BILL START RECORDING

Pollard's $p-1$ Algorithm for Factoring (1974)

An Example That Does Not Quite Work

Want to factor 11227.
If p is a prime factor of 11227:

An Example That Does Not Quite Work

Want to factor 11227.
If p is a prime factor of 11227:

1. p divides 11227.

An Example That Does Not Quite Work

Want to factor 11227.
If p is a prime factor of 11227:

1. p divides 11227.
2. p divides $2^{p-1} - 1$ (this is always true by Fermat's little Thm).

An Example That Does Not Quite Work

Want to factor 11227.
If p is a prime factor of 11227:

1. p divides 11227.
2. p divides $2^{p-1} - 1$ (this is always true by Fermat's little Thm).
3. So $\mathrm{GCD}(2^{p-1} - 1, 11227)$ divides 11227.

An Example That Does Not Quite Work

Want to factor 11227.
If p is a prime factor of 11227:

1. p divides 11227.
2. p divides $2^{p-1} - 1$ (this is always true by Fermat's little Thm).
3. So $\mathrm{GCD}(2^{p-1} - 1, 11227)$ divides 11227.
4. So $\mathrm{GCD}(2^{p-1} - 1 \bmod 11227, 11227)$ divides 11227.

An Example That Does Not Quite Work

Want to factor 11227.
If p is a prime factor of 11227:

1. p divides 11227.
2. p divides $2^{p-1} - 1$ (this is always true by Fermat's little Thm).
3. So $\mathrm{GCD}(2^{p-1} - 1, 11227)$ divides 11227.
4. So $\mathrm{GCD}(2^{p-1} - 1 \bmod 11227, 11227)$ divides 11227.

Lets find $\mathrm{GCD}(2^{p-1} - 1 \bmod 11227, 11227)$. Good idea?

An Example That Does Not Quite Work

Want to factor 11227.
If p is a prime factor of 11227:

1. p divides 11227.
2. p divides $2^{p-1}-1$ (this is always true by Fermat's little Thm).
3. So $\mathrm{GCD}(2^{p-1}-1, 11227)$ divides 11227.
4. So $\mathrm{GCD}(2^{p-1}-1 \bmod 11227, 11227)$ divides 11227.

Lets find $\mathrm{GCD}(2^{p-1}-1 \bmod 11227, 11227)$. Good idea?

We do not know p :-(If we did know p we would be done.

Making the Example Work

Want to factor 11227.
If p is a prime factor of 11227. We do not know p.

Making the Example Work

Want to factor 11227.
If p is a prime factor of 11227. We do not know p.

1. p divides 11227

Making the Example Work

Want to factor 11227.
If p is a prime factor of 11227. We do not know p.

1. p divides 11227
2. p divides $2^{p-1} - 1$ (this is always true by Fermat's little Thm)

Making the Example Work

Want to factor 11227.
If p is a prime factor of 11227. We do not know p.

1. p divides 11227
2. p divides $2^{p-1} - 1$ (this is always true by Fermat's little Thm)
3. p divides $2^{k(p-1)} - 1 \bmod 11227$ for any k

Making the Example Work

Want to factor 11227.
If p is a prime factor of 11227. We do not know p.

1. p divides 11227
2. p divides $2^{p-1} - 1$ (this is always true by Fermat's little Thm)
3. p divides $2^{k(p-1)} - 1 \bmod 11227$ for any k
4. Raise 2 to a power that we **hope** has $p - 1$ as a divisor.

Making the Example Work

Want to factor 11227.
If p is a prime factor of 11227. We do not know p.

1. p divides 11227
2. p divides $2^{p-1}-1$ (this is always true by Fermat's little Thm)
3. p divides $2^{k(p-1)}-1$ mod 11227 for any k
4. Raise 2 to a power that we **hope** has $p-1$ as a divisor.

$$\mathrm{GCD}(2^{2^3\times 3^3}-1 \bmod 11227, 11227) = \mathrm{GCD}(2^{216}-1 \bmod 11227, 11227)$$

$$= \mathrm{GCD}(1417, 11227) = 109$$

Making the Example Work

Want to factor 11227.
If p is a prime factor of 11227. We do not know p.

1. p divides 11227
2. p divides $2^{p-1} - 1$ (this is always true by Fermat's little Thm)
3. p divides $2^{k(p-1)} - 1 \bmod 11227$ for any k
4. Raise 2 to a power that we **hope** has $p - 1$ as a divisor.

$$\mathrm{GCD}(2^{2^3 \times 3^3} - 1 \bmod 11227, 11227) = \mathrm{GCD}(2^{216} - 1 \bmod 11227, 11227)$$

$$= \mathrm{GCD}(1417, 11227) = 109$$

Great! We got a factor of 11227 without having to factor!

Making the Example Work

Want to factor 11227.
If p is a prime factor of 11227. We do not know p.

1. p divides 11227
2. p divides $2^{p-1} - 1$ (this is always true by Fermat's little Thm)
3. p divides $2^{k(p-1)} - 1$ mod 11227 for any k
4. Raise 2 to a power that we **hope** has $p - 1$ as a divisor.

$\mathrm{GCD}(2^{2^3 \times 3^3} - 1 \bmod 11227, 11227) = \mathrm{GCD}(2^{216} - 1 \bmod 11227, 11227)$

$$= \mathrm{GCD}(1417, 11227) = 109$$

Great! We got a factor of 11227 without having to factor!
Why Worked 109 was a factor and $108 = 2^2 \times 3^3$, small factors.

General Idea

Fermat's Little Theorem If p is prime and a is coprime to p then $a^{p-1} \equiv 1 \pmod{p}$.

General Idea

Fermat's Little Theorem If p is prime and a is coprime to p then $a^{p-1} \equiv 1 \pmod{p}$.

Idea $a^{p-1} - 1 \equiv 0 \pmod{p}$. Pick an a at random. If p is a factor of N then:

General Idea

Fermat's Little Theorem If p is prime and a is coprime to p then $a^{p-1} \equiv 1 \pmod{p}$.

Idea $a^{p-1} - 1 \equiv 0 \pmod{p}$. Pick an a at random. If p is a factor of N then:

- p divides $a^{p-1} - 1$ (always).

General Idea

Fermat's Little Theorem If p is prime and a is coprime to p then $a^{p-1} \equiv 1 \pmod{p}$.

Idea $a^{p-1} - 1 \equiv 0 \pmod{p}$. Pick an a at random. If p is a factor of N then:

- p divides $a^{p-1} - 1$ (always).
- p divides N (our hypothesis).

General Idea

Fermat's Little Theorem If p is prime and a is coprime to p then $a^{p-1} \equiv 1 \pmod{p}$.

Idea $a^{p-1} - 1 \equiv 0 \pmod{p}$. Pick an a at random. If p is a factor of N then:

- p divides $a^{p-1} - 1$ (always).
- p divides N (our hypothesis).
- Hence $\mathrm{GCD}(a^{p-1} - 1 \bmod N, N)$ will be a factor of N.

General Idea

Fermat's Little Theorem If p is prime and a is coprime to p then $a^{p-1} \equiv 1 \pmod{p}$.

Idea $a^{p-1} - 1 \equiv 0 \pmod{p}$. Pick an a at random. If p is a factor of N then:

- p divides $a^{p-1} - 1$ (always).
- p divides N (our hypothesis).
- Hence $\mathrm{GCD}(a^{p-1} - 1 \bmod N, N)$ will be a factor of N.

Two problems:

General Idea

Fermat's Little Theorem If p is prime and a is coprime to p then $a^{p-1} \equiv 1 \pmod{p}$.

Idea $a^{p-1} - 1 \equiv 0 \pmod{p}$. Pick an a at random. If p is a factor of N then:

- p divides $a^{p-1} - 1$ (always).
- p divides N (our hypothesis).
- Hence $\mathrm{GCD}(a^{p-1} - 1 \bmod N, N)$ will be a factor of N.

Two problems:

- The GCD might be 1 or N. Thats okay- we can try another a.

General Idea

Fermat's Little Theorem If p is prime and a is coprime to p then $a^{p-1} \equiv 1 \pmod{p}$.

Idea $a^{p-1} - 1 \equiv 0 \pmod{p}$. Pick an a at random. If p is a factor of N then:

- p divides $a^{p-1} - 1$ (always).
- p divides N (our hypothesis).
- Hence $\mathrm{GCD}(a^{p-1} - 1 \bmod N, N)$ will be a factor of N.

Two problems:

- The GCD might be 1 or N. Thats okay- we can try another a.
- **We don't have p.** If we did, we'd be done!

Do You Believe in Hope ?

$a^{p-1} \equiv 1 \pmod{p}$. So for all k, $a^{k(p-1)} \equiv 1 \pmod{p}$.

Do You Believe in Hope ?

$a^{p-1} \equiv 1 \pmod p$. So for all k, $a^{k(p-1)} \equiv 1 \pmod p$.

Idea Let M be a number with LOTS of factors.

Do You Believe in Hope ?

$a^{p-1} \equiv 1 \pmod{p}$. So for all k, $a^{k(p-1)} \equiv 1 \pmod{p}$.
Idea Let M be a number with LOTS of factors.
Hope $p - 1$ is a factor of M.

Do You Believe in Hope ?

$a^{p-1} \equiv 1 \pmod{p}$. So for all k, $a^{k(p-1)} \equiv 1 \pmod{p}$.
Idea Let M be a number with LOTS of factors.
Hope $p-1$ is a factor of M.

$\mathrm{GCD}(a^M - 1, N)$ is non-trivial factor of N if **Hope** is correct.

Do You Believe in Hope ?

$a^{p-1} \equiv 1 \pmod{p}$. So for all k, $a^{k(p-1)} \equiv 1 \pmod{p}$.
Idea Let M be a number with LOTS of factors.
Hope $p-1$ is a factor of M.

$\mathrm{GCD}(a^M - 1, N)$ is non-trivial factor of N if **Hope** is correct.

How could we **not** get a non-trivial factor?

Do You Believe in **Hope** ?

$a^{p-1} \equiv 1 \pmod{p}$. So for all k, $a^{k(p-1)} \equiv 1 \pmod{p}$.
Idea Let M be a number with LOTS of factors.
Hope $p - 1$ is a factor of M.

$\mathrm{GCD}(a^M - 1, N)$ is non-trivial factor of N if **Hope** is correct.

How could we **not** get a non-trivial factor?

- $\mathrm{GCD}(a^M - 1, N) = 1$. So $p - 1$ does not divide M. M needs to have more factors in it.

Do You Believe in Hope ?

$a^{p-1} \equiv 1 \pmod{p}$. So for all k, $a^{k(p-1)} \equiv 1 \pmod{p}$.
Idea Let M be a number with LOTS of factors.
Hope $p - 1$ is a factor of M.

$\mathrm{GCD}(a^M - 1, N)$ is non-trivial factor of N if **Hope** is correct.

How could we **not** get a non-trivial factor?

- $\mathrm{GCD}(a^M - 1, N) = 1$. So $p - 1$ does not divide M. M needs to have more factors in it.
- $\mathrm{GCD}(a^M - 1, N) = N$. So $a^M - 1$ has $p - 1$ and $\frac{N}{p-1}$ in it. Need M to have less factors.

Do You Believe in Hope ?

$a^{p-1} \equiv 1 \pmod{p}$. So for all k, $a^{k(p-1)} \equiv 1 \pmod{p}$.
Idea Let M be a number with LOTS of factors.
Hope $p-1$ is a factor of M.

$\mathrm{GCD}(a^M - 1, N)$ is non-trivial factor of N if **Hope** is correct.

How could we **not** get a non-trivial factor?

- $\mathrm{GCD}(a^M - 1, N) = 1$. So $p-1$ does not divide M. M needs to have more factors in it.
- $\mathrm{GCD}(a^M - 1, N) = N$. So $a^M - 1$ has $p-1$ and $\frac{N}{p-1}$ in it. Need M to have less factors.

Want M to have lots of small factors so avoids prob 1.

Do You Believe in Hope ?

$a^{p-1} \equiv 1 \pmod{p}$. So for all k, $a^{k(p-1)} \equiv 1 \pmod{p}$.
Idea Let M be a number with LOTS of factors.
Hope $p-1$ is a factor of M.

$\mathrm{GCD}(a^M - 1, N)$ is non-trivial factor of N if **Hope** is correct.

How could we **not** get a non-trivial factor?

- $\mathrm{GCD}(a^M - 1, N) = 1$. So $p-1$ does not divide M. M needs to have more factors in it.
- $\mathrm{GCD}(a^M - 1, N) = N$. So $a^M - 1$ has $p-1$ and $\frac{N}{p-1}$ in it. Need M to have less factors.

Want M to have lots of small factors so avoids prob 1.
Want M to have not so many factors so avoids prob 2.

Do You Believe in Hope ? (cont)

Hope Want pick M with **many** small factors, but might adjust.
Let B be a parameter.

Do You Believe in Hope ? (cont)

Hope Want pick M with **many** small factors, but might adjust.
Let B be a parameter. Will let

$$M = \prod_{q \le B, q \text{ prime}} q^{\lceil \log_q(B) \rceil}.$$

Do You Believe in Hope ? (cont)

Hope Want pick M with **many** small factors, but might adjust. Let B be a parameter. Will let

$$M = \prod_{q \le B, q \text{ prime}} q^{\lceil \log_q(B) \rceil}.$$

- If B is big then gets lots of factors.

Do You Believe in **Hope** ? (cont)

Hope Want pick M with **many** small factors, but might adjust. Let B be a parameter. Will let

$$M = \prod_{q \le B, q \text{ prime}} q^{\lceil \log_q(B) \rceil}.$$

- If B is big then gets lots of factors.
- If B is small then do not get that many factors.

Do You Believe in **Hope** ? (cont)

Hope Want pick M with **many** small factors, but might adjust. Let B be a parameter. Will let

$$M = \prod_{q \le B, q \text{ prime}} q^{\lceil \log_q(B) \rceil}.$$

- If B is big then gets lots of factors.
- If B is small then do not get that many factors.
- Goldilocks Problem–want B that is just right.

Do You Believe in Hope ? (cont)

Hope Want pick M with **many** small factors, but might adjust. Let B be a parameter. Will let

$$M = \prod_{q \le B, q \text{ prime}} q^{\lceil \log_q(B) \rceil}.$$

- If B is big then gets lots of factors.
- If B is small then do not get that many factors.
- Goldilocks Problem–want B that is just right.
- Can't quite do that. Instead we try a B and then adjust it.

Example of B, M

Let B be a parameter.

Example of B, M

Let B be a parameter.

$$M = \prod_{q \leq B, q \text{ prime}} q^{\lceil \log_q(B) \rceil}.$$

Example of B, M

Let B be a parameter.

$$M = \prod_{q \le B, q \text{ prime}} q^{\lceil \log_q(B) \rceil}.$$

If $B = 10$

Example of B, M

Let B be a parameter.

$$M = \prod_{q \leq B, q \text{ prime}} q^{\lceil \log_q(B) \rceil}.$$

If $B = 10$
$q = 2$, $\lceil \log_2(10) \rceil = 3$. So 2^3.

Example of B, M

Let B be a parameter.

$$M = \prod_{q \le B, q \text{ prime}} q^{\lceil \log_q(B) \rceil}.$$

If $B = 10$
$q = 2$, $\lceil \log_2(10) \rceil = 3$. So 2^3.
$q = 3$, $\lceil \log_3(10) \rceil = 4$. So 3^4.

Example of B, M

Let B be a parameter.

$$M = \prod_{q \le B, q \text{ prime}} q^{\lceil \log_q(B) \rceil}.$$

If $B = 10$
$q = 2$, $\lceil \log_2(10) \rceil = 3$. So 2^3.
$q = 3$, $\lceil \log_3(10) \rceil = 4$. So 3^4.
$q = 5$, $\lceil \log_5(10) \rceil = 2$. So 5^2.

Example of B, M

Let B be a parameter.

$$M = \prod_{q \le B, q \text{ prime}} q^{\lceil \log_q(B) \rceil}.$$

If $B = 10$
$q = 2$, $\lceil \log_2(10) \rceil = 3$. So 2^3.
$q = 3$, $\lceil \log_3(10) \rceil = 4$. So 3^4.
$q = 5$, $\lceil \log_5(10) \rceil = 2$. So 5^2.
$q = 7$, $\lceil \log_7(10) \rceil = 2$. So 7^2.

Example of B, M

Let B be a parameter.

$$M = \prod_{q \leq B, q \text{ prime}} q^{\lceil \log_q(B) \rceil}.$$

If $B = 10$
$q = 2$, $\lceil \log_2(10) \rceil = 3$. So 2^3.
$q = 3$, $\lceil \log_3(10) \rceil = 4$. So 3^4.
$q = 5$, $\lceil \log_5(10) \rceil = 2$. So 5^2.
$q = 7$, $\lceil \log_7(10) \rceil = 2$. So 7^2.

$$M = 2^4 \times 3^4 \times 5^2 \times 7^2$$

Example of B, M

Let B be a parameter.

$$M = \prod_{q \le B, q \text{ prime}} q^{\lceil \log_q(B) \rceil}.$$

If $B = 10$

$q = 2$, $\lceil \log_2(10) \rceil = 3$. So 2^3.

$q = 3$, $\lceil \log_3(10) \rceil = 4$. So 3^4.

$q = 5$, $\lceil \log_5(10) \rceil = 2$. So 5^2.

$q = 7$, $\lceil \log_7(10) \rceil = 2$. So 7^2.

$$M = 2^4 \times 3^4 \times 5^2 \times 7^2$$

If $p - 1 = 2^w 3^x 5^y 7^z$ where $0 \le w, x \le 4$, $0 \le y, z \le 2$ then

Example of B, M

Let B be a parameter.

$$M = \prod_{q \le B, q \text{ prime}} q^{\lceil \log_q(B) \rceil}.$$

If $B = 10$
$q = 2$, $\lceil \log_2(10) \rceil = 3$. So 2^3.
$q = 3$, $\lceil \log_3(10) \rceil = 4$. So 3^4.
$q = 5$, $\lceil \log_5(10) \rceil = 2$. So 5^2.
$q = 7$, $\lceil \log_7(10) \rceil = 2$. So 7^2.

$$M = 2^4 \times 3^4 \times 5^2 \times 7^2$$

If $p - 1 = 2^w 3^x 5^y 7^z$ where $0 \le w, x \le 4$, $0 \le y, z \le 2$ then

$$\mathrm{GCD}(a^M - 1, N) \text{ will be a multiple of } p.$$

Do You Believe in Hope ? The Algorithm

Parameter B and hence also

$$M = \prod_{q \leq B, q \text{ prime}} q^{\lceil \log_q(B) \rceil}.$$

Do You Believe in Hope ? The Algorithm

Parameter B and hence also

$$M = \prod_{q \le B, q \text{ prime}} q^{\lceil \log_q(B) \rceil}.$$

```
FOUND = FALSE
while NOT FOUND
     a=RAND(1,N-1)
     d=GCD(a^M-1 mod N, N)
     if d=1 then increase B
     if d=N then decrease B
     if (d NE 1) and (d NE N) then FOUND=TRUE
output(d)
```

Do You Believe in Hope ? The Algorithm

Parameter B and hence also

$$M = \prod_{q \le B, q \text{ prime}} q^{\lceil \log_q(B) \rceil}.$$

```
FOUND = FALSE
while NOT FOUND
     a=RAND(1,N-1)
     d=GCD(a^M-1 mod N, N)
     if d=1 then increase B
     if d=N then decrease B
     if (d NE 1) and (d NE N) then FOUND=TRUE
output(d)
```

FACT If $p-1$ has all factors $\le B$ then runtime is $B \log B (\log N)^2$.

Do You Believe in Hope ? The Algorithm

Parameter B and hence also

$$M = \prod_{q \le B, q \text{ prime}} q^{\lceil \log_q(B) \rceil}.$$

```
FOUND = FALSE
while NOT FOUND
     a=RAND(1,N-1)
     d=GCD(a^M-1 mod N, N)
     if d=1 then increase B
     if d=N then decrease B
     if (d NE 1) and (d NE N) then FOUND=TRUE
output(d)
```

FACT If $p-1$ has all factors $\le B$ then runtime is $B \log B (\log N)^2$.
FACT B big then runtime Bad but prob works.

Do You Believe in Hope ? The Algorithm

Parameter B and hence also

$$M = \prod_{q \le B, q \text{ prime}} q^{\lceil \log_q(B) \rceil}.$$

```
FOUND = FALSE
while NOT FOUND
      a=RAND(1,N-1)
      d=GCD(a^M-1 mod N, N)
      if d=1 then increase B
      if d=N then decrease B
      if (d NE 1) and (d NE N) then FOUND=TRUE
output(d)
```

FACT If $p-1$ has all factors $\le B$ then runtime is $B \log B (\log N)^2$.
FACT B big then runtime Bad but prob works.
FACT Works well if $p-1$ only has small factors.

In Practice

A rule-of-thumb in practice is to take $B \sim N^{1/6}$.

In Practice

A rule-of-thumb in practice is to take $B \sim N^{1/6}$.

1. Fairly big so the M will be big enough.

In Practice

A rule-of-thumb in practice is to take $B \sim N^{1/6}$.

1. Fairly big so the M will be big enough.
2. Run time $N^{1/6}(\log N)^3$ pretty good, though still exp in $\log N$.

In Practice

A rule-of-thumb in practice is to take $B \sim N^{1/6}$.

1. Fairly big so the M will be big enough.
2. Run time $N^{1/6}(\log N)^3$ pretty good, though still exp in $\log N$.
3. **Warning** This **does not** mean we have an $N^{1/6}(\log N)^3$ algorithm for factoring. It only means we have that if $p-1$ has all factors $\leq N^{1/6}$.

Advice for Alice and Bob

Advice for Alice and Bob

1. Want p, q primes such that $p-1$ and $q-1$ have some large factors.

Advice for Alice and Bob

1. Want p, q primes such that $p-1$ and $q-1$ have some large factors.
2. Do we know a way to make sure that $p-1$ and $q-1$ have some large factors?

Advice for Alice and Bob

1. Want p, q primes such that $p - 1$ and $q - 1$ have some large factors.
2. Do we know a way to make sure that $p - 1$ and $q - 1$ have some large factors?
3. Make p, q **safe primes** . Then $p - 1 = 2r$ where r is prime, and $q - 1 = 2s$ where s is prime.

Advice for Alice and Bob

1. Want p, q primes such that $p-1$ and $q-1$ have some large factors.
2. Do we know a way to make sure that $p-1$ and $q-1$ have some large factors?
3. Make p, q **safe primes** . Then $p-1=2r$ where r is prime, and $q-1=2s$ where s is prime.

The usual lesson, so I sound like a broken record, not that your generation knows what a broken record sounds like or even is Because of Pollard's $p-1$ algorithm, Alice and Bob need to use safe primes. A new way to **up their game** .

BILL STOP RECORDING