Public-key cryptography

Daniel J. Bernstein

Tanja Lange

Part II:

Factorization

15 August 2017

Sage scripts for some algorithms, joint work with Heninger:

facthacks.cr.yp.to

Q sieve

Sieving small integers $i > 0$ using primes $2, 3, 5, 7$:

1								
2	2							
3					3			
4	2	2						
5							5	
6	2				3			
7								7
8	2	2	2					
9					3	3		
10	2						5	
11								
12	2	2			3			
13								
14	2							7
15					3		5	
16	2	2	2	2				
17								
18	2				3	3		
19								
20	2	2					5	

etc.

Public-key cryptography

Daniel J. Bernstein
Tanja Lange

Part II:
Factorization

15 August 2017

Sage scripts for some algorithms,
joint work with Heninger:
facthacks.cr.yp.to

Q sieve

Sieving i and $611 + i$ for small i
using primes $2, 3, 5, 7$:

1				
2	2			
3		3		
4	2 2			
5			5	
6	2	3		
7				7
8	2 2 2			
9		3 3		
10	2		5	
11				
12	2 2	3		
13				
14	2			7
15		3	5	
16	2 2 2 2			
17				
18	2	3 3		
19				
20	2 2		5	

612	2 2	3 3		
613				
614	2			
615		3	5	
616	2 2 2			7
617				
618	2	3		
619				
620	2 2		5	
621		3 3 3		
622	2			
623				7
624	2 2 2 2	3		
625			5 5 5 5	
626	2			
627		3		
628	2 2			
629				
630	2	3 3	5	7
631				

etc.

ey cryptography

. Bernstein

ange

ation

ust 2017

---

ipts for some algorithms,

rk with Heninger:

cks.cr.yp.to

Q sieve

Sieving i and $611 + i$ for small i using primes $2, 3, 5, 7$:

1				
2	2			
3		3		
4	2 2			
5			5	
6	2	3		
7				7
8	2 2 2			
9		3 3		
10	2		5	
11				
12	2 2	3		
13				
14	2			7
15		3	5	
16	2 2 2 2			
17				
18	2	3 3		
19				
20	2 2		5	

612	2 2	3 3		
613				
614	2			
615		3	5	
616	2 2 2			7
617				
618	2	3		
619				
620	2 2		5	
621		3 3 3		
622	2			
623				7
624	2 2 2 2	3		
625			5 5 5 5	
626	2			
627		3		
628	2 2			
629				
630	2	3 3	5	7
631				

etc.

Have co

the “co

for some

$14 \cdot 625$

$64 \cdot 675$

$75 \cdot 686$

$14 \cdot 64 \cdot$

$= 2^8 3^4 5$

gcd$\{611$

$= 47.$

$611 = 4$

graphy

n

ome algorithms,

eninger:

p.to

Q sieve

Sieving i and $611 + i$ for small i using primes $2, 3, 5, 7$:

i	2	3	5	7
1				
2	2			
3		3		
4	2 2			
5			5	
6	2	3		
7				7
8	2 2 2			
9		3 3		
10	2		5	
11				
12	2 2	3		
13				
14	2			7
15		3	5	
16	2 2 2 2			
17				
18	2	3 3		
19				
20	2 2		5	

$611+i$	2	3	5	7
612	2 2	3 3		
613				
614	2			
615		3	5	
616	2 2 2			7
617				
618	2	3		
619				
620	2 2		5	
621		3 3 3		
622	2			
623				7
624	2 2 2 2	3		
625			5 5 5 5	
626	2			
627		3		
628	2 2			
629				
630	2	3 3	5	7
631				

etc.

Have complete fac

the “congruences”

for some i's.

$14 \cdot 625 = 2^1 3^0 5^4$

$64 \cdot 675 = 2^6 3^3 5^2$

$75 \cdot 686 = 2^1 3^1 5^2$

$14 \cdot 64 \cdot 75 \cdot 625 \cdot$

$= 2^8 3^4 5^8 7^4 = (2^4$

$\gcd\{611, 14 \cdot 64 \cdot$

$= 47.$

$611 = 47 \cdot 13.$

thms,

Q sieve

Sieving i and $611+i$ for small i using primes $2, 3, 5, 7$:

i	2	3	5	7
1				
2	2			
3		3		
4	2 2			
5			5	
6	2	3		
7				7
8	2 2 2			
9		3 3		
10	2		5	
11				
12	2 2	3		
13				
14	2			7
15		3	5	
16	2 2 2 2			
17				
18	2	3 3		
19				
20	2 2		5	

$611+i$	2	3	5	7
612	2 2	3 3		
613				
614	2			
615		3	5	
616	2 2 2			7
617				
618	2	3		
619				
620	2 2		5	
621		3 3 3		
622	2			
623				7
624	2 2 2 2	3		
625			5 5 5 5	
626	2			
627		3		
628	2 2			
629				
630	2	3 3	5	7
631				

etc.

Have complete factorization the "congruences" $i(611+i$ for some i's.

$14 \cdot 625 = 2^1 3^0 5^4 7^1.$

$64 \cdot 675 = 2^6 3^3 5^2 7^0.$

$75 \cdot 686 = 2^1 3^1 5^2 7^3.$

$14 \cdot 64 \cdot 75 \cdot 625 \cdot 675 \cdot 686$

$= 2^8 3^4 5^8 7^4 = (2^4 3^2 5^4 7^2)^2.$

$\gcd\{611, 14 \cdot 64 \cdot 75 - 2^4 3^2$

$= 47.$

$611 = 47 \cdot 13.$

Q sieve

Sieving i and $611 + i$ for small i using primes $2, 3, 5, 7$:

1								
2	2							
3					3			
4	2	2						
5							5	
6	2				3			
7								7
8	2	2	2					
9					3	3		
10	2						5	
11								
12	2	2			3			
13								
14	2							7
15					3		5	
16	2	2	2	2				
17								
18	2				3	3		
19								
20	2	2					5	

612	2	2			3	3						
613												
614	2											
615					3			5				
616	2	2	2									7
617												
618	2				3							
619												
620	2	2						5				
621					3	3	3					
622	2											
623												7
624	2	2	2	2	3							
625								5	5	5	5	
626	2											
627					3							
628	2	2										
629												
630	2				3	3		5				7
631												

etc.

Have complete factorization of the "congruences" $i(611 + i)$ for some i's.

$14 \cdot 625 = 2^1 3^0 5^4 7^1$.
$64 \cdot 675 = 2^6 3^3 5^2 7^0$.
$75 \cdot 686 = 2^1 3^1 5^2 7^3$.

$14 \cdot 64 \cdot 75 \cdot 625 \cdot 675 \cdot 686$
$= 2^8 3^4 5^8 7^4 = (2^4 3^2 5^4 7^2)^2$.

$\gcd\{611, 14 \cdot 64 \cdot 75 - 2^4 3^2 5^4 7^2\}$
$= 47$.

$611 = 47 \cdot 13$.

i and $611 + i$ for small *i*

imes $2, 3, 5, 7$:

	5	
		7
3		
	5	
		7
	5	
3		
	5	

612	2	2			3	3						
613												
614	2											
615					3			5				
616	2	2	2									7
617												
618	2				3							
619												
620	2	2						5				
621					3	3	3					
622	2											
623												7
624	2	2	2	2	3							
625								5	5	5	5	
626	2											
627					3							
628	2	2										
629												
630	2				3	3		5				7
631												

Have complete factorization of the "congruences" $i(611 + i)$ for some i's.

$14 \cdot 625 = 2^1 3^0 5^4 7^1$.
$64 \cdot 675 = 2^6 3^3 5^2 7^0$.
$75 \cdot 686 = 2^1 3^1 5^2 7^3$.

$14 \cdot 64 \cdot 75 \cdot 625 \cdot 675 \cdot 686$
$= 2^8 3^4 5^8 7^4 = (2^4 3^2 5^4 7^2)^2$.

$\gcd\{611, 14 \cdot 64 \cdot 75 - 2^4 3^2 5^4 7^2\}$
$= 47$.

$611 = 47 \cdot 13$.

Why did

Was it ju

gcd{611

+ i for small i

5, 7:

2	3 3		
	3	5	
2 2			7
	3		
2		5	
	3 3 3		
			7
2 2 2	3		
		5 5 5 5	
	3		
2			
	3 3	5	7

Have complete factorization of the "congruences" $i(611 + i)$ for some i's.

$14 \cdot 625 = 2^1 3^0 5^4 7^1$.
$64 \cdot 675 = 2^6 3^3 5^2 7^0$.
$75 \cdot 686 = 2^1 3^1 5^2 7^3$.

$14 \cdot 64 \cdot 75 \cdot 625 \cdot 675 \cdot 686$
$= 2^8 3^4 5^8 7^4 = (2^4 3^2 5^4 7^2)^2$.

$\gcd\{611, 14 \cdot 64 \cdot 75 - 2^4 3^2 5^4 7^2\}$
$= 47$.

$611 = 47 \cdot 13$.

Why did this find
Was it just blind l
$\gcd\{611, \text{random}\}$

nall i

7

7

5 5 5

7

Have complete factorization of the "congruences" $i(611 + i)$ for some i's.

$14 \cdot 625 = 2^1 3^0 5^4 7^1$.
$64 \cdot 675 = 2^6 3^3 5^2 7^0$.
$75 \cdot 686 = 2^1 3^1 5^2 7^3$.

$14 \cdot 64 \cdot 75 \cdot 625 \cdot 675 \cdot 686$
$= 2^8 3^4 5^8 7^4 = (2^4 3^2 5^4 7^2)^2$.

$\gcd\{611, 14 \cdot 64 \cdot 75 - 2^4 3^2 5^4 7^2\}$
$= 47$.

$611 = 47 \cdot 13$.

Why did this find a factor o

Was it just blind luck:

$\gcd\{611, \text{random}\} = 47$?

Have complete factorization of the "congruences" $i(611+i)$ for some i's.

$14 \cdot 625 = 2^1 3^0 5^4 7^1$.
$64 \cdot 675 = 2^6 3^3 5^2 7^0$.
$75 \cdot 686 = 2^1 3^1 5^2 7^3$.

$14 \cdot 64 \cdot 75 \cdot 625 \cdot 675 \cdot 686$
$= 2^8 3^4 5^8 7^4 = (2^4 3^2 5^4 7^2)^2$.

$\gcd\{611, 14 \cdot 64 \cdot 75 - 2^4 3^2 5^4 7^2\}$
$= 47$.

$611 = 47 \cdot 13$.

Why did this find a factor of 611? Was it just blind luck: $\gcd\{611, \text{random}\} = 47$?

Have complete factorization of the "congruences" $i(611+i)$ for some i's.

$14 \cdot 625 = 2^1 3^0 5^4 7^1$.
$64 \cdot 675 = 2^6 3^3 5^2 7^0$.
$75 \cdot 686 = 2^1 3^1 5^2 7^3$.

$14 \cdot 64 \cdot 75 \cdot 625 \cdot 675 \cdot 686$
$= 2^8 3^4 5^8 7^4 = (2^4 3^2 5^4 7^2)^2$.

$\gcd\{611, 14 \cdot 64 \cdot 75 - 2^4 3^2 5^4 7^2\}$
$= 47$.

$611 = 47 \cdot 13$.

Why did this find a factor of 611? Was it just blind luck: $\gcd\{611, \text{random}\} = 47$?

No.

By construction 611 divides $s^2 - t^2$ where $s = 14 \cdot 64 \cdot 75$ and $t = 2^4 3^2 5^4 7^2$.
So each prime > 7 dividing 611 divides either $s - t$ or $s + t$.

Not terribly surprising (but not guaranteed in advance!) that one prime divided $s - t$ and the other divided $s + t$.

mplete factorization of
ngruences" $i(611+i)$
e i's.

$= 2^1 3^0 5^4 7^1$.
$= 2^6 3^3 5^2 7^0$.
$= 2^1 3^1 5^2 7^3$.

$75 \cdot 625 \cdot 675 \cdot 686$
$^8 7^4 = (2^4 3^2 5^4 7^2)^2$.

$., 14 \cdot 64 \cdot 75 - 2^4 3^2 5^4 7^2\}$

$7 \cdot 13$.

Why did this find a factor of 611?
Was it just blind luck:
$\gcd\{611, \text{random}\} = 47$?

No.

By construction 611 divides $s^2 - t^2$
where $s = 14 \cdot 64 \cdot 75$
and $t = 2^4 3^2 5^4 7^2$.
So each prime > 7 dividing 611
divides either $s - t$ or $s + t$.

Not terribly surprising
(but not guaranteed in advance!)
that one prime divided $s - t$
and the other divided $s + t$.

Why did
complete
have squ
Was it ju

ctorization of

$i(611+i)$

7^1.

7^0.

7^3.

$675 \cdot 686$

$3^2 5^4 7^2)^2$.

$75 - 2^4 3^2 5^4 7^2\}$

Why did this find a factor of 611?
Was it just blind luck:
$\gcd\{611, \text{random}\} = 47$?

No.

By construction 611 divides $s^2 - t^2$
where $s = 14 \cdot 64 \cdot 75$
and $t = 2^4 3^2 5^4 7^2$.
So each prime > 7 dividing 611
divides either $s - t$ or $s + t$.

Not terribly surprising
(but not guaranteed in advance!)
that one prime divided $s - t$
and the other divided $s + t$.

Why did the first t
completely factore
have square produ
Was it just blind l

of

)

$5^4 7^2\}$

Why did this find a factor of 611?
Was it just blind luck:
$\gcd\{611, \text{random}\} = 47$?

No.

By construction 611 divides $s^2 - t^2$
where $s = 14 \cdot 64 \cdot 75$
and $t = 2^4 3^2 5^4 7^2$.
So each prime > 7 dividing 611
divides either $s - t$ or $s + t$.

Not terribly surprising
(but not guaranteed in advance!)
that one prime divided $s - t$
and the other divided $s + t$.

Why did the first three
completely factored congrue
have square product?
Was it just blind luck?

Why did this find a factor of 611?
Was it just blind luck:
$\gcd\{611, \text{random}\} = 47$?

No.

By construction 611 divides $s^2 - t^2$
where $s = 14 \cdot 64 \cdot 75$
and $t = 2^4 3^2 5^4 7^2$.
So each prime > 7 dividing 611
divides either $s - t$ or $s + t$.

Not terribly surprising
(but not guaranteed in advance!)
that one prime divided $s - t$
and the other divided $s + t$.

Why did the first three
completely factored congruences
have square product?
Was it just blind luck?

Why did this find a factor of 611?
Was it just blind luck:
$\gcd\{611, \text{random}\} = 47$?

No.

By construction 611 divides $s^2 - t^2$
where $s = 14 \cdot 64 \cdot 75$
and $t = 2^4 3^2 5^4 7^2$.
So each prime > 7 dividing 611
divides either $s - t$ or $s + t$.

Not terribly surprising
(but not guaranteed in advance!)
that one prime divided $s - t$
and the other divided $s + t$.

Why did the first three
completely factored congruences
have square product?
Was it just blind luck?

Yes. The exponent vectors
$(1, 0, 4, 1), (6, 3, 2, 0), (1, 1, 2, 3)$
happened to have sum 0 mod 2.

Why did this find a factor of 611?
Was it just blind luck:
$\gcd\{611, \text{random}\} = 47$?

No.

By construction 611 divides $s^2 - t^2$
where $s = 14 \cdot 64 \cdot 75$
and $t = 2^4 3^2 5^4 7^2$.
So each prime > 7 dividing 611
divides either $s - t$ or $s + t$.

Not terribly surprising
(but not guaranteed in advance!)
that one prime divided $s - t$
and the other divided $s + t$.

Why did the first three
completely factored congruences
have square product?
Was it just blind luck?

Yes. The exponent vectors
$(1, 0, 4, 1), (6, 3, 2, 0), (1, 1, 2, 3)$
happened to have sum 0 mod 2.

But we didn't need this luck!
Given long sequence of vectors,
easily find nonempty subsequence
with sum 0 mod 2.

l this find a factor of 611?
ust blind luck:
, random} $= 47$?

truction 611 divides $s^2 - t^2$
$= 14 \cdot 64 \cdot 75$
$2^4 3^2 5^4 7^2$.
prime > 7 dividing 611
either $s - t$ or $s + t$.

ibly surprising
guaranteed in advance!)
e prime divided $s - t$
other divided $s + t$.

Why did the first three
completely factored congruences
have square product?
Was it just blind luck?

Yes. The exponent vectors
$(1, 0, 4, 1), (6, 3, 2, 0), (1, 1, 2, 3)$
happened to have sum 0 mod 2.

But we didn't need this luck!
Given long sequence of vectors,
easily find nonempty subsequence
with sum 0 mod 2.

This is l
Guarant
if numbe
exceeds

e.g. for
$1(n +$
$4(n +$
$15(n +$
$49(n +$
$64(n +$

$\mathbf{F}_2$-kerne
gen by (
e.g., $1(n$
is a squa

a factor of 611?

uck:

$= 47$?

11 divides $s^2 - t^2$

$\cdot$ 75

7 dividing 611

t or $s + t$.

sing

ed in advance!)

vided $s - t$

ded $s + t$.

Why did the first three
completely factored congruences
have square product?
Was it just blind luck?

Yes. The exponent vectors
$(1, 0, 4, 1), (6, 3, 2, 0), (1, 1, 2, 3)$
happened to have sum 0 mod 2.

But we didn't need this luck!
Given long sequence of vectors,
easily find nonempty subsequence
with sum 0 mod 2.

This is linear algeb
Guaranteed to finc
if number of vecto
exceeds length of

e.g. for $n = 671$:
$1(n + 1) = 2^5 3$
$4(n + 4) = 2^2 3$
$15(n + 15) = 2^1 3$
$49(n + 49) = 2^4 3$
$64(n + 64) = 2^6 3$

$\mathbf{F}_2$-kernel of expon
gen by (0 1 0 1 1)
e.g., $1(n + 1)15(n$
is a square.

f 611?

$s^2 - t^2$

611

nce!)

t

Why did the first three
completely factored congruences
have square product?
Was it just blind luck?

Yes. The exponent vectors
$(1, 0, 4, 1), (6, 3, 2, 0), (1, 1, 2, 3)$
happened to have sum 0 mod 2.

But we didn't need this luck!
Given long sequence of vectors,
easily find nonempty subsequence
with sum 0 mod 2.

This is linear algebra over **F**
Guaranteed to find subseque
if number of vectors
exceeds length of each vecto

e.g. for $n = 671$:

$$1(n + 1) = 2^5 3^1 5^0 7^1;$$
$$4(n + 4) = 2^2 3^3 5^2 7^0;$$
$$15(n + 15) = 2^1 3^1 5^1 7^3;$$
$$49(n + 49) = 2^4 3^2 5^1 7^2;$$
$$64(n + 64) = 2^6 3^1 5^1 7^2.$$

$\mathbf{F}_2$-kernel of exponent matri
gen by (0 1 0 1 1) and (1 0
e.g., $1(n+1)15(n+15)49(n$
is a square.

Why did the first three completely factored congruences have square product? Was it just blind luck?

Yes. The exponent vectors $(1,0,4,1),(6,3,2,0),(1,1,2,3)$ happened to have sum 0 mod 2.

But we didn't need this luck! Given long sequence of vectors, easily find nonempty subsequence with sum 0 mod 2.

This is linear algebra over $\mathbf{F}_2$. Guaranteed to find subsequence if number of vectors exceeds length of each vector.

e.g. for $n = 671$:

$1(n+\ 1) = 2^5 3^1 5^0 7^1$;

$4(n+\ 4) = 2^2 3^3 5^2 7^0$;

$15(n+15) = 2^1 3^1 5^1 7^3$;

$49(n+49) = 2^4 3^2 5^1 7^2$;

$64(n+64) = 2^6 3^1 5^1 7^2$.

$\mathbf{F}_2$-kernel of exponent matrix is gen by $(0\ 1\ 0\ 1\ 1)$ and $(1\ 0\ 1\ 1\ 0)$; e.g., $1(n+1)15(n+15)49(n+49)$ is a square.

l the first three
ely factored congruences
uare product?
ust blind luck?

e exponent vectors
$1), (6,3,2,0), (1,1,2,3)$
d to have sum 0 mod 2.

didn't need this luck!
ng sequence of vectors,
nd nonempty subsequence
n 0 mod 2.

This is linear algebra over $\mathbf{F}_2$.
Guaranteed to find subsequence if number of vectors exceeds length of each vector.

e.g. for $n = 671$:

$$1(n+\ 1) = 2^5 3^1 5^0 7^1;$$
$$4(n+\ 4) = 2^2 3^3 5^2 7^0;$$
$$15(n+15) = 2^1 3^1 5^1 7^3;$$
$$49(n+49) = 2^4 3^2 5^1 7^2;$$
$$64(n+64) = 2^6 3^1 5^1 7^2.$$

$\mathbf{F}_2$-kernel of exponent matrix is gen by (0 1 0 1 1) and (1 0 1 1 0); e.g., $1(n+1)15(n+15)49(n+49)$ is a square.

Plausible
separate
of any n

Given n

Try to c
for $i \in \{$
into proc

Look for
with $i(n$
and with

Compute
$s = \prod_{i \in I} i$

three
ed congruences
ct?
uck?

t vectors
0), (1, 1, 2, 3)
sum 0 mod 2.

d this luck!
ce of vectors,
pty subsequence
2.

This is linear algebra over $\mathbf{F}_2$.
Guaranteed to find subsequence if number of vectors exceeds length of each vector.

e.g. for $n = 671$:

$$1(n + 1) = 2^5 3^1 5^0 7^1;$$
$$4(n + 4) = 2^2 3^3 5^2 7^0;$$
$$15(n + 15) = 2^1 3^1 5^1 7^3;$$
$$49(n + 49) = 2^4 3^2 5^1 7^2;$$
$$64(n + 64) = 2^6 3^1 5^1 7^2.$$

$\mathbf{F}_2$-kernel of exponent matrix is gen by (0 1 0 1 1) and (1 0 1 1 0);
e.g., $1(n+1)15(n+15)49(n+49)$ is a square.

Plausible conjectu
separate the odd p
of any n, not just

Given n and paran

Try to completely
for $i \in \{1, 2, 3, \ldots$
into products of pr

Look for nonempty
with $i(n + i)$ com
and with $\prod_{i \in I} i(n +$

Compute gcd$\{n, s$
$s = \prod_{i \in I} i$ and $t =$

nces

2, 3)

od 2.

k!

ors,

uence

This is linear algebra over $\mathbf{F}_2$.
Guaranteed to find subsequence if number of vectors exceeds length of each vector.

e.g. for $n = 671$:

$$1(n + 1) = 2^5 3^1 5^0 7^1;$$
$$4(n + 4) = 2^2 3^3 5^2 7^0;$$
$$15(n + 15) = 2^1 3^1 5^1 7^3;$$
$$49(n + 49) = 2^4 3^2 5^1 7^2;$$
$$64(n + 64) = 2^6 3^1 5^1 7^2.$$

$\mathbf{F}_2$-kernel of exponent matrix is gen by (0 1 0 1 1) and (1 0 1 1 0); e.g., $1(n+1)15(n+15)49(n+49)$ is a square.

Plausible conjecture: $\mathbf{Q}$ siev
separate the odd prime divis
of any n, not just 611.

Given n and parameter y:

Try to completely factor $i(n$
for $i \in \{1, 2, 3, \ldots, y^2\}$
into products of primes $\le y$.

Look for nonempty set I of
with $i(n + i)$ completely fac
and with $\prod_{i \in I} i(n + i)$ square

Compute $\gcd\{n, s - t\}$ whe
$s = \prod_{i \in I} i$ and $t = \sqrt{\prod_{i \in I} i(n$

This is linear algebra over $\mathbf{F}_2$.
Guaranteed to find subsequence if number of vectors exceeds length of each vector.

e.g. for $n = 671$:

$$
\begin{aligned}
1(n+\ 1) &= 2^5 3^1 5^0 7^1;\\
4(n+\ 4) &= 2^2 3^3 5^2 7^0;\\
15(n+15) &= 2^1 3^1 5^1 7^3;\\
49(n+49) &= 2^4 3^2 5^1 7^2;\\
64(n+64) &= 2^6 3^1 5^1 7^2.
\end{aligned}
$$

$\mathbf{F}_2$-kernel of exponent matrix is gen by (0 1 0 1 1) and (1 0 1 1 0); e.g., $1(n+1)15(n+15)49(n+49)$ is a square.

Plausible conjecture: $\mathbf{Q}$ sieve can separate the odd prime divisors of any n, not just 611.

Given n and parameter y:

Try to completely factor $i(n+i)$ for $i \in \{1, 2, 3, \ldots, y^2\}$ into products of primes $\le y$.

Look for nonempty set I of i's with $i(n+i)$ completely factored and with $\prod_{i \in I} i(n+i)$ square.

Compute $\gcd\{n, s-t\}$ where $s = \prod_{i \in I} i$ and $t = \sqrt{\prod_{i \in I} i(n+i)}$.

inear algebra over $\mathbf{F}_2$.
eed to find subsequence
er of vectors
length of each vector.

$n = 671$:
$1) = 2^5 3^1 5^0 7^1$;
$4) = 2^2 3^3 5^2 7^0$;
$15) = 2^1 3^1 5^1 7^3$;
$49) = 2^4 3^2 5^1 7^2$;
$64) = 2^6 3^1 5^1 7^2$.

el of exponent matrix is
0 1 0 1 1) and (1 0 1 1 0);
$+1)15(n+15)49(n+49)$
are.

Plausible conjecture: **Q** sieve can separate the odd prime divisors of any n, not just 611.

Given n and parameter y:

Try to completely factor $i(n+i)$ for $i \in \{1, 2, 3, \ldots, y^2\}$ into products of primes $\le y$.

Look for nonempty set I of i's with $i(n+i)$ completely factored and with $\prod_{i \in I} i(n+i)$ square.

Compute $\gcd\{n, s-t\}$ where $s = \prod_{i \in I} i$ and $t = \sqrt{\prod_{i \in I} i(n+i)}$.

How larg
for this t

Uniform
has $n^{1/}$
roughly

Plausible
Q sieve
with $y =$
for all n
here $o(1$

ora over $\mathbf{F}_2$.
d subsequence
ors
each vector.

$^1 5^0 7^1$;
$^3 5^2 7^0$;
$^1 5^1 7^3$;
$^2 5^1 7^2$;
$^1 5^1 7^2$.

nent matrix is
and (1 0 1 1 0);
$+15)49(n+49)$

Plausible conjecture: **Q** sieve can separate the odd prime divisors of any n, not just 611.

Given n and parameter y:

Try to completely factor $i(n+i)$ for $i \in \{1, 2, 3, \ldots, y^2\}$ into products of primes $\leq y$.

Look for nonempty set I of i's with $i(n+i)$ completely factored and with $\prod_{i \in I} i(n+i)$ square.

Compute $\gcd\{n, s-t\}$ where $s = \prod_{i \in I} i$ and $t = \sqrt{\prod_{i \in I} i(n+i)}$.

How large does y
for this to find a s

Uniform random in
has $n^{1/u}$-smoothn
roughly u^{-u}.

Plausible conjectu
Q sieve succeeds
with $y = \lfloor n^{1/u} \rfloor$
for all $n \geq u^{(1+o(1$
here $o(1)$ is as u -

2.
ence

or.

x is
1 1 0);
$n+49)$

Plausible conjecture: **Q** sieve can separate the odd prime divisors of any n, not just 611.

Given n and parameter y:

Try to completely factor $i(n+i)$ for $i \in \{1, 2, 3, \ldots, y^2\}$ into products of primes $\le y$.

Look for nonempty set I of i's with $i(n+i)$ completely factored and with $\prod_{i \in I} i(n+i)$ square.

Compute $\gcd\{n, s-t\}$ where $s = \prod_{i \in I} i$ and $t = \sqrt{\prod_{i \in I} i(n+i)}$.

How large does y have to be for this to find a square?

Uniform random integer in [
has $n^{1/u}$-smoothness chance
roughly u^{-u}.

Plausible conjecture:
Q sieve succeeds
with $y = \lfloor n^{1/u} \rfloor$
for all $n \ge u^{(1+o(1))u^2}$;
here $o(1)$ is as $u \to \infty$.

Plausible conjecture: $\mathbf{Q}$ sieve can separate the odd prime divisors of any n, not just 611.

Given n and parameter y:

Try to completely factor $i(n+i)$ for $i \in \{1, 2, 3, \ldots, y^2\}$ into products of primes $\le y$.

Look for nonempty set I of i's with $i(n+i)$ completely factored and with $\prod_{i \in I} i(n+i)$ square.

Compute $\gcd\{n, s-t\}$ where $s = \prod_{i \in I} i$ and $t = \sqrt{\prod_{i \in I} i(n+i)}$.

How large does y have to be for this to find a square?

Uniform random integer in $[1, n]$ has $n^{1/u}$-smoothness chance roughly u^{-u}.

Plausible conjecture:
$\mathbf{Q}$ sieve succeeds
with $y = \lfloor n^{1/u} \rfloor$
for all $n \ge u^{(1+o(1))u^2}$;
here $o(1)$ is as $u \to \infty$.

e conjecture: **Q** sieve can
the odd prime divisors
, not just 611.

and parameter y:

ompletely factor $i(n+i)$
$1, 2, 3, \ldots, y^2\}$
ducts of primes $\leq y$.

nonempty set I of i's
$+ i)$ completely factored
n $\prod_{i \in I} i(n+i)$ square.

e $\gcd\{n, s-t\}$ where
and $t = \sqrt{\prod_{i \in I} i(n+i)}$.

How large does y have to be
for this to find a square?

Uniform random integer in $[1, n]$
has $n^{1/u}$-smoothness chance
roughly u^{-u}.

Plausible conjecture:
Q sieve succeeds
with $y = \lfloor n^{1/u} \rfloor$
for all $n \geq u^{(1+o(1))u^2}$;
here $o(1)$ is as $u \to \infty$.

More ge
exp $\sqrt{(}$
conjectu
is $1/y^{c+}$

Find enc
by chang
replace y
exp $\sqrt{(}$

Increasir
increases
reduces
So linear
when y

re: $\mathbf{Q}$ sieve can
prime divisors
611.

meter y:

factor $i(n+i)$
$, y^2\}$
rimes $\le y$.

y set I of i's
pletely factored
$i)$ square.

$-t\}$ where
$\sqrt{\prod_{i \in I} i(n+i)}$.

How large does y have to be for this to find a square?

Uniform random integer in $[1, n]$ has $n^{1/u}$-smoothness chance roughly u^{-u}.

Plausible conjecture:
$\mathbf{Q}$ sieve succeeds
with $y = \lfloor n^{1/u} \rfloor$
for all $n \ge u^{(1+o(1))u^2}$;
here $o(1)$ is as $u \to \infty$.

More generally, if
$\exp\sqrt{\left(\frac{1}{2c} + o(1)\right)}$
conjectured y-smo
is $1/y^{c+o(1)}$.

Find enough smoo
by changing the ra
replace y^2 with y^c
$\exp\sqrt{\left(\frac{(c+1)^2+o(1)}{2c}\right.}$

Increasing c past 1
increases number
reduces linear-alge
So linear algebra
when y is chosen

e can
ors

$+ i)$

i's
ctored
.

re
$+ i)$.

How large does y have to be for this to find a square?

Uniform random integer in $[1, n]$ has $n^{1/u}$-smoothness chance roughly u^{-u}.

Plausible conjecture:
$\mathbf{Q}$ sieve succeeds
with $y = \lfloor n^{1/u} \rfloor$
for all $n \geq u^{(1+o(1))u^2}$;
here $o(1)$ is as $u \to \infty$.

More generally, if $y \in$
$\exp \sqrt{\left(\frac{1}{2c} + o(1)\right) \log n \log \mathrm{lo}}$
conjectured y-smoothness ch
is $1/y^{c+o(1)}$.

Find enough smooth congru
by changing the range of i's
replace y^2 with $y^{c+1+o(1)} =$
$\exp \sqrt{\left(\frac{(c+1)^2+o(1)}{2c}\right) \log n \log}$

Increasing c past 1
increases number of i's but
reduces linear-algebra cost.
So linear algebra never domi
when y is chosen properly.

How large does y have to be for this to find a square?

Uniform random integer in $[1, n]$ has $n^{1/u}$-smoothness chance roughly u^{-u}.

Plausible conjecture:
$\mathbf{Q}$ sieve succeeds
with $y = \lfloor n^{1/u} \rfloor$
for all $n \ge u^{(1+o(1))u^2}$;
here $o(1)$ is as $u \to \infty$.

More generally, if $y \in \exp\sqrt{\left(\frac{1}{2c} + o(1)\right)\log n \log\log n}$, conjectured y-smoothness chance is $1/y^{c+o(1)}$.

Find enough smooth congruences by changing the range of i's: replace y^2 with $y^{c+1+o(1)} = \exp\sqrt{\left(\frac{(c+1)^2+o(1)}{2c}\right)\log n \log\log n}$.

Increasing c past 1
increases number of i's but
reduces linear-algebra cost.
So linear algebra never dominates
when y is chosen properly.

ge does y have to be
to find a square?

random integer in $[1, n]$
^{u}-smoothness chance
u^{-u}.

e conjecture:
succeeds
$= \lfloor n^{1/u} \rfloor$
$\geq u^{(1+o(1))u^2}$;
) is as $u \to \infty$.

More generally, if $y \in \exp\sqrt{\left(\frac{1}{2c} + o(1)\right)\log n \log\log n}$, conjectured y-smoothness chance is $1/y^{c+o(1)}$.

Find enough smooth congruences by changing the range of i's: replace y^2 with $y^{c+1+o(1)} = \exp\sqrt{\left(\frac{(c+1)^2+o(1)}{2c}\right)\log n \log\log n}$.

Increasing c past 1 increases number of i's but reduces linear-algebra cost. So linear algebra never dominates when y is chosen properly.

Improvin

Smoothn
degrades
Smaller

Crude ar
$\approx yn$ if
$\approx y^2 n$ if

More ca
$n + i$ do
i is alwa
only 30%

Can we
to avoid

have to be
quare?

nteger in $[1, n]$
ess chance

re:

$1))u^2$;

$\to \infty$.

More generally, if $y \in \exp\sqrt{\left(\frac{1}{2c} + o(1)\right)\log n \log\log n}$,
conjectured y-smoothness chance
is $1/y^{c+o(1)}$.

Find enough smooth congruences
by changing the range of i's:
replace y^2 with $y^{c+1+o(1)} = \exp\sqrt{\left(\frac{(c+1)^2+o(1)}{2c}\right)\log n \log\log n}$.

Increasing c past 1
increases number of i's but
reduces linear-algebra cost.
So linear algebra never dominates
when y is chosen properly.

Improving smooth

Smoothness chanc
degrades as i grow
Smaller for $i \approx y^2$

Crude analysis: $i($
$\approx yn$ if $i \approx y$;
$\approx y^2 n$ if $i \approx y^2$.

More careful analy
$n + i$ doesn't degr
i is always smooth
only 30% chance f

Can we select con
to avoid this degra

e

$1, n]$

e

More generally, if $y \in \exp\sqrt{\left(\frac{1}{2c} + o(1)\right)\log n \log\log n}$, conjectured y-smoothness chance is $1/y^{c+o(1)}$.

Find enough smooth congruences by changing the range of i's: replace y^2 with $y^{c+1+o(1)} = \exp\sqrt{\left(\frac{(c+1)^2+o(1)}{2c}\right)\log n \log\log n}$.

Increasing c past 1 increases number of i's but reduces linear-algebra cost. So linear algebra never dominates when y is chosen properly.

Improving smoothness chanc

Smoothness chance of $i(n +$
degrades as i grows.
Smaller for $i \approx y^2$ than for i

Crude analysis: $i(n + i)$ gro
$\approx yn$ if $i \approx y$;
$\approx y^2 n$ if $i \approx y^2$.

More careful analysis:
$n + i$ doesn't degrade, but
i is always smooth for $i \leq y$
only 30% chance for $i \approx y^2$.

Can we select congruences
to avoid this degradation?

More generally, if $y \in \exp\sqrt{\left(\frac{1}{2c} + o(1)\right)\log n \log\log n}$, conjectured y-smoothness chance is $1/y^{c+o(1)}$.

Find enough smooth congruences by changing the range of i's: replace y^2 with $y^{c+1+o(1)} = \exp\sqrt{\left(\frac{(c+1)^2+o(1)}{2c}\right)\log n \log\log n}$.

Increasing c past 1 increases number of i's but reduces linear-algebra cost. So linear algebra never dominates when y is chosen properly.

Improving smoothness chances

Smoothness chance of $i(n+i)$ degrades as i grows. Smaller for $i \approx y^2$ than for $i \approx y$.

Crude analysis: $i(n+i)$ grows.
$\approx yn$ if $i \approx y$;
$\approx y^2 n$ if $i \approx y^2$.

More careful analysis:
$n+i$ doesn't degrade, but
i is always smooth for $i \le y$,
only 30% chance for $i \approx y^2$.

Can we select congruences to avoid this degradation?

nerally, if $y \in$

$\frac{1}{2c} + o(1)\big) \log n \log\log n$,

red y-smoothness chance

$o(1)$.

ough smooth congruences

ging the range of i's:

y^2 with $y^{c+1+o(1)} =$

$\frac{(c+1)^2+o(1)}{2c}\Big) \log n \log\log n$.

ng c past 1

s number of i's but

linear-algebra cost.

r algebra never dominates

is chosen properly.

Improving smoothness chances

Smoothness chance of $i(n+i)$ degrades as i grows. Smaller for $i \approx y^2$ than for $i \approx y$.

Crude analysis: $i(n+i)$ grows.
$\approx yn$ if $i \approx y$;
$\approx y^2 n$ if $i \approx y^2$.

More careful analysis:
$n+i$ doesn't degrade, but
i is always smooth for $i \le y$,
only 30% chance for $i \approx y^2$.

Can we select congruences to avoid this degradation?

Choose

Choose

arithmet

where q

e.g. pro

$2q - (n$

etc.

Check sm

generaliz

for i's in

e.g. che

smooth

Try man

Rare for

$y \in$

log n log log n,

oothness chance

oth congruences

ange of i's:

$c{+}1{+}o(1)$ =

$2\big)$ log n log log n.

1

of i's but

ebra cost.

never dominates

properly.

Improving smoothness chances

Smoothness chance of $i(n+i)$ degrades as i grows.
Smaller for $i \approx y^2$ than for $i \approx y$.

Crude analysis: $i(n+i)$ grows.
$\approx yn$ if $i \approx y$;
$\approx y^2 n$ if $i \approx y^2$.

More careful analysis:
$n+i$ doesn't degrade, but
i is always smooth for $i \le y$,
only 30% chance for $i \approx y^2$.

Can we select congruences to avoid this degradation?

Choose q, square o

Choose a "q-subla

arithmetic progres

where q divides ea

e.g. progression q

$2q - (n \bmod q)$, $3q$

etc.

Check smoothness

generalized congru

for i's in this subla

e.g. check whethe

smooth for $i = q$ -

Try many large q's

Rare for i's to ove

og n,
hance

ences
:

g log n.

inates

Improving smoothness chances

Smoothness chance of $i(n+i)$ degrades as i grows.
Smaller for $i \approx y^2$ than for $i \approx y$.

Crude analysis: $i(n+i)$ grows.
$\approx yn$ if $i \approx y$;
$\approx y^2 n$ if $i \approx y^2$.

More careful analysis:
$n+i$ doesn't degrade, but
i is always smooth for $i \le y$,
only 30% chance for $i \approx y^2$.

Can we select congruences to avoid this degradation?

Choose q, square of large pr
Choose a "q-sublattice" of i
arithmetic progression of i's
where q divides each $i(n+$
e.g. progression $q - (n \bmod$
$2q - (n \bmod q)$, $3q - (n \bmod$
etc.

Check smoothness of
generalized congruence $i(n$
for i's in this sublattice.
e.g. check whether $i, (n+i)$
smooth for $i = q - (n \bmod$

Try many large q's.
Rare for i's to overlap.

Improving smoothness chances

Smoothness chance of $i(n+i)$ degrades as i grows.
Smaller for $i \approx y^2$ than for $i \approx y$.

Crude analysis: $i(n+i)$ grows.
$\approx yn$ if $i \approx y$;
$\approx y^2 n$ if $i \approx y^2$.

More careful analysis:
$n+i$ doesn't degrade, but
i is always smooth for $i \le y$,
only 30% chance for $i \approx y^2$.

Can we select congruences to avoid this degradation?

Choose q, square of large prime.
Choose a "q-sublattice" of i's:
arithmetic progression of i's
where q divides each $i(n+i)$.
e.g. progression $q - (n \bmod q)$,
$2q - (n \bmod q)$, $3q - (n \bmod q)$,
etc.

Check smoothness of
generalized congruence $i(n+i)/q$
for i's in this sublattice.
e.g. check whether $i, (n+i)/q$ are smooth for $i = q - (n \bmod q)$ etc.

Try many large q's.
Rare for i's to overlap.

ng smoothness chances

ness chance of $i(n+i)$
s as i grows.
for $i \approx y^2$ than for $i \approx y$.

nalysis: $i(n+i)$ grows.
$i \approx y$;
f $i \approx y^2$.

reful analysis:
oesn't degrade, but
ys smooth for $i \leq y$,
% chance for $i \approx y^2$.

select congruences
this degradation?

Choose q, square of large prime.
Choose a "q-sublattice" of i's:
arithmetic progression of i's
where q divides each $i(n+i)$.
e.g. progression $q - (n \bmod q)$,
$2q - (n \bmod q)$, $3q - (n \bmod q)$,
etc.

Check smoothness of
generalized congruence $i(n+i)/q$
for i's in this sublattice.
e.g. check whether $i, (n+i)/q$ are
smooth for $i = q - (n \bmod q)$ etc.

Try many large q's.
Rare for i's to overlap.

e.g. $n =$

Original

i	n
1	3
2	3
3	3

Use 997

$i \in 8024$

8024
17964
27904

ness chances

ce of $i(n+i)$
vs.
than for $i \approx y$.

$n+i)$ grows.

sis:
rade, but
for $i \le y$,
for $i \approx y^2$.

gruences
adation?

Choose q, square of large prime.
Choose a "q-sublattice" of i's:
arithmetic progression of i's
where q divides each $i(n+i)$.
e.g. progression $q - (n \bmod q)$,
$2q - (n \bmod q)$, $3q - (n \bmod q)$,
etc.

Check smoothness of
generalized congruence $i(n+i)/q$
for i's in this sublattice.
e.g. check whether $i, (n+i)/q$ are
smooth for $i = q - (n \bmod q)$ etc.

Try many large q's.
Rare for i's to overlap.

e.g. $n = 3141592$

Original **Q** sieve:

i	$n+i$
1	314159265
2	314159265
3	314159265

Use 997^2-sublattic
$i \in 802458 + 9940$

i	$(n$
802458	316
1796467	316
2790476	316

ces

- i)

i ≈ y.

ws.

,

.

Choose q, square of large prime.
Choose a "q-sublattice" of i's:
arithmetic progression of i's
where q divides each $i(n + i)$.
e.g. progression $q - (n \bmod q)$,
$2q - (n \bmod q)$, $3q - (n \bmod q)$,
etc.

Check smoothness of
generalized congruence $i(n + i)/q$
for i's in this sublattice.
e.g. check whether $i, (n+i)/q$ are
smooth for $i = q - (n \bmod q)$ etc.

Try many large q's.
Rare for i's to overlap.

e.g. $n = 31415926535897932$

Original $\mathbf{Q}$ sieve:

i	$n + i$
1	3141592653589793324
2	3141592653589793325
3	3141592653589793326

Use 997^2-sublattice,
$i \in 802458 + 994009\mathbf{Z}$:

i	$(n + i)/997^2$
802458	3160527373090
1796467	3160527373100
2790476	3160527373110

Choose q, square of large prime.
Choose a "q-sublattice" of i's:
arithmetic progression of i's
where q divides each $i(n+i)$.
e.g. progression $q-(n \bmod q)$,
$2q-(n \bmod q)$, $3q-(n \bmod q)$,
etc.

Check smoothness of
generalized congruence $i(n+i)/q$
for i's in this sublattice.
e.g. check whether $i, (n+i)/q$ are
smooth for $i = q-(n \bmod q)$ etc.

Try many large q's.
Rare for i's to overlap.

e.g. $n = 314159265358979323$:

Original $\mathbf{Q}$ sieve:

i	$n+i$
1	314159265358979324
2	314159265358979325
3	314159265358979326

Use 997^2-sublattice,
$i \in 802458 + 994009\mathbf{Z}$:

i	$(n+i)/997^2$
802458	316052737309
1796467	316052737310
2790476	316052737311

q, square of large prime.
a "q-sublattice" of i's:
tic progression of i's
divides each $i(n+i)$.
gression $q-(n \bmod q)$,
mod q), $3q-(n \bmod q)$,

moothness of
zed congruence $i(n+i)/q$
this sublattice.
ck whether $i, (n+i)/q$ are
for $i = q-(n \bmod q)$ etc.

y large q's.
i's to overlap.

e.g. $n = 314159265358979323$:

Original **Q** sieve:

i	$n+i$
1	314159265358979324
2	314159265358979325
3	314159265358979326

Use 997^2-sublattice,
$i \in 802458 + 994009\mathbf{Z}$:

i	$(n+i)/997^2$
802458	316052737309
1796467	316052737310
2790476	316052737311

Crude ar
eliminate
Have pra
of gener
$(q-(n$ m
between

More ca
are even
For $q \approx$
$i \approx (n +$
so smoo
$(u/2)^{-u}$
2^u times

of large prime.
ttice" of i's:
sion of i's
ch $i(n+i)$.
$-(n \bmod q)$,
$q-(n \bmod q)$,

s of
uence $i(n+i)/q$
attice.
er $i, (n+i)/q$ are
$-(n \bmod q)$ etc.

s.
erlap.

e.g. $n = 314159265358979323$:

Original **Q** sieve:

i	$n+i$
1	314159265358979324
2	314159265358979325
3	314159265358979326

Use 997^2-sublattice,
$i \in 802458 + 994009\mathbf{Z}$:

i	$(n+i)/997^2$
802458	316052737309
1796467	316052737310
2790476	316052737311

Crude analysis: Su
eliminate the grow
Have practically u
of generalized con
$(q-(n \bmod q))\frac{n+}{}$
between 0 and n.

More careful analy
are even better tha
For $q \approx n^{1/2}$ have
$i \approx (n+i)/q \approx n$
so smoothness cha
$(u/2)^{-u/2}(u/2)^{-u}$
2^u times larger tha

ime.

's:

i).

q),

d q),

$+ i)/q$

$)/q$ are

q) etc.

e.g. $n = 314159265358979323$:

Original $\mathbf{Q}$ sieve:

i	$n+i$
1	314159265358979324
2	314159265358979325
3	314159265358979326

Use 997^2-sublattice,

$i \in 802458 + 994009\mathbf{Z}$:

i	$(n+i)/997^2$
802458	316052737309
1796467	316052737310
2790476	316052737311

Crude analysis: Sublattices

eliminate the growth probler

Have practically unlimited su

of generalized congruences

$(q-(n \bmod q))\dfrac{n+q-(n \bmod}{q}$

between 0 and n.

More careful analysis: Subla

are even better than that!

For $q \approx n^{1/2}$ have

$i \approx (n+i)/q \approx n^{1/2} \approx y^{u/}$

so smoothness chance is rou

$(u/2)^{-u/2}(u/2)^{-u/2} = 2^u/$

2^u times larger than before.

e.g. $n = 314159265358979323$:

Original $\mathbf{Q}$ sieve:

i	$n+i$
1	314159265358979324
2	314159265358979325
3	314159265358979326

Use 997^2-sublattice,
$i \in 802458 + 994009\mathbf{Z}$:

i	$(n+i)/997^2$
802458	316052737309
1796467	316052737310
2790476	316052737311

Crude analysis: Sublattices eliminate the growth problem. Have practically unlimited supply of generalized congruences

$$(q-(n \bmod q))\frac{n+q-(n \bmod q)}{q}$$

between 0 and n.

More careful analysis: Sublattices are even better than that!
For $q \approx n^{1/2}$ have
$i \approx (n+i)/q \approx n^{1/2} \approx y^{u/2}$
so smoothness chance is roughly
$(u/2)^{-u/2}(u/2)^{-u/2} = 2^u/u^u$,
2^u times larger than before.

= 314159265358979323:

Q sieve:

$n + i$

314159265358979324

314159265358979325

314159265358979326

^{2}-sublattice,

$458 + 994009\mathbf{Z}$:

i	$(n+i)/997^2$
58	316052737309
67	316052737310
76	316052737311

Crude analysis: Sublattices eliminate the growth problem. Have practically unlimited supply of generalized congruences

$$(q-(n \bmod q))\frac{n+q-(n \bmod q)}{q}$$

between 0 and n.

More careful analysis: Sublattices are even better than that!
For $q \approx n^{1/2}$ have
$i \approx (n+i)/q \approx n^{1/2} \approx y^{u/2}$
so smoothness chance is roughly
$(u/2)^{-u/2}(u/2)^{-u/2} = 2^u/u^u$,
2^u times larger than before.

Even lar

from cha

"Quadra

$i^2 - n$ w

have i^2

much sm

65358979323:

358979324

358979325

358979326

ce,

009**Z**:

$+ i)/997^2$

052737309

052737310

052737311

Crude analysis: Sublattices eliminate the growth problem. Have practically unlimited supply of generalized congruences

$$(q-(n \bmod q))\frac{n+q-(n \bmod q)}{q}$$

between 0 and n.

More careful analysis: Sublattices are even better than that! For $q \approx n^{1/2}$ have $i \approx (n+i)/q \approx n^{1/2} \approx y^{u/2}$ so smoothness chance is roughly $(u/2)^{-u/2}(u/2)^{-u/2} = 2^u/u^u$, 2^u times larger than before.

Even larger improv

from changing pol

“Quadratic sieve”

$i^2 - n$ with $i \approx \surd$

have $i^2 - n \approx n^{1/}$

much smaller than

323:

4

5

6

9

0

1

Crude analysis: Sublattices eliminate the growth problem.
Have practically unlimited supply of generalized congruences

$$(q-(n \bmod q))\frac{n+q-(n \bmod q)}{q}$$

between 0 and n.

More careful analysis: Sublattices are even better than that!
For $q \approx n^{1/2}$ have
$i \approx (n+i)/q \approx n^{1/2} \approx y^{u/2}$
so smoothness chance is roughly
$(u/2)^{-u/2}(u/2)^{-u/2} = 2^u/u^u$,
2^u times larger than before.

Even larger improvements from changing polynomial $i($

"Quadratic sieve" (QS) uses
$i^2 - n$ with $i \approx \sqrt{n}$;
have $i^2 - n \approx n^{1/2+o(1)}$,
much smaller than n.

Crude analysis: Sublattices eliminate the growth problem.
Have practically unlimited supply of generalized congruences

$$(q-(n \bmod q))\frac{n+q-(n \bmod q)}{q}$$

between 0 and n.

More careful analysis: Sublattices are even better than that!
For $q \approx n^{1/2}$ have
$i \approx (n+i)/q \approx n^{1/2} \approx y^{u/2}$
so smoothness chance is roughly
$(u/2)^{-u/2}(u/2)^{-u/2} = 2^u/u^u$,
2^u times larger than before.

Even larger improvements from changing polynomial $i(n+i)$.

"Quadratic sieve" (QS) uses
$i^2 - n$ with $i \approx \sqrt{n}$;
have $i^2 - n \approx n^{1/2+o(1)}$,
much smaller than n.

Crude analysis: Sublattices eliminate the growth problem.
Have practically unlimited supply of generalized congruences

$$(q-(n \bmod q))\frac{n+q-(n \bmod q)}{q}$$

between 0 and n.

More careful analysis: Sublattices are even better than that!
For $q \approx n^{1/2}$ have
$i \approx (n+i)/q \approx n^{1/2} \approx y^{u/2}$
so smoothness chance is roughly
$(u/2)^{-u/2}(u/2)^{-u/2} = 2^u/u^u$,
2^u times larger than before.

Even larger improvements from changing polynomial $i(n+i)$.

"Quadratic sieve" (QS) uses
$i^2 - n$ with $i \approx \sqrt{n}$;
have $i^2 - n \approx n^{1/2+o(1)}$,
much smaller than n.

"MPQS" improves $o(1)$
using sublattices: $(i^2 - n)/q$.
But still $\approx n^{1/2}$.

Crude analysis: Sublattices eliminate the growth problem. Have practically unlimited supply of generalized congruences

$$(q-(n \bmod q))\frac{n+q-(n \bmod q)}{q}$$

between 0 and n.

More careful analysis: Sublattices are even better than that! For $q \approx n^{1/2}$ have $i \approx (n+i)/q \approx n^{1/2} \approx y^{u/2}$ so smoothness chance is roughly $(u/2)^{-u/2}(u/2)^{-u/2} = 2^u/u^u$, 2^u times larger than before.

Even larger improvements from changing polynomial $i(n+i)$.

"Quadratic sieve" (QS) uses $i^2 - n$ with $i \approx \sqrt{n}$; have $i^2 - n \approx n^{1/2+o(1)}$, much smaller than n.

"MPQS" improves $o(1)$ using sublattices: $(i^2 - n)/q$. But still $\approx n^{1/2}$.

"Number-field sieve" (NFS) achieves $n^{o(1)}$.

nalysis: Sublattices

e the growth problem.

actically unlimited supply

alized congruences

$\text{nod}\, q))\dfrac{n+q-(n \bmod q)}{q}$

0 and n.

reful analysis: Sublattices

better than that!

$n^{1/2}$ have

$-\, i)/q \approx n^{1/2} \approx y^{u/2}$

thness chance is roughly

$^{/2}(u/2)^{-u/2} = 2^u/u^u$,

s larger than before.

Even larger improvements
from changing polynomial $i(n+i)$.

"Quadratic sieve" (QS) uses
$i^2 - n$ with $i \approx \sqrt{n}$;
have $i^2 - n \approx n^{1/2+o(1)}$,
much smaller than n.

"MPQS" improves $o(1)$
using sublattices: $(i^2 - n)/q$.
But still $\approx n^{1/2}$.

"Number-field sieve" (NFS)
achieves $n^{o(1)}$.

Generali

The **Q** s

the num

Recall h

factors 6

Form a s

as produ

for sever

14(625)

= 4410

gcd{611

= 47.

ublattices

vth problem.

nlimited supply

gruences

$$\frac{q-(n \bmod q)}{q}$$

ysis: Sublattices

an that!

e

$^{1/2} \approx y^{u/2}$

ance is roughly

$^{u/2} = 2^u/u^u$,

an before.

Even larger improvements from changing polynomial $i(n+i)$.

"Quadratic sieve" (QS) uses $i^2 - n$ with $i \approx \sqrt{n}$; have $i^2 - n \approx n^{1/2+o(1)}$, much smaller than n.

"MPQS" improves $o(1)$ using sublattices: $(i^2 - n)/q$. But still $\approx n^{1/2}$.

"Number-field sieve" (NFS) achieves $n^{o(1)}$.

Generalizing beyon

The **Q** sieve is a s

the number-field s

Recall how the **Q**

factors 611:

Form a square

as product of $i(i -$

for several pairs $(i$

$14(625) \cdot 64(675)$

$= 4410000^2$.

$\gcd\{611, 14 \cdot 64 \cdot 7$

$= 47$.

m.

upply

d q)

ttices

2

ghly

u^u,

Even larger improvements from changing polynomial $i(n+i)$.

"Quadratic sieve" (QS) uses $i^2 - n$ with $i \approx \sqrt{n}$; have $i^2 - n \approx n^{1/2+o(1)}$, much smaller than n.

"MPQS" improves $o(1)$ using sublattices: $(i^2 - n)/q$. But still $\approx n^{1/2}$.

"Number-field sieve" (NFS) achieves $n^{o(1)}$.

Generalizing beyond $\mathbf{Q}$

The $\mathbf{Q}$ sieve is a special cas
the number-field sieve.

Recall how the $\mathbf{Q}$ sieve factors 611:

Form a square as product of $i(i + 611j)$ for several pairs (i, j):
$14(625) \cdot 64(675) \cdot 75(686) = 4410000^2$.

$\gcd\{611, 14 \cdot 64 \cdot 75 - 44100$
$= 47$.

Even larger improvements from changing polynomial $i(n+i)$.

"Quadratic sieve" (QS) uses $i^2 - n$ with $i \approx \sqrt{n}$; have $i^2 - n \approx n^{1/2+o(1)}$, much smaller than n.

"MPQS" improves $o(1)$ using sublattices: $(i^2 - n)/q$. But still $\approx n^{1/2}$.

"Number-field sieve" (NFS) achieves $n^{o(1)}$.

Generalizing beyond **Q**

The **Q** sieve is a special case of the number-field sieve.

Recall how the **Q** sieve factors 611:

Form a square as product of $i(i + 611j)$ for several pairs (i, j):
$14(625) \cdot 64(675) \cdot 75(686)$
$= 4410000^2$.

$\gcd\{611, 14 \cdot 64 \cdot 75 - 4410000\}$
$= 47$.

ger improvements
anging polynomial $i(n+i)$.

tic sieve" (QS) uses
vith $i \approx \sqrt{n}$;
$- n \approx n^{1/2+o(1)}$,
naller than n.

' improves $o(1)$
blattices: $(i^2 - n)/q$.
$\approx n^{1/2}$.

r-field sieve" (NFS)
$n^{o(1)}$.

Generalizing beyond $\mathbf{Q}$

The $\mathbf{Q}$ sieve is a special case of the number-field sieve.

Recall how the $\mathbf{Q}$ sieve factors 611:

Form a square
as product of $i(i + 611j)$
for several pairs (i, j):
$14(625) \cdot 64(675) \cdot 75(686)$
$= 4410000^2$.

$\gcd\{611, 14 \cdot 64 \cdot 75 - 4410000\}$
$= 47$.

The $\mathbf{Q}($
factors 6

Form a s
as produ
for sever
$(-11 +$
$\cdot$ (3
$= (112$

Comput
$s = (-1$
$t = 112$
gcd{611

vements

ynomial $i(n+i)$.

(QS) uses

n;

$2+o(1)$,

n n.

s $o(1)$

$(i^2-n)/q$.

ve" (NFS)

Generalizing beyond $\mathbf{Q}$

The $\mathbf{Q}$ sieve is a special case of the number-field sieve.

Recall how the $\mathbf{Q}$ sieve factors 611:

Form a square as product of $i(i+611j)$ for several pairs (i,j):

$14(625)\cdot 64(675)\cdot 75(686)$
$= 4410000^2$.

$\gcd\{611, 14\cdot 64\cdot 75 - 4410000\}$
$= 47$.

The $\mathbf{Q}(\sqrt{14})$ sieve

factors 611 as foll

Form a square

as product of $(i +$

for several pairs $(i$

$(-11+3\cdot 25)(-1$

$\cdot (3+25)(3$

$= (112-16\sqrt{14})^2$

Compute

$s = (-11+3\cdot 25)$

$t = 112-16\cdot 25,$

$\gcd\{611, s-t\} =$

$(n+i)$.

s

q.

Generalizing beyond **Q**

The **Q** sieve is a special case of the number-field sieve.

Recall how the **Q** sieve factors 611:

Form a square as product of $i(i+611j)$ for several pairs (i,j):
$14(625) \cdot 64(675) \cdot 75(686)$
$= 4410000^2$.

$\gcd\{611, 14 \cdot 64 \cdot 75 - 4410000\}$
$= 47$.

The $\mathbf{Q}(\sqrt{14})$ sieve factors 611 as follows:

Form a square as product of $(i+25j)(i+$ for several pairs (i,j):
$(-11+3\cdot 25)(-11+3\sqrt{14}$
$\quad \cdot (3+25)(3+\sqrt{14})$
$= (112-16\sqrt{14})^2$.

Compute
$s = (-11+3\cdot 25)\cdot(3+25$
$t = 112 - 16\cdot 25$,
$\gcd\{611, s-t\} = 13$.

Generalizing beyond **Q**

The **Q** sieve is a special case of the number-field sieve.

Recall how the **Q** sieve factors 611:

Form a square as product of $i(i + 611j)$ for several pairs (i, j):
$14(625) \cdot 64(675) \cdot 75(686)$
$= 4410000^2$.

$\gcd\{611, 14 \cdot 64 \cdot 75 - 4410000\}$
$= 47$.

The $\mathbf{Q}(\sqrt{14})$ sieve factors 611 as follows:

Form a square as product of $(i + 25j)(i + \sqrt{14}j)$ for several pairs (i, j):
$(-11 + 3 \cdot 25)(-11 + 3\sqrt{14})$
$\quad \cdot (3 + 25)(3 + \sqrt{14})$
$= (112 - 16\sqrt{14})^2$.

Compute
$s = (-11 + 3 \cdot 25) \cdot (3 + 25)$,
$t = 112 - 16 \cdot 25$,
$\gcd\{611, s - t\} = 13$.

zing beyond **Q**

ieve is a special case of
ber-field sieve.

ow the **Q** sieve
611:

square
ict of $i(i + 611j)$
ral pairs (i, j):
$\cdot 64(675) \cdot 75(686)$
00^2.

$, 14 \cdot 64 \cdot 75 - 4410000\}$

The $\mathbf{Q}(\sqrt{14})$ sieve
factors 611 as follows:

Form a square
as product of $(i + 25j)(i + \sqrt{14}j)$
for several pairs (i, j):
$(-11 + 3 \cdot 25)(-11 + 3\sqrt{14})$
$\quad \cdot (3 + 25)(3 + \sqrt{14})$
$= (112 - 16\sqrt{14})^2$.

Compute
$s = (-11 + 3 \cdot 25) \cdot (3 + 25)$,
$t = 112 - 16 \cdot 25$,
$\gcd\{611, s - t\} = 13$.

Why doe

Answer:
$\mathbf{Z}[\sqrt{14}]$
since 25

Apply ri
$(-11 +$
$\cdot (3$
$= (112 -$

i.e. $s^2 =$

Unsurpri

nd **Q**

pecial case of

ieve.

sieve

$+ 611j)$

$, j)$:

$\cdot 75(686)$

$75 - 4410000\}$

The $\mathbf{Q}(\sqrt{14})$ sieve

factors 611 as follows:

Form a square

as product of $(i + 25j)(i + \sqrt{14}j)$

for several pairs (i, j):

$$(-11 + 3 \cdot 25)(-11 + 3\sqrt{14})$$
$$\cdot (3 + 25)(3 + \sqrt{14})$$
$$= (112 - 16\sqrt{14})^2.$$

Compute

$s = (-11 + 3 \cdot 25) \cdot (3 + 25)$,

$t = 112 - 16 \cdot 25$,

$\gcd\{611, s - t\} = 13$.

Why does this wor

Answer: Have ring

$\mathbf{Z}[\sqrt{14}] \to \mathbf{Z}/611$,

since $25^2 = 14$ in

Apply ring morphi

$(-11 + 3 \cdot 25)(-1$

$\cdot (3 + 25)(3$

$= (112 - 16 \cdot 25)^2$

i.e. $s^2 = t^2$ in $\mathbf{Z}/6$

Unsurprising to fin

e of

000}

The $\mathbf{Q}(\sqrt{14})$ sieve
factors 611 as follows:

Form a square
as product of $(i + 25j)(i + \sqrt{14}j)$
for several pairs (i, j):

$$(-11 + 3 \cdot 25)(-11 + 3\sqrt{14}) \cdot (3 + 25)(3 + \sqrt{14}) = (112 - 16\sqrt{14})^2.$$

Compute
$s = (-11 + 3 \cdot 25) \cdot (3 + 25)$,
$t = 112 - 16 \cdot 25$,
$\gcd\{611, s - t\} = 13$.

Why does this work?

Answer: Have ring morphis
$\mathbf{Z}[\sqrt{14}] \to \mathbf{Z}/611$, $\sqrt{14} \mapsto 2$
since $25^2 = 14$ in $\mathbf{Z}/611$.

Apply ring morphism to squ

$$(-11 + 3 \cdot 25)(-11 + 3 \cdot 25 \cdot (3 + 25)(3 + 25) = (112 - 16 \cdot 25)^2 \text{ in } \mathbf{Z}/611$$

i.e. $s^2 = t^2$ in $\mathbf{Z}/611$.

Unsurprising to find factor.

The $\mathbf{Q}(\sqrt{14})$ sieve
factors 611 as follows:

Form a square
as product of $(i + 25j)(i + \sqrt{14}j)$
for several pairs (i, j):

$$(-11 + 3 \cdot 25)(-11 + 3\sqrt{14}) \cdot (3 + 25)(3 + \sqrt{14}) = (112 - 16\sqrt{14})^2.$$

Compute
$s = (-11 + 3 \cdot 25) \cdot (3 + 25)$,
$t = 112 - 16 \cdot 25$,
$\gcd\{611, s - t\} = 13$.

Why does this work?

Answer: Have ring morphism
$\mathbf{Z}[\sqrt{14}] \to \mathbf{Z}/611$, $\sqrt{14} \mapsto 25$,
since $25^2 = 14$ in $\mathbf{Z}/611$.

Apply ring morphism to square:

$$(-11 + 3 \cdot 25)(-11 + 3 \cdot 25) \cdot (3 + 25)(3 + 25) = (112 - 16 \cdot 25)^2 \text{ in } \mathbf{Z}/611.$$

i.e. $s^2 = t^2$ in $\mathbf{Z}/611$.

Unsurprising to find factor.

$\sqrt{14}$) sieve

611 as follows:

square

uct of $(i + 25j)(i + \sqrt{14}j)$

ral pairs (i, j):

$3 \cdot 25)(-11 + 3\sqrt{14})$

$3 + 25)(3 + \sqrt{14})$

$- 16\sqrt{14})^2$.

e

$1 + 3 \cdot 25) \cdot (3 + 25)$,

$- 16 \cdot 25$,

$, s - t\} = 13$.

Why does this work?

Answer: Have ring morphism $\mathbf{Z}[\sqrt{14}] \to \mathbf{Z}/611$, $\sqrt{14} \mapsto 25$, since $25^2 = 14$ in $\mathbf{Z}/611$.

Apply ring morphism to square:

$$(-11 + 3 \cdot 25)(-11 + 3 \cdot 25)$$
$$\cdot (3 + 25)(3 + 25)$$
$$= (112 - 16 \cdot 25)^2 \text{ in } \mathbf{Z}/611.$$

i.e. $s^2 = t^2$ in $\mathbf{Z}/611$.

Unsurprising to find factor.

Generali

to $(f, m$

$m \in \mathbf{Z}$,

Write d

$f = f_d x$

Can take

but large

better pa

Pick $\alpha \in$

Then f_d

monic g

$\mathbf{Q}(\alpha) \leftarrow$

e

ows:

$25j)(i + \sqrt{14}j)$

$, j)$:

$1 + 3\sqrt{14})$

$+ \sqrt{14})$

^{2}.

$) \cdot (3 + 25)$,

13.

Why does this work?

Answer: Have ring morphism $\mathbf{Z}[\sqrt{14}] \to \mathbf{Z}/611$, $\sqrt{14} \mapsto 25$, since $25^2 = 14$ in $\mathbf{Z}/611$.

Apply ring morphism to square:

$$(-11 + 3 \cdot 25)(-11 + 3 \cdot 25) \cdot (3 + 25)(3 + 25) = (112 - 16 \cdot 25)^2 \text{ in } \mathbf{Z}/611.$$

i.e. $s^2 = t^2$ in $\mathbf{Z}/611$.

Unsurprising to find factor.

Generalize from $(x$

to (f, m) with irre

$m \in \mathbf{Z}$, $f(m) \in n$

Write $d = \deg f$,

$f = f_d x^d + \cdots +$

Can take $f_d = 1$ fo

but larger f_d allow

better parameter s

Pick $\alpha \in \mathbf{C}$, root o

Then $f_d\alpha$ is a roo

monic $g = f_d^{d-1} f($

$\mathbf{Q}(\alpha) \leftarrow \mathcal{O} \leftarrow \mathbf{Z}[f_d\alpha$

$\sqrt{14}j$)

)

),

Why does this work?

Answer: Have ring morphism $\mathbf{Z}[\sqrt{14}] \to \mathbf{Z}/611$, $\sqrt{14} \mapsto 25$, since $25^2 = 14$ in $\mathbf{Z}/611$.

Apply ring morphism to square:

$$(-11 + 3 \cdot 25)(-11 + 3 \cdot 25) \cdot (3 + 25)(3 + 25)$$
$$= (112 - 16 \cdot 25)^2 \text{ in } \mathbf{Z}/611.$$

i.e. $s^2 = t^2$ in $\mathbf{Z}/611$.

Unsurprising to find factor.

Generalize from $(x^2 - 14, 25$

to (f, m) with irred $f \in \mathbf{Z}[x$

$m \in \mathbf{Z}$, $f(m) \in n\mathbf{Z}$.

Write $d = \deg f$,

$f = f_d x^d + \cdots + f_1 x^1 + f_0$

Can take $f_d = 1$ for simplici

but larger f_d allows

better parameter selection.

Pick $\alpha \in \mathbf{C}$, root of f.

Then $f_d\alpha$ is a root of

monic $g = f_d^{d-1} f(x/f_d) \in \mathbf{Z}$

$\mathbf{Q}(\alpha) \leftarrow \mathcal{O} \leftarrow \mathbf{Z}[f_d\alpha] \xrightarrow{f_d\alpha \mapsto f_d m}$

Why does this work?

Answer: Have ring morphism
$\mathbf{Z}[\sqrt{14}] \to \mathbf{Z}/611$, $\sqrt{14} \mapsto 25$,
since $25^2 = 14$ in $\mathbf{Z}/611$.

Apply ring morphism to square:
$$(-11 + 3 \cdot 25)(-11 + 3 \cdot 25) \cdot (3 + 25)(3 + 25) = (112 - 16 \cdot 25)^2 \text{ in } \mathbf{Z}/611.$$

i.e. $s^2 = t^2$ in $\mathbf{Z}/611$.

Unsurprising to find factor.

Generalize from $(x^2 - 14, 25)$
to (f, m) with irred $f \in \mathbf{Z}[x]$,
$m \in \mathbf{Z}$, $f(m) \in n\mathbf{Z}$.

Write $d = \deg f$,
$f = f_d x^d + \cdots + f_1 x^1 + f_0 x^0$.

Can take $f_d = 1$ for simplicity,
but larger f_d allows
better parameter selection.

Pick $\alpha \in \mathbf{C}$, root of f.
Then $f_d \alpha$ is a root of
monic $g = f_d^{d-1} f(x/f_d) \in \mathbf{Z}[x]$.

$$\mathbf{Q}(\alpha) \leftarrow \mathcal{O} \leftarrow \mathbf{Z}[f_d \alpha] \xrightarrow{f_d\alpha \mapsto f_d m} \mathbf{Z}/n$$

es this work?

Have ring morphism

$\to \mathbf{Z}/611$, $\sqrt{14} \mapsto 25$,

$^2 = 14$ in $\mathbf{Z}/611$.

ng morphism to square:

$3 \cdot 25)(-11 + 3 \cdot 25)$

$3 + 25)(3 + 25)$

$- 16 \cdot 25)^2$ in $\mathbf{Z}/611$.

$= t^2$ in $\mathbf{Z}/611$.

sing to find factor.

Generalize from $(x^2 - 14, 25)$ to (f, m) with irred $f \in \mathbf{Z}[x]$, $m \in \mathbf{Z}$, $f(m) \in n\mathbf{Z}$.

Write $d = \deg f$,
$f = f_d x^d + \cdots + f_1 x^1 + f_0 x^0$.

Can take $f_d = 1$ for simplicity, but larger f_d allows better parameter selection.

Pick $\alpha \in \mathbf{C}$, root of f.
Then $f_d\alpha$ is a root of monic $g = f_d^{d-1} f(x/f_d) \in \mathbf{Z}[x]$.

$$\mathbf{Q}(\alpha) \leftarrow \mathcal{O} \leftarrow \mathbf{Z}[f_d\alpha] \xrightarrow{f_d\alpha \mapsto f_d m} \mathbf{Z}/n$$

Build sq

congruer

with $i\mathbf{Z}$

Could re

higher-d

quadrati

for some

But let's

Say we h

$\prod_{(i,j) \in S}$

in $\mathbf{Q}(\alpha)$

rk?

g morphism
$\sqrt{14} \mapsto 25$,
$\mathbf{Z}/611$.

sm to square:
$1 + 3 \cdot 25)$
$+ 25)$
^{2} in $\mathbf{Z}/611$.

611.

nd factor.

Generalize from $(x^2 - 14, 25)$
to (f, m) with irred $f \in \mathbf{Z}[x]$,
$m \in \mathbf{Z}$, $f(m) \in n\mathbf{Z}$.

Write $d = \deg f$,
$f = f_d x^d + \cdots + f_1 x^1 + f_0 x^0$.

Can take $f_d = 1$ for simplicity,
but larger f_d allows
better parameter selection.

Pick $\alpha \in \mathbf{C}$, root of f.
Then $f_d\alpha$ is a root of
monic $g = f_d^{d-1} f(x/f_d) \in \mathbf{Z}[x]$.

$$\mathbf{Q}(\alpha) \leftarrow \mathcal{O} \leftarrow \mathbf{Z}[f_d\alpha] \xrightarrow{f_d\alpha \mapsto f_d m} \mathbf{Z}/n$$

Build square in $\mathbf{Q}($
congruences $(i - j$
with $i\mathbf{Z} + j\mathbf{Z} = \mathbf{Z}$

Could replace $i - j$
higher-deg irred in
quadratics seem fa
for some number f
But let's not both

Say we have a squ
$\prod_{(i,j) \in S} (i - jm)($
in $\mathbf{Q}(\alpha)$; now wha

n

25,

are:

)

.

Generalize from $(x^2 - 14, 25)$ to (f, m) with irred $f \in \mathbf{Z}[x]$, $m \in \mathbf{Z}$, $f(m) \in n\mathbf{Z}$.

Write $d = \deg f$, $f = f_d x^d + \cdots + f_1 x^1 + f_0 x^0$.

Can take $f_d = 1$ for simplicity, but larger f_d allows better parameter selection.

Pick $\alpha \in \mathbf{C}$, root of f. Then $f_d\alpha$ is a root of monic $g = f_d^{d-1} f(x/f_d) \in \mathbf{Z}[x]$.

$$\mathbf{Q}(\alpha) \leftarrow \mathcal{O} \leftarrow \mathbf{Z}[f_d\alpha] \xrightarrow{f_d\alpha \mapsto f_d m} \mathbf{Z}/n$$

Build square in $\mathbf{Q}(\alpha)$ from congruences $(i - jm)(i - j$ with $i\mathbf{Z} + j\mathbf{Z} = \mathbf{Z}$ and $j > 0$

Could replace $i - jx$ by higher-deg irred in $\mathbf{Z}[x]$; quadratics seem fairly small for some number fields. But let's not bother.

Say we have a square $\prod_{(i,j) \in S} (i - jm)(i - j\alpha)$ in $\mathbf{Q}(\alpha)$; now what?

Generalize from $(x^2 - 14, 25)$
to (f, m) with irred $f \in \mathbf{Z}[x]$,
$m \in \mathbf{Z}$, $f(m) \in n\mathbf{Z}$.

Write $d = \deg f$,
$f = f_d x^d + \cdots + f_1 x^1 + f_0 x^0$.

Can take $f_d = 1$ for simplicity,
but larger f_d allows
better parameter selection.

Pick $\alpha \in \mathbf{C}$, root of f.
Then $f_d \alpha$ is a root of
monic $g = f_d^{d-1} f(x/f_d) \in \mathbf{Z}[x]$.

$$\mathbf{Q}(\alpha) \leftarrow \mathcal{O} \leftarrow \mathbf{Z}[f_d \alpha] \xrightarrow{f_d \alpha \mapsto f_d m} \mathbf{Z}/n$$

Build square in $\mathbf{Q}(\alpha)$ from
congruences $(i - jm)(i - j\alpha)$
with $i\mathbf{Z} + j\mathbf{Z} = \mathbf{Z}$ and $j > 0$.

Could replace $i - jx$ by
higher-deg irred in $\mathbf{Z}[x]$;
quadratics seem fairly small
for some number fields.
But let's not bother.

Say we have a square
$\prod_{(i,j) \in S} (i - jm)(i - j\alpha)$
in $\mathbf{Q}(\alpha)$; now what?

ze from $(x^2 - 14, 25)$
) with irred $f \in \mathbf{Z}[x]$,
$f(m) \in n\mathbf{Z}$.

$= \deg f$,
$^d + \cdots + f_1 x^1 + f_0 x^0$.

e $f_d = 1$ for simplicity,
er f_d allows
arameter selection.

$\in \mathbf{C}$, root of f.
α is a root of
$= f_d^{d-1} f(x/f_d) \in \mathbf{Z}[x]$.

$\mathcal{O} \leftarrow \mathbf{Z}[f_d\alpha] \xrightarrow{f_d\alpha \mapsto f_d m} \mathbf{Z}/n$

Build square in $\mathbf{Q}(\alpha)$ from congruences $(i - jm)(i - j\alpha)$ with $i\mathbf{Z} + j\mathbf{Z} = \mathbf{Z}$ and $j > 0$.

Could replace $i - jx$ by higher-deg irred in $\mathbf{Z}[x]$; quadratics seem fairly small for some number fields. But let's not bother.

Say we have a square
$\prod_{(i,j)\in S}(i - jm)(i - j\alpha)$
in $\mathbf{Q}(\alpha)$; now what?

$\prod(i - j$
is a squa
ring of i

Multiply
putting s
compute
$\prod(i - j$

Then ap
$\varphi : \mathbf{Z}[f_d$
$f_d\alpha$ to f
$\varphi(r) - g$
In $\mathbf{Z}/n$
$g'(f_d m)$

$x^2 - 14, 25)$
ed $f \in \mathbf{Z}[x]$,
$\mathbf{Z}$.

$f_1 x^1 + f_0 x^0$.

or simplicity,
ws
selection.

of f.
t of
$(x/f_d) \in \mathbf{Z}[x]$.

$] \xrightarrow{f_d\alpha \mapsto f_d m} \mathbf{Z}/n$

Build square in $\mathbf{Q}(\alpha)$ from congruences $(i - jm)(i - j\alpha)$ with $i\mathbf{Z} + j\mathbf{Z} = \mathbf{Z}$ and $j > 0$.

Could replace $i - jx$ by higher-deg irred in $\mathbf{Z}[x]$; quadratics seem fairly small for some number fields. But let's not bother.

Say we have a square $\prod_{(i,j) \in S} (i - jm)(i - j\alpha)$ in $\mathbf{Q}(\alpha)$; now what?

$\prod(i - jm)(i - j\alpha$
is a square in $\mathcal{O}$,
ring of integers of

Multiply by $g'(f_d\alpha$
putting square roo
compute r with r^2
$\prod(i - jm)(i - j\alpha$

Then apply the rin
$\varphi : \mathbf{Z}[f_d\alpha] \to \mathbf{Z}/n$
$f_d\alpha$ to $f_d m$. Com
$\varphi(r) - g'(f_d m) \prod$
In $\mathbf{Z}/n$ have $\varphi(r)^2$
$g'(f_d m)^2 \prod(i - j$

5)

x],

x^0.

ty,

$\mathbf{Z}[x]$.

$\to \mathbf{Z}/n$

Build square in $\mathbf{Q}(\alpha)$ from congruences $(i - jm)(i - j\alpha)$ with $i\mathbf{Z} + j\mathbf{Z} = \mathbf{Z}$ and $j > 0$.

Could replace $i - jx$ by higher-deg irred in $\mathbf{Z}[x]$; quadratics seem fairly small for some number fields. But let's not bother.

Say we have a square $\prod_{(i,j)\in S}(i - jm)(i - j\alpha)$ in $\mathbf{Q}(\alpha)$; now what?

$\prod(i - jm)(i - j\alpha)f_d^2$ is a square in $\mathcal{O}$, ring of integers of $\mathbf{Q}(\alpha)$.

Multiply by $g'(f_d\alpha)^2$, putting square root into $\mathbf{Z}[f$ compute r with $r^2 = g'(f_d\alpha$ $\prod(i - jm)(i - j\alpha)f_d^2$.

Then apply the ring morphis $\varphi : \mathbf{Z}[f_d\alpha] \to \mathbf{Z}/n$ taking $f_d\alpha$ to $f_d m$. Compute gcd{ $\varphi(r) - g'(f_d m)\prod(i - jm)f$ In $\mathbf{Z}/n$ have $\varphi(r)^2 =$ $g'(f_d m)^2 \prod(i - jm)^2 f_d^2$.

Build square in $\mathbf{Q}(\alpha)$ from congruences $(i - jm)(i - j\alpha)$ with $i\mathbf{Z} + j\mathbf{Z} = \mathbf{Z}$ and $j > 0$.

Could replace $i - jx$ by higher-deg irred in $\mathbf{Z}[x]$; quadratics seem fairly small for some number fields. But let's not bother.

Say we have a square $\prod_{(i,j)\in S}(i - jm)(i - j\alpha)$ in $\mathbf{Q}(\alpha)$; now what?

$\prod(i - jm)(i - j\alpha)f_d^2$ is a square in $\mathcal{O}$, ring of integers of $\mathbf{Q}(\alpha)$.

Multiply by $g'(f_d\alpha)^2$, putting square root into $\mathbf{Z}[f_d\alpha]$: compute r with $r^2 = g'(f_d\alpha)^2 \cdot \prod(i - jm)(i - j\alpha)f_d^2$.

Then apply the ring morphism $\varphi : \mathbf{Z}[f_d\alpha] \to \mathbf{Z}/n$ taking $f_d\alpha$ to $f_d m$. Compute $\gcd\{n, \varphi(r) - g'(f_d m)\prod(i - jm)f_d\}$. In $\mathbf{Z}/n$ have $\varphi(r)^2 = g'(f_d m)^2 \prod(i - jm)^2 f_d^2$.

uare in $\mathbf{Q}(\alpha)$ from
nces $(i - j\,m)(i - j\,\alpha)$
$+ j\mathbf{Z} = \mathbf{Z}$ and $j > 0$.

eplace $i - jx$ by
eg irred in $\mathbf{Z}[x]$;
cs seem fairly small
e number fields.
s not bother.

have a square
$(i - j\,m)(i - j\,\alpha)$
; now what?

$\prod (i - j\,m)(i - j\,\alpha) f_d^2$
is a square in $\mathcal{O}$,
ring of integers of $\mathbf{Q}(\alpha)$.

Multiply by $g'(f_d\alpha)^2$,
putting square root into $\mathbf{Z}[f_d\alpha]$:
compute r with $r^2 = g'(f_d\alpha)^2 \cdot$
$\prod (i - j\,m)(i - j\,\alpha) f_d^2$.

Then apply the ring morphism
$\varphi : \mathbf{Z}[f_d\alpha] \to \mathbf{Z}/n$ taking
$f_d\alpha$ to $f_d m$. Compute $\gcd\{n,$
$\varphi(r) - g'(f_d m) \prod (i - j\,m) f_d\}$.
In $\mathbf{Z}/n$ have $\varphi(r)^2 =$
$g'(f_d m)^2 \prod (i - j\,m)^2 f_d^2$.

How to
of congr

Start wi
e.g., y^2

Look for
y-smoot
y-smoot
$f_d i^d + \cdot$
Here "y-
"has no

Find enc
Perform
exponen

(α) from
$j\,m)(i - j\,\alpha)$
and $j > 0$.

$j x$ by
$\mathbf{Z}[x]$;
airly small
fields.
er.

uare
$(i - j\,\alpha)$
t?

$\prod (i - j\,m)(i - j\,\alpha) f_d^2$
is a square in $\mathcal{O}$,
ring of integers of $\mathbf{Q}(\alpha)$.

Multiply by $g'(f_d\alpha)^2$,
putting square root into $\mathbf{Z}[f_d\alpha]$:
compute r with $r^2 = g'(f_d\alpha)^2 \cdot$
$\prod (i - j\,m)(i - j\,\alpha) f_d^2$.

Then apply the ring morphism
$\varphi : \mathbf{Z}[f_d\alpha] \to \mathbf{Z}/n$ taking
$f_d\alpha$ to $f_d m$. Compute $\gcd\{n,$
$\varphi(r) - g'(f_d m) \prod (i - j\,m) f_d\}$.
In $\mathbf{Z}/n$ have $\varphi(r)^2 =$
$g'(f_d m)^2 \prod (i - j\,m)^2 f_d^2$.

How to find squar
of congruences $(i$

Start with congrue
e.g., y^2 pairs $(i, j$

Look for y-smooth
y-smooth $i - j\,m$
y-smooth f_d norm
$f_d i^d + \cdots + f_0 j^d$
Here "y-smooth"
"has no prime divi

Find enough smoo
Perform linear alge
exponent vectors r

$\alpha)$

0.

$\prod(i - jm)(i - j\alpha)f_d^2$
is a square in $\mathcal{O}$,
ring of integers of $\mathbf{Q}(\alpha)$.

Multiply by $g'(f_d\alpha)^2$,
putting square root into $\mathbf{Z}[f_d\alpha]$:
compute r with $r^2 = g'(f_d\alpha)^2 \cdot$
$\prod(i - jm)(i - j\alpha)f_d^2$.

Then apply the ring morphism
$\varphi : \mathbf{Z}[f_d\alpha] \to \mathbf{Z}/n$ taking
$f_d\alpha$ to $f_d m$. Compute $\gcd\{n,$
$\varphi(r) - g'(f_d m)\prod(i - jm)f_d\}$.
In $\mathbf{Z}/n$ have $\varphi(r)^2 =$
$g'(f_d m)^2 \prod(i - jm)^2 f_d^2$.

How to find square product
of congruences $(i - jm)(i -$

Start with congruences for,
e.g., y^2 pairs (i, j).

Look for y-smooth congruer
y-smooth $i - jm$ and
y-smooth $f_d\,\mathrm{norm}(i - j\alpha) =$
$f_d i^d + \cdots + f_0 j^d = j^d f(i/j$
Here "y-smooth" means
"has no prime divisor $> y$."

Find enough smooth congru
Perform linear algebra on
exponent vectors mod 2.

$\prod(i - jm)(i - j\alpha)f_d^2$
is a square in $\mathcal{O}$,
ring of integers of $\mathbf{Q}(\alpha)$.

Multiply by $g'(f_d\alpha)^2$,
putting square root into $\mathbf{Z}[f_d\alpha]$:
compute r with $r^2 = g'(f_d\alpha)^2 \cdot$
$\prod(i - jm)(i - j\alpha)f_d^2$.

Then apply the ring morphism
$\varphi : \mathbf{Z}[f_d\alpha] \to \mathbf{Z}/n$ taking
$f_d\alpha$ to $f_d m$. Compute gcd$\{n,$
$\varphi(r) - g'(f_d m)\prod(i - jm)f_d\}$.
In $\mathbf{Z}/n$ have $\varphi(r)^2 =$
$g'(f_d m)^2 \prod(i - jm)^2 f_d^2$.

How to find square product
of congruences $(i - jm)(i - j\alpha)$?

Start with congruences for,
e.g., y^2 pairs (i, j).

Look for y-smooth congruences:
y-smooth $i - jm$ and
y-smooth $f_d\,\text{norm}(i - j\alpha) =$
$f_d i^d + \cdots + f_0 j^d = j^d f(i/j)$.
Here "y-smooth" means
"has no prime divisor $> y$."

Find enough smooth congruences.
Perform linear algebra on
exponent vectors mod 2.

$m)(i - j\alpha)f_d^2$
are in $\mathcal{O}$,
ntegers of $\mathbf{Q}(\alpha)$.

by $g'(f_d\alpha)^2$,
square root into $\mathbf{Z}[f_d\alpha]$:
e r with $r^2 = g'(f_d\alpha)^2$.
$m)(i - j\alpha)f_d^2$.

ply the ring morphism
$\alpha] \to \mathbf{Z}/n$ taking
$f_d m$. Compute gcd$\{n$,
$g'(f_d m) \prod (i - j m) f_d\}$.
have $\varphi(r)^2 =$
$^2 \prod (i - j m)^2 f_d^2$.

How to find square product
of congruences $(i - j m)(i - j\alpha)$?

Start with congruences for,
e.g., y^2 pairs (i, j).

Look for y-smooth congruences:
y-smooth $i - j m$ and
y-smooth $f_d \operatorname{norm}(i - j\alpha) =$
$f_d i^d + \cdots + f_0 j^d = j^d f(i/j)$.
Here "y-smooth" means
"has no prime divisor $> y$."

Find enough smooth congruences.
Perform linear algebra on
exponent vectors mod 2.

Asympto

Number
in numb
with the
is $L^{1.90..}$
exp((log

What ar

Choose
$d/(\log n$
$\in 1.40$.

$\alpha)f_d^2$

$\mathbf{Q}(\alpha)$.

$\alpha)^2$,

ot into $\mathbf{Z}[f_d\alpha]$:

$^2 = g'(f_d\alpha)^2$.

$\alpha)f_d^2$.

ng morphism

taking

npute gcd$\{n,$

$(i - jm)f_d\}$.

$^2 =$

$m)^2 f_d^2$.

How to find square product
of congruences $(i - jm)(i - j\alpha)$?

Start with congruences for,
e.g., y^2 pairs (i, j).

Look for y-smooth congruences:
y-smooth $i - jm$ and
y-smooth $f_d\,\mathrm{norm}(i - j\alpha) =$
$f_d i^d + \cdots + f_0 j^d = j^d f(i/j)$.
Here "y-smooth" means
"has no prime divisor $> y$."

Find enough smooth congruences.
Perform linear algebra on
exponent vectors mod 2.

Asymptotic cost e

Number of bit ope
in number-field sie
with theorists' par
is $L^{1.90\ldots+o(1)}$ whe
$\exp((\log n)^{1/3}(\log$

What are theorists

Choose degree d w
$d/(\log n)^{1/3}(\log \mathrm{lo}$
$\in 1.40\ldots + o(1)$.

$[_d\alpha]$:
$\alpha)^2$.

sm

n,
$f_d\}$.

How to find square product of congruences $(i - jm)(i - j\alpha)$?

Start with congruences for, e.g., y^2 pairs (i, j).

Look for y-smooth congruences: y-smooth $i - jm$ and y-smooth $f_d \operatorname{norm}(i - j\alpha) = f_d i^d + \cdots + f_0 j^d = j^d f(i/j)$.
Here "y-smooth" means "has no prime divisor $> y$."

Find enough smooth congruences. Perform linear algebra on exponent vectors mod 2.

Asymptotic cost exponents

Number of bit operations in number-field sieve, with theorists' parameters, is $L^{1.90\ldots+o(1)}$ where $L = \exp((\log n)^{1/3}(\log\log n)^{2/3})$

What are theorists' paramet

Choose degree d with $d/(\log n)^{1/3}(\log\log n)^{-1/3} \in 1.40\ldots + o(1)$.

How to find square product of congruences $(i - jm)(i - j\alpha)$?

Start with congruences for, e.g., y^2 pairs (i, j).

Look for y-smooth congruences: y-smooth $i - jm$ and y-smooth $f_d \operatorname{norm}(i - j\alpha) = f_d i^d + \cdots + f_0 j^d = j^d f(i/j)$. Here "$y$-smooth" means "has no prime divisor $> y$."

Find enough smooth congruences. Perform linear algebra on exponent vectors mod 2.

Asymptotic cost exponents

Number of bit operations in number-field sieve, with theorists' parameters, is $L^{1.90\ldots+o(1)}$ where $L = \exp((\log n)^{1/3}(\log\log n)^{2/3})$.

What are theorists' parameters?

Choose degree d with $d/(\log n)^{1/3}(\log\log n)^{-1/3} \in 1.40\ldots + o(1)$.

find square product
uences $(i - j m)(i - j\alpha)$?

th congruences for,
pairs (i, j).

y-smooth congruences:
h $i - j m$ and
h $f_d \operatorname{norm}(i - j\alpha) =$
$\cdots + f_0 j^d = j^d f(i/j)$.
-smooth" means
prime divisor $> y$."

ough smooth congruences.
linear algebra on
t vectors mod 2.

Asymptotic cost exponents

Number of bit operations
in number-field sieve,
with theorists' parameters,
is $L^{1.90\ldots+o(1)}$ where $L =$
$\exp((\log n)^{1/3}(\log\log n)^{2/3})$.

What are theorists' parameters?

Choose degree d with
$d/(\log n)^{1/3}(\log\log n)^{-1/3}$
$\in 1.40\ldots + o(1)$.

Choose i
Write n
$m^d + f_d$
with eac
Choose
in case t

Test smo
for all co
with 1 $\leq$
using pri

$L^{1.90\ldots+}$

Conjectu
smooth

e product
$-jm)(i-j\alpha)$?

ences for,
).

n congruences:
and
$(i-j\alpha) =$
$= j^d f(i/j)$.
means
sor $> y$."

oth congruences.
ebra on
mod 2.

Asymptotic cost exponents

Number of bit operations in number-field sieve, with theorists' parameters, is $L^{1.90\ldots+o(1)}$ where $L = \exp((\log n)^{1/3}(\log\log n)^{2/3})$.

What are theorists' parameters?

Choose degree d with $d/(\log n)^{1/3}(\log\log n)^{-1/3} \in 1.40\ldots + o(1)$.

Choose integer m
Write n as
$m^d + f_{d-1}m^{d-1}$ +
with each f_k belov
Choose f with sor
in case there are b

Test smoothness o
for all coprime pai
with $1 \le i, j \le L^{0}$
using primes $\le L^{0.}$

$L^{1.90\ldots+o(1)}$ pairs.
Conjecturally $L^{1.65}$
smooth values of

$- j\alpha)$?

nces:

=

).

ences.

Asymptotic cost exponents

Number of bit operations in number-field sieve, with theorists' parameters, is $L^{1.90\ldots+o(1)}$ where $L = \exp((\log n)^{1/3}(\log\log n)^{2/3})$.

What are theorists' parameters?

Choose degree d with $d/(\log n)^{1/3}(\log\log n)^{-1/3} \in 1.40\ldots + o(1)$.

Choose integer $m \approx n^{1/d}$.
Write n as
$m^d + f_{d-1}m^{d-1} + \cdots + f_1 r$
with each f_k below $n^{(1+o(1)}$
Choose f with some random
in case there are bad f's.

Test smoothness of $i - jm$
for all coprime pairs (i, j)
with $1 \le i, j \le L^{0.95\ldots+o(1)}$,
using primes $\le L^{0.95\ldots+o(1)}$.

$L^{1.90\ldots+o(1)}$ pairs.
Conjecturally $L^{1.65\ldots+o(1)}$
smooth values of $i - jm$.

Asymptotic cost exponents

Number of bit operations
in number-field sieve,
with theorists' parameters,
is $L^{1.90\ldots+o(1)}$ where $L =$
$\exp((\log n)^{1/3}(\log\log n)^{2/3})$.

What are theorists' parameters?

Choose degree d with
$d/(\log n)^{1/3}(\log\log n)^{-1/3}$
$\in 1.40\ldots + o(1)$.

Choose integer $m \approx n^{1/d}$.
Write n as
$m^d + f_{d-1}m^{d-1} + \cdots + f_1 m + f_0$
with each f_k below $n^{(1+o(1))/d}$.
Choose f with some randomness
in case there are bad f's.

Test smoothness of $i - jm$
for all coprime pairs (i, j)
with $1 \le i, j \le L^{0.95\ldots+o(1)}$,
using primes $\le L^{0.95\ldots+o(1)}$.

$L^{1.90\ldots+o(1)}$ pairs.
Conjecturally $L^{1.65\ldots+o(1)}$
smooth values of $i - jm$.

otic cost exponents

of bit operations
er-field sieve,
orists' parameters,
$.+o(1)$ where $L =$
$n)^{1/3}(\log\log n)^{2/3})$.

e theorists' parameters?

degree d with
$)^{1/3}(\log\log n)^{-1/3}$
$.. + o(1)$.

Choose integer $m \approx n^{1/d}$.
Write n as
$m^d + f_{d-1}m^{d-1} + \cdots + f_1 m + f_0$
with each f_k below $n^{(1+o(1))/d}$.
Choose f with some randomness
in case there are bad f's.

Test smoothness of $i - jm$
for all coprime pairs (i, j)
with $1 \le i, j \le L^{0.95\ldots+o(1)}$,
using primes $\le L^{0.95\ldots+o(1)}$.

$L^{1.90\ldots+o(1)}$ pairs.
Conjecturally $L^{1.65\ldots+o(1)}$
smooth values of $i - jm$.

Use $L^{0.1}$

For each
with smo
test smo
and $i -$
using pri

$L^{1.77\ldots+}$
Each $|j^{d}$
Conjectu
smooth

$L^{0.95\ldots+}$
in the ex

xponents

erations
eve,
ameters,
ere $L =$
$\log n)^{2/3})$.

s' parameters?

vith
g $n)^{-1/3}$

Choose integer $m \approx n^{1/d}$.
Write n as
$m^d + f_{d-1} m^{d-1} + \cdots + f_1 m + f_0$
with each f_k below $n^{(1+o(1))/d}$.
Choose f with some randomness
in case there are bad f's.

Test smoothness of $i - jm$
for all coprime pairs (i, j)
with $1 \le i, j \le L^{0.95\ldots+o(1)}$,
using primes $\le L^{0.95\ldots+o(1)}$.

$L^{1.90\ldots+o(1)}$ pairs.
Conjecturally $L^{1.65\ldots+o(1)}$
smooth values of $i - jm$.

Use $L^{0.12\ldots+o(1)}$ nu

For each (i, j)
with smooth $i - j$
test smoothness o
and $i - j\beta$ and so
using primes $\le L^{0.}$

$L^{1.77\ldots+o(1)}$ tests.
Each $|j^d f(i/j)| \le$
Conjecturally $L^{0.95}$
smooth congruenc

$L^{0.95\ldots+o(1)}$ compo
in the exponent ve

).

ers?

Choose integer $m \approx n^{1/d}$.

Write n as

$m^d + f_{d-1}m^{d-1} + \cdots + f_1 m + f_0$

with each f_k below $n^{(1+o(1))/d}$.

Choose f with some randomness in case there are bad f's.

Test smoothness of $i - jm$ for all coprime pairs (i, j) with $1 \le i, j \le L^{0.95\ldots+o(1)}$, using primes $\le L^{0.95\ldots+o(1)}$.

$L^{1.90\ldots+o(1)}$ pairs.

Conjecturally $L^{1.65\ldots+o(1)}$ smooth values of $i - jm$.

Use $L^{0.12\ldots+o(1)}$ number fiel

For each (i, j) with smooth $i - jm$, test smoothness of $i - j\alpha$ and $i - j\beta$ and so on, using primes $\le L^{0.82\ldots+o(1)}$.

$L^{1.77\ldots+o(1)}$ tests.

Each $|j^d f(i/j)| \le m^{2.86\ldots+o}$

Conjecturally $L^{0.95\ldots+o(1)}$ smooth congruences.

$L^{0.95\ldots+o(1)}$ components in the exponent vectors.

Choose integer $m \approx n^{1/d}$.
Write n as
$m^d + f_{d-1} m^{d-1} + \cdots + f_1 m + f_0$
with each f_k below $n^{(1+o(1))/d}$.
Choose f with some randomness in case there are bad f's.

Test smoothness of $i - jm$ for all coprime pairs (i, j) with $1 \le i, j \le L^{0.95\ldots+o(1)}$, using primes $\le L^{0.95\ldots+o(1)}$.

$L^{1.90\ldots+o(1)}$ pairs.
Conjecturally $L^{1.65\ldots+o(1)}$ smooth values of $i - jm$.

Use $L^{0.12\ldots+o(1)}$ number fields.

For each (i, j) with smooth $i - jm$, test smoothness of $i - j\alpha$ and $i - j\beta$ and so on, using primes $\le L^{0.82\ldots+o(1)}$.

$L^{1.77\ldots+o(1)}$ tests.
Each $|j^d f(i/j)| \le m^{2.86\ldots+o(1)}$.
Conjecturally $L^{0.95\ldots+o(1)}$ smooth congruences.

$L^{0.95\ldots+o(1)}$ components in the exponent vectors.

integer $m \approx n^{1/d}$.
as
$_{-1} m^{d-1} + \cdots + f_1 m + f_0$
h f_k below $n^{(1+o(1))/d}$.
f with some randomness
here are bad f's.

oothness of $i - jm$
prime pairs (i, j)
$\leq i, j \leq L^{0.95\ldots+o(1)}$,
imes $\leq L^{0.95\ldots+o(1)}$.

$^{o(1)}$ pairs.
urally $L^{1.65\ldots+o(1)}$
values of $i - jm$.

Use $L^{0.12\ldots+o(1)}$ number fields.

For each (i, j)
with smooth $i - jm$,
test smoothness of $i - j\alpha$
and $i - j\beta$ and so on,
using primes $\leq L^{0.82\ldots+o(1)}$.

$L^{1.77\ldots+o(1)}$ tests.
Each $|j^d f(i/j)| \leq m^{2.86\ldots+o(1)}$.
Conjecturally $L^{0.95\ldots+o(1)}$
smooth congruences.

$L^{0.95\ldots+o(1)}$ components
in the exponent vectors.

Three si

$(\log n)^{1/}$
y, i, j.

$(\log n)^{2/}$
m, $i - j$

$\log n$ bit

Unavoid
usual sm
forces (l
balancin
forces d
and $d \log$

$\approx n^{1/d}$.

$\cdots + f_1 m + f_0$

w $n^{(1+o(1))/d}$.

me randomness

ad f's.

f $i - j m$

rs (i, j)

$.95\ldots+o(1)$,

$95\ldots+o(1)$.

$5\ldots+o(1)$

$i - j m$.

Use $L^{0.12\ldots+o(1)}$ number fields.

For each (i, j)
with smooth $i - j m$,
test smoothness of $i - j \alpha$
and $i - j \beta$ and so on,
using primes $\le L^{0.82\ldots+o(1)}$.

$L^{1.77\ldots+o(1)}$ tests.
Each $|j^d f(i/j)| \le m^{2.86\ldots+o(1)}$.
Conjecturally $L^{0.95\ldots+o(1)}$
smooth congruences.

$L^{0.95\ldots+o(1)}$ components
in the exponent vectors.

Three sizes of num

$(\log n)^{1/3}(\log\log n$
y, i, j.

$(\log n)^{2/3}(\log\log n$
m, $i - j m$, $j^d f(i$

$\log n$ bits: n.

Unavoidably 1/3 i
usual smoothness
forces $(\log y)^2 \approx$ l
balancing norms w
forces $d \log y \approx$ log
and $d \log m \approx$ log

$m + f_0$

$)/d$.

nness

Use $L^{0.12\ldots+o(1)}$ number fields.

For each (i, j)
with smooth $i - jm$,
test smoothness of $i - j\alpha$
and $i - j\beta$ and so on,
using primes $\le L^{0.82\ldots+o(1)}$.

$L^{1.77\ldots+o(1)}$ tests.
Each $|j^d f(i/j)| \le m^{2.86\ldots+o(1)}$.
Conjecturally $L^{0.95\ldots+o(1)}$
smooth congruences.

$L^{0.95\ldots+o(1)}$ components
in the exponent vectors.

Three sizes of numbers here

$(\log n)^{1/3}(\log\log n)^{2/3}$ bits:
y, i, j.

$(\log n)^{2/3}(\log\log n)^{1/3}$ bits:
m, $i - jm$, $j^d f(i/j)$.

$\log n$ bits: n.

Unavoidably 1/3 in exponen
usual smoothness optimizati
forces $(\log y)^2 \approx \log m$;
balancing norms with m
forces $d \log y \approx \log m$;
and $d \log m \approx \log n$.

Use $L^{0.12\ldots+o(1)}$ number fields.

For each (i, j)
with smooth $i - jm$,
test smoothness of $i - j\alpha$
and $i - j\beta$ and so on,
using primes $\le L^{0.82\ldots+o(1)}$.

$L^{1.77\ldots+o(1)}$ tests.
Each $|j^d f(i/j)| \le m^{2.86\ldots+o(1)}$.
Conjecturally $L^{0.95\ldots+o(1)}$
smooth congruences.

$L^{0.95\ldots+o(1)}$ components
in the exponent vectors.

Three sizes of numbers here:

$(\log n)^{1/3}(\log\log n)^{2/3}$ bits:
y, i, j.

$(\log n)^{2/3}(\log\log n)^{1/3}$ bits:
m, $i - jm$, $j^d f(i/j)$.

$\log n$ bits: n.

Unavoidably $1/3$ in exponent:
usual smoothness optimization
forces $(\log y)^2 \approx \log m$;
balancing norms with m
forces $d \log y \approx \log m$;
and $d \log m \approx \log n$.

$^{2\ldots+o(1)}$ number fields.

n (i, j)
ooth $i - jm$,
oothness of $i - j\alpha$
$j\beta$ and so on,
imes $\le L^{0.82\ldots+o(1)}$.

$o(1)$ tests.
$^d f(i/j)| \le m^{2.86\ldots+o(1)}$.
urally $L^{0.95\ldots+o(1)}$
congruences.

$o(1)$ components
xponent vectors.

Three sizes of numbers here:

$(\log n)^{1/3}(\log\log n)^{2/3}$ bits:
y, i, j.

$(\log n)^{2/3}(\log\log n)^{1/3}$ bits:
m, $i - jm$, $j^d f(i/j)$.

$\log n$ bits: n.

Unavoidably 1/3 in exponent:
usual smoothness optimization
forces $(\log y)^2 \approx \log m$;
balancing norms with m
forces $d \log y \approx \log m$;
and $d \log m \approx \log n$.

Batch N

The nun
$L^{1.90\ldots+}$
finding s
$L^{1.77\ldots+}$
finding s

Many n
$L^{1.90\ldots+}$
to find s

Oops, lin
fix by re
But still
batch in
factoring

umber fields.

m,

f $i - j\alpha$

on,

$82\ldots+o(1)$.

$m^{2.86\ldots+o(1)}$.

$5\ldots+o(1)$

es.

onents

ectors.

Three sizes of numbers here:

$(\log n)^{1/3}(\log\log n)^{2/3}$ bits:
y, i, j.

$(\log n)^{2/3}(\log\log n)^{1/3}$ bits:
m, $i - jm$, $j^d f(i/j)$.

$\log n$ bits: n.

Unavoidably 1/3 in exponent:
usual smoothness optimization
forces $(\log y)^2 \approx \log m$;
balancing norms with m
forces $d \log y \approx \log m$;
and $d \log m \approx \log n$.

<u>Batch NFS</u>

The number-field
$L^{1.90\ldots+o(1)}$ bit op
finding smooth i –
$L^{1.77\ldots+o(1)}$ bit op
finding smooth j^d

Many n's can shar
$L^{1.90\ldots+o(1)}$ bit op
to find squares for

Oops, linear algebr
fix by reducing y.
But still end up fa
batch in much less
factoring each n s

ds.

$o(1)$.

Three sizes of numbers here:

$(\log n)^{1/3}(\log\log n)^{2/3}$ bits: y, i, j.

$(\log n)^{2/3}(\log\log n)^{1/3}$ bits: m, $i - jm$, $j^d f(i/j)$.

$\log n$ bits: n.

Unavoidably $1/3$ in exponent: usual smoothness optimization forces $(\log y)^2 \approx \log m$; balancing norms with m forces $d \log y \approx \log m$; and $d \log m \approx \log n$.

Batch NFS

The number-field sieve used $L^{1.90\ldots+o(1)}$ bit operations finding smooth $i - jm$; only $L^{1.77\ldots+o(1)}$ bit operations finding smooth $j^d f(i/j)$.

Many n's can share one m; $L^{1.90\ldots+o(1)}$ bit operations to find squares for *all* n's.

Oops, linear algebra hurts; fix by reducing y. But still end up factoring batch in much less time tha factoring each n separately.

Three sizes of numbers here:

$(\log n)^{1/3}(\log\log n)^{2/3}$ bits:
y, i, j.

$(\log n)^{2/3}(\log\log n)^{1/3}$ bits:
m, $i - jm$, $j^d f(i/j)$.

$\log n$ bits: n.

Unavoidably $1/3$ in exponent:
usual smoothness optimization
forces $(\log y)^2 \approx \log m$;
balancing norms with m
forces $d \log y \approx \log m$;
and $d \log m \approx \log n$.

Batch NFS

The number-field sieve used
$L^{1.90\ldots+o(1)}$ bit operations
finding smooth $i - jm$; only
$L^{1.77\ldots+o(1)}$ bit operations
finding smooth $j^d f(i/j)$.

Many n's can share one m;
$L^{1.90\ldots+o(1)}$ bit operations
to find squares for *all* n's.

Oops, linear algebra hurts;
fix by reducing y.
But still end up factoring
batch in much less time than
factoring each n separately.

zes of numbers here:

$/3(\log\log n)^{2/3}$ bits:

$/3(\log\log n)^{1/3}$ bits:
$m,\ j^d f(i/j)$.

ts: n.

ably $1/3$ in exponent:
noothness optimization
$\text{og } y)^2 \approx \log m$;
g norms with m
$\log y \approx \log m$;
$\text{g } m \approx \log n$.

Batch NFS

The number-field sieve used
$L^{1.90\ldots+o(1)}$ bit operations
finding smooth $i - jm$; only
$L^{1.77\ldots+o(1)}$ bit operations
finding smooth $j^d f(i/j)$.

Many n's can share one m;
$L^{1.90\ldots+o(1)}$ bit operations
to find squares for *all* n's.

Oops, linear algebra hurts;
fix by reducing y.
But still end up factoring
batch in much less time than
factoring each n separately.

Asympto
paramet

$d/(\log n$
$\in 1.10\,.$

Primes $\leq$

$1 \leq i, j$

Computa
finds L^{1}
smooth

$L^{1.64\ldots+}$
for each

nbers here:

$n)^{2/3}$ bits:

$n)^{1/3}$ bits:

$/j)$.

n exponent:

optimization

og m;

vith m

g m;

n.

Batch NFS

The number-field sieve used $L^{1.90\ldots+o(1)}$ bit operations finding smooth $i - jm$; only $L^{1.77\ldots+o(1)}$ bit operations finding smooth $j^d f(i/j)$.

Many n's can share one m; $L^{1.90\ldots+o(1)}$ bit operations to find squares for *all* n's.

Oops, linear algebra hurts; fix by reducing y.
But still end up factoring batch in much less time than factoring each n separately.

Asymptotic batch-

parameters:

$d/(\log n)^{1/3}(\log \mathrm{lo}$

$\in 1.10\ldots + o(1)$.

Primes $\le L^{0.82\ldots+o}$

$1 \le i, j \le L^{1.00\ldots+}$

Computation inde

finds $L^{1.64\ldots+o(1)}$

smooth values $i -$

$L^{1.64\ldots+o(1)}$ operat

for each target n.

:

t:

on

Batch NFS

The number-field sieve used $L^{1.90\ldots+o(1)}$ bit operations finding smooth $i - jm$; only $L^{1.77\ldots+o(1)}$ bit operations finding smooth $j^d f(i/j)$.

Many n's can share one m; $L^{1.90\ldots+o(1)}$ bit operations to find squares for *all* n's.

Oops, linear algebra hurts; fix by reducing y.
But still end up factoring batch in much less time than factoring each n separately.

Asymptotic batch-NFS parameters:

$d/(\log n)^{1/3}(\log\log n)^{-1/3} \in 1.10\ldots + o(1)$.

Primes $\le L^{0.82\ldots+o(1)}$.

$1 \le i, j \le L^{1.00\ldots+o(1)}$.

Computation independent of finds $L^{1.64\ldots+o(1)}$ smooth values $i - jm$.

$L^{1.64\ldots+o(1)}$ operations for each target n.

Batch NFS

The number-field sieve used $L^{1.90...+o(1)}$ bit operations finding smooth $i - jm$; only $L^{1.77...+o(1)}$ bit operations finding smooth $j^d f(i/j)$.

Many n's can share one m; $L^{1.90...+o(1)}$ bit operations to find squares for *all* n's.

Oops, linear algebra hurts; fix by reducing y.
But still end up factoring batch in much less time than factoring each n separately.

Asymptotic batch-NFS parameters:

$d/(\log n)^{1/3}(\log\log n)^{-1/3} \in 1.10\ldots + o(1)$.

Primes $\le L^{0.82...+o(1)}$.

$1 \le i, j \le L^{1.00...+o(1)}$.

Computation independent of n finds $L^{1.64...+o(1)}$ smooth values $i - jm$.

$L^{1.64...+o(1)}$ operations for each target n.

Batch NFS

The number-field sieve used $L^{1.90\ldots+o(1)}$ bit operations finding smooth $i - jm$; only $L^{1.77\ldots+o(1)}$ bit operations finding smooth $j^d f(i/j)$.

Many n's can share one m; $L^{1.90\ldots+o(1)}$ bit operations to find squares for *all* n's.

Oops, linear algebra hurts; fix by reducing y.
But still end up factoring batch in much less time than factoring each n separately.

Asymptotic batch-NFS parameters:

$d/(\log n)^{1/3}(\log\log n)^{-1/3} \in 1.10\ldots + o(1)$.

Primes $\le L^{0.82\ldots+o(1)}$.

$1 \le i, j \le L^{1.00\ldots+o(1)}$.

Computation independent of n finds $L^{1.64\ldots+o(1)}$ smooth values $i - jm$.

$L^{1.64\ldots+o(1)}$ operations for each target n.
Wait: how do we recognize smooth integers so quickly?

FS

mber-field sieve used
$o(1)$ bit operations
smooth $i - jm$; only
$o(1)$ bit operations
smooth $j^d f(i/j)$.

's can share one m;
$o(1)$ bit operations
squares for *all* n's.

near algebra hurts;
ducing y.
end up factoring
much less time than
g each n separately.

Asymptotic batch-NFS parameters:

$d/(\log n)^{1/3}(\log\log n)^{-1/3} \in 1.10\ldots + o(1)$.

Primes $\le L^{0.82\ldots+o(1)}$.

$1 \le i, j \le L^{1.00\ldots+o(1)}$.

Computation independent of n finds $L^{1.64\ldots+o(1)}$ smooth values $i - jm$.

$L^{1.64\ldots+o(1)}$ operations for each target n.
Wait: how do we recognize smooth integers so quickly?

The rho

Define ρ

Every pr
$(\rho_1 - \rho_2$
$\cdots(\rho_{357}$
Also ma

Can com
$\approx 2^{14}$ m
very littl

Compare
for trial

sieve used
erations
$- j m$; only
erations
$f(i/j)$.

re one m;
erations
all n's.

ra hurts;

ctoring
s time than
eparately.

Asymptotic batch-NFS parameters:

$d/(\log n)^{1/3}(\log\log n)^{-1/3} \in 1.10\ldots + o(1)$.

Primes $\le L^{0.82\ldots+o(1)}$.

$1 \le i, j \le L^{1.00\ldots+o(1)}$.

Computation independent of n finds $L^{1.64\ldots+o(1)}$ smooth values $i - jm$.

$L^{1.64\ldots+o(1)}$ operations for each target n.

Wait: how do we recognize smooth integers so quickly?

The rho method

Define $\rho_0 = 0$, ρ_{k-}

Every prime $\le 2^{20}$
$(\rho_1 - \rho_2)(\rho_2 - \rho_4$
$\cdots(\rho_{3575} - \rho_{7150})$
Also many larger p

Can compute gcd{
$\approx 2^{14}$ multiplicatio
very little memory

Compare to $\approx 2^{16}$
for trial division up

Asymptotic batch-NFS parameters:

$d/(\log n)^{1/3}(\log\log n)^{-1/3} \in 1.10\ldots + o(1)$.

Primes $\le L^{0.82\ldots+o(1)}$.

$1 \le i, j \le L^{1.00\ldots+o(1)}$.

Computation independent of n finds $L^{1.64\ldots+o(1)}$ smooth values $i - jm$.

$L^{1.64\ldots+o(1)}$ operations for each target n.

Wait: how do we recognize smooth integers so quickly?

The rho method

Define $\rho_0 = 0$, $\rho_{k+1} = \rho_k^2 +$

Every prime $\le 2^{20}$ divides S
$(\rho_1 - \rho_2)(\rho_2 - \rho_4)(\rho_3 - \rho_6)$
$\cdots(\rho_{3575} - \rho_{7150})$.
Also many larger primes.

Can compute $\gcd\{c, S\}$ usin
$\approx 2^{14}$ multiplications mod c
very little memory.

Compare to $\approx 2^{16}$ divisions
for trial division up to 2^{20}.

Asymptotic batch-NFS

parameters:

$d/(\log n)^{1/3}(\log\log n)^{-1/3}$
$\in 1.10\ldots + o(1)$.

Primes $\le L^{0.82\ldots+o(1)}$.

$1 \le i, j \le L^{1.00\ldots+o(1)}$.

Computation independent of n
finds $L^{1.64\ldots+o(1)}$
smooth values $i - jm$.

$L^{1.64\ldots+o(1)}$ operations
for each target n.
Wait: how do we recognize
smooth integers so quickly?

The rho method

Define $\rho_0 = 0$, $\rho_{k+1} = \rho_k^2 + 11$.

Every prime $\le 2^{20}$ divides $S =$
$(\rho_1 - \rho_2)(\rho_2 - \rho_4)(\rho_3 - \rho_6)$
$\cdots(\rho_{3575} - \rho_{7150})$.
Also many larger primes.

Can compute $\gcd\{c, S\}$ using
$\approx 2^{14}$ multiplications mod c,
very little memory.

Compare to $\approx 2^{16}$ divisions
for trial division up to 2^{20}.

otic batch-NFS

ers:

$)^{1/3}(\log\log n)^{-1/3}$

$\ldots + o(1)$.

$\leq L^{0.82\ldots+o(1)}$.

$\leq L^{1.00\ldots+o(1)}$.

ation independent of n

$64\ldots+o(1)$

values $i - jm$.

$o(1)$ operations

target n.

ow do we recognize

integers so quickly?

The rho method

Define $\rho_0 = 0$, $\rho_{k+1} = \rho_k^2 + 11$.

Every prime $\leq 2^{20}$ divides $S = (\rho_1 - \rho_2)(\rho_2 - \rho_4)(\rho_3 - \rho_6) \cdots (\rho_{3575} - \rho_{7150})$.
Also many larger primes.

Can compute $\gcd\{c, S\}$ using $\approx 2^{14}$ multiplications mod c, very little memory.

Compare to $\approx 2^{16}$ divisions for trial division up to 2^{20}.

More ge

Comput

$(\rho_1 - \rho_2$

How big

for all pr

Plausible

so $y^{1/2+}$

Reason:

ρ_1 mod p

If ρ_i mod

then ρ_k

for $k \in$ (

-NFS

g $n)^{-1/3}$

$o(1)$.

$-o(1)$.

pendent of n

$j\,m$.

tions

recognize

o quickly?

The rho method

Define $\rho_0 = 0$, $\rho_{k+1} = \rho_k^2 + 11$.

Every prime $\le 2^{20}$ divides $S =$
$(\rho_1 - \rho_2)(\rho_2 - \rho_4)(\rho_3 - \rho_6)$
$\cdots(\rho_{3575} - \rho_{7150})$.
Also many larger primes.

Can compute $\gcd\{c, S\}$ using
$\approx 2^{14}$ multiplications mod c,
very little memory.

Compare to $\approx 2^{16}$ divisions
for trial division up to 2^{20}.

More generally: C
Compute $\gcd\{c, S$
$(\rho_1 - \rho_2)(\rho_2 - \rho_4$

How big does z ha
for all primes $\le y$ t

Plausible conjectu
so $y^{1/2+o(1)}$ mults

Reason: Consider
$\rho_1 \bmod p$, $\rho_2 \bmod p$
If $\rho_i \bmod p = \rho_j$ m
then $\rho_k \bmod p = \rho$
for $k \in (j - i)\mathbf{Z} \cap$

f n

The rho method

Define $\rho_0 = 0$, $\rho_{k+1} = \rho_k^2 + 11$.

Every prime $\le 2^{20}$ divides $S =$
$(\rho_1 - \rho_2)(\rho_2 - \rho_4)(\rho_3 - \rho_6)$
$\cdots(\rho_{3575} - \rho_{7150})$.
Also many larger primes.

Can compute $\gcd\{c, S\}$ using $\approx 2^{14}$ multiplications mod c, very little memory.

Compare to $\approx 2^{16}$ divisions for trial division up to 2^{20}.

More generally: Choose z.
Compute $\gcd\{c, S\}$ where S
$(\rho_1 - \rho_2)(\rho_2 - \rho_4)\cdots(\rho_z -$

How big does z have to be for all primes $\le y$ to divide S

Plausible conjecture: $y^{1/2+o}$
so $y^{1/2+o(1)}$ mults mod c.

Reason: Consider first collis
$\rho_1 \bmod p$, $\rho_2 \bmod p$, ….
If $\rho_i \bmod p = \rho_j \bmod p$
then $\rho_k \bmod p = \rho_{2k} \bmod p$
for $k \in (j - i)\mathbf{Z} \cap [i, \infty] \cap [$

The rho method

Define $\rho_0 = 0$, $\rho_{k+1} = \rho_k^2 + 11$.

Every prime $\le 2^{20}$ divides $S = (\rho_1 - \rho_2)(\rho_2 - \rho_4)(\rho_3 - \rho_6) \cdots (\rho_{3575} - \rho_{7150})$.
Also many larger primes.

Can compute $\gcd\{c, S\}$ using $\approx 2^{14}$ multiplications mod c, very little memory.

Compare to $\approx 2^{16}$ divisions for trial division up to 2^{20}.

More generally: Choose z.
Compute $\gcd\{c, S\}$ where $S = (\rho_1 - \rho_2)(\rho_2 - \rho_4) \cdots (\rho_z - \rho_{2z})$.

How big does z have to be for all primes $\le y$ to divide S?

Plausible conjecture: $y^{1/2+o(1)}$; so $y^{1/2+o(1)}$ mults mod c.

Reason: Consider first collision in $\rho_1 \bmod p, \rho_2 \bmod p, \ldots$.
If $\rho_i \bmod p = \rho_j \bmod p$ then $\rho_k \bmod p = \rho_{2k} \bmod p$ for $k \in (j - i)\mathbf{Z} \cap [i, \infty] \cap [j, \infty]$.

method

$_0 = 0$, $\rho_{k+1} = \rho_k^2 + 11$.

ime $\leq 2^{20}$ divides $S =$

$)(\rho_2 - \rho_4)(\rho_3 - \rho_6)$

$_5 - \rho_{7150})$.

ny larger primes.

npute gcd$\{c, S\}$ using

ultiplications mod c,

e memory.

e to $\approx 2^{16}$ divisions

division up to 2^{20}.

More generally: Choose z.
Compute gcd$\{c, S\}$ where $S =$
$(\rho_1 - \rho_2)(\rho_2 - \rho_4) \cdots (\rho_z - \rho_{2z})$.

How big does z have to be
for all primes $\leq y$ to divide S?

Plausible conjecture: $y^{1/2+o(1)}$;
so $y^{1/2+o(1)}$ mults mod c.

Reason: Consider first collision in
$\rho_1 \bmod p, \rho_2 \bmod p, \ldots$.
If $\rho_i \bmod p = \rho_j \bmod p$
then $\rho_k \bmod p = \rho_{2k} \bmod p$
for $k \in (j - i)\mathbf{Z} \cap [i, \infty] \cap [j, \infty]$.

The $p -$

$S_1 = 2^{2}$

has prim

3, 5, 7,

37, 41,

89, 97,

137, 151

These di

70 of th

156 of t

296 of t

470 of t

etc.

$_{+1} = \rho_k^2 + 11.$

divides $S =$

$)(\rho_3 - \rho_6)$

$).$

primes.

$\{c, S\}$ using

ons mod c,

.

divisions

o to 2^{20}.

More generally: Choose z.

Compute $\gcd\{c, S\}$ where $S =$ $(\rho_1 - \rho_2)(\rho_2 - \rho_4) \cdots (\rho_z - \rho_{2z})$.

How big does z have to be for all primes $\le y$ to divide S?

Plausible conjecture: $y^{1/2+o(1)}$; so $y^{1/2+o(1)}$ mults mod c.

Reason: Consider first collision in $\rho_1 \bmod p, \rho_2 \bmod p, \ldots$.
If $\rho_i \bmod p = \rho_j \bmod p$
then $\rho_k \bmod p = \rho_{2k} \bmod p$
for $k \in (j - i)\mathbf{Z} \cap [i, \infty] \cap [j, \infty]$.

<u>The $p - 1$ method</u>

$S_1 = 2^{232792560} -$

has prime divisors

3, 5, 7, 11, 13, 17

37, 41, 43, 53, 61,

89, 97, 103, 109,

137, 151, 157, 181

These divisors incl

70 of the 168 prim

156 of the 1229 p

296 of the 9592 p

470 of the 78498

etc.

11.

=

)

ng

,

More generally: Choose z.
Compute $\gcd\{c, S\}$ where $S = (\rho_1 - \rho_2)(\rho_2 - \rho_4)\cdots(\rho_z - \rho_{2z})$.

How big does z have to be for all primes $\le y$ to divide S?

Plausible conjecture: $y^{1/2+o(1)}$; so $y^{1/2+o(1)}$ mults mod c.

Reason: Consider first collision in $\rho_1 \bmod p, \rho_2 \bmod p, \ldots$.
If $\rho_i \bmod p = \rho_j \bmod p$ then $\rho_k \bmod p = \rho_{2k} \bmod p$ for $k \in (j - i)\mathbf{Z} \cap [i, \infty] \cap [j, \infty]$.

The $p - 1$ method

$S_1 = 2^{232792560} - 1$
has prime divisors
3, 5, 7, 11, 13, 17, 19, 23, 2
37, 41, 43, 53, 61, 67, 71, 7
89, 97, 103, 109, 113, 127,
137, 151, 157, 181, 191, 19

These divisors include
70 of the 168 primes $\le 10^3$;
156 of the 1229 primes $\le$10
296 of the 9592 primes $\le$10
470 of the 78498 primes $\le$1
etc.

More generally: Choose z.
Compute $\gcd\{c, S\}$ where $S = (\rho_1 - \rho_2)(\rho_2 - \rho_4)\cdots(\rho_z - \rho_{2z})$.

How big does z have to be for all primes $\le y$ to divide S?

Plausible conjecture: $y^{1/2+o(1)}$; so $y^{1/2+o(1)}$ mults mod c.

Reason: Consider first collision in $\rho_1 \bmod p, \rho_2 \bmod p, \ldots$.
If $\rho_i \bmod p = \rho_j \bmod p$ then $\rho_k \bmod p = \rho_{2k} \bmod p$ for $k \in (j-i)\mathbf{Z} \cap [i,\infty] \cap [j,\infty]$.

The $p - 1$ method

$S_1 = 2^{232792560} - 1$
has prime divisors
3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 53, 61, 67, 71, 73, 79, 89, 97, 103, 109, 113, 127, 131, 137, 151, 157, 181, 191, 199 etc.

These divisors include
70 of the 168 primes $\le 10^3$;
156 of the 1229 primes $\le 10^4$;
296 of the 9592 primes $\le 10^5$;
470 of the 78498 primes $\le 10^6$;
etc.

nerally: Choose z.

e $\gcd\{c, S\}$ where $S =$

$)(\rho_2 - \rho_4)\cdots(\rho_z - \rho_{2z})$.

does z have to be

rimes $\le y$ to divide S?

e conjecture: $y^{1/2+o(1)}$;

$o(1)$ mults mod c.

Consider first collision in

$p, \rho_2 \bmod p, \ldots$.

d $p = \rho_j \bmod p$

mod $p = \rho_{2k} \bmod p$

$(j - i)\mathbf{Z} \cap [i, \infty] \cap [j, \infty]$.

The $p - 1$ method

$S_1 = 2^{232792560} - 1$

has prime divisors

3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 53, 61, 67, 71, 73, 79, 89, 97, 103, 109, 113, 127, 131, 137, 151, 157, 181, 191, 199 etc.

These divisors include

70 of the 168 primes $\le 10^3$;

156 of the 1229 primes $\le 10^4$;

296 of the 9592 primes $\le 10^5$;

470 of the 78498 primes $\le 10^6$;

etc.

An odd

divides 2

iff order

multiplic

divides s

Many wa

2327925

Why so

Answer:

$=$ lcm{1

$= 2^4 \cdot 3$

hoose z.

$\}$ where $S =$

$)\cdots(\rho_z - \rho_{2z})$.

ave to be

to divide S?

re: $y^{1/2+o(1)}$;

mod c.

first collision in

$, \ldots$.

nod p

$_{2k}$ mod p

$[i, \infty] \cap [j, \infty]$.

The $p - 1$ method

$S_1 = 2^{232792560} - 1$

has prime divisors

3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 53, 61, 67, 71, 73, 79, 89, 97, 103, 109, 113, 127, 131, 137, 151, 157, 181, 191, 199 etc.

These divisors include

70 of the 168 primes $\le 10^3$;

156 of the 1229 primes $\le 10^4$;

296 of the 9592 primes $\le 10^5$;

470 of the 78498 primes $\le 10^6$;

etc.

An odd prime p

divides $2^{232792560}$

iff order of 2 in th

multiplicative grou

divides $s = 23279$

Many ways for thi

232792560 has 96

Why so many?

Answer: $s = 2327$

$= \mathrm{lcm}\{1, 2, 3, 4, \ldots$

$= 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$

$S =$

$\rho_{2z})$.

S?

(1);

ion in

$j, \infty]$.

The $p-1$ method

$S_1 = 2^{232792560} - 1$
has prime divisors
3, 5, 7, 11, 13, 17, 19, 23, 29, 31,
37, 41, 43, 53, 61, 67, 71, 73, 79,
89, 97, 103, 109, 113, 127, 131,
137, 151, 157, 181, 191, 199 etc.

These divisors include
70 of the 168 primes $\le 10^3$;
156 of the 1229 primes $\le 10^4$;
296 of the 9592 primes $\le 10^5$;
470 of the 78498 primes $\le 10^6$;
etc.

An odd prime p
divides $2^{232792560} - 1$
iff order of 2 in the
multiplicative group $\mathbf{F}_p^*$
divides $s = 232792560$.

Many ways for this to happe
232792560 has 960 divisors.

Why so many?
Answer: $s = 232792560$
$= \text{lcm}\{1, 2, 3, 4, \ldots, 20\}$
$= 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot$

The $p-1$ method

$S_1 = 2^{232792560} - 1$
has prime divisors
3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 53, 61, 67, 71, 73, 79, 89, 97, 103, 109, 113, 127, 131, 137, 151, 157, 181, 191, 199 etc.

These divisors include
70 of the 168 primes $\le 10^3$;
156 of the 1229 primes $\le 10^4$;
296 of the 9592 primes $\le 10^5$;
470 of the 78498 primes $\le 10^6$;
etc.

An odd prime p
divides $2^{232792560} - 1$
iff order of 2 in the
multiplicative group $\mathbf{F}_p^*$
divides $s = 232792560$.

Many ways for this to happen:
232792560 has 960 divisors.

Why so many?
Answer: $s = 232792560$
$= \text{lcm}\{1, 2, 3, 4, \ldots, 20\}$
$= 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19.$

1 method

$32792560 - 1$

ne divisors

11, 13, 17, 19, 23, 29, 31,

43, 53, 61, 67, 71, 73, 79,

103, 109, 113, 127, 131,

., 157, 181, 191, 199 etc.

ivisors include

e 168 primes $\le 10^3$;

he 1229 primes $\le 10^4$;

he 9592 primes $\le 10^5$;

he 78498 primes $\le 10^6$;

An odd prime p
divides $2^{232792560} - 1$
iff order of 2 in the
multiplicative group $\mathbf{F}_p^*$
divides $s = 232792560$.

Many ways for this to happen:
232792560 has 960 divisors.

Why so many?
Answer: $s = 232792560$
$= \text{lcm}\{1, 2, 3, 4, \ldots, 20\}$
$= 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19.$

Can com

using 41

(Side no

Ring ope

This con

$2^2 = 2 \cdot$

$2^{12} = 2^6$

$2^{55}; 2^{110}$

$2^{3552}; 2^7$

$2^{56834}; 2$

$2^{909345};$

$2^{3637383}$

$2^{1454953}$

$2^{11639628}$

1

1

, 19, 23, 29, 31,
, 67, 71, 73, 79,
113, 127, 131,
1, 191, 199 etc.

ude
nes $\le 10^3$;
rimes $\le 10^4$;
rimes $\le 10^5$;
primes $\le 10^6$;

An odd prime p divides $2^{232792560} - 1$ iff order of 2 in the multiplicative group $\mathbf{F}_p^*$ divides $s = 232792560$.

Many ways for this to happen: 232792560 has 960 divisors.

Why so many?
Answer: $s = 232792560$
$= \text{lcm}\{1, 2, 3, 4, \ldots, 20\}$
$= 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19.$

Can compute 2^{232}
using 41 ring oper
(Side note: 41 is r

Ring operation: 0,

This computation:
$2^2 = 2 \cdot 2$; $2^3 = 2^2$
$2^{12} = 2^6 \cdot 2^6$; $2^{13} =$
2^{55}; 2^{110}; 2^{111}; 2^{22}
2^{3552}; 2^{7104}; 2^{1420}
2^{56834}; 2^{113668}; 2^{22}
2^{909345}; $2^{1818690}$; 2
$2^{3637383}$; $2^{7274766}$;
$2^{14549535}$; $2^{2909907}$
$2^{116396280}$; 2^{232792}

29, 31,
3, 79,
131,
9 etc.

^{4};
^{5};
0^6;

An odd prime p
divides $2^{232792560} - 1$
iff order of 2 in the
multiplicative group $\mathbf{F}_p^*$
divides $s = 232792560$.

Many ways for this to happen:
232792560 has 960 divisors.

Why so many?
Answer: $s = 232792560$
$= \mathrm{lcm}\{1, 2, 3, 4, \ldots, 20\}$
$= 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$.

Can compute $2^{232792560} - 1$
using 41 ring operations.
(Side note: 41 is not minim

Ring operation: 0, 1, $+$, $-$,

This computation: 1; $2 = 1$
$2^2 = 2 \cdot 2$; $2^3 = 2^2 \cdot 2$; $2^6 =$
$2^{12} = 2^6 \cdot 2^6$; $2^{13} = 2^{12} \cdot 2$; 2^{26};
2^{55}; 2^{110}; 2^{111}; 2^{222}; 2^{444}; 2^{88}
2^{3552}; 2^{7104}; 2^{14208}; 2^{28416}; 2
2^{56834};2^{113668};2^{227336};2^{45467}
2^{909345}; $2^{1818690}$; $2^{1818691}$; 2^{3}
$2^{3637383}$; $2^{7274766}$; $2^{7274767}$; 2
$2^{14549535}$; $2^{29099070}$; $2^{5819814}$
$2^{116396280}$; $2^{232792560}$; 2^{23279}

An odd prime p
divides $2^{232792560} - 1$
iff order of 2 in the
multiplicative group $\mathbf{F}_p^*$
divides $s = 232792560$.

Many ways for this to happen:
232792560 has 960 divisors.

Why so many?
Answer: $s = 232792560$
$= \mathrm{lcm}\{1, 2, 3, 4, \ldots, 20\}$
$= 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$.

Can compute $2^{232792560} - 1$
using 41 ring operations.
(Side note: 41 is not minimal.)

Ring operation: 0, 1, $+$, $-$, $\cdot$.

This computation: 1; $2 = 1 + 1$;
$2^2 = 2 \cdot 2$; $2^3 = 2^2 \cdot 2$; $2^6 = 2^3 \cdot 2^3$;
$2^{12} = 2^6 \cdot 2^6$; $2^{13} = 2^{12} \cdot 2$; 2^{26}; 2^{27}; 2^{54};
2^{55}; 2^{110}; 2^{111}; 2^{222}; 2^{444}; 2^{888}; 2^{1776};
2^{3552}; 2^{7104}; 2^{14208}; 2^{28416}; 2^{28417};
2^{56834}; 2^{113668}; 2^{227336}; 2^{454672}; 2^{909344};
2^{909345}; $2^{1818690}$; $2^{1818691}$; $2^{3637382}$;
$2^{3637383}$; $2^{7274766}$; $2^{7274767}$; $2^{14549534}$;
$2^{14549535}$; $2^{29099070}$; $2^{58198140}$;
$2^{116396280}$; $2^{232792560}$; $2^{232792560} - 1$.

prime p

$2^{232792560} - 1$

of 2 in the

cative group $\mathbf{F}_p^*$

$s = 232792560$.

ays for this to happen:

60 has 960 divisors.

many?

$s = 232792560$

$, 2, 3, 4, \ldots, 20\}$

$^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$.

Can compute $2^{232792560} - 1$
using 41 ring operations.
(Side note: 41 is not minimal.)

Ring operation: 0, 1, $+$, $-$, $\cdot$.

This computation: 1; $2 = 1 + 1$;
$2^2 = 2 \cdot 2$; $2^3 = 2^2 \cdot 2$; $2^6 = 2^3 \cdot 2^3$;
$2^{12} = 2^6 \cdot 2^6$; $2^{13} = 2^{12} \cdot 2$; 2^{26}; 2^{27}; 2^{54};
2^{55}; 2^{110}; 2^{111}; 2^{222}; 2^{444}; 2^{888}; 2^{1776};
2^{3552}; 2^{7104}; 2^{14208}; 2^{28416}; 2^{28417};
2^{56834}; 2^{113668}; 2^{227336}; 2^{454672}; 2^{909344};
2^{909345}; $2^{1818690}$; $2^{1818691}$; $2^{3637382}$;
$2^{3637383}$; $2^{7274766}$; $2^{7274767}$; $2^{14549534}$;
$2^{14549535}$; $2^{29099070}$; $2^{58198140}$;
$2^{116396280}$; $2^{232792560}$; $2^{232792560} - 1$.

Given po

can com

using 41

Notatior

e.g. $n =$

2^{27} moc

2^{54} moc

2^{55} moc

2^{110} moc

$2^{2327925}$

$- 1$

e

up $\mathbf{F}_p^*$

2560.

s to happen:

0 divisors.

92560

$\ldots, 20\}$

$1 \cdot 13 \cdot 17 \cdot 19.$

Can compute $2^{232792560} - 1$
using 41 ring operations.
(Side note: 41 is not minimal.)

Ring operation: $0, 1, +, -, \cdot$.

This computation: 1; $2 = 1 + 1$;
$2^2 = 2 \cdot 2$; $2^3 = 2^2 \cdot 2$; $2^6 = 2^3 \cdot 2^3$;
$2^{12} = 2^6 \cdot 2^6$; $2^{13} = 2^{12} \cdot 2$; 2^{26}; 2^{27}; 2^{54};
2^{55}; 2^{110}; 2^{111}; 2^{222}; 2^{444}; 2^{888}; 2^{1776};
2^{3552}; 2^{7104}; 2^{14208}; 2^{28416}; 2^{28417};
2^{56834}; 2^{113668}; 2^{227336}; 2^{454672}; 2^{909344};
2^{909345}; $2^{1818690}$; $2^{1818691}$; $2^{3637382}$;
$2^{3637383}$; $2^{7274766}$; $2^{7274767}$; $2^{14549534}$;
$2^{14549535}$; $2^{29099070}$; $2^{58198140}$;
$2^{116396280}$; $2^{232792560}$; $2^{232792560} - 1$.

Given positive inte

can compute 2^{2327}

using 41 operation

Notation: $a \bmod b$

e.g. $n = 85972312$

$2^{27} \bmod n = 1342$

$2^{54} \bmod n = 1342$

$= 9350$

$2^{55} \bmod n = 1871$

$2^{110} \bmod n = 1871$

$= 1458$

$2^{232792560} - 1 \bmod$

en:

19.

Can compute $2^{232792560} - 1$ using 41 ring operations.

(Side note: 41 is not minimal.)

Ring operation: 0, 1, $+$, $-$, $\cdot$.

This computation: 1; $2 = 1 + 1$; $2^2 = 2 \cdot 2$; $2^3 = 2^2 \cdot 2$; $2^6 = 2^3 \cdot 2^3$; $2^{12} = 2^6 \cdot 2^6$; $2^{13} = 2^{12} \cdot 2$; 2^{26}; 2^{27}; 2^{54}; 2^{55}; 2^{110}; 2^{111}; 2^{222}; 2^{444}; 2^{888}; 2^{1776}; 2^{3552}; 2^{7104}; 2^{14208}; 2^{28416}; 2^{28417}; 2^{56834}; 2^{113668}; 2^{227336}; 2^{454672}; 2^{909344}; 2^{909345}; $2^{1818690}$; $2^{1818691}$; $2^{3637382}$; $2^{3637383}$; $2^{7274766}$; $2^{7274767}$; $2^{14549534}$; $2^{14549535}$; $2^{29099070}$; $2^{58198140}$; $2^{116396280}$; $2^{232792560}$; $2^{232792560} - 1$.

Given positive integer n, can compute $2^{232792560} - 1$ using 41 operations in $\mathbf{Z}/n$.

Notation: $a \bmod b = a - b\lfloor$

e.g. $n = 8597231219$: ...

$2^{27} \bmod n = 134217728$;

$2^{54} \bmod n = 134217728^2$ m

$= 935663516$;

$2^{55} \bmod n = 1871327032$;

$2^{110} \bmod n = 1871327032^2$

$= 1458876811$; .

$2^{232792560} - 1 \bmod n = 56260$

Can compute $2^{232792560} - 1$
using 41 ring operations.
(Side note: 41 is not minimal.)

Ring operation: 0, 1, $+$, $-$, $\cdot$.

This computation: 1; $2 = 1 + 1$;
$2^2 = 2 \cdot 2$; $2^3 = 2^2 \cdot 2$; $2^6 = 2^3 \cdot 2^3$;
$2^{12} = 2^6 \cdot 2^6$; $2^{13} = 2^{12} \cdot 2$; 2^{26}; 2^{27}; 2^{54};
2^{55}; 2^{110}; 2^{111}; 2^{222}; 2^{444}; 2^{888}; 2^{1776};
2^{3552}; 2^{7104}; 2^{14208}; 2^{28416}; 2^{28417};
2^{56834};2^{113668};2^{227336};2^{454672};2^{909344};
2^{909345}; $2^{1818690}$; $2^{1818691}$; $2^{3637382}$;
$2^{3637383}$; $2^{7274766}$; $2^{7274767}$; $2^{14549534}$;
$2^{14549535}$; $2^{29099070}$; $2^{58198140}$;
$2^{116396280}$; $2^{232792560}$; $2^{232792560} - 1$.

Given positive integer n,
can compute $2^{232792560} - 1 \bmod n$
using 41 operations in $\mathbf{Z}/n$.
Notation: $a \bmod b = a - b\lfloor a/b \rfloor$.

e.g. $n = 8597231219$: ...

$$
\begin{aligned}
2^{27} \bmod n &= 134217728;\\
2^{54} \bmod n &= 134217728^2 \bmod n\\
&= 935663516;\\
2^{55} \bmod n &= 1871327032;\\
2^{110} \bmod n &= 1871327032^2 \bmod n\\
&= 1458876811; \ldots;\\
2^{232792560} - 1 \bmod n &= 5626089344.
\end{aligned}
$$

Can compute $2^{232792560} - 1$
using 41 ring operations.
(Side note: 41 is not minimal.)

Ring operation: 0, 1, $+$, $-$, $\cdot$.

This computation: 1; $2 = 1 + 1$;
$2^2 = 2 \cdot 2$; $2^3 = 2^2 \cdot 2$; $2^6 = 2^3 \cdot 2^3$;
$2^{12} = 2^6 \cdot 2^6$; $2^{13} = 2^{12} \cdot 2$; 2^{26}; 2^{27}; 2^{54};
2^{55}; 2^{110}; 2^{111}; 2^{222}; 2^{444}; 2^{888}; 2^{1776};
2^{3552}; 2^{7104}; 2^{14208}; 2^{28416}; 2^{28417};
2^{56834}; 2^{113668}; 2^{227336}; 2^{454672}; 2^{909344};
2^{909345}; $2^{1818690}$; $2^{1818691}$; $2^{3637382}$;
$2^{3637383}$; $2^{7274766}$; $2^{7274767}$; $2^{14549534}$;
$2^{14549535}$; $2^{29099070}$; $2^{58198140}$;
$2^{116396280}$; $2^{232792560}$; $2^{232792560} - 1$.

Given positive integer n,
can compute $2^{232792560} - 1 \bmod n$
using 41 operations in $\mathbf{Z}/n$.
Notation: $a \bmod b = a - b\lfloor a/b \rfloor$.

e.g. $n = 8597231219$: ...

$2^{27} \bmod n = 134217728$;
$2^{54} \bmod n = 134217728^2 \bmod n$
$= 935663516$;
$2^{55} \bmod n = 1871327032$;
$2^{110} \bmod n = 1871327032^2 \bmod n$
$= 1458876811$; ...;
$2^{232792560} - 1 \bmod n = 5626089344$.

Easy extra computation (Euclid):
$\gcd\{5626089344, n\} = 991$.

npute $2^{232792560} - 1$
ring operations.
ote: 41 is not minimal.)

eration: 0, 1, $+$, $-$, $\cdot$.

mputation: 1; $2 = 1 + 1$;
2; $2^3 = 2^2 \cdot 2$; $2^6 = 2^3 \cdot 2^3$;
$\cdot 2^6$; $2^{13} = 2^{12} \cdot 2$; 2^{26}; 2^{27}; 2^{54};
; 2^{111}; 2^{222}; 2^{444}; 2^{888}; 2^{1776};
7104; 2^{14208}; 2^{28416}; 2^{28417};
113668; 2^{227336}; 2^{454672}; 2^{909344};
$2^{1818690}$; $2^{1818691}$; $2^{3637382}$;
; $2^{7274766}$; $2^{7274767}$; $2^{14549534}$;
5; $2^{29099070}$; $2^{58198140}$;
80; $2^{232792560}$; $2^{232792560} - 1$.

Given positive integer n,
can compute $2^{232792560} - 1 \bmod n$
using 41 operations in $\mathbf{Z}/n$.
Notation: $a \bmod b = a - b\lfloor a/b \rfloor$.

e.g. $n = 8597231219$: ...

$$2^{27} \bmod n = 134217728;$$
$$2^{54} \bmod n = 134217728^2 \bmod n = 935663516;$$
$$2^{55} \bmod n = 1871327032;$$
$$2^{110} \bmod n = 1871327032^2 \bmod n = 1458876811; \ldots;$$
$$2^{232792560} - 1 \bmod n = 5626089344.$$

Easy extra computation (Euclid):
$\gcd\{5626089344, n\} = 991$.

This p –
quickly f
Main wo

Could in
n's divis
The 167
would ha

Not clea
Dividing
is faster
The p –
only 70
trial divi

$^{792560} - 1$

ations.

not minimal.)

, 1, +, −, ·.

1; $2 = 1 + 1$;

$\cdot 2$; $2^6 = 2^3 \cdot 2^3$;

$2^{12} \cdot 2$; 2^{26}; 2^{27}; 2^{54};

^{2}; 2^{444}; 2^{888}; 2^{1776};

^{3}; 2^{28416}; 2^{28417};

^{7336}; 2^{454672}; 2^{909344};

^{1818691}; $2^{3637382}$;

$2^{7274767}$; $2^{14549534}$;

^{0}; $2^{58198140}$;

^{560}; $2^{232792560} - 1$.

Given positive integer n,
can compute $2^{232792560} - 1 \bmod n$
using 41 operations in $\mathbf{Z}/n$.
Notation: $a \bmod b = a - b\lfloor a/b \rfloor$.

e.g. $n = 8597231219$: . . .

$$
\begin{aligned}
2^{27} \bmod n &= 134217728; \\
2^{54} \bmod n &= 134217728^2 \bmod n \\
&= 935663516; \\
2^{55} \bmod n &= 1871327032; \\
2^{110} \bmod n &= 1871327032^2 \bmod n \\
&= 1458876811; \ \ldots; \\
2^{232792560} - 1 \bmod n &= 5626089344.
\end{aligned}
$$

Easy extra computation (Euclid):
$\gcd\{5626089344, n\} = 991$.

This $p - 1$ metho
quickly factored n
Main work: 27 squ

Could instead hav
n's divisibility by
The 167th trial div
would have found

Not clear which m
Dividing by small
is faster than squa
The $p - 1$ method
only 70 of the prin
trial division finds

al.)

·.

$+ 1$;

$2^3 \cdot 2^3$;

$2^{27}; 2^{54}$;

$^{88}; 2^{1776}$;

^{28417};

$^{72}; 2^{909344}$;

^{3637382};

$2^{14549534}$;

^{0};

$^{2560} - 1$.

Given positive integer n,
can compute $2^{232792560} - 1 \bmod n$
using 41 operations in $\mathbf{Z}/n$.
Notation: $a \bmod b = a - b\lfloor a/b \rfloor$.

e.g. $n = 8597231219$: ...

$$2^{27} \bmod n = 134217728;$$
$$2^{54} \bmod n = 134217728^2 \bmod n = 935663516;$$
$$2^{55} \bmod n = 1871327032;$$
$$2^{110} \bmod n = 1871327032^2 \bmod n = 1458876811; \ldots;$$
$$2^{232792560} - 1 \bmod n = 5626089344.$$

Easy extra computation (Euclid):
$\gcd\{5626089344, n\} = 991$.

This $p - 1$ method (1974 Po
quickly factored $n = 859723$
Main work: 27 squarings mo

Could instead have checked
n's divisibility by $2, 3, 5, \ldots$
The 167th trial division
would have found divisor 99

Not clear which method is b
Dividing by small p
is faster than squaring mod
The $p - 1$ method finds
only 70 of the primes ≤ 1000
trial division finds all 168 pr

Given positive integer n,
can compute $2^{232792560} - 1 \bmod n$
using 41 operations in $\mathbf{Z}/n$.
Notation: $a \bmod b = a - b\lfloor a/b \rfloor$.

e.g. $n = 8597231219$: ...

$$
\begin{aligned}
2^{27} \bmod n &= 134217728; \\
2^{54} \bmod n &= 134217728^2 \bmod n \\
&= 935663516; \\
2^{55} \bmod n &= 1871327032; \\
2^{110} \bmod n &= 1871327032^2 \bmod n \\
&= 1458876811; \ldots; \\
2^{232792560} - 1 \bmod n &= 5626089344.
\end{aligned}
$$

Easy extra computation (Euclid):
$\gcd\{5626089344, n\} = 991$.

This $p-1$ method (1974 Pollard)
quickly factored $n = 8597231219$.
Main work: 27 squarings mod n.

Could instead have checked
n's divisibility by $2, 3, 5, \ldots$.
The 167th trial division
would have found divisor 991.

Not clear which method is better.
Dividing by small p
is faster than squaring mod n.
The $p-1$ method finds
only 70 of the primes ≤ 1000;
trial division finds all 168 primes.

ositive integer n,
pute $2^{232792560} - 1 \bmod n$
operations in $\mathbf{Z}/n$.
n: $a \bmod b = a - b\lfloor a/b \rfloor$.

= 8597231219: . . .
d n $= 134217728$;
d n $= 134217728^2 \bmod n$
$= 935663516$;
d n $= 1871327032$;
d n $= 1871327032^2 \bmod n$
$= 1458876811$; . . . ;
$^{60} - 1 \bmod n = 5626089344$.

tra computation (Euclid):
6089344, $n\} = 991$.

This $p-1$ method (1974 Pollard) quickly factored $n = 8597231219$. Main work: 27 squarings mod n.

Could instead have checked n's divisibility by $2, 3, 5, \ldots$. The 167th trial division would have found divisor 991.

Not clear which method is better. Dividing by small p is faster than squaring mod n. The $p-1$ method finds only 70 of the primes ≤ 1000; trial division finds all 168 primes.

Scale up
$s =$ lcm
using 13
find 231

Is a squa
faster th

Or $s =$ l
using 14
find 180

Is a squa
faster th

Extra be
no need

eger n,
$^{792560} - 1 \bmod n$
ns in $\mathbf{Z}/n$.
$b = a - b\lfloor a/b \rfloor$.

219: ...
217728;
$217728^2 \bmod n$
663516;
1327032;
$1327032^2 \bmod n$
8876811; ...;
$n = 5626089344$.

tation (Euclid):
$n\} = 991$.

This $p - 1$ method (1974 Pollard) quickly factored $n = 8597231219$. Main work: 27 squarings mod n.

Could instead have checked n's divisibility by $2, 3, 5, \ldots$. The 167th trial division would have found divisor 991.

Not clear which method is better. Dividing by small p is faster than squaring mod n. The $p - 1$ method finds only 70 of the primes ≤ 1000; trial division finds all 168 primes.

Scale up to larger
$s = \text{lcm}\{1, 2, 3, 4,$
using 136 squarin
find 2317 of the p

Is a squaring mod
faster than 17 tria

Or $s = \text{lcm}\{1, 2, 3$
using 1438 squarin
find 180121 of the

Is a squaring mod
faster than 125 tri

Extra benefit:
no need to store t

mod n

$a/b\rfloor$.

od n

mod n

. . ;

089344.

clid):

This $p-1$ method (1974 Pollard) quickly factored $n = 8597231219$. Main work: 27 squarings mod n.

Could instead have checked n's divisibility by $2, 3, 5, \ldots$. The 167th trial division would have found divisor 991.

Not clear which method is better. Dividing by small p is faster than squaring mod n. The $p-1$ method finds only 70 of the primes ≤ 1000; trial division finds all 168 primes.

Scale up to larger exponent $s = \text{lcm}\{1, 2, 3, 4, \ldots, 100\}$: using 136 squarings mod n find 2317 of the primes $\le$10

Is a squaring mod n faster than 17 trial divisions

Or $s = \text{lcm}\{1, 2, 3, 4, \ldots, 10$ using 1438 squarings mod n find 180121 of the primes $\le$

Is a squaring mod n faster than 125 trial division

Extra benefit: no need to store the primes.

This $p-1$ method (1974 Pollard) quickly factored $n = 8597231219$. Main work: 27 squarings mod n.

Could instead have checked n's divisibility by $2, 3, 5, \ldots$. The 167th trial division would have found divisor 991.

Not clear which method is better. Dividing by small p is faster than squaring mod n. The $p-1$ method finds only 70 of the primes ≤ 1000; trial division finds all 168 primes.

Scale up to larger exponent $s = \text{lcm}\{1, 2, 3, 4, \ldots, 100\}$: using 136 squarings mod n find 2317 of the primes $\le 10^5$.

Is a squaring mod n faster than 17 trial divisions?

Or $s = \text{lcm}\{1, 2, 3, 4, \ldots, 1000\}$: using 1438 squarings mod n find 180121 of the primes $\le 10^7$.

Is a squaring mod n faster than 125 trial divisions?

Extra benefit: no need to store the primes.

- 1 method (1974 Pollard)
factored $n = 8597231219$.
rk: 27 squarings mod n.

stead have checked
ibility by $2, 3, 5, \ldots$.
th trial division
ave found divisor 991.

r which method is better.
by small p
than squaring mod n.
1 method finds
of the primes ≤ 1000;
sion finds all 168 primes.

Scale up to larger exponent
$s = \text{lcm}\{1, 2, 3, 4, \ldots, 100\}$:
using 136 squarings mod n
find 2317 of the primes $\le 10^5$.

Is a squaring mod n
faster than 17 trial divisions?

Or $s = \text{lcm}\{1, 2, 3, 4, \ldots, 1000\}$:
using 1438 squarings mod n
find 180121 of the primes $\le 10^7$.

Is a squaring mod n
faster than 125 trial divisions?

Extra benefit:
no need to store the primes.

Plausible
$\exp\sqrt{(\frac{1}{2}$
then $p-$
for H/K
Same if
order of

So unifo
divides 2
with pro

$(1.4\ldots$
produce

Similar t
finds far

d (1974 Pollard)

= 8597231219.

uarings mod n.

e checked

2, 3, 5, ...

vision

divisor 991.

ethod is better.

p

ring mod n.

l finds

mes ≤1000;

all 168 primes.

Scale up to larger exponent
$s = \mathrm{lcm}\{1, 2, 3, 4, \ldots, 100\}$:
using 136 squarings mod n
find 2317 of the primes $\le 10^5$.

Is a squaring mod n
faster than 17 trial divisions?

Or $s = \mathrm{lcm}\{1, 2, 3, 4, \ldots, 1000\}$:
using 1438 squarings mod n
find 180121 of the primes $\le 10^7$.

Is a squaring mod n
faster than 125 trial divisions?

Extra benefit:
no need to store the primes.

Plausible conjectu

$\exp\sqrt{\left(\frac{1}{2} + o(1)\right)\mathrm{lo}$

then $p{-}1$ divides l

for $H/K^{1+o(1)}$ pri

Same if $p - 1$ is re

order of 2 in $\mathbf{F}_p^*$.

So uniform randor

divides $2^{\mathrm{lcm}\{1,2,\ldots,}$

with probability 1/

$(1.4\ldots + o(1))K$ s

produce $2^{\mathrm{lcm}\{1,2,\ldots}$

Similar time spent

finds far fewer pri

ollard)
31219.
od n.

1.

etter.

n.

0;
imes.

Scale up to larger exponent
$s = \text{lcm}\{1, 2, 3, 4, \ldots, 100\}$:
using 136 squarings mod n
find 2317 of the primes $\le 10^5$.

Is a squaring mod n
faster than 17 trial divisions?

Or $s = \text{lcm}\{1, 2, 3, 4, \ldots, 1000\}$:
using 1438 squarings mod n
find 180121 of the primes $\le 10^7$.

Is a squaring mod n
faster than 125 trial divisions?

Extra benefit:
no need to store the primes.

Plausible conjecture: if K is
$\exp\sqrt{\left(\frac{1}{2} + o(1)\right)\log H \log \text{lo}}$
then $p-1$ divides $\text{lcm}\{1, 2, \ldots$
for $H/K^{1+o(1)}$ primes $p \le H$
Same if $p - 1$ is replaced by
order of 2 in $\mathbf{F}_p^*$.

So uniform random prime p
divides $2^{\text{lcm}\{1,2,\ldots,K\}} - 1$
with probability $1/K^{1+o(1)}$.

$(1.4\ldots + o(1))K$ squarings
produce $2^{\text{lcm}\{1,2,\ldots,K\}} - 1$ mo

Similar time spent on trial d
finds far fewer primes for lar

Scale up to larger exponent
$s = \operatorname{lcm}\{1, 2, 3, 4, \ldots, 100\}$:
using 136 squarings mod n
find 2317 of the primes $\le 10^5$.

Is a squaring mod n
faster than 17 trial divisions?

Or $s = \operatorname{lcm}\{1, 2, 3, 4, \ldots, 1000\}$:
using 1438 squarings mod n
find 180121 of the primes $\le 10^7$.

Is a squaring mod n
faster than 125 trial divisions?

Extra benefit:
no need to store the primes.

Plausible conjecture: if K is
$\exp\sqrt{\left(\frac{1}{2} + o(1)\right)\log H \log\log H}$
then $p-1$ divides $\operatorname{lcm}\{1, 2, \ldots, K\}$
for $H/K^{1+o(1)}$ primes $p \le H$.
Same if $p - 1$ is replaced by
order of 2 in $\mathbf{F}_p^*$.

So uniform random prime $p \le H$
divides $2^{\operatorname{lcm}\{1,2,\ldots,K\}} - 1$
with probability $1/K^{1+o(1)}$.

$(1.4\ldots + o(1))K$ squarings mod n
produce $2^{\operatorname{lcm}\{1,2,\ldots,K\}} - 1 \bmod n$.

Similar time spent on trial division
finds far fewer primes for large H.

to larger exponent
$\{1, 2, 3, 4, \ldots, 100\}$:
6 squarings mod n
7 of the primes $\le 10^5$.

aring mod n
an 17 trial divisions?

cm$\{1, 2, 3, 4, \ldots, 1000\}$:
38 squarings mod n
121 of the primes $\le 10^7$.

aring mod n
an 125 trial divisions?

enefit:
to store the primes.

Plausible conjecture: if K is
$\exp\sqrt{(\frac{1}{2}+o(1))\log H \log\log H}$
then $p-1$ divides $\mathrm{lcm}\{1, 2, \ldots, K\}$
for $H/K^{1+o(1)}$ primes $p \le H$.
Same if $p-1$ is replaced by
order of 2 in $\mathbf{F}_p^*$.

So uniform random prime $p \le H$
divides $2^{\mathrm{lcm}\{1,2,\ldots,K\}} - 1$
with probability $1/K^{1+o(1)}$.

$(1.4\ldots + o(1))K$ squarings mod n
produce $2^{\mathrm{lcm}\{1,2,\ldots,K\}} - 1 \bmod n$.

Similar time spent on trial division
finds far fewer primes for large H.

The $p+$

(1982 W

Define (
2327925
(3/5, 4/

The inte
is divisib
82 of the
223 of t
455 of t
720 of t
etc.

exponent

$\ldots, 100\}$:

gs mod n

rimes $\leq 10^5$.

n

l divisions?

$, 4, \ldots, 1000\}$:

ngs mod n

e primes $\leq 10^7$.

n

al divisions?

he primes.

Plausible conjecture: if K is
$\exp\sqrt{\left(\frac{1}{2}+o(1)\right)\log H \log\log H}$
then $p-1$ divides $\operatorname{lcm}\{1, 2, \ldots, K\}$
for $H/K^{1+o(1)}$ primes $p \leq H$.
Same if $p-1$ is replaced by
order of 2 in $\mathbf{F}_p^*$.

So uniform random prime $p \leq H$
divides $2^{\operatorname{lcm}\{1,2,\ldots,K\}} - 1$
with probability $1/K^{1+o(1)}$.

$(1.4\ldots + o(1))K$ squarings mod n
produce $2^{\operatorname{lcm}\{1,2,\ldots,K\}} - 1 \bmod n$.

Similar time spent on trial division
finds far fewer primes for large H.

<u>The $p+1$ factoriz</u>

(1982 Williams)

Define $(X, Y) \in \mathbf{Q}$
232792560th mult
$(3/5, 4/5)$ in the g

The integer $S_2 =$
is divisible by
82 of the primes $\leq$
223 of the primes
455 of the primes
720 of the primes
etc.

^{5}.

?

$00\}$:

10^7.

s?

Plausible conjecture: if K is
$\exp\sqrt{\left(\frac{1}{2}+o(1)\right)\log H \log\log H}$
then $p-1$ divides $\operatorname{lcm}\{1,2,\ldots,K\}$
for $H/K^{1+o(1)}$ primes $p \le H$.
Same if $p-1$ is replaced by
order of 2 in $\mathbf{F}_p^*$.

So uniform random prime $p \le H$
divides $2^{\operatorname{lcm}\{1,2,\ldots,K\}}-1$
with probability $1/K^{1+o(1)}$.

$(1.4\ldots+o(1))K$ squarings mod n
produce $2^{\operatorname{lcm}\{1,2,\ldots,K\}}-1 \bmod n$.

Similar time spent on trial division
finds far fewer primes for large H.

The $p+1$ factorization met

(1982 Williams)

Define $(X,Y) \in \mathbf{Q}\times\mathbf{Q}$ as t
232792560th multiple of
$(3/5, 4/5)$ in the group Cloc

The integer $S_2 = 5^{232792560}$
is divisible by
82 of the primes $\le 10^3$;
223 of the primes $\le 10^4$;
455 of the primes $\le 10^5$;
720 of the primes $\le 10^6$;
etc.

Plausible conjecture: if K is $\exp\sqrt{(\frac{1}{2}+o(1))\log H\log\log H}$ then $p-1$ divides $\operatorname{lcm}\{1,2,\ldots,K\}$ for $H/K^{1+o(1)}$ primes $p \le H$.
Same if $p-1$ is replaced by order of 2 in $\mathbf{F}_p^*$.

So uniform random prime $p \le H$ divides $2^{\operatorname{lcm}\{1,2,\ldots,K\}}-1$ with probability $1/K^{1+o(1)}$.

$(1.4\ldots+o(1))K$ squarings mod n produce $2^{\operatorname{lcm}\{1,2,\ldots,K\}}-1 \bmod n$.

Similar time spent on trial division finds far fewer primes for large H.

The $p+1$ factorization method

(1982 Williams)

Define $(X,Y) \in \mathbf{Q}\times\mathbf{Q}$ as the 232792560th multiple of $(3/5,4/5)$ in the group $\mathrm{Clock}(\mathbf{Q})$.

The integer $S_2 = 5^{232792560}X$ is divisible by
82 of the primes $\le 10^3$;
223 of the primes $\le 10^4$;
455 of the primes $\le 10^5$;
720 of the primes $\le 10^6$;
etc.

e conjecture: if K is

$_2 + o(1)\big)\log H \log\log H$

1 divides $\operatorname{lcm}\{1, 2, \ldots, K\}$

$^{1+o(1)}$ primes $p \le H$.

$p-1$ is replaced by

2 in $\mathbf{F}_p^*$.

rm random prime $p \le H$

$2^{\operatorname{lcm}\{1,2,\ldots,K\}} - 1$

bability $1/K^{1+o(1)}$.

$+\, o(1))K$ squarings mod n

$2^{\operatorname{lcm}\{1,2,\ldots,K\}} - 1 \bmod n$.

time spent on trial division

fewer primes for large H.

The $p+1$ factorization method

(1982 Williams)

Define $(X, Y) \in \mathbf{Q} \times \mathbf{Q}$ as the 232792560th multiple of $(3/5, 4/5)$ in the group $\text{Clock}(\mathbf{Q})$.

The integer $S_2 = 5^{232792560} X$ is divisible by
82 of the primes $\le 10^3$;
223 of the primes $\le 10^4$;
455 of the primes $\le 10^5$;
720 of the primes $\le 10^6$;
etc.

Given ar

compute

and com

hoping t

Many p'

are foun

If -1 is

and $p +$

then 5^{23}

Proof: p

so $(4/5$

so $(p +$

in the gr

so 2327

re: if K is

og $H \log\log H$

lcm$\{1, 2, \ldots, K\}$

mes $p \le H$.

eplaced by

m prime $p \le H$

$K\} - 1$

$/K^{1+o(1)}$.

squarings mod n

$,K\} - 1 \bmod n$.

on trial division

mes for large H.

The $p+1$ factorization method

(1982 Williams)

Define $(X, Y) \in \mathbf{Q} \times \mathbf{Q}$ as the 232792560th multiple of $(3/5, 4/5)$ in the group Clock($\mathbf{Q}$).

The integer $S_2 = 5^{232792560} X$ is divisible by
82 of the primes $\le 10^3$;
223 of the primes $\le 10^4$;
455 of the primes $\le 10^5$;
720 of the primes $\le 10^6$;
etc.

Given an integer n

compute $5^{23279256}$

and compute gcd

hoping to factor n

Many p's not foun

are found by Clock

If -1 is not a squa

and $p+1$ divides

then $5^{232792560} X$ r

Proof: $p \equiv 3 \quad$ (m

so $(4/5 + 3i/5)^p$ =

so $(p+1)(3/5, 4/$

in the group Clock

so $232792560(3/5$

g H

$\ldots, K\}$

H.

$\leq H$

mod n

od n.

ivision

ge H.

The $p+1$ factorization method

(1982 Williams)

Define $(X, Y) \in \mathbf{Q} \times \mathbf{Q}$ as the 232792560th multiple of $(3/5, 4/5)$ in the group Clock($\mathbf{Q}$).

The integer $S_2 = 5^{232792560} X$ is divisible by
82 of the primes $\leq 10^3$;
223 of the primes $\leq 10^4$;
455 of the primes $\leq 10^5$;
720 of the primes $\leq 10^6$;
etc.

Given an integer n, compute $5^{232792560} X \bmod n$ and compute gcd with n, hoping to factor n.

Many p's not found by $\mathbf{F}_p^*$ are found by Clock($\mathbf{F}_p$).

If -1 is not a square mod p and $p+1$ divides 23279256 then $5^{232792560} X \bmod p = 0$

Proof: $p \equiv 3 \pmod 4$,
so $(4/5 + 3i/5)^p = 4/5 - 3$
so $(p+1)(3/5, 4/5) = (0, 1$
in the group Clock($\mathbf{F}_p$),
so $232792560(3/5, 4/5) = ($

The $p+1$ factorization method

(1982 Williams)

Define $(X, Y) \in \mathbf{Q} \times \mathbf{Q}$ as the 232792560th multiple of $(3/5, 4/5)$ in the group $\text{Clock}(\mathbf{Q})$.

The integer $S_2 = 5^{232792560} X$ is divisible by
82 of the primes $\le 10^3$;
223 of the primes $\le 10^4$;
455 of the primes $\le 10^5$;
720 of the primes $\le 10^6$;
etc.

Given an integer n, compute $5^{232792560} X \bmod n$ and compute gcd with n, hoping to factor n.

Many p's not found by $\mathbf{F}_p^*$ are found by $\text{Clock}(\mathbf{F}_p)$.

If -1 is not a square mod p and $p+1$ divides 232792560 then $5^{232792560} X \bmod p = 0$.

Proof: $p \equiv 3 \pmod 4$,
so $(4/5 + 3i/5)^p = 4/5 - 3i/5$,
so $(p+1)(3/5, 4/5) = (0, 1)$
in the group $\text{Clock}(\mathbf{F}_p)$,
so $232792560(3/5, 4/5) = (0, 1)$.

1 factorization method

Villiams)

$X, Y) \in \mathbf{Q} \times \mathbf{Q}$ as the

60th multiple of

5) in the group Clock($\mathbf{Q}$).

eger $S_2 = 5^{232792560} X$

ble by

e primes $\leq 10^3$;

he primes $\leq 10^4$;

he primes $\leq 10^5$;

he primes $\leq 10^6$;

Given an integer n, compute $5^{232792560} X \bmod n$ and compute gcd with n, hoping to factor n.

Many p's not found by $\mathbf{F}_p^*$ are found by Clock($\mathbf{F}_p$).

If -1 is not a square mod p and $p + 1$ divides 232792560 then $5^{232792560} X \bmod p = 0$.

Proof: $p \equiv 3 \pmod 4$, so $(4/5 + 3i/5)^p = 4/5 - 3i/5$, so $(p + 1)(3/5, 4/5) = (0, 1)$ in the group Clock($\mathbf{F}_p$), so $232792560(3/5, 4/5) = (0, 1)$.

The ellip

Replace

a rando

Order of

$\in [p + 1$

If a curv

Good ne

All prim

seem to

reasonab

Time su

ation method

$\times$ **Q** as the

iple of

roup Clock(**Q**).

$5^{232792560}X$

$\leq 10^3$;

$\leq 10^4$;

$\leq 10^5$;

$\leq 10^6$;

Given an integer n, compute $5^{232792560}X \bmod n$ and compute gcd with n, hoping to factor n.

Many p's not found by $\mathbf{F}_p^*$ are found by Clock($\mathbf{F}_p$).

If -1 is not a square mod p and $p+1$ divides 232792560 then $5^{232792560}X \bmod p = 0$.

Proof: $p \equiv 3 \pmod 4$,
so $(4/5 + 3i/5)^p = 4/5 - 3i/5$,
so $(p+1)(3/5, 4/5) = (0, 1)$
in the group Clock($\mathbf{F}_p$),
so $232792560(3/5, 4/5) = (0, 1)$.

The elliptic-curve

Replace clock grou
a random elliptic c

Order of elliptic-cu
$\in [p + 1 - 2\sqrt{p}, p$
If a curve fails, try

Good news (for th
All primes $\leq H$
seem to be found
reasonable numbe
Time subexponent

hod

he

$\text{ck}(\mathbf{Q})$.

X

Given an integer n,
compute $5^{232792560}X \bmod n$
and compute gcd with n,
hoping to factor n.

Many p's not found by $\mathbf{F}_p^*$
are found by $\text{Clock}(\mathbf{F}_p)$.

If -1 is not a square mod p
and $p+1$ divides 232792560
then $5^{232792560}X \bmod p = 0$.

Proof: $p \equiv 3 \pmod 4$,
so $(4/5+3i/5)^p = 4/5-3i/5$,
so $(p+1)(3/5,4/5) = (0,1)$
in the group $\text{Clock}(\mathbf{F}_p)$,
so $232792560(3/5,4/5) = (0,1)$.

The elliptic-curve method

Replace clock group with
a random elliptic curve.

Order of elliptic-curve group
$\in [p+1-2\sqrt{p}, p+1+2\sqrt{}$
If a curve fails, try another.

Good news (for the attacker
All primes $\le H$
seem to be found after a
reasonable number of curves
Time subexponential in H.

Given an integer n,
compute $5^{232792560}X \bmod n$
and compute gcd with n,
hoping to factor n.

Many p's not found by $\mathbf{F}_p^*$
are found by Clock($\mathbf{F}_p$).

If -1 is not a square mod p
and $p+1$ divides 232792560
then $5^{232792560}X \bmod p = 0$.

Proof: $p \equiv 3 \pmod 4$,
so $(4/5 + 3i/5)^p = 4/5 - 3i/5$,
so $(p+1)(3/5, 4/5) = (0, 1)$
in the group Clock($\mathbf{F}_p$),
so $232792560(3/5, 4/5) = (0, 1)$.

The elliptic-curve method

Replace clock group with
a random elliptic curve.

Order of elliptic-curve group
$\in [p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}]$.
If a curve fails, try another.

Good news (for the attacker):
All primes $\le H$
seem to be found after a
reasonable number of curves.
Time subexponential in H.

n integer n,
e $5^{232792560}X$ mod n
npute gcd with n,
to factor n.

s not found by $\mathbf{F}_p^*$
d by Clock($\mathbf{F}_p$).

not a square mod p
1 divides 232792560
$^{2792560}X \bmod p = 0$.

$p \equiv 3 \pmod 4$,
$+ 3i/5)^p = 4/5 - 3i/5$,
$1)(3/5, 4/5) = (0, 1)$
roup Clock($\mathbf{F}_p$),
$92560(3/5, 4/5) = (0, 1)$.

The elliptic-curve method

Replace clock group with a random elliptic curve.

Order of elliptic-curve group $\in [p+1-2\sqrt{p}, p+1+2\sqrt{p}]$. If a curve fails, try another.

Good news (for the attacker): *All* primes $\leq H$ seem to be found after a reasonable number of curves. Time subexponential in H.

More rea

eecm.cr

cr.yp.t

smartfa
"Factori
certified
Coppers

eprint.
"A kilob
logarithr

eprint.
"Compu
applicati
[lattice-b

n,

$^0X \bmod n$

with n,

.

nd by $\mathbf{F}_p^*$

$(\mathbf{F}_p)$.

are mod p

232792560

mod $p = 0$.

od 4),

$= 4/5 - 3i/5$,

$5) = (0, 1)$

$(\mathbf{F}_p)$,

$, 4/5) = (0, 1)$.

The elliptic-curve method

Replace clock group with a random elliptic curve.

Order of elliptic-curve group $\in [p+1-2\sqrt{p}, p+1+2\sqrt{p}]$. If a curve fails, try another.

Good news (for the attacker): *All* primes $\leq H$ seem to be found after a reasonable number of curves. Time subexponential in H.

More reading

eecm.cr.yp.to

cr.yp.to/papers

smartfacts.cr.y

"Factoring RSA ke

certified smart car

Coppersmith in th

eprint.iacr.org

"A kilobit hidden S

logarithm computa

eprint.iacr.org

"Computing gener

application to cryp

[lattice-based] FHE

n

0

.

$i/5$,

)

$0, 1)$.

The elliptic-curve method

Replace clock group with a random elliptic curve.

Order of elliptic-curve group $\in [p+1-2\sqrt{p}, p+1+2\sqrt{p}]$.
If a curve fails, try another.

Good news (for the attacker):
All primes $\leq H$
seem to be found after a reasonable number of curves.
Time subexponential in H.

More reading

`eecm.cr.yp.to`

`cr.yp.to/papers.html#ba`

`smartfacts.cr.yp.to`
"Factoring RSA keys from certified smart cards: Coppersmith in the wild"

`eprint.iacr.org/2016/96`
"A kilobit hidden SNFS disc logarithm computation"

`eprint.iacr.org/2017/14`
"Computing generator . . . a application to cryptanalysis [lattice-based] FHE scheme"

The elliptic-curve method

Replace clock group with a random elliptic curve.

Order of elliptic-curve group $\in [p+1-2\sqrt{p}, p+1+2\sqrt{p}]$. If a curve fails, try another.

Good news (for the attacker): *All* primes $\le H$ seem to be found after a reasonable number of curves. Time subexponential in H.

More reading

`eecm.cr.yp.to`

`cr.yp.to/papers.html#batchnfs`

`smartfacts.cr.yp.to`
"Factoring RSA keys from certified smart cards: Coppersmith in the wild"

`eprint.iacr.org/2016/961`
"A kilobit hidden SNFS discrete logarithm computation"

`eprint.iacr.org/2017/142`
"Computing generator . . . and application to cryptanalysis of a [lattice-based] FHE scheme"