. Jevons argued with Hermann von Helmholtz about non-Euclidean Geometry.

What Math or CS Did Jevons Know or Know of?

Did Jevons ask any mathematicians about this?

1. Jevons worked in logic and knew De Morgan.
2. Jevons argued with Hermann von Helmholtz about non-Euclidean Geometry.
3. **Upshot** He was in contact with math people and could have found a number theorist to ask. But he seems not to have.

What Math or CS Did Jevons Know or Know of?

Did Jevons ask any mathematicians about this?

1. Jevons worked in logic and knew De Morgan.
2. Jevons argued with Hermann von Helmholtz about non-Euclidean Geometry.
3. **Upshot** He was in contact with math people and could have found a number theorist to ask. But he seems not to have.

Did Jevons know about the work of Charles Babbage?

What Math or CS Did Jevons Know or Know of?

Did Jevons ask any mathematicians about this?

1. Jevons worked in logic and knew De Morgan.
2. Jevons argued with Hermann von Helmholtz about non-Euclidean Geometry.
3. **Upshot** He was in contact with math people and could have found a number theorist to ask. But he seems not to have.

Did Jevons know about the work of Charles Babbage?

1. Charles Babbage and Ada Lovelace were early computer scientists who worked together. (Calling them **computer scientists** is whiggish history.)

What Math or CS Did Jevons Know or Know of?

Did Jevons ask any mathematicians about this?

1. Jevons worked in logic and knew De Morgan.
2. Jevons argued with Hermann von Helmholtz about non-Euclidean Geometry.
3. **Upshot** He was in contact with math people and could have found a number theorist to ask. But he seems not to have.

Did Jevons know about the work of Charles Babbage?

1. Charles Babbage and Ada Lovelace were early computer scientists who worked together. (Calling them **computer scientists** is whiggish history.)
2. Charles Babbage also worked in Theology and wrote **The Ninth Bridgewater Treatise.** Jevons intended to write **The Tenth Bridgewater Treatise.**

What Math or CS Did Jevons Know or Know of?

Did Jevons ask any mathematicians about this?

1. Jevons worked in logic and knew De Morgan.
2. Jevons argued with Hermann von Helmholtz about non-Euclidean Geometry.
3. **Upshot** He was in contact with math people and could have found a number theorist to ask. But he seems not to have.

Did Jevons know about the work of Charles Babbage?

1. Charles Babbage and Ada Lovelace were early computer scientists who worked together. (Calling them **computer scientists** is whiggish history.)
2. Charles Babbage also worked in Theology and wrote **The Ninth Bridgewater Treatise.** Jevons intended to write **The Tenth Bridgewater Treatise.**
3. **Upshot** He knew who Babbage was and could have asked his opinion. But he seems not to have.

My Opinion and a Point

My Opinion and a Point

1. Jevons could have asked mathematicians about the Jevons' Number, but didn't.

My Opinion and a Point

1. Jevons could have asked mathematicians about the Jevons' Number, but didn't.
2. Jevons could have asked computer scientists (Babbage, Lovelace) about the Jevons' Number, but didn't.

My Opinion and a Point

1. Jevons could have asked mathematicians about the Jevons' Number, but didn't.
2. Jevons could have asked computer scientists (Babbage, Lovelace) about the Jevons' Number, but didn't.
3. Jevons thought that since he couldn't have factored the Jevons' Numbers if it was just given to him, nobody could.

My Opinion and a Point

1. Jevons could have asked mathematicians about the Jevons' Number, but didn't.
2. Jevons could have asked computer scientists (Babbage, Lovelace) about the Jevons' Number, but didn't.
3. Jevons thought that since he couldn't have factored the Jevons' Numbers if it was just given to him, nobody could.

Many crypto systems are easily broken. Why? If Alice invents a crypto system that is easily broken then likely:

My Opinion and a Point

1. Jevons could have asked mathematicians about the Jevons' Number, but didn't.
2. Jevons could have asked computer scientists (Babbage, Lovelace) about the Jevons' Number, but didn't.
3. Jevons thought that since he couldn't have factored the Jevons' Numbers if it was just given to him, nobody could.

Many crypto systems are easily broken. Why? If Alice invents a crypto system that is easily broken then likely:

1. Alice could have asked mathematicians about the Alice System, but didn't.

My Opinion and a Point

1. Jevons could have asked mathematicians about the Jevons' Number, but didn't.
2. Jevons could have asked computer scientists (Babbage, Lovelace) about the Jevons' Number, but didn't.
3. Jevons thought that since he couldn't have factored the Jevons' Numbers if it was just given to him, nobody could.

Many crypto systems are easily broken. Why? If Alice invents a crypto system that is easily broken then likely:

1. Alice could have asked mathematicians about the Alice System, but didn't.
2. Alice could have asked computer scientists about the Alice System, but didn't.

My Opinion and a Point

1. Jevons could have asked mathematicians about the Jevons' Number, but didn't.
2. Jevons could have asked computer scientists (Babbage, Lovelace) about the Jevons' Number, but didn't.
3. Jevons thought that since he couldn't have factored the Jevons' Numbers if it was just given to him, nobody could.

Many crypto systems are easily broken. Why? If Alice invents a crypto system that is easily broken then likely:

1. Alice could have asked mathematicians about the Alice System, but didn't.
2. Alice could have asked computer scientists about the Alice System, but didn't.
3. Alice thought that since she couldn't have broken Alice's system, nobody could.

My Opinion and a Point

1. Jevons could have asked mathematicians about the Jevons' Number, but didn't.
2. Jevons could have asked computer scientists (Babbage, Lovelace) about the Jevons' Number, but didn't.
3. Jevons thought that since he couldn't have factored the Jevons' Numbers if it was just given to him, nobody could.

Many crypto systems are easily broken. Why? If Alice invents a crypto system that is easily broken then likely:

1. Alice could have asked mathematicians about the Alice System, but didn't.
2. Alice could have asked computer scientists about the Alice System, but didn't.
3. Alice thought that since she couldn't have broken Alice's system, nobody could.

A lesson for us all!

Eric's Opinion

Eric, one of the TA's, when proofreading these slides, said the following:

Eric's Opinion

Eric, one of the TA's, when proofreading these slides, said the following:

1. Reasonable that he didn't realize that computers would get so much better.

Eric's Opinion

Eric, one of the TA's, when proofreading these slides, said the following:

1. Reasonable that he didn't realize that computers would get so much better.
2. Foolish since $J = 8,616,460,799$ isn't THAT big. Someone with enough determination could divide J by $2, 3, \ldots, \lceil \sqrt{J} \rceil$. This is only $\lceil \sqrt{J} \rceil = 92825$ trial divisions. Leave it to you to see if this is reasonable to finish in (say) 1 year.

Eric's Opinion of Jevons

My TA Eric is double majoring in Math and Economics.

Eric's Opinion of Jevons

My TA Eric is double majoring in Math and Economics.

When he proofread these slides he emailed me:

> *I've heard of Jevons before because he's also an economist. I am not surprised that he claimed J could not be factored, because the Modus Operandi of 19th century economists is to make bold predictions that are totally wrong.*

My Opinion and a Counterpoint

Conjecture Jevons was arrogant. Likely true.

My Opinion and a Counterpoint

Conjecture Jevons was arrogant. Likely true.

Conjecture We have the arrogance of hindsight.

My Opinion and a Counterpoint

Conjecture Jevons was arrogant. Likely true.
Conjecture We have the arrogance of hindsight.

- It's easy for **us** to say

What a moron! He should have asked a Number Theorist

My Opinion and a Counterpoint

Conjecture Jevons was arrogant. Likely true.
Conjecture We have the arrogance of hindsight.

- It's easy for **us** to say

What a moron! He should have asked a Number Theorist

What was he going to do, Google **Number Theorist** ?

My Opinion and a Counterpoint

Conjecture Jevons was arrogant. Likely true.

Conjecture We have the arrogance of hindsight.

- It's easy for **us** to say

What a moron! He should have asked a Number Theorist

What was he going to do, Google **Number Theorist** ?

- It's easy for **us** to say

My Opinion and a Counterpoint

Conjecture Jevons was arrogant. Likely true.

Conjecture We have the arrogance of hindsight.

- It's easy for **us** to say

What a moron! He should have asked a Number Theorist

What was he going to do, Google **Number Theorist** ?

- It's easy for **us** to say

What a moron! He should have asked a Babbage or Lovelace

My Opinion and a Counterpoint

Conjecture Jevons was arrogant. Likely true.

Conjecture We have the arrogance of hindsight.

- It's easy for **us** to say

  What a moron! He should have asked a Number Theorist

  What was he going to do, Google **Number Theorist** ?

- It's easy for **us** to say

  What a moron! He should have asked a Babbage or Lovelace

  We know about the role of computers to speed up calculations, but it's reasonable it never dawned on him.

My Opinion and a Counterpoint

Conjecture Jevons was arrogant. Likely true.
Conjecture We have the arrogance of hindsight.

- It's easy for **us** to say

  What a moron! He should have asked a Number Theorist

  What was he going to do, Google **Number Theorist** ?
- It's easy for **us** to say

  What a moron! He should have asked a Babbage or Lovelace

  We know about the role of computers to speed up calculations, but it's reasonable it never dawned on him.
- **Conclusion**
  - His arrogance: assumed the world would not change much.
  - Our arrogance: knowing how much the world did change.

Factoring Algorithms

Recall Factoring Algorithm Ground Rules

Recall Factoring Algorithm Ground Rules

- We only consider algorithms that, given N, find a non-trivial factor of N.

Recall Factoring Algorithm Ground Rules

- We only consider algorithms that, given N, find a non-trivial factor of N.
- We measure the run time as a function of $\lg N$ which is the *length* of the input. We may use L for this.

Recall Factoring Algorithm Ground Rules

- We only consider algorithms that, given N, find a non-trivial factor of N.
- We measure the run time as a function of $\lg N$ which is the *length* of the input. We may use L for this.
- We count $+$, $-$, $\times$, $\div$ as ONE step. A more refined analysis would count them as $(\lg x)^2$ steps where x is the largest number you are dealing with.

Recall Factoring Algorithm Ground Rules

- We only consider algorithms that, given N, find a non-trivial factor of N.
- We measure the run time as a function of $\lg N$ which is the *length* of the input. We may use L for this.
- We count $+$, $-$, $\times$, $\div$ as ONE step. A more refined analysis would count them as $(\lg x)^2$ steps where x is the largest number you are dealing with.
- We leave out the O-of but always mean O-of

Recall Factoring Algorithm Ground Rules

- We only consider algorithms that, given N, find a non-trivial factor of N.
- We measure the run time as a function of $\lg N$ which is the *length* of the input. We may use L for this.
- We count $+$, $-$, $\times$, $\div$ as ONE step. A more refined analysis would count them as $(\lg x)^2$ steps where x is the largest number you are dealing with.
- We leave out the O-of but always mean O-of
- We leave out the *expected time* but always mean it. Our algorithms are randomized.

Easy Factoring Algorithm

Easy Factoring Algorithm

1. Input(N)

Easy Factoring Algorithm

1. Input(N)
2. For $x = 2$ to $\lfloor N^{1/2} \rfloor$

   If x divides N then return x (and jump out of loop!).

Easy Factoring Algorithm

1. Input(N)
2. For $x = 2$ to $\lfloor N^{1/2} \rfloor$
   If x divides N then return x (and jump out of loop!).

This takes time $N^{1/2} = 2^{L/2}$.

Easy Factoring Algorithm

1. Input(N)
2. For $x = 2$ to $\lfloor N^{1/2} \rfloor$
   If x divides N then return x (and jump out of loop!).

This takes time $N^{1/2} = 2^{L/2}$.

Goal Do much better than time $N^{1/2}$.

Easy Factoring Algorithm

1. Input(N)
2. For $x = 2$ to $\lfloor N^{1/2} \rfloor$
   If x divides N then return x (and jump out of loop!).

This takes time $N^{1/2} = 2^{L/2}$.

Goal Do much better than time $N^{1/2}$.
How Much Better? Ignoring (1) constants, (2) the lack of proofs of the runtimes, and (3) cheating a byte, we have:

Easy Factoring Algorithm

1. Input(N)
2. For $x = 2$ to $\lfloor N^{1/2} \rfloor$
   If x divides N then return x (and jump out of loop!).

This takes time $N^{1/2} = 2^{L/2}$.

Goal Do much better than time $N^{1/2}$.
How Much Better? Ignoring (1) constants, (2) the lack of proofs of the runtimes, and (3) cheating a byte, we have:

- Easy: $N^{1/2} = 2^{L/2}$.

Easy Factoring Algorithm

1. Input(N)
2. For $x = 2$ to $\lfloor N^{1/2} \rfloor$
   If x divides N then return x (and jump out of loop!).

This takes time $N^{1/2} = 2^{L/2}$.

Goal Do much better than time $N^{1/2}$.
How Much Better? Ignoring (1) constants, (2) the lack of proofs of the runtimes, and (3) cheating a byte, we have:

- Easy: $N^{1/2} = 2^{L/2}$.
- Pollard-Rho Algorithm: $N^{1/4} = 2^{L/4}$.

Easy Factoring Algorithm

1. Input(N)
2. For $x = 2$ to $\lfloor N^{1/2} \rfloor$

   If x divides N then return x (and jump out of loop!).

This takes time $N^{1/2} = 2^{L/2}$.

Goal Do much better than time $N^{1/2}$.
How Much Better? Ignoring (1) constants, (2) the lack of proofs of the runtimes, and (3) cheating a byte, we have:

- Easy: $N^{1/2} = 2^{L/2}$.
- Pollard-Rho Algorithm: $N^{1/4} = 2^{L/4}$.
- Quad Sieve: $N^{1/L^{1/2}} = 2^{L^{1/2}}$.

Easy Factoring Algorithm

1. Input(N)
2. For $x = 2$ to $\lfloor N^{1/2} \rfloor$
   If x divides N then return x (and jump out of loop!).

This takes time $N^{1/2} = 2^{L/2}$.

Goal Do much better than time $N^{1/2}$.
How Much Better? Ignoring (1) constants, (2) the lack of proofs of the runtimes, and (3) cheating a byte, we have:

- Easy: $N^{1/2} = 2^{L/2}$.
- Pollard-Rho Algorithm: $N^{1/4} = 2^{L/4}$.
- Quad Sieve: $N^{1/L^{1/2}} = 2^{L^{1/2}}$.
- Number Field Sieve (best known): $N^{1/L^{2/3}} = 2^{L^{1/3}}$.

BILL STOP RECORDING