BILL AND NATHAN, RECORD LECTURE!!!!

BILL RECORD LECTURE!!!

Factoring
Is Probably Not NPC

BILL START RECORDING

Factoring: Some History

Jevons' Number

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

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

$$8,616,460,799$$

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 (Died at 46, 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 (Died at 46, 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 (Died at 46, 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 (Died at 46, 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 (Died at 46, 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 (Died at 46, 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 (Died at 46, 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 (Died at 46, 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 (Died at 46, 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 (Died at 46, 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 (Died at 46, 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!

Was Jevons Arrogant?

Conjecture Jevons was arrogant. Likely true.

Was Jevons Arrogant?

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

Was Jevons Arrogant?

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

Was Jevons Arrogant?

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** ?

Was Jevons Arrogant?

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

Was Jevons Arrogant?

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

Was Jevons Arrogant?

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.

Was Jevons Arrogant?

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

Factoring Algorithm Ground Rules

Factoring Algorithm Ground Rules

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

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.

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 $N^{1/2}$.

Hard Factoring Algorithms

How Much Better can we do than the easy algorithm?

Hard Factoring Algorithms

How Much Better can we do than the easy algorithm?

Ignoring (1) constants, (2) the lack of proofs of the runtimes, and (3) allowing randomized algorithms, we have:

Hard Factoring Algorithms

How Much Better can we do than the easy algorithm?

Ignoring (1) constants, (2) the lack of proofs of the runtimes, and (3) allowing randomized algorithms, we have:

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

Hard Factoring Algorithms

How Much Better can we do than the easy algorithm?

Ignoring (1) constants, (2) the lack of proofs of the runtimes, and (3) allowing randomized algorithms, we have:

- Easy: $N^{1/2} = 2^{L/2}$.
- Pollard-Rho Algorithm (1975): $N^{1/4} = 2^{L/4}$.

Hard Factoring Algorithms

How Much Better can we do than the easy algorithm?

Ignoring (1) constants, (2) the lack of proofs of the runtimes, and (3) allowing randomized algorithms, we have:

- Easy: $N^{1/2} = 2^{L/2}$.
- Pollard-Rho Algorithm (1975): $N^{1/4} = 2^{L/4}$.
- Quad Sieve (1981): $N^{1/L^{1/2}} = 2^{L^{1/2}}$.

Hard Factoring Algorithms

How Much Better can we do than the easy algorithm?

Ignoring (1) constants, (2) the lack of proofs of the runtimes, and (3) allowing randomized algorithms, we have:

- Easy: $N^{1/2} = 2^{L/2}$.
- Pollard-Rho Algorithm (1975): $N^{1/4} = 2^{L/4}$.
- Quad Sieve (1981): $N^{1/L^{1/2}} = 2^{L^{1/2}}$.
- Number Field Sieve ($\sim$1990): $N^{1/L^{2/3}} = 2^{L^{1/3}}$.

Hard Factoring Algorithms

How Much Better can we do than the easy algorithm?

Ignoring (1) constants, (2) the lack of proofs of the runtimes, and (3) allowing randomized algorithms, we have:

- Easy: $N^{1/2} = 2^{L/2}$.
- Pollard-Rho Algorithm (1975): $N^{1/4} = 2^{L/4}$.
- Quad Sieve (1981): $N^{1/L^{1/2}} = 2^{L^{1/2}}$.
- Number Field Sieve ($\sim$1990): $N^{1/L^{2/3}} = 2^{L^{1/3}}$.
- SVP algorithm (2020): Unclear!

Final Comments on Factoring

Final Comments on Factoring

1) The Number Field Sieve ($\sim$1990): $N^{1/L^{2/3}} = 2^{L^{1/3}}$ was the last big advance on the math ends for factoring.

Final Comments on Factoring

1) The Number Field Sieve ($\sim$1990): $N^{1/L^{2/3}} = 2^{L^{1/3}}$ was the last big advance on the math ends for factoring.

2) The Current Techniques can not do much better.

Final Comments on Factoring

1) The Number Field Sieve ($\sim$1990): $N^{1/L^{2/3}} = 2^{L^{1/3}}$ was the last big advance on the math ends for factoring.

2) The Current Techniques can not do much better.

3) There are reasons to think Factoring is **not** NP-complete.

Final Comments on Factoring

1) The Number Field Sieve ($\sim$1990): $N^{1/L^{2/3}} = 2^{L^{1/3}}$ was the last big advance on the math ends for factoring.

2) The Current Techniques can not do much better.

3) There are reasons to think Factoring is **not** NP-complete.

4) Factoring is in Quantum P but that won't be a problem for a while, if ever.

Final Comments on Factoring

1) The Number Field Sieve ($\sim$1990): $N^{1/L^{2/3}} = 2^{L^{1/3}}$ was the last big advance on the math ends for factoring.

2) The Current Techniques can not do much better.

3) There are reasons to think Factoring is **not** NP-complete.

4) Factoring is in Quantum P but that won't be a problem for a while, if ever.

5) Number Theory is a legit example of Math done with no application in mind that ended up having real applications.