BILL, RECORD LECTURE!!!!

BILL RECORD LECTURE!!!

Primality Testing

Primality Testing

Warning The next few slides will culminate in a test for primality that may FAIL.

Primality Testing

Warning The next few slides will culminate in a test for primality that may FAIL.

It is NOT used.

Primality Testing

Warning The next few slides will culminate in a test for primality that may FAIL.

It is NOT used.

But the **ideas** are used in real algorithm.

Is This a Natural Number?

Is the following a natural number?

$$\frac{1002!}{417!585!}$$

Is This a Natural Number?

Is the following a natural number?

$$\frac{1002!}{417!585!}$$

Yes

Is This a Natural Number?

Is the following a natural number?

$$\frac{1002!}{417!585!}$$

Yes

Hard Proof Look at factors and stuff.

Is This a Natural Number?

Is the following a natural number?

$$\frac{1002!}{417!585!}$$

Yes

Hard Proof Look at factors and stuff.

Easy Proof

The number of ways to pick 417 people out of 1002 is

$$\frac{1002!}{417!585!}.$$

Is This a Natural Number?

Is the following a natural number?

$$\frac{1002!}{417!585!}$$

Yes

Hard Proof Look at factors and stuff.

Easy Proof
The number of ways to pick 417 people out of 1002 is

$$\frac{1002!}{417!585!}.$$

So $\frac{1002!}{417!585!}$ is the answer to a question that has a nat numb answer.

Is This a Natural Number?

Is the following a natural number?

$$\frac{1002!}{417!585!}$$

Yes

Hard Proof Look at factors and stuff.

Easy Proof
The number of ways to pick 417 people out of 1002 is

$$\frac{1002!}{417!585!}.$$

So $\frac{1002!}{417!585!}$ is the answer to a question that has a nat numb answer.
Yes that really is the proof.

More Generally: Yes, This is a Natural Number

Theorem NAT For all $k, n \in \mathbb{N}$, $k \leq n$, $\frac{n!}{k!(n-k)!} \in \mathbb{N}$.

Proof

$\frac{n!}{k!(n-k)!}$ is the number of ways to choose k objects out of n.

So it answers a question that has a nat numb answer.

So its a natural number.

End of Proof

More Generally: Yes, This is a Natural Number

Theorem NAT For all $k, n \in \mathbb{N}$, $k \le n$, $\frac{n!}{k!(n-k)!} \in \mathbb{N}$.

Proof

$\frac{n!}{k!(n-k)!}$ is the number of ways to choose k objects out of n.

So it answers a question that has a nat numb answer.

So its a natural number.

End of Proof

Notation $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

The Binomial Theorem

Recall

The Binomial Theorem

For any $n \in \mathbb{N}$,

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}.$$

Lemma on $\frac{p!}{i!(p-i)!}$

Lemma If p prime, $1 \leq i \leq p-1$, then $\frac{p!}{i!(p-i)!} \in \mathbb{N}$ and is divisible by p.

Lemma on $\frac{p!}{i!(p-i)!}$

Lemma If p prime, $1 \leq i \leq p-1$, then $\frac{p!}{i!(p-i)!} \in \mathbb{N}$ and is divisible by p.
Proof $\frac{p!}{i!(p-i)!} \in \mathbb{N}$ by Theorem NAT.

Lemma on $\frac{p!}{i!(p-i)!}$

Lemma If p prime, $1 \le i \le p-1$, then $\frac{p!}{i!(p-i)!} \in \mathbb{N}$ and is divisible by p.

Proof $\frac{p!}{i!(p-i)!} \in \mathbb{N}$ by Theorem NAT.

Why does p divide $\frac{p!}{i!(p-i)!}$?

Lemma on $\frac{p!}{i!(p-i)!}$

Lemma If p prime, $1 \leq i \leq p-1$, then $\frac{p!}{i!(p-i)!} \in \mathbb{N}$ and is divisible by p.
Proof $\frac{p!}{i!(p-i)!} \in \mathbb{N}$ by Theorem NAT.
Why does p divide $\frac{p!}{i!(p-i)!}$?
p divides the numerator, p does not divide the denominator, and **p is prime**. Hence p divides the number.
End of Proof

Primality Testing

Fermat's Little Thm

Lemma If p prime, $a \in \mathbb{N}$ then $a^p \equiv a \pmod{p}$.

Primality Testing

Fermat's Little Thm
Lemma If p prime, $a \in \mathbb{N}$ then $a^p \equiv a \pmod{p}$.
Proof Fix prime p. By induction on a. **Base Case** $1^p \equiv 1$.

Primality Testing

Fermat's Little Thm
Lemma If p prime, $a \in \mathbb{N}$ then $a^p \equiv a \pmod{p}$.
Proof Fix prime p. By induction on a. **Base Case** $1^p \equiv 1$.
Ind Hyp $a^p \equiv a \pmod{p}$.

Primality Testing

Fermat's Little Thm

Lemma If p prime, $a \in \mathbb{N}$ then $a^p \equiv a \pmod{p}$.

Proof Fix prime p. By induction on a. **Base Case** $1^p \equiv 1$.

Ind Hyp $a^p \equiv a \pmod{p}$.

Ind Step $(a+1)^p = \binom{p}{p} a^p + \binom{p}{p-1} a^{p-1} + \cdots + \binom{p}{1} a^1 + \binom{p}{0} a^0$.

Primality Testing

Fermat's Little Thm

Lemma If p prime, $a \in \mathbb{N}$ then $a^p \equiv a \pmod{p}$.

Proof Fix prime p. By induction on a. **Base Case** $1^p \equiv 1$.

Ind Hyp $a^p \equiv a \pmod{p}$.

Ind Step $(a+1)^p = \binom{p}{p}a^p + \binom{p}{p-1}a^{p-1} + \cdots + \binom{p}{1}a^1 + \binom{p}{0}a^0$.

By previous lemma $\binom{p}{1} \equiv \binom{p}{2} \equiv \cdots \equiv \binom{p}{p-1} \equiv 0$. Hence

Primality Testing

Fermat's Little Thm
Lemma If p prime, $a \in \mathbb{N}$ then $a^p \equiv a \pmod{p}$.
Proof Fix prime p. By induction on a. **Base Case** $1^p \equiv 1$.
Ind Hyp $a^p \equiv a \pmod{p}$.
Ind Step $(a+1)^p = \binom{p}{p}a^p + \binom{p}{p-1}a^{p-1} + \cdots + \binom{p}{1}a^1 + \binom{p}{0}a^0$.
By previous lemma $\binom{p}{1} \equiv \binom{p}{2} \equiv \cdots \equiv \binom{p}{p-1} \equiv 0$. Hence

$$(a+1)^p \equiv \binom{p}{p}a^p + \binom{p}{0}a^0 \equiv a^p + 1 \equiv a + 1.$$

(Used $a^p \equiv a \pmod{p}$ which is from Ind Hyp.)
End of Proof

A Primality Testing Algorithm

Prior Slides If p is prime and $a \in \mathbb{N}$ then $a^p \equiv a \pmod{p}$.

A Primality Testing Algorithm

Prior Slides If p is prime and $a \in \mathbb{N}$ then $a^p \equiv a \pmod{p}$.
What has been observed If p is NOT prime then USUALLY for MOST a, $a^p \not\equiv a \pmod{p}$.

A Primality Testing Algorithm

Prior Slides If p is prime and $a \in \mathbb{N}$ then $a^p \equiv a \pmod{p}$.
What has been observed If p is NOT prime then USUALLY for MOST a, $a^p \not\equiv a \pmod{p}$.
Primality Algorithm

A Primality Testing Algorithm

Prior Slides If p is prime and $a \in \mathbb{N}$ then $a^p \equiv a \pmod{p}$.
What has been observed If p is NOT prime then USUALLY for MOST a, $a^p \not\equiv a \pmod{p}$.
Primality Algorithm

1. Input p. (In algorithm all arithmetic is mod p.)

A Primality Testing Algorithm

Prior Slides If p is prime and $a \in \mathbb{N}$ then $a^p \equiv a \pmod{p}$.
What has been observed If p is NOT prime then USUALLY for MOST a, $a^p \not\equiv a \pmod{p}$.
Primality Algorithm

1. Input p. (In algorithm all arithmetic is mod p.)
2. Form rand $R \subseteq \{2, \ldots, p-1\}$ of size $\sim \lg p$.

A Primality Testing Algorithm

Prior Slides If p is prime and $a \in \mathbb{N}$ then $a^p \equiv a \pmod{p}$.
What has been observed If p is NOT prime then USUALLY for MOST a, $a^p \not\equiv a \pmod{p}$.
Primality Algorithm

1. Input p. (In algorithm all arithmetic is mod p.)
2. Form rand $R \subseteq \{2, \ldots, p-1\}$ of size $\sim \lg p$.
3. For each $a \in R$ compute a^p.

A Primality Testing Algorithm

Prior Slides If p is prime and $a \in \mathbb{N}$ then $a^p \equiv a \pmod{p}$.
What has been observed If p is NOT prime then USUALLY for MOST a, $a^p \not\equiv a \pmod{p}$.
Primality Algorithm

1. Input p. (In algorithm all arithmetic is mod p.)
2. Form rand $R \subseteq \{2, \ldots, p-1\}$ of size $\sim \lg p$.
3. For each $a \in R$ compute a^p.
    3.1 If ever get $a^p \not\equiv a$ then p NOT PRIME (we are sure).

A Primality Testing Algorithm

Prior Slides If p is prime and $a \in \mathbb{N}$ then $a^p \equiv a \pmod{p}$.
What has been observed If p is NOT prime then USUALLY for MOST a, $a^p \not\equiv a \pmod{p}$.
Primality Algorithm

1. Input p. (In algorithm all arithmetic is mod p.)
2. Form rand $R \subseteq \{2, \ldots, p-1\}$ of size $\sim \lg p$.
3. For each $a \in R$ compute a^p.
   3.1 If ever get $a^p \not\equiv a$ then p NOT PRIME (we are sure).
   3.2 If for all a, $a^p \equiv a$ then PRIME (we are not sure).

Two reasons for our uncertainty:

A Primality Testing Algorithm

Prior Slides If p is prime and $a \in \mathbb{N}$ then $a^p \equiv a \pmod{p}$.
What has been observed If p is NOT prime then USUALLY for MOST a, $a^p \not\equiv a \pmod{p}$.
Primality Algorithm

1. Input p. (In algorithm all arithmetic is mod p.)
2. Form rand $R \subseteq \{2, \ldots, p-1\}$ of size $\sim \lg p$.
3. For each $a \in R$ compute a^p.
   3.1 If ever get $a^p \not\equiv a$ then p NOT PRIME (we are sure).
   3.2 If for all a, $a^p \equiv a$ then PRIME (we are not sure).

Two reasons for our uncertainty:

- p is composite but we were unlucky with R.

A Primality Testing Algorithm

Prior Slides If p is prime and $a \in \mathbb{N}$ then $a^p \equiv a \pmod{p}$.
What has been observed If p is NOT prime then USUALLY for MOST a, $a^p \not\equiv a \pmod{p}$.
Primality Algorithm

1. Input p. (In algorithm all arithmetic is mod p.)
2. Form rand $R \subseteq \{2, \ldots, p-1\}$ of size $\sim \lg p$.
3. For each $a \in R$ compute a^p.
   3.1 If ever get $a^p \not\equiv a$ then p NOT PRIME (we are sure).
   3.2 If for all a, $a^p \equiv a$ then PRIME (we are not sure).

Two reasons for our uncertainty:

- p is composite but we were unlucky with R.
- There are some composite p such that **for all** a, $a^p \equiv a$.

Primality Testing – What is Really True

Primality Testing – What is Really True

1. Exists algorithm that only has first problem, possible bad luck.

Primality Testing – What is Really True

1. Exists algorithm that only has first problem, possible bad luck.
2. That algorithm has prob of failure $\leq \frac{1}{2^p}$. Good enough!

Primality Testing – What is Really True

1. Exists algorithm that only has first problem, possible bad luck.
2. That algorithm has prob of failure $\leq \frac{1}{2^p}$. Good enough!
3. Exists deterministic poly time algorithm but is much slower.

Primality Testing – What is Really True

1. Exists algorithm that only has first problem, possible bad luck.
2. That algorithm has prob of failure $\le \frac{1}{2^p}$. Good enough!
3. Exists deterministic poly time algorithm but is much slower.
4. n is a **Shen Number** if, for all a, $a^n \equiv a$. These are the numbers my algorithm FAILS on.

Primality Testing – What is Really True

1. Exists algorithm that only has first problem, possible bad luck.
2. That algorithm has prob of failure $\leq \frac{1}{2^p}$. Good enough!
3. Exists deterministic poly time algorithm but is much slower.
4. n is a **Shen Number** if, for all a, $a^n \equiv a$. These are the numbers my algorithm FAILS on.
5. There are an infinite number of Shen numbers, but they are rare. How rare? HW!

Generating Primes

- We just gave a fast algorithm for **testing** if p is prime.

Generating Primes

- We just gave a fast algorithm for **testing** if p is prime.
- We want to **generate** primes.

Generating Primes

- We just gave a fast algorithm for **testing** if p is prime.
- We want to **generate** primes.

New Problem Given L, return an L-bit prime.

Generating Primes

- We just gave a fast algorithm for **testing** if p is prime.
- We want to **generate** primes.

New Problem Given L, return an L-bit prime.
Clarification An L-bit prime has a 1 as left most bit.

Alg for Generating Primes

First Attempt at, given L, generating a prime of length L.

Alg for Generating Primes

First Attempt at, given L, generating a prime of length L.

1. Input(L).

Alg for Generating Primes

First Attempt at, given L, generating a prime of length L.

1. Input(L).
2. Pick $y \in \{0, 1\}^{L-1}$ at rand.

Alg for Generating Primes

First Attempt at, given L, generating a prime of length L.

1. Input(L).
2. Pick $y \in \{0,1\}^{L-1}$ at rand.
3. $x = 1y$ (so x is a L-bit number).

Alg for Generating Primes

First Attempt at, given L, generating a prime of length L.

1. Input(L).
2. Pick $y \in \{0,1\}^{L-1}$ at rand.
3. $x = 1y$ (so x is a L-bit number).
4. Test if x is prime.

Alg for Generating Primes

First Attempt at, given L, generating a prime of length L.

1. Input(L).
2. Pick $y \in \{0,1\}^{L-1}$ at rand.
3. $x = 1y$ (so x is a L-bit number).
4. Test if x is prime.
5. If x is prime then output x and stop, else goto step 2.

Alg for Generating Primes

First Attempt at, given L, generating a prime of length L.

1. Input(L).
2. Pick $y \in \{0,1\}^{L-1}$ at rand.
3. $x = 1y$ (so x is a L-bit number).
4. Test if x is prime.
5. If x is prime then output x and stop, else goto step 2.

Is this a good algorithm?

Alg for Generating Primes

First Attempt at, given L, generating a prime of length L.

1. Input(L).
2. Pick $y \in \{0,1\}^{L-1}$ at rand.
3. $x = 1y$ (so x is a L-bit number).
4. Test if x is prime.
5. If x is prime then output x and stop, else goto step 2.

Is this a good algorithm?
PRO Math: returns a prime $\sim 3L^2$ tries with high prob.

Alg for Generating Primes

First Attempt at, given L, generating a prime of length L.

1. Input(L).
2. Pick $y \in \{0,1\}^{L-1}$ at rand.
3. $x = 1y$ (so x is a L-bit number).
4. Test if x is prime.
5. If x is prime then output x and stop, else goto step 2.

Is this a good algorithm?
PRO Math: returns a prime $\sim 3L^2$ tries with high prob.
CON Tests lots of numbers that are obv not prime—e.g, evens.

Generating Safe Primes

Definition p is a *safe prime* if p is prime and $\frac{p-1}{2}$ is prime.

First Attempt at, given L, generating a safe prime of length L

Generating Safe Primes

Definition p is a *safe prime* if p is prime and $\frac{p-1}{2}$ is prime.

First Attempt at, given L, generating a safe prime of length L

1. Input(L).

Generating Safe Primes

Definition p is a *safe prime* if p is prime and $\frac{p-1}{2}$ is prime.

First Attempt at, given L, generating a safe prime of length L

1. Input(L).
2. Pick $y \in \{0,1\}^{L-1}$ at rand.

Generating Safe Primes

Definition p is a *safe prime* if p is prime and $\frac{p-1}{2}$ is prime.

First Attempt at, given L, generating a safe prime of length L

1. Input(L).
2. Pick $y \in \{0,1\}^{L-1}$ at rand.
3. $x = 1y$ (note that x is a L-bit number).

Generating Safe Primes

Definition p is a *safe prime* if p is prime and $\frac{p-1}{2}$ is prime.

First Attempt at, given L, generating a safe prime of length L

1. Input(L).
2. Pick $y \in \{0,1\}^{L-1}$ at rand.
3. $x = 1y$ (note that x is a L-bit number).
4. Test if x and $\frac{x-1}{2}$ are prime.

Generating Safe Primes

Definition p is a *safe prime* if p is prime and $\frac{p-1}{2}$ is prime.

First Attempt at, given L, generating a safe prime of length L

1. Input(L).
2. Pick $y \in \{0,1\}^{L-1}$ at rand.
3. $x = 1y$ (note that x is a L-bit number).
4. Test if x and $\frac{x-1}{2}$ are prime.
5. If they both are then output x and stop, else goto step 2.

Generating Safe Primes

Definition p is a *safe prime* if p is prime and $\frac{p-1}{2}$ is prime.

First Attempt at, given L, generating a safe prime of length L

1. Input(L).
2. Pick $y \in \{0,1\}^{L-1}$ at rand.
3. $x = 1y$ (note that x is a L-bit number).
4. Test if x and $\frac{x-1}{2}$ are prime.
5. If they both are then output x and stop, else goto step 2.

Is this a good algorithm?

Generating Safe Primes

Definition p is a *safe prime* if p is prime and $\frac{p-1}{2}$ is prime.

First Attempt at, given L, generating a safe prime of length L

1. Input(L).
2. Pick $y \in \{0,1\}^{L-1}$ at rand.
3. $x = 1y$ (note that x is a L-bit number).
4. Test if x and $\frac{x-1}{2}$ are prime.
5. If they both are then output x and stop, else goto step 2.

Is this a good algorithm?

PRO Math: returns prime quickly with high prob.

Generating Safe Primes

Definition p is a *safe prime* if p is prime and $\frac{p-1}{2}$ is prime.

First Attempt at, given L, generating a safe prime of length L

1. Input(L).
2. Pick $y \in \{0,1\}^{L-1}$ at rand.
3. $x = 1y$ (note that x is a L-bit number).
4. Test if x and $\frac{x-1}{2}$ are prime.
5. If they both are then output x and stop, else goto step 2.

Is this a good algorithm?

PRO Math: returns prime quickly with high prob.

CON Tests lots of numbers that are obv not prime—e.g, evens.

Speed Prime-Finding: $n \not\equiv 0 \pmod 2$

We use $L - 1$-bit strings, including ones that end in 0, which are even.

Speed Prime-Finding: $n \not\equiv 0 \pmod 2$

We use $L-1$-bit strings, including ones that end in 0, which are even.
IDEA Pick $L-2$ bit string, put 1 on its right and on its left.
Is this a good idea? Vote.

Speed Prime-Finding: $n \not\equiv 0 \pmod 2$

We use $L - 1$-bit strings, including ones that end in 0, which are even.
IDEA Pick $L - 2$ bit string, put 1 on its right and on its left.
Is this a good idea? Vote.

PRO Do not waste time testing even numbers.

Speed Prime-Finding: $n \not\equiv 0 \pmod 2$

We use $L-1$-bit strings, including ones that end in 0, which are even.
IDEA Pick $L-2$ bit string, put 1 on its right and on its left.
Is this a good idea? Vote.

PRO Do not waste time testing even numbers.
CON Does it really save that much time?

Speed Prime-Finding: $n \not\equiv 0 \pmod{2}$

We use $L-1$-bit strings, including ones that end in 0, which are even.
IDEA Pick $L-2$ bit string, put 1 on its right and on its left.
Is this a good idea? Vote.

PRO Do not waste time testing even numbers.
CON Does it really save that much time?
CAVEAT Extend so we don't test numbers div by 3? Discuss.

Speed Prime-Finding: $n \not\equiv 0 \pmod{2}$

We use $L-1$-bit strings, including ones that end in 0, which are even.
IDEA Pick $L-2$ bit string, put 1 on its right and on its left.
Is this a good idea? Vote.

PRO Do not waste time testing even numbers.
CON Does it really save that much time?
CAVEAT Extend so we don't test numbers div by 3? Discuss.
Yes.

Speed Up Prime-Finding: $\not\equiv 0 \pmod{2, 3}$

2 divides n iff $(\exists k)[n = 2k]$
2 does not divide n iff $(\exists k)[n = 2k + 1]$

Speed Up Prime-Finding: $\not\equiv 0 \pmod{2,3}$

2 divides n iff $(\exists k)[n = 2k]$
2 does not divide n iff $(\exists k)[n = 2k + 1]$

3 divides n iff $(\exists k)[n = 3k]$
3 does not divide n iff $(\exists k)(\exists i \in \{1, 2\})[n = 3k + i]$

Speed Up Prime-Finding: $\not\equiv 0 \pmod{2, 3}$

2 divides n iff $(\exists k)[n = 2k]$
2 does not divide n iff $(\exists k)[n = 2k + 1]$

3 divides n iff $(\exists k)[n = 3k]$
3 does not divide n iff $(\exists k)(\exists i \in \{1, 2\})[n = 3k + i]$

How to get both?

Speed Up Prime-Finding: $\not\equiv 0 \pmod{2,3}$

2 divides n iff $(\exists k)[n = 2k]$
2 does not divide n iff $(\exists k)[n = 2k + 1]$

3 divides n iff $(\exists k)[n = 3k]$
3 does not divide n iff $(\exists k)(\exists i \in \{1, 2\})[n = 3k + i]$

How to get both?
Neither 2 nor 3 divides n iff $(\exists k)(\exists i \in \{1, 5\})[n = 6k + i]$

Speed Up Prime-Finding: $\not\equiv 0 \pmod{2, 3}$

2 divides n iff $(\exists k)[n = 2k]$
2 does not divide n iff $(\exists k)[n = 2k + 1]$

3 divides n iff $(\exists k)[n = 3k]$
3 does not divide n iff $(\exists k)(\exists i \in \{1, 2\})[n = 3k + i]$

How to get both?
Neither 2 nor 3 divides n iff $(\exists k)(\exists i \in \{1, 5\})[n = 6k + i]$

So need to generate numbers of the form $6k + 1$ and $6k + 5$.

Speed Up Prime-Finding: $\not\equiv 0 \pmod{2, 3}$

2 divides n iff $(\exists k)[n = 2k]$
2 does not divide n iff $(\exists k)[n = 2k + 1]$

3 divides n iff $(\exists k)[n = 3k]$
3 does not divide n iff $(\exists k)(\exists i \in \{1, 2\})[n = 3k + i]$

How to get both?
Neither 2 nor 3 divides n iff $(\exists k)(\exists i \in \{1, 5\})[n = 6k + i]$

So need to generate numbers of the form $6k + 1$ and $6k + 5$.
Caveat Might get a prime **of length $L - 1$**. We ignore this.

Alg for Gen Primes that Ignores $n \equiv 0 \pmod{2,3}$

Alg for Gen Primes that Ignores $n \equiv 0 \pmod{2, 3}$

1. Input L, want L bit prime.

Alg for Gen Primes that Ignores $n \equiv 0 \pmod{2, 3}$

1. Input L, want L bit prime.
2. Pick $y \in \{0,1\}^{L-3}$ (an $(L-3)$-bit number).

Alg for Gen Primes that Ignores $n \equiv 0 \pmod{2, 3}$

1. Input L, want L bit prime.
2. Pick $y \in \{0,1\}^{L-3}$ (an $(L-3)$-bit number).
3. Let $x = 1y$ (an $L-2$ bit number).

Alg for Gen Primes that Ignores $n \equiv 0 \pmod{2,3}$

1. Input L, want L bit prime.
2. Pick $y \in \{0,1\}^{L-3}$ (an $(L-3)$-bit number).
3. Let $x = 1y$ (an $L-2$ bit number).
4. Test if $6x+1$ is prime. ($(L-1)$-bit or L-bit number). If yes then output $6x+1$. If not then goto Step 2.

Alg for Gen Primes that Ignores $n \equiv 0 \pmod{2,3}$

1. Input L, want L bit prime.
2. Pick $y \in \{0,1\}^{L-3}$ (an $(L-3)$-bit number).
3. Let $x = 1y$ (an $L-2$ bit number).
4. Test if $6x+1$ is prime. (($L-1$)-bit or L-bit number). If yes then output $6x+1$. If not then goto Step 2.

Is this a good idea? Vote

Alg for Gen Primes that Ignores $n \equiv 0 \pmod{2,3}$

1. Input L, want L bit prime.
2. Pick $y \in \{0,1\}^{L-3}$ (an $(L-3)$-bit number).
3. Let $x = 1y$ (an $L-2$ bit number).
4. Test if $6x+1$ is prime. ($(L-1)$-bit or L-bit number). If yes then output $6x+1$. If not then goto Step 2.

Is this a good idea? Vote

PRO Do not waste time testing numbers $\equiv 0$ mod 2 or 3.

Alg for Gen Primes that Ignores $n \equiv 0 \pmod{2, 3}$

1. Input L, want L bit prime.
2. Pick $y \in \{0,1\}^{L-3}$ (an $(L-3)$-bit number).
3. Let $x = 1y$ (an $L-2$ bit number).
4. Test if $6x+1$ is prime. ($(L-1)$-bit or L-bit number). If yes then output $6x+1$. If not then goto Step 2.

Is this a good idea? Vote

PRO Do not waste time testing numbers $\equiv 0$ mod 2 or 3.
CON Uses primes of form $6k+1$. Not random enough?

Alg for Gen Primes that Ignores $n \equiv 0 \pmod{2, 3}$

1. Input L, want L bit prime.
2. Pick $y \in \{0,1\}^{L-3}$ (an $(L-3)$-bit number).
3. Let $x = 1y$ (an $L-2$ bit number).
4. Test if $6x+1$ is prime. ($(L-1)$-bit or L-bit number). If yes then output $6x+1$. If not then goto Step 2.

Is this a good idea? Vote

PRO Do not waste time testing numbers $\equiv 0$ mod 2 or 3.
CON Uses primes of form $6k+1$. Not random enough?
CAVEAT Can we modify to avoid this problem?

Alg for Gen Primes that Ignores $n \equiv 0 \pmod{2, 3}$

1. Input L, want L bit prime.
2. Pick $y \in \{0, 1\}^{L-3}$ (an $(L-3)$-bit number).
3. Let $x = 1y$ (an $L-2$ bit number).
4. Test if $6x+1$ is prime. ($(L-1)$-bit or L-bit number). If yes then output $6x+1$. If not then goto Step 2.

Is this a good idea? Vote

PRO Do not waste time testing numbers $\equiv 0$ mod 2 or 3.
CON Uses primes of form $6k+1$. Not random enough?
CAVEAT Can we modify to avoid this problem?
Yes.

Speed Up Alg Prime-Finding: $\not\equiv 0 \mod 2, 3$

Speed Up Alg Prime-Finding: $\not\equiv 0 \pmod{2, 3}$

1. Input L.

Speed Up Alg Prime-Finding: $\not\equiv 0 \mod 2, 3$

1. Input L.
2. Pick $y \in \{0,1\}^{L-3}$ (an $L-3$-bit number).

Speed Up Alg Prime-Finding: $\not\equiv 0 \mod 2, 3$

1. Input L.
2. Pick $y \in \{0,1\}^{L-3}$ (an $L-3$-bit number).
3. Let $x = 1y$ (an $L-2$ bit number).

Speed Up Alg Prime-Finding: $\not\equiv 0 \pmod{2, 3}$

1. Input L.
2. Pick $y \in \{0,1\}^{L-3}$ (an $L-3$-bit number).
3. Let $x = 1y$ (an $L-2$ bit number).
4. Pick $i \in \{1,5\}$ at random.

Speed Up Alg Prime-Finding: $\not\equiv 0 \mod 2, 3$

1. Input L.
2. Pick $y \in \{0,1\}^{L-3}$ (an $L-3$-bit number).
3. Let $x = 1y$ (an $L-2$ bit number).
4. Pick $i \in \{1,5\}$ at random.
5. Test if $6x + i$ is prime (($L-1$)-bit or L-bit number). If yes then done, if not then try goto step 2.

Speed Up Alg Prime-Finding: $\not\equiv 0 \pmod{2, 3}$

1. Input L.
2. Pick $y \in \{0, 1\}^{L-3}$ (an $L - 3$-bit number).
3. Let $x = 1y$ (an $L - 2$ bit number).
4. Pick $i \in \{1, 5\}$ at random.
5. Test if $6x + i$ is prime ($(L - 1)$-bit or L-bit number). If yes then done, if not then try goto step 2.

Is this a good idea? Vote.

Speed Up Alg Prime-Finding: $\not\equiv 0 \mod 2, 3$

1. Input L.
2. Pick $y \in \{0,1\}^{L-3}$ (an $L-3$-bit number).
3. Let $x = 1y$ (an $L-2$ bit number).
4. Pick $i \in \{1,5\}$ at random.
5. Test if $6x+i$ is prime (($L-1$)-bit or L-bit number). If yes then done, if not then try goto step 2.

Is this a good idea? Vote.

PRO Do not waste time testing numbers $\equiv 0 \pmod{2, 3}$.

Speed Up Alg Prime-Finding: $\not\equiv 0 \mod 2, 3$

1. Input L.
2. Pick $y \in \{0,1\}^{L-3}$ (an $L-3$-bit number).
3. Let $x = 1y$ (an $L-2$ bit number).
4. Pick $i \in \{1,5\}$ at random.
5. Test if $6x+i$ is prime (($L-1$)-bit or L-bit number). If yes then done, if not then try goto step 2.

Is this a good idea? Vote.

PRO Do not waste time testing numbers $\equiv 0 \pmod{2,3}$.

CON Getting more complicated. Is it worth it? Do not know.

Speed Up Alg Prime-Finding: $\not\equiv 0 \pmod{2, 3}$

1. Input L.
2. Pick $y \in \{0, 1\}^{L-3}$ (an $L - 3$-bit number).
3. Let $x = 1y$ (an $L - 2$ bit number).
4. Pick $i \in \{1, 5\}$ at random.
5. Test if $6x + i$ is prime (($L - 1$)-bit or L-bit number). If yes then done, if not then try goto step 2.

Is this a good idea? Vote.

PRO Do not waste time testing numbers $\equiv 0 \pmod{2, 3}$.

CON Getting more complicated. Is it worth it? Do not know.

CAVEAT Extend to 2,3,5? 2,3,5,7? etc.

BILL, STOP RECORDING LECTURE!!!!

BILL STOP RECORDING LECTURE!!!