Discrete-log attacks
and factorization
Part II

Tanja Lange
Technische Universiteit Eindhoven

14 June 2019

with some slides by
Daniel J. Bernstein

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.

-log attacks
orization

ange
che Universiteit Eindhoven

2019

ne slides by
. Bernstein

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.

Q sieve

Sieving
using pri

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

etc.

ks

siteit Eindhoven

y

n

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.

Q sieve

Sieving i and 611
using primes $2, 3, 5$

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

etc.

hoven

Q sieve

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

i								
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.

Q sieve

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

i								
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	

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

etc.

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.

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.

small integers $i > 0$
imes $2, 3, 5, 7$:

	5
	7
3	
	5
	7
	5
3	
	5

$\mathbf{Q}$ 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 co
the “cor
for some

$14 \cdot 625$

$64 \cdot 675$

$75 \cdot 686$

$14 \cdot 64 \cdot$
$= 2^8 3^4 5$

$\gcd\{611$
$= 47.$

$611 = 4$

gers $i > 0$

5, 7:

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.

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

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

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

$14 \cdot 64 \cdot 75 \cdot 625 \cdot$ 6

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

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

$= 47.$

$611 = 47 \cdot 13.$

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
the “congruences” $i(611 +$
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

No.

By const

where s

and $t =$

So each

divides e

Not terr

(but not

that one

and the

$+ \, i$ 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

$\gcd\{611, \text{random}\}$

No.

By construction 61

where $s = 14 \cdot 64$

and $t = 2^4 3^2 5^4 7^2$.

So each prime > 7

divides either $s -$

Not terribly surpris

(but not guarantee

that one prime div

and the other divi

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

No.

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

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

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

Yes. The
$(1, 0, 4, 1$
happene

But we c
Given lo
easily fir
with sum

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

Yes. The exponen
$(1, 0, 4, 1), (6, 3, 2,$
happened to have

But we didn't need
Given long sequen
easily find nonemp
with sum 0 mod 2

of

f)

$5^4 7^2\}$

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?

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

But we didn't need this luck
Given long sequence of vect
easily find nonempty subseq
with 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!)
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
Guarante
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 find
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 $\mathbf{F}$
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 $n = 671$:

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

$\mathbf{F}_2$-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.

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 $n = 671$:

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

$\mathbf{F}_2$-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
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,
oty 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 parar

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

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 $n = 671$:

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

$\mathbf{F}_2$-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: $\mathbf{Q}$ 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 $t = \sqrt{\prod_{i \in I} i(n\ \cdots}$

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 $\leq y$.

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

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: $\mathbf{Q}$ 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 $\leq y$.

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 larg
for this t

Uniform
has $n^{1/u}$
roughly

Plausible
$\mathbf{Q}$ sieve
with $y =$
for all n
here $o(1$

bra 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: $\mathbf{Q}$ 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 $\leq y$.

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
$\mathbf{Q}$ 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: $\mathbf{Q}$ 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 [
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 $u \to \infty$.

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

Plausible conjecture:
Q sieve succeeds
with $y = \lfloor n^{1/u} \rfloor$
for all $n \ge u^{(1+o(1))u^2}$;
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 $\sqrt{(\frac{}{2}}$
conjectu
is $1/y^{c+}$

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

Increasi
increase
reduces
So linea
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
sors

$+ i)$

.

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:
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 $y \in$
$\exp \sqrt{\left(\frac{1}{2c} + o(1)\right) \log n \log lo}$
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 $n \geq u^{(1+o(1))u^2}$;
here $o(1)$ is as $u \to \infty$.

More generally, if $y \in \exp\sqrt{\left(\frac{1}{2c} + o(1)\right)\log n \log\log n}$, 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
$\approx y^2 n$ i

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 $i \le y$
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:
$c+1+o(1)$ =

$)$ 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 c
Choose a "q-subla
arithmetic progres
where q divides ea
e.g. progression q
$2q - (n \bmod q)$, 3
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
s:

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 $q - (n$ mod
$2q - (n \bmod q)$, $3q - (n$ mo
etc.

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

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 $i \le y$,
% 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 997^2
$i \in 8024$

8024
17964
27904

ness chances

ce of $i(n+i)$

vs.

than for $i \approx y$.

$n+i)$ grows.

ysis:

rade, but

for $i \leq y$,

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 $\mathbf{Q}$ 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

$-i)$

$i \approx y$.

ows.

,

.

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	31415926535897932
2	31415926535897932
3	31415926535897932

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

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

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

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 $\mathbf{Q}$ 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 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 **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	$(n+i)/997^2$
458	316052737309
467	316052737310
476	316052737311

Crude analysis: Sublattices eliminate the growth problem. Have practically unlimited supply of generalized congruences $(q-(n \bmod q))\dfrac{n+q-(n \bmod q)}{q}$ 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

"MPQS"

using su

But still

"Numbe

achieves

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

"MPQS" improves

using sublattices:

But still $\approx n^{1/2}$.

"Number-field siev

achieves $n^{o(1)}$.

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.

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

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

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 $i(n+i)$.

"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

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

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 $\mathbf{Q}$ s

the num

Recall h

factors 6

Form a s

as produ

for sever

14(625)

$= 4410$

gcd{611

$= 47$.

ublattices

wth 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 $\mathbf{Q}$ sieve is a s

the number-field s

Recall how the $\mathbf{Q}$

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 $n^{o(1)}$.

<u>Generalizing beyond **Q**</u>

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

er-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
$(-11 +$
$\cdot (3$
$= (112$

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

vements

ynomial $i(n+i)$.

(QS) uses

$\overline{n}$;

$^{/2+o(1)}$,

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 $\mathbf{Q}$

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 follows:

Form a square
as product of $(i + 25j)(i +$
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
$s = (-11 + 3 \cdot 25) \cdot (3 + 25$
$t = 112 - 16 \cdot 25$,
$\gcd\{611, s - t\} = 13$.

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 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 $\mathbf{Q}$

sieve is a special case of
ber-field sieve.

ow the $\mathbf{Q}$ sieve
611:

square
uct of $i(i+611j)$
ral pairs (i,j):
$\cdot\, 64(675)\cdot 75(686)$
000^2.

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

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):

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

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 25^2

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

i.e. $s^2 =$

Unsurpri

nd $\mathbf{Q}$

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):

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

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

Why does this work?

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

Apply ring morphism to squa
$(-11 + 3 \cdot 25)(-11 + 3 \cdot 25$
$\quad \cdot (3 + 25)(3 + 25)$
$= (112 - 16 \cdot 25)^2$ 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 $r \in$

Then f_d

monic g

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

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 $d=\deg f$,

$f\;=f_dx^d+\cdots+$

Can take $f_d=1$ f

but larger f_d allow

better parameter s

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

Then f_dr is a root

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

$\mathbf{Q}(r)\leftarrow\mathcal{O}\leftarrow\mathbf{Z}[f_dr]$

$\sqrt{14}j\,)$

$)$

$),$

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:
$(-11 + 3 \cdot 25)(-11 + 3 \cdot 25)$
$\quad \cdot (3 + 25)(3 + 25)$
$= (112 - 16 \cdot 25)^2$ 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 $r \in \mathbf{C}$, root of f.
Then $f_d r$ is a root of
monic $g = f_d^{d-1} f(x/f_d) \in \mathbf{Z}$

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

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

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

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

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

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 $\mathbf{Q}(r)$;

rk?

g morphism

$\sqrt{14} \mapsto 25$,

$\mathbf{Z}/611$.

sm to square:

$1 + 3 \cdot 25)$

$+ 25)$

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

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

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

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

Say we have a squ
$\prod_{(i,j) \in S} (i - j\, m)($
in $\mathbf{Q}(r)$; now what

m

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

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

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

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
$\prod_{(i,j) \in S} (i - jm)(i - jr)$
in $\mathbf{Q}(r)$; 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 $r \in \mathbf{C}$, root of f. Then $f_d r$ is a root of monic $g = f_d^{d-1} f(x/f_d) \in \mathbf{Z}[x]$.

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

Build square in $\mathbf{Q}(r)$ from congruences $(i - jm)(i - jr)$ 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 $\prod_{(i,j) \in S} (i - jm)(i - jr)$ in $\mathbf{Q}(r)$; 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.
r is a root of
$= f_d^{d-1} f(x/f_d) \in \mathbf{Z}[x]$.

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

Build square in $\mathbf{Q}(r)$ from
congruences $(i - jm)(i - jr)$
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
$\prod_{(i,j) \in S} (i - jm)(i - jr)$
in $\mathbf{Q}(r)$; now what?

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

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

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

$x^2 - 14, 25)$

ed $f \in \mathbf{Z}[x]$,

$\mathbf{Z}$.

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

or simplicity,

vs

selection.

of f.

t of

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

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

Build square in $\mathbf{Q}(r)$ from congruences $(i - jm)(i - jr)$ 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 $\prod_{(i,j) \in S} (i - jm)(i - jr)$ in $\mathbf{Q}(r)$; now what?

$\prod (i - jm)(i - jr$

is a square in $\mathcal{O}$,

ring of integers of

Multiply by $g'(f_d r$

putting square roo

compute r with r^2

$\prod (i - jm)(i - jr$

Then apply the rin

$\varphi : \mathbf{Z}[f_d r] \to \mathbf{Z}/n$

$f_d r$ 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 $\mathbf{Q}(r)$ from congruences $(i - jm)(i - jr)$ 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 $\prod_{(i,j)\in S}(i - jm)(i - jr)$ in $\mathbf{Q}(r)$; now what?

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

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

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

Build square in $\mathbf{Q}(r)$ from congruences $(i - j\,m)(i - j\,r)$ 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 $\prod_{(i,j)\in S}(i - j\,m)(i - j\,r)$ in $\mathbf{Q}(r)$; now what?

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

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

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

uare in $\mathbf{Q}(r)$ from
nces $(i - j\,m)(i - j\,r)$
$+\,j\mathbf{Z} = \mathbf{Z}$ 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
$_{}(i - j\,m)(i - j\,r)$
now what?

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

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

Then apply the ring morphism
$\varphi : \mathbf{Z}[f_d r] \to \mathbf{Z}/n$ taking
$f_d r$ 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
$f_d i^d + \cdot$
Norm co
Here "y
"has no

Find enc
Perform
exponen

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

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

are
$(i - j\,r)$
t?

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

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

Then apply the ring morphism
$\varphi : \mathbf{Z}[f_d r] \to \mathbf{Z}/n$ taking
$f_d r$ 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(
$f_d i^d + \cdots + f_0 j^d$
Norm covers all d
Here "y-smooth"
"has no prime divi

Find enough smoo
Perform linear alge
exponent vectors

$r)$

0.

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

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

Then apply the ring morphism
$\varphi : \mathbf{Z}[f_d r] \to \mathbf{Z}/n$ taking
$f_d r$ 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 square product
of congruences $(i - j\,m)(i -$

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

Look for y-smooth congruen
y-smooth $i - j\,m$ and
y-smooth $f_d$norm$(i - j\,r) =$
$f_d i^d + \cdots + f_0 j^d = j^d f(i/j$
Norm covers all d roots r.
Here "y-smooth" means
"has no prime divisor $> y$."

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

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

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

Then apply the ring morphism
$\varphi : \mathbf{Z}[f_d r] \to \mathbf{Z}/n$ taking
$f_d r$ 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 $(i - jm)(i - jr)$?

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

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

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

$m)(i - j\,r)f_d^2$

are in $\mathcal{O}$,

ntegers of $\mathbf{Q}(r)$.

by $g'(f_d r)^2$,

square root into $\mathbf{Z}[f_d r]$:

e r with $r^2 = g'(f_d r)^2$.

$m)(i - j\,r)f_d^2$.

ply the ring morphism

$r] \to \mathbf{Z}/n$ taking

$_d m$. 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 $(i - j\,m)(i - j\,r)$?

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

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

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

Polynom

Many f'

How to

minimize

General

Enumera

For each

informat

distribut

distribut

$)f_d^2$

$\mathbf{Q}(r)$.

$)^2$,

t into $\mathbf{Z}[f_d r]$:

$^2 = g'(f_d r)^2$.

$)f_d^2$.

ng morphism

taking

pute gcd$\{n$,

$(i - j\,m)f_d\}$.

$^2 =$

$m)^2 f_d^2$.

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

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

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

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

Polynomial selecti

Many f's possible

How to find f tha
minimizes NFS tin

General strategy:
Enumerate many
For each f, estima
information about
distribution of j^{deg}
distribution of smo

$_d r]$:
$)^2$.

sm

n,

$f_d\}$.

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

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

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

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

Polynomial selection

Many f's possible for n.
How to find f that
minimizes NFS time?

General strategy:
Enumerate many f's.
For each f, estimate time us
information about f arithme
distribution of $j^{\deg f} f(i/j)$,
distribution of smooth numb

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

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

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

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

Polynomial selection

Many f's possible for n.
How to find f that minimizes NFS time?

General strategy:
Enumerate many f's.
For each f, estimate time using information about f arithmetic, distribution of $j^{\deg f} f(i/j)$, distribution of smooth numbers.

find square product
uences $(i - jm)(i - jr)$?

th congruences for,
pairs (i, j).

y-smooth congruences:
h $i - jm$ and
h $f_d$norm$(i - jr) =$
$\cdots + f_0 j^d = j^d f(i/j)$.
overs all d roots r.
-smooth" means
prime divisor $> y$."

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

Polynomial selection

Many f's possible for n.
How to find f that
minimizes NFS time?

General strategy:
Enumerate many f's.
For each f, estimate time using
information about f arithmetic,
distribution of $j^{\deg f} f(i/j)$,
distribution of smooth numbers.

Let's res
$(x - m)$

Take m
Expand
$n = f_5 n$
Can use

Have f_5
Typically
are on s

(1993 B

e product

$-jm)(i-jr)$?

ences for,

).

n congruences:

and

$(i-jr) =$

$= j^d f(i/j)$.

roots r.

means

sor $> y$."

oth congruences.

ebra on

mod 2.

Polynomial selection

Many f's possible for n.

How to find f that

minimizes NFS time?

General strategy:

Enumerate many f's.

For each f, estimate time using

information about f arithmetic,

distribution of $j^{\deg f} f(i/j)$,

distribution of smooth numbers.

Let's restrict atten

$(x - m)(f_5 x^5 + f$

Take m near $n^{1/6}$

Expand n in base

$n = f_5 m^5 + f_4 m^4$

Can use negative c

Have $f_5 \approx n^{1/6}$.

Typically all the f_i

are on scale of $n^{1/}$

(1993 Buhler Lens

$- j r)$?

nces:

$)$.

ences.

Polynomial selection

Many f's possible for n.
How to find f that minimizes NFS time?

General strategy:
Enumerate many f's.
For each f, estimate time using information about f arithmetic, distribution of $j^{\deg f} f(i/j)$, distribution of smooth numbers.

Let's restrict attention to $f($
$(x - m)(f_5 x^5 + f_4 x^4 + \cdots$

Take m near $n^{1/6}$.
Expand n in base m:
$n = f_5 m^5 + f_4 m^4 + \cdots + f$
Can use negative coefficients

Have $f_5 \approx n^{1/6}$.
Typically all the f_i's are on scale of $n^{1/6}$.

(1993 Buhler Lenstra Pomer

Polynomial selection

Many f's possible for n.
How to find f that minimizes NFS time?

General strategy:
Enumerate many f's.
For each f, estimate time using information about f arithmetic, distribution of $j^{\deg f} f(i/j)$, distribution of smooth numbers.

Let's restrict attention to $f(x) = (x - m)(f_5 x^5 + f_4 x^4 + \cdots + f_0)$.

Take m near $n^{1/6}$.
Expand n in base m:
$n = f_5 m^5 + f_4 m^4 + \cdots + f_0$.
Can use negative coefficients.

Have $f_5 \approx n^{1/6}$.
Typically all the f_i's are on scale of $n^{1/6}$.

(1993 Buhler Lenstra Pomerance)

nial selection

's possible for n.
find f that
es NFS time?

strategy:
ate many f's.
f, estimate time using
tion about f arithmetic,
ion of $j^{\deg f} f(i/j)$,
ion of smooth numbers.

Let's restrict attention to $f(x) = (x - m)(f_5 x^5 + f_4 x^4 + \cdots + f_0)$.

Take m near $n^{1/6}$.
Expand n in base m:
$n = f_5 m^5 + f_4 m^4 + \cdots + f_0$.
Can use negative coefficients.

Have $f_5 \approx n^{1/6}$.
Typically all the f_i's
are on scale of $n^{1/6}$.

(1993 Buhler Lenstra Pomerance)

To reduc

Enumera
for m ne

Have f_5
f_4, f_3, f_2
as large
Hope th
on scale

Conjectu
within ro
Then $(i$
is on sca
for i, j c
Several r

on

for n.

t

ne?

f's.

ate time using

f arithmetic,

$^{g f} f(i/j)$,

ooth numbers.

Let's restrict attention to $f(x) = (x - m)(f_5 x^5 + f_4 x^4 + \cdots + f_0)$.

Take m near $n^{1/6}$.
Expand n in base m:
$n = f_5 m^5 + f_4 m^4 + \cdots + f_0$.
Can use negative coefficients.

Have $f_5 \approx n^{1/6}$.
Typically all the f_i's
are on scale of $n^{1/6}$.

(1993 Buhler Lenstra Pomerance)

To reduce f value

Enumerate many p
for m near $B^{0.25} n$

Have $f_5 \approx B^{-1.25}$
f_4, f_3, f_2, f_1, f_0 co
as large as $B^{0.25} n$
Hope that they ar
on scale of $B^{-1.25}$

Conjecturally this
within roughly B^{7}
Then $(i - jm)(f_5$
is on scale of B^{-1}
for i, j on scale of
Several more ways

sing
etic,

pers.

Let's restrict attention to $f(x) = (x - m)(f_5x^5 + f_4x^4 + \cdots + f_0)$.

Take m near $n^{1/6}$.
Expand n in base m:
$n = f_5m^5 + f_4m^4 + \cdots + f_0$.
Can use negative coefficients.

Have $f_5 \approx n^{1/6}$.
Typically all the f_i's
are on scale of $n^{1/6}$.

(1993 Buhler Lenstra Pomerance)

To reduce f values by factor

Enumerate many possibilitie
for m near $B^{0.25}n^{1/6}$.

Have $f_5 \approx B^{-1.25}n^{1/6}$.
f_4, f_3, f_2, f_1, f_0 could be
as large as $B^{0.25}n^{1/6}$.
Hope that they are smaller,
on scale of $B^{-1.25}n^{1/6}$.

Conjecturally this happens
within roughly $B^{7.5}$ trials.
Then $(i - jm)(f_5i^5 + \cdots +$
is on scale of $B^{-1}R^6n^{2/6}$
for i, j on scale of R.
Several more ways; depends

Let's restrict attention to $f(x) = (x - m)(f_5 x^5 + f_4 x^4 + \cdots + f_0)$.

Take m near $n^{1/6}$.
Expand n in base m:
$n = f_5 m^5 + f_4 m^4 + \cdots + f_0$.
Can use negative coefficients.

Have $f_5 \approx n^{1/6}$.
Typically all the f_i's
are on scale of $n^{1/6}$.

(1993 Buhler Lenstra Pomerance)

To reduce f values by factor B:

Enumerate many possibilities
for m near $B^{0.25} n^{1/6}$.

Have $f_5 \approx B^{-1.25} n^{1/6}$.
f_4, f_3, f_2, f_1, f_0 could be
as large as $B^{0.25} n^{1/6}$.
Hope that they are smaller,
on scale of $B^{-1.25} n^{1/6}$.

Conjecturally this happens
within roughly $B^{7.5}$ trials.
Then $(i - jm)(f_5 i^5 + \cdots + f_0 j^5)$
is on scale of $B^{-1} R^6 n^{2/6}$
for i, j on scale of R.
Several more ways; depends on n.

strict attention to $f(x) =$
$(f_5 x^5 + f_4 x^4 + \cdots + f_0)$.

near $n^{1/6}$.

n in base m:
$n^5 + f_4 m^4 + \cdots + f_0$.
negative coefficients.

$\approx n^{1/6}$.
all the f_i's
cale of $n^{1/6}$.

uhler Lenstra Pomerance)

To reduce f values by factor B:

Enumerate many possibilities
for m near $B^{0.25} n^{1/6}$.

Have $f_5 \approx B^{-1.25} n^{1/6}$.
f_4, f_3, f_2, f_1, f_0 could be
as large as $B^{0.25} n^{1/6}$.
Hope that they are smaller,
on scale of $B^{-1.25} n^{1/6}$.

Conjecturally this happens
within roughly $B^{7.5}$ trials.
Then $(i - jm)(f_5 i^5 + \cdots + f_0 j^5)$
is on scale of $B^{-1} R^6 n^{2/6}$
for i, j on scale of R.
Several more ways; depends on n.

Asympto

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

What ar

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

ntion to $f(x) =$
$_4 x^4 + \cdots + f_0)$.

.

m:
$^4 + \cdots + f_0$.
coefficients.

$_j$'s
$/6$.

stra Pomerance)

To reduce f values by factor B:

Enumerate many possibilities for m near $B^{0.25} n^{1/6}$.

Have $f_5 \approx B^{-1.25} n^{1/6}$.
f_4, f_3, f_2, f_1, f_0 could be as large as $B^{0.25} n^{1/6}$.
Hope that they are smaller, on scale of $B^{-1.25} n^{1/6}$.

Conjecturally this happens within roughly $B^{7.5}$ trials.
Then $(i - j\,m)(f_5 i^5 + \cdots + f_0 j^5)$ is on scale of $B^{-1} R^6 n^{2/6}$ for i, j on scale of R.
Several more ways; depends on n.

<u>Asymptotic cost e</u>

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

$(x) =$

$+ f_0)$.

f_0.

s.

rance)

To reduce f values by factor B:

Enumerate many possibilities for m near $B^{0.25} n^{1/6}$.

Have $f_5 \approx B^{-1.25} n^{1/6}$.
f_4, f_3, f_2, f_1, f_0 could be as large as $B^{0.25} n^{1/6}$.
Hope that they are smaller, on scale of $B^{-1.25} n^{1/6}$.

Conjecturally this happens within roughly $B^{7.5}$ trials.
Then $(i - j\,m)(f_5 i^5 + \cdots + f_0 j^5)$ is on scale of $B^{-1} R^6 n^{2/6}$ for i, j on scale of R.
Several more ways; depends on n.

<u>Asymptotic cost exponents</u>

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

To reduce f values by factor B:

Enumerate many possibilities for m near $B^{0.25} n^{1/6}$.

Have $f_5 \approx B^{-1.25} n^{1/6}$.
f_4, f_3, f_2, f_1, f_0 could be as large as $B^{0.25} n^{1/6}$.
Hope that they are smaller, on scale of $B^{-1.25} n^{1/6}$.

Conjecturally this happens within roughly $B^{7.5}$ trials.
Then $(i - j\,m)(f_5 i^5 + \cdots + f_0 j^5)$ is on scale of $B^{-1} R^6 n^{2/6}$ for i, j on scale of R.
Several more ways; depends on n.

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

ce f values by factor B:

ate many possibilities
ear $B^{0.25}n^{1/6}$.

$\approx B^{-1.25}n^{1/6}$.

$_2, f_1, f_0$ could be
as $B^{0.25}n^{1/6}$.

at they are smaller,
of $B^{-1.25}n^{1/6}$.

urally this happens
oughly $B^{7.5}$ trials.

$- j m)(f_5 i^5 + \cdots + f_0 j^5)$
ale of $B^{-1}R^6 n^{2/6}$
on scale of R.

more ways; depends on n.

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 sm
for all co
with $1 \leq$
using pri

$L^{1.90\ldots+}$

Conjectu
smooth

s by factor B:

possibilities

$^{1/6}$.

$n^{1/6}$.

uld be

$^{1/6}$.

e smaller,

$n^{1/6}$.

happens

$^{.5}$ trials.

$i^5 + \cdots + f_0 j^5)$

$R^6 n^{2/6}$

R.

; depends on n.

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 belo
Choose f with so
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

r B:

s

$f_0 j^5)$

on n.

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 sm
test sm
and $i -$
using pr

$L^{1.77\ldots+}$
Each $|j$
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 $i - jr$
and $i - j\beta$ and so on,
using primes $\le L^{0.82\ldots+o(1)}$.

$L^{1.77\ldots+o(1)}$ tests.
Each $|j^d f(i/j)| \le m^{2.86\ldots+}$
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 $i - jr$
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
$_{-1} m^{d-1} + \cdots + f_1 m + f_0$
ch f_k below $n^{(1+o(1))/d}$.
f with some randomness
there are bad f's.

oothness of $i - jm$
oprime 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 $i - jr$
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 $i - j r$
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 $(\log y)^2 \approx \mathrm{l}$
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 $i - jr$
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 $i - jr$
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 $d \log m \approx \log n$.

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

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

$o(1)$ tests.
$^{d}f(i/j)| \leq m^{2.86...+o(1)}$.
urally $L^{0.95...+o(1)}$
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 num
$L^{1.90...+o}$
finding s
$L^{1.77...+o}$
finding s

Many n
$L^{1.90...+o}$
to find s

Oops, li
fix by re
But still
batch in
factoring

umber fields.

m,

f $i - j r$

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 $d \log m \approx \log n$.

Batch NFS

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 algeb
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

og $y)^2 \approx \log m$;

g norms with m

$\log y \approx \log m$;

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.

Asympt

paramet

$d/(\log n$

$\in 1.10$.

Primes $\leq$

$1 \leq i, j$

Comput

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:

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

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

Primes $\leq L^{0.82\ldots+}$

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

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

FS

mber-field sieve used
$^{o(1)}$ bit operations
smooth $i - j\,m$; 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 $i - j\,m$.

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

Batch N

Expand
$n = n_7 n$
with $0 \le$

Assume
$n_7 x^7 +$

Choose
consider
that $-H$
and gcd

Choose
$y = 2^{66}$

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 $i - j m$.

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

Batch NFS for RS

Expand n in base
$n = n_7 m^7 + n_6 m$
with $0 \le n_0, n_1, .$

Assume irreducibil
$n_7 x^7 + n_6 x^6 + \cdot\cdot$

Choose height H
consider pairs $(a,$
that $-H \le a \le H$
and $\gcd\{a, b\} = 1$

Choose smoothnes
$y = 2^{66} + 2^{55}$.

n

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.

Batch NFS for RSA-3072

Expand n in base $m = 2^{384}$
$n = n_7 m^7 + n_6 m^6 + \cdots +$
with $0 \le n_0, n_1, \ldots, n_7 < m$

Assume irreducibility of
$n_7 x^7 + n_6 x^6 + \cdots + n_0$.

Choose height $H = 2^{62} + 2^{61}$
consider pairs $(a, b) \in \mathbf{Z} \times \mathbf{Z}$
that $-H \le a \le H$, $0 < b \le$
and $\gcd\{a, b\} = 1$.

Choose smoothness bound
$y = 2^{66} + 2^{55}$.

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.

Batch NFS for RSA-3072

Expand n in base $m = 2^{384}$:
$n = n_7 m^7 + n_6 m^6 + \cdots + n_0$
with $0 \le n_0, n_1, \ldots, n_7 < m$.

Assume irreducibility of
$n_7 x^7 + n_6 x^6 + \cdots + n_0$.

Choose height $H = 2^{62}+2^{61}+2^{57}$: consider pairs $(a, b) \in \mathbf{Z} \times \mathbf{Z}$ such that $-H \le a \le H$, $0 < b \le H$, and $\gcd\{a, b\} = 1$.

Choose smoothness bound $y = 2^{66} + 2^{55}$.

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 $i - j\,m$.

$o(1)$ operations
target n.

Batch NFS for RSA-3072

Expand n in base $m = 2^{384}$:
$n = n_7 m^7 + n_6 m^6 + \cdots + n_0$
with $0 \leq n_0, n_1, \ldots, n_7 < m$.

Assume irreducibility of
$n_7 x^7 + n_6 x^6 + \cdots + n_0$.

Choose height $H = 2^{62} + 2^{61} + 2^{57}$:
consider pairs $(a, b) \in \mathbf{Z} \times \mathbf{Z}$ such
that $-H \leq a \leq H$, $0 < b \leq H$,
and $\gcd\{a, b\} = 1$.

Choose smoothness bound
$y = 2^{66} + 2^{55}$.

There ar
$12H^2/\pi$
pairs $(a,$

Find all
y-smoot
$c = n_7 a$

Combine
into a fa
if there a

Number
$\approx 2y/$ lo

-NFS

$g\, n)^{-1/3}$

$o(1)$.

$-o(1)$.

pendent of n

$j\, m$.

tions

Batch NFS for RSA-3072

Expand n in base $m = 2^{384}$:
$n = n_7 m^7 + n_6 m^6 + \cdots + n_0$
with $0 \le n_0, n_1, \ldots, n_7 < m$.

Assume irreducibility of
$n_7 x^7 + n_6 x^6 + \cdots + n_0$.

Choose height $H = 2^{62}+2^{61}+2^{57}$:
consider pairs $(a, b) \in \mathbf{Z} \times \mathbf{Z}$ such
that $-H \le a \le H$, $0 < b \le H$,
and $\gcd\{a, b\} = 1$.

Choose smoothness bound
$y = 2^{66} + 2^{55}$.

There are about
$12H^2/\pi^2 \approx 2^{125.5}$
pairs (a, b).

Find all pairs $(a, b$
y-smooth $(a - bm$
$c = n_7 a^7 + n_6 a^6 b$

Combine these con
into a factorization
if there are enough

Number of congru
$\approx 2y/\log y \approx 2^{62.}$

f n

Batch NFS for RSA-3072

Expand n in base $m = 2^{384}$:
$n = n_7 m^7 + n_6 m^6 + \cdots + n_0$
with $0 \le n_0, n_1, \ldots, n_7 < m$.

Assume irreducibility of
$n_7 x^7 + n_6 x^6 + \cdots + n_0$.

Choose height $H = 2^{62}+2^{61}+2^{57}$:
consider pairs $(a, b) \in \mathbf{Z} \times \mathbf{Z}$ such
that $-H \le a \le H$, $0 < b \le H$,
and $\gcd\{a, b\} = 1$.

Choose smoothness bound
$y = 2^{66} + 2^{55}$.

There are about
$12H^2/\pi^2 \approx 2^{125.51}$
pairs (a, b).

Find all pairs (a, b) with
y-smooth $(a - bm)c$ where
$c = n_7 a^7 + n_6 a^6 b + \cdots + n$

Combine these congruences
into a factorization of n,
if there are enough congruen

Number of congruences nee
$\approx 2y/\log y \approx 2^{62.06}$.

Batch NFS for RSA-3072

Expand n in base $m = 2^{384}$:
$n = n_7 m^7 + n_6 m^6 + \cdots + n_0$
with $0 \le n_0, n_1, \ldots, n_7 < m$.

Assume irreducibility of
$n_7 x^7 + n_6 x^6 + \cdots + n_0$.

Choose height $H = 2^{62}+2^{61}+2^{57}$:
consider pairs $(a, b) \in \mathbf{Z} \times \mathbf{Z}$ such
that $-H \le a \le H$, $0 < b \le H$,
and $\gcd\{a, b\} = 1$.

Choose smoothness bound
$y = 2^{66} + 2^{55}$.

There are about
$12H^2/\pi^2 \approx 2^{125.51}$
pairs (a, b).

Find all pairs (a, b) with
y-smooth $(a - bm)c$ where
$c = n_7 a^7 + n_6 a^6 b + \cdots + n_0 b^7$.

Combine these congruences
into a factorization of n,
if there are enough congruences.

Number of congruences needed
$\approx 2y/\log y \approx 2^{62.06}$.

FS for RSA-3072

n in base $m = 2^{384}$:
$m^7 + n_6 m^6 + \cdots + n_0$
$\leq n_0, n_1, \ldots, n_7 < m$.

irreducibility of
$n_6 x^6 + \cdots + n_0$.

height $H = 2^{62}+2^{61}+2^{57}$:
pairs $(a, b) \in \mathbf{Z} \times \mathbf{Z}$ such
$H \leq a \leq H$, $0 < b \leq H$,
$\{a, b\} = 1$.

smoothness bound
$+ 2^{55}$.

There are about
$12H^2/\pi^2 \approx 2^{125.51}$
pairs (a, b).

Find all pairs (a, b) with
y-smooth $(a - bm)c$ where
$c = n_7 a^7 + n_6 a^6 b + \cdots + n_0 b^7$.

Combine these congruences
into a factorization of n,
if there are enough congruences.

Number of congruences needed
$\approx 2y/\log y \approx 2^{62.06}$.

Heuristic
$a - bm$
chance a
integer i
and this
where u

Have u
and u^{-u}
so there
$2^{107.09}$ p
such tha

A-3072

$m = 2^{384}$:

$^{6} + \cdots + n_0$

$\ldots, n_7 < m$.

ity of

$\cdot + n_0$.

$= 2^{62}+2^{61}+2^{57}$:

$b) \in \mathbf{Z} \times \mathbf{Z}$ such

$, 0 < b \le H$,

.

ss bound

There are about
$12H^2/\pi^2 \approx 2^{125.51}$
pairs (a, b).

Find all pairs (a, b) with
y-smooth $(a - bm)c$ where
$c = n_7 a^7 + n_6 a^6 b + \cdots + n_0 b^7$.

Combine these congruences
into a factorization of n,
if there are enough congruences.

Number of congruences needed
$\approx 2y/\log y \approx 2^{62.06}$.

Heuristic approxim
$a - bm$ has same
chance as a unifor
integer in $[1, Hm]$
and this chance is
where $u = (\log(H$

Have $u \approx 6.707$
and $u^{-u} \approx 2^{-18.4}$
so there are about
$2^{107.09}$ pairs (a, b)
such that $a - bm$

:

n_0

n.

${}^1 + 2^{57}$:

Z such

H,

There are about
$12H^2/\pi^2 \approx 2^{125.51}$
pairs (a, b).

Find all pairs (a, b) with
y-smooth $(a - bm)c$ where
$c = n_7 a^7 + n_6 a^6 b + \cdots + n_0 b^7$.

Combine these congruences
into a factorization of n,
if there are enough congruences.

Number of congruences needed
$\approx 2y/\log y \approx 2^{62.06}$.

Heuristic approximation:
$a - bm$ has same y-smooth
chance as a uniform random
integer in $[1, Hm]$,
and this chance is u^{-u}
where $u = (\log(Hm))/\log y$

Have $u \approx 6.707$
and $u^{-u} \approx 2^{-18.42}$,
so there are about
$2^{107.09}$ pairs (a, b)
such that $a - bm$ is smooth

There are about
$12H^2/\pi^2 \approx 2^{125.51}$
pairs (a, b).

Find all pairs (a, b) with
y-smooth $(a - bm)c$ where
$c = n_7 a^7 + n_6 a^6 b + \cdots + n_0 b^7$.

Combine these congruences
into a factorization of n,
if there are enough congruences.

Number of congruences needed
$\approx 2y/\log y \approx 2^{62.06}$.

Heuristic approximation:
$a - bm$ has same y-smoothness
chance as a uniform random
integer in $[1, Hm]$,
and this chance is u^{-u}
where $u = (\log(Hm))/\log y$.

Have $u \approx 6.707$
and $u^{-u} \approx 2^{-18.42}$,
so there are about
$2^{107.09}$ pairs (a, b)
such that $a - bm$ is smooth.

re about
$^2 \approx 2^{125.51}$
b).

pairs (a, b) with
h $(a - bm)c$ where
$^7 + n_6 a^6 b + \cdots + n_0 b^7$.

e these congruences
ctorization of n,
are enough congruences.

of congruences needed
g $y \approx 2^{62.06}$.

Heuristic approximation:
$a - bm$ has same y-smoothness
chance as a uniform random
integer in $[1, Hm]$,
and this chance is u^{-u}
where $u = (\log(Hm))/\log y$.

Have $u \approx 6.707$
and $u^{-u} \approx 2^{-18.42}$,
so there are about
$2^{107.09}$ pairs (a, b)
such that $a - bm$ is smooth.

Heuristic
c has sa
as a unif
$[1, 8H^7 n$
and this
where v

Have v
and v^{-v}
so there
$2^{62.08}$ pa
$a - bm$

Safely al

1

) with

)c where

$+\cdots+n_0b^7$.

ngruences

n of n,

n congruences.

ences needed

06.

Heuristic approximation:

$a-bm$ has same y-smoothness chance as a uniform random integer in $[1,Hm]$, and this chance is u^{-u} where $u=(\log(Hm))/\log y$.

Have $u\approx 6.707$ and $u^{-u}\approx 2^{-18.42}$, so there are about $2^{107.09}$ pairs (a,b) such that $a-bm$ is smooth.

Heuristic approxim

c has same y-smoo

as a uniform rando

$[1,8H^7m]$,

and this chance is

where $v=(\log(8H$

Have $v\approx 12.395$

and $v^{-v}\approx 2^{-45.01}$

so there are about

$2^{62.08}$ pairs (a,b)

$a-bm$ and c are

Safely above $2^{62.0}$

$_0 b^7$.

nces.

ded

Heuristic approximation:

$a - bm$ has same y-smoothness chance as a uniform random integer in $[1, Hm]$,

and this chance is u^{-u} where $u = (\log(Hm))/\log y$.

Have $u \approx 6.707$ and $u^{-u} \approx 2^{-18.42}$, so there are about $2^{107.09}$ pairs (a, b) such that $a - bm$ is smooth.

Heuristic approximation:

c has same y-smoothness ch

as a uniform random integer

$[1, 8H^7 m]$,

and this chance is v^{-v}

where $v = (\log(8H^7 m))/\log$

Have $v \approx 12.395$ and $v^{-v} \approx 2^{-45.01}$, so there are about $2^{62.08}$ pairs (a, b) such that $a - bm$ and c are both smoo

Safely above $2^{62.06}$.

Heuristic approximation:
$a - bm$ has same y-smoothness chance as a uniform random integer in $[1, Hm]$,
and this chance is u^{-u}
where $u = (\log(Hm))/\log y$.

Have $u \approx 6.707$
and $u^{-u} \approx 2^{-18.42}$,
so there are about $2^{107.09}$ pairs (a, b)
such that $a - bm$ is smooth.

Heuristic approximation:
c has same y-smoothness chance as a uniform random integer in $[1, 8H^7m]$,
and this chance is v^{-v}
where $v = (\log(8H^7m))/\log y$.

Have $v \approx 12.395$
and $v^{-v} \approx 2^{-45.01}$,
so there are about $2^{62.08}$ pairs (a, b) such that $a - bm$ and c are both smooth.

Safely above $2^{62.06}$.

c approximation:
has same y-smoothness
as a uniform random
n $[1, Hm]$,
chance is u^{-u}
$= (\log(Hm))/\log y$.

≈ 6.707
$\approx 2^{-18.42}$,
are about
pairs (a, b)
t $a - bm$ is smooth.

Heuristic approximation:
c has same y-smoothness chance
as a uniform random integer in
$[1, 8H^7 m]$,
and this chance is v^{-v}
where $v = (\log(8H^7 m))/\log y$.

Have $v \approx 12.395$
and $v^{-v} \approx 2^{-45.01}$,
so there are about
$2^{62.08}$ pairs (a, b) such that
$a - bm$ and c are both smooth.

Safely above $2^{62.06}$.

Biggest
Check 2
to find t
where a

This ste
reused b

nation:
y-smoothness
m random
,
u^{-u}
$m))/\log y$.

^{2},
:

is smooth.

Heuristic approximation:
c has same y-smoothness chance
as a uniform random integer in
$[1, 8H^7 m]$,
and this chance is v^{-v}
where $v = (\log(8H^7 m))/\log y$.

Have $v \approx 12.395$
and $v^{-v} \approx 2^{-45.01}$,
so there are about
$2^{62.08}$ pairs (a, b) such that
$a - bm$ and c are both smooth.

Safely above $2^{62.06}$.

Biggest step in co
Check $2^{125.51}$ pair
to find the $2^{107.09}$
where $a - bm$ is s

This step is indepe
reused by many in

ness

n

y.

.

Heuristic approximation:
c has same y-smoothness chance
as a uniform random integer in
$[1, 8H^7m]$,
and this chance is v^{-v}
where $v = (\log(8H^7m))/\log y$.

Have $v \approx 12.395$
and $v^{-v} \approx 2^{-45.01}$,
so there are about
$2^{62.08}$ pairs (a, b) such that
$a - bm$ and c are both smooth.

Safely above $2^{62.06}$.

Biggest step in computation
Check $2^{125.51}$ pairs (a, b)
to find the $2^{107.09}$ pairs
where $a - bm$ is smooth.

This step is independent of
reused by many integers N.

Heuristic approximation:
c has same y-smoothness chance as a uniform random integer in $[1, 8H^7 m]$,
and this chance is v^{-v}
where $v = (\log(8H^7 m))/\log y$.

Have $v \approx 12.395$
and $v^{-v} \approx 2^{-45.01}$,
so there are about
$2^{62.08}$ pairs (a, b) such that
$a - bm$ and c are both smooth.

Safely above $2^{62.06}$.

Biggest step in computation:
Check $2^{125.51}$ pairs (a, b)
to find the $2^{107.09}$ pairs
where $a - bm$ is smooth.

This step is independent of N,
reused by many integers N.

Heuristic approximation:
c has same y-smoothness chance as a uniform random integer in $[1, 8H^7m]$,
and this chance is v^{-v} where $v = (\log(8H^7m))/\log y$.

Have $v \approx 12.395$ and $v^{-v} \approx 2^{-45.01}$,
so there are about $2^{62.08}$ pairs (a, b) such that $a - bm$ and c are both smooth.

Safely above $2^{62.06}$.

Biggest step in computation:
Check $2^{125.51}$ pairs (a, b) to find the $2^{107.09}$ pairs where $a - bm$ is smooth.

This step is independent of N, reused by many integers N.

Biggest step depending on N:
Check $2^{107.09}$ pairs (a, b) to see whether c is smooth.

This is much less computation! . . . or is it?

c approximation:
me y-smoothness chance
form random integer in
$m]$,
chance is v^{-v}
$= (\log(8H^7 m))/\log y$.

≈ 12.395
$\approx 2^{-45.01}$,
are about
airs (a, b) such that
and c are both smooth.

bove $2^{62.06}$.

Biggest step in computation:
Check $2^{125.51}$ pairs (a, b)
to find the $2^{107.09}$ pairs
where $a - bm$ is smooth.

This step is independent of N,
reused by many integers N.

Biggest step depending on N:
Check $2^{107.09}$ pairs (a, b)
to see whether c is smooth.

This is much less
computation! . . . or is it?

The 2^{107}
are not
so no ea
for prim

nation:

othness chance

om integer in

v^{-v}

$H^7 m))/\log y$.

^{1},

such that

both smooth.

^{6}.

Biggest step in computation:
Check $2^{125.51}$ pairs (a, b)
to find the $2^{107.09}$ pairs
where $a - bm$ is smooth.

This step is independent of N,
reused by many integers N.

Biggest step depending on N:
Check $2^{107.09}$ pairs (a, b)
to see whether c is smooth.

This is much less
computation! . . . or is it?

The $2^{107.09}$ pairs (

are not consecutiv

so no easy way to

for prime divisors

nance
r in

g y.

oth.

Biggest step in computation:
Check $2^{125.51}$ pairs (a, b)
to find the $2^{107.09}$ pairs
where $a - bm$ is smooth.

This step is independent of N,
reused by many integers N.

Biggest step depending on N:
Check $2^{107.09}$ pairs (a, b)
to see whether c is smooth.

This is much less
computation! . . . or is it?

The $2^{107.09}$ pairs (a, b)
are not consecutive,
so no easy way to sieve
for prime divisors of c.

Biggest step in computation:
Check $2^{125.51}$ pairs (a, b)
to find the $2^{107.09}$ pairs
where $a - bm$ is smooth.

This step is independent of N,
reused by many integers N.

Biggest step depending on N:
Check $2^{107.09}$ pairs (a, b)
to see whether c is smooth.

This is much less
computation! . . . or is it?

The $2^{107.09}$ pairs (a, b)
are not consecutive,
so no easy way to sieve
for prime divisors of c.

Biggest step in computation:
Check $2^{125.51}$ pairs (a, b)
to find the $2^{107.09}$ pairs
where $a - bm$ is smooth.

This step is independent of N,
reused by many integers N.

Biggest step depending on N:
Check $2^{107.09}$ pairs (a, b)
to see whether c is smooth.

This is much less
computation! . . . or is it?

The $2^{107.09}$ pairs (a, b)
are not consecutive,
so no easy way to sieve
for prime divisors of c.

Fix: factor each number
separately:
start with trial division,
then Pollard rho,
then Pollard $p - 1$,
then ECM.

Biggest step in computation:
Check $2^{125.51}$ pairs (a, b)
to find the $2^{107.09}$ pairs
where $a - bm$ is smooth.

This step is independent of N,
reused by many integers N.

Biggest step depending on N:
Check $2^{107.09}$ pairs (a, b)
to see whether c is smooth.

This is much less
computation! . . . or is it?

The $2^{107.09}$ pairs (a, b)
are not consecutive,
so no easy way to sieve
for prime divisors of c.

Fix: factor each number
separately:
start with trial division,
then Pollard rho,
then Pollard $p - 1$,
then ECM.

Most of them covered in
http://facthacks.cr.yp.to/

step in computation:
$^{125.51}$ pairs (a, b)
he $2^{107.09}$ pairs
$- bm$ is smooth.

p is independent of N,
y many integers N.

step depending on N:
$^{107.09}$ pairs (a, b)
hether c is smooth.

much less
ation! . . . or is it?

The $2^{107.09}$ pairs (a, b)
are not consecutive,
so no easy way to sieve
for prime divisors of c.

Fix: factor each number
separately:
start with trial division,
then Pollard rho,
then Pollard $p - 1$,
then ECM.

Most of them covered in
http://facthacks.cr.yp.to/

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

mputation:
s (a, b)
pairs
mooth.

endent of N,
tegers N.

nding on N:
s (a, b)
s smooth.

or is it?

The $2^{107.09}$ pairs (a, b)
are not consecutive,
so no easy way to sieve
for prime divisors of c.

Fix: factor each number
separately:
start with trial division,
then Pollard rho,
then Pollard $p-1$,
then ECM.

Most of them covered in
http://facthacks.cr.yp.to/

The rho method

Define $\rho_0 = 0$, ρ_{k-}

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

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

Compare to $\approx 2^{16}$
for trial division up

:

N,

V:

The $2^{107.09}$ pairs (a, b) are not consecutive, so no easy way to sieve for prime divisors of c.

Fix: factor each number separately: start with trial division, then Pollard rho, then Pollard $p-1$, then ECM.

Most of them covered in http://facthacks.cr.yp.to/

The rho method

Define $\rho_0 = 0$, $\rho_{k+1} = \rho_k^2 +$

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 $\gcd\{c, S\}$ usin
$\approx 2^{14}$ multiplications mod c
very little memory.

Compare to $\approx 2^{16}$ divisions
for trial division up to 2^{20}.

The $2^{107.09}$ pairs (a, b) are not consecutive, so no easy way to sieve for prime divisors of c.

Fix: factor each number separately:
start with trial division,
then Pollard rho,
then Pollard $p-1$,
then ECM.

Most of them covered in http://facthacks.cr.yp.to/

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}.

$^{7.09}$ pairs (a, b)
consecutive,
sy way to sieve
e divisors of c.

tor each number
ly:
th trial division,
llard rho,
llard $p - 1$,
M.

them covered in
acthacks.cr.yp.to/

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 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 $k \in$ (

(a, b)
e,
sieve
of c.

umber

ision,

,

ered in
r.yp.to/

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 $\le y$

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 $k \in (j - i)\mathbf{Z} \cap$

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

Plausible conjecture: $y^{1/2+o}$
so $y^{1/2+o(1)}$ mults mod c.

Reason: Consider first collis
$\rho_1 \bmod p, \rho_2 \bmod p, \ldots$.
If $\rho_i \bmod p = \rho_j \bmod p$
then $\rho_k \bmod p = \rho_{2k} \bmod p$
for $k \in (j-i)\mathbf{Z} \cap [i, \infty] \cap [$

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

$\rho_0 = 0$, $\rho_{k+1} = \rho_k^2 + 11$.

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 $p -$

$S_1 = 2^{2}$
divisors
3, 5, 7,
37, 41, 4
89, 97, 1
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>

$S_1 = 2^{232792560}$ –
divisors
3, 5, 7, 11, 13, 17
37, 41, 43, 53, 61,
89, 97, 103, 109, 1
137, 151, 157, 181

These divisors incl
70 of the 168 prim
156 of the 1229 pr
296 of the 9592 pr
470 of the 78498 p
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 pr
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 $\leq y$ 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 $k \in (j - i)\mathbf{Z} \cap [i, \infty] \cap [j, \infty]$.

<u>The $p-1$ method</u>

$S_1 = 2^{232792560} - 1$ 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 $\leq 10^3$;
156 of the 1229 primes $\leq 10^4$;
296 of the 9592 primes $\leq 10^5$;
470 of the 78498 primes $\leq 10^6$;
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 $p = \rho_{2k} \bmod p$

$(j - i)\mathbf{Z} \cap [i, \infty] \cap [j, \infty]$.

<u>The $p - 1$ method</u>

$S_1 = 2^{232792560} - 1$ 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:

$= \mathrm{lcm}\{1$

$= 2^4 \cdot 3^2$

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

$_{2k} \bmod p$

$[i, \infty] \cap [j, \infty]$.

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 $\leq 10^3$;
156 of the 1229 primes $\leq 10^4$;
296 of the 9592 primes $\leq 10^5$;
470 of the 78498 primes $\leq 10^6$;
etc.

An odd prime p
divides $2^{232792560}$
iff order of 2 in th
multiplicative grou
divides $s = 232792$

Many ways for thi
232792560 has 96

Why so many?
Answer: $s = 2327$
$= \mathrm{lcm}\{1, 2, 3, 4, 5,$
$= 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 1$

$S =$

ρ_{2z}).

S?

$o(1)$;

ion in

j, ∞].

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: $s = 232792560$
$= \mathrm{lcm}\{1, 2, 3, 4, 5, \ldots, 20\}$
$= 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot$

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 $\leq 10^3$;
156 of the 1229 primes $\leq 10^4$;
296 of the 9592 primes $\leq 10^5$;
470 of the 78498 primes $\leq 10^6$;
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: $s = 232792560$
$= \text{lcm}\{1, 2, 3, 4, 5, \ldots, 20\}$
$= 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19.$

1 method

$232792560 - 1$ has prime

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 $\leq 10^3$;
he 1229 primes $\leq 10^4$;
he 9592 primes $\leq 10^5$;
he 78498 primes $\leq 10^6$;

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: $s = 232792560$
$= \text{lcm}\{1, 2, 3, 4, 5, \ldots, 20\}$
$= 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$.

Can com
using 41
(Side no

Ring ope

This co
$2^2 = 2 \cdot$
$2^{12} = 2^6$
$2^{55}; 2^{110}$
$2^{3552}; 2^7$
$2^{56834}; 2^1$
$2^{909345};$
$2^{3637383}$
$2^{14549535}$
$2^{11639628}$

1

$-$ 1 has prime

, 19, 23, 29, 31,
, 67, 71, 73, 79,
113, 127, 131,
1, 191, 199 etc.

ude
nes $\leq 10^3$;
rimes $\leq 10^4$;
rimes $\leq 10^5$;
primes $\leq 10^6$;

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: $s = 232792560$
$= \operatorname{lcm}\{1, 2, 3, 4, 5, \ldots, 20\}$
$= 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$.

Can compute 2^{232}
using 41 ring oper
(Side note: 41 is n

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^{222}
2^{3552}; 2^{7104}; 2^{14208}
2^{56834}; 2^{113668}; 2^{2273}
2^{909345}; $2^{1818690}$; 2
$2^{3637383}$; $2^{7274766}$;
$2^{14549535}$; $2^{2909907}$
$2^{116396280}$; $2^{2327925}$

ime

29, 31,
73, 79,
131,
9 etc.

0^4;
0^5;
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: $s = 232792560$
$= \text{lcm}\{1, 2, 3, 4, 5, \ldots, 20\}$
$= 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$.

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^{454672};
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: $s = 232792560$
$= \operatorname{lcm}\{1, 2, 3, 4, 5, \ldots, 20\}$
$= 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19.$

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?

$s = 232792560$

$, 2, 3, 4, 5, \ldots, 20\}$

$^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$.

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

Notation

e.g. $c =$

2^{27} mod

2^{54} mod

2^{55} mod

2^{110} mod

$2^{2327925}$

$-\ 1$

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. $c = 85972312$
$2^{27} \bmod c = 1342$
$2^{54} \bmod c = 1342$
$= 9356$
$2^{55} \bmod c = 1871$
$2^{110} \bmod c = 1871$
$= 1458$
$2^{232792560} - 1 \bmod$

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 $\mathbf{Z}/c$.
Notation: $a \bmod b = a - b\lfloor$

e.g. $c = 8597231219$: ...
$2^{27} \bmod c = 134217728$;
$2^{54} \bmod c = 134217728^2$ m
$= 935663516$;
$2^{55} \bmod c = 1871327032$;
$2^{110} \bmod c = 1871327032^2$ n
$= 1458876811$; .
$2^{232792560} - 1 \bmod c = 56260$

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 $2^{232792560} - 1 \bmod c$
using 41 operations in $\mathbf{Z}/c$.
Notation: $a \bmod b = a - b\lfloor a/b \rfloor$.

e.g. $c = 8597231219$: ...
$2^{27} \bmod c = 134217728$;
$2^{54} \bmod c = 134217728^2 \bmod n$
$= 935663516$;
$2^{55} \bmod c = 1871327032$;
$2^{110} \bmod c = 1871327032^2 \bmod c$
$= 1458876811$; ...;
$2^{232792560} - 1 \bmod c = 5626089344$.

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 $2^{232792560} - 1 \bmod c$ using 41 operations in $\mathbf{Z}/c$.
Notation: $a \bmod b = a - b\lfloor a/b \rfloor$.

e.g. $c = 8597231219$: ...

$2^{27} \bmod c = 134217728$;

$2^{54} \bmod c = 134217728^2 \bmod n$
$= 935663516$;

$2^{55} \bmod c = 1871327032$;

$2^{110} \bmod c = 1871327032^2 \bmod c$
$= 1458876811$; ...;

$2^{232792560} - 1 \bmod c = 5626089344$.

Easy extra computation (Euclid): $\gcd\{5626089344, c\} = 991$.

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};
13668; 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 $2^{232792560} - 1 \bmod c$
using 41 operations in $\mathbf{Z}/c$.
Notation: $a \bmod b = a - b\lfloor a/b \rfloor$.

e.g. $c = 8597231219$: ...

$$2^{27} \bmod c = 134217728;$$
$$2^{54} \bmod c = 134217728^2 \bmod n = 935663516;$$
$$2^{55} \bmod c = 1871327032;$$
$$2^{110} \bmod c = 1871327032^2 \bmod c = 1458876811; \ldots;$$
$$2^{232792560} - 1 \bmod c = 5626089344.$$

Easy extra computation (Euclid):
$\gcd\{5626089344, c\} = 991$.

This $p -$
quickly f
Main wo

Could in
c's divisi
The 167
would ha

Not clea
Dividing
is faster
The $p -$
only 70
trial divi

$^{792560}-1$

ations.

not minimal.)

, 1, $+$, $-$, $\cdot$.

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};

; 2^{28416}; 2^{28417};

336; 2^{454672}; 2^{909344};

$2^{1818691}$; $2^{3637382}$;

$2^{7274767}$; $2^{14549534}$;

0; $2^{58198140}$;

560; $2^{232792560}-1$.

Given positive integer n,
can compute $2^{232792560} - 1 \bmod c$
using 41 operations in $\mathbf{Z}/c$.
Notation: $a \bmod b = a - b\lfloor a/b \rfloor$.

e.g. $c = 8597231219$: ...

$$2^{27} \bmod c = 134217728;$$
$$2^{54} \bmod c = 134217728^2 \bmod n = 935663516;$$
$$2^{55} \bmod c = 1871327032;$$
$$2^{110} \bmod c = 1871327032^2 \bmod c = 1458876811; \ldots;$$
$$2^{232792560} - 1 \bmod c = 5626089344.$$

Easy extra computation (Euclid):
$\gcd\{5626089344, c\} = 991$.

This $p - 1$ metho
quickly factored c
Main work: 27 squ

Could instead hav
c's divisibility by 2
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};

;2^{909344};

^{3637382};

^{14549534};

^{0};

${}^{2560} - 1$.

Given positive integer n,
can compute $2^{232792560} - 1 \bmod c$
using 41 operations in $\mathbf{Z}/c$.
Notation: $a \bmod b = a - b\lfloor a/b \rfloor$.

e.g. $c = 8597231219$: ...

$2^{27} \bmod c = 134217728$;

$2^{54} \bmod c = 134217728^2 \bmod n$

$= 935663516$;

$2^{55} \bmod c = 1871327032$;

$2^{110} \bmod c = 1871327032^2 \bmod c$

$= 1458876811$; ... ;

$2^{232792560} - 1 \bmod c = 5626089344$.

Easy extra computation (Euclid):
$\gcd\{5626089344, c\} = 991$.

This $p - 1$ method (1974 Po
quickly factored $c = 859723$
Main work: 27 squarings mo

Could instead have checked
c'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 ≤ 100
trial division finds all 168 pr

Given positive integer n,
can compute $2^{232792560} - 1 \bmod c$
using 41 operations in $\mathbf{Z}/c$.
Notation: $a \bmod b = a - b\lfloor a/b \rfloor$.

e.g. $c = 8597231219$: ...

$2^{27} \bmod c = 134217728$;

$2^{54} \bmod c = 134217728^2 \bmod n$
$= 935663516$;

$2^{55} \bmod c = 1871327032$;

$2^{110} \bmod c = 1871327032^2 \bmod c$
$= 1458876811; \ldots;$

$2^{232792560} - 1 \bmod c = 5626089344$.

Easy extra computation (Euclid):
$\gcd\{5626089344, c\} = 991$.

This $p - 1$ method (1974 Pollard)
quickly factored $c = 8597231219$.
Main work: 27 squarings mod c.

Could instead have checked
c'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 c.
The $p - 1$ method finds
only 70 of the primes ≤ 1000;
trial division finds all 168 primes.

ositive integer n,
pute $2^{232792560} - 1 \bmod c$
operations in $\mathbf{Z}/c$.
n: $a \bmod b = a - b\lfloor a/b \rfloor$.

8597231219: ...
d $c = 134217728$;
d $c = 134217728^2 \bmod n$
$= 935663516$;
d $c = 1871327032$;
d $c = 1871327032^2 \bmod c$
$= 1458876811; \ldots;$
$^{60} - 1 \bmod c = 5626089344$.

tra computation (Euclid):
$6089344, c\} = 991$.

This $p - 1$ method (1974 Pollard) quickly factored $c = 8597231219$. Main work: 27 squarings mod c.

Could instead have checked c'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 c. The $p - 1$ method finds only 70 of the primes ≤ 1000; trial division finds all 168 primes.

Scale up
$s = \text{lcm}$
using 13
find 231

Is a squa
faster th

Or
$s = \text{lcm}$
using 14
find 180

Is a squa
faster th

Extra be
no need

eger n,
$^{792560} - 1 \bmod c$
ns in $\mathbf{Z}/c$.
$= a - b\lfloor a/b \rfloor$.

219: ...
217728;
$217728^2 \bmod n$
563516;
1327032;
$1327032^2 \bmod c$
3876811; ...;
$c = 5626089344$.

tation (Euclid):
$c\} = 991$.

This $p-1$ method (1974 Pollard) quickly factored $c = 8597231219$. Main work: 27 squarings mod c.

Could instead have checked c'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 c. The $p-1$ method finds only 70 of the primes ≤ 1000; trial division finds all 168 primes.

Scale up to larger
$s = \mathrm{lcm}\{1, 2, 3, 4,$
using 136 squaring
find 2317 of the p

Is a squaring mod
faster than 17 tria

Or
$s = \mathrm{lcm}\{1, 2, 3, 4,$
using 1438 squarin
find 180121 of the

Is a squaring mod
faster than 125 tri

Extra benefit:
no need to store t

mod c

$a/b\rfloor$.

od n

nod c

..;

89344.

clid):

This $p-1$ method (1974 Pollard) quickly factored $c = 8597231219$. Main work: 27 squarings mod c.

Could instead have checked c'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 c. The $p-1$ method finds only 70 of the primes ≤ 1000; trial division finds all 168 primes.

Scale up to larger exponent

$s = \operatorname{lcm}\{1, 2, 3, 4, 5, \ldots, 100$

using 136 squarings mod c

find 2317 of the primes ≤ 1

Is a squaring mod c

faster than 17 trial divisions

Or

$s = \operatorname{lcm}\{1, 2, 3, 4, 5, \ldots, 100$

using 1438 squarings mod c

find 180121 of the primes $\leq$

Is a squaring mod c

faster than 125 trial division

Extra benefit:

no need to store the primes.

This $p-1$ method (1974 Pollard) quickly factored $c = 8597231219$. Main work: 27 squarings mod c.

Could instead have checked c'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 c. The $p-1$ method finds only 70 of the primes ≤ 1000; trial division finds all 168 primes.

Scale up to larger exponent $s = \mathrm{lcm}\{1, 2, 3, 4, 5, \ldots, 100\}$: using 136 squarings mod c find 2317 of the primes $\le 10^5$.

Is a squaring mod c faster than 17 trial divisions?

Or $s = \mathrm{lcm}\{1, 2, 3, 4, 5, \ldots, 1000\}$: using 1438 squarings mod c find 180121 of the primes $\le 10^7$.

Is a squaring mod c faster than 125 trial divisions?

Extra benefit: no need to store the primes.

-1 method (1974 Pollard)
factored $c = 8597231219$.
ork: 27 squarings mod c.

stead have checked
bility by $2, 3, 5, \ldots$.
th trial division
ave found divisor 991.

r which method is better.
by small p
than squaring mod c.
1 method finds
of the primes ≤ 1000;
sion finds all 168 primes.

Scale up to larger exponent
$s = \text{lcm}\{1, 2, 3, 4, 5, \ldots, 100\}$:
using 136 squarings mod c
find 2317 of the primes $\leq 10^5$.

Is a squaring mod c
faster than 17 trial divisions?

Or
$s = \text{lcm}\{1, 2, 3, 4, 5, \ldots, 1000\}$:
using 1438 squarings mod c
find 180121 of the primes $\leq 10^7$.

Is a squaring mod c
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 c.

e checked
$2, 3, 5, \ldots.$
vision
divisor 991.

ethod is better.
p
aring mod c.
l finds
mes ≤ 1000;
all 168 primes.

Scale up to larger exponent
$s = \operatorname{lcm}\{1, 2, 3, 4, 5, \ldots, 100\}$:
using 136 squarings mod c
find 2317 of the primes $\le 10^5$.

Is a squaring mod c
faster than 17 trial divisions?

Or
$s = \operatorname{lcm}\{1, 2, 3, 4, 5, \ldots, 1000\}$:
using 1438 squarings mod c
find 180121 of the primes $\le 10^7$.

Is a squaring mod c
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 $H/K^{1+o(1)}$ prin
Same if $p-1$ is re
order of 2 in $\mathbf{F}_p^*$.

So uniform randor
divides $2^{\operatorname{lcm}\{1,2,\ldots,}$
with probability 1/

$(1.4\ldots + o(1))K$
produce $2^{\operatorname{lcm}\{1,2,\ldots}$

Similar time spent
finds far fewer prin

ollard)

1219.

od c.

1.

etter.

c.

0;

imes.

Scale up to larger exponent
$s = \operatorname{lcm}\{1,2,3,4,5,\ldots,100\}$:
using 136 squarings mod c
find 2317 of the primes $\le 10^5$.

Is a squaring mod c
faster than 17 trial divisions?

Or
$s = \operatorname{lcm}\{1,2,3,4,5,\ldots,1000\}$:
using 1438 squarings mod c
find 180121 of the primes $\le 10^7$.

Is a squaring mod c
faster than 125 trial divisions?

Extra benefit:
no need to store the primes.

Plausible conjecture: if K is
$\exp\sqrt{\left(\frac{1}{2}+o(1)\right)\log H \log \mathrm{lo}}$
then $p-1$ divides $\operatorname{lcm}\{1,2,\ldots$
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 $2^{\operatorname{lcm}\{1,2,\ldots,K\}}-1$
with probability $1/K^{1+o(1)}$.

$(1.4\ldots+o(1))K$ squarings
produce $2^{\operatorname{lcm}\{1,2,\ldots,K\}}-1\,\mathrm{m}$

Similar time spent on trial d
finds far fewer primes for lar

Scale up to larger exponent
$s = \text{lcm}\{1, 2, 3, 4, 5, \ldots, 100\}$:
using 136 squarings mod c
find 2317 of the primes $\le 10^5$.

Is a squaring mod c
faster than 17 trial divisions?

Or
$s = \text{lcm}\{1, 2, 3, 4, 5, \ldots, 1000\}$:
using 1438 squarings mod c
find 180121 of the primes $\le 10^7$.

Is a squaring mod c
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 $\text{lcm}\{1, 2, \ldots, K\}$
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 $2^{\text{lcm}\{1,2,\ldots,K\}} - 1$
with probability $1/K^{1+o(1)}$.

$(1.4\ldots + o(1))K$ squarings mod c
produce $2^{\text{lcm}\{1,2,\ldots,K\}} - 1 \bmod c$.

Similar time spent on trial division
finds far fewer primes for large H.

to larger exponent

$\{1, 2, 3, 4, 5, \ldots, 100\}$:

6 squarings mod c

7 of the primes $\leq 10^5$.

aring mod c

an 17 trial divisions?

$\{1, 2, 3, 4, 5, \ldots, 1000\}$:

38 squarings mod c

121 of the primes $\leq 10^7$.

aring mod c

an 125 trial divisions?

enefit:

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 $p \leq H$.
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 c produce $2^{\operatorname{lcm}\{1,2,\ldots,K\}} - 1 \bmod c$.

Similar time spent on trial division finds far fewer primes for large H.

Safe prin

This me
to facto
have sm

To const
avoid su

ANSI do
using "s
primes o
when ge

This do
NFS no
algorith

exponent
5, . . . , 100}:
gs mod c
rimes $\leq 10^5$.

c
l divisions?

5, . . . , 1000}:
ngs mod c
e primes $\leq 10^7$.

c
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 c produce $2^{\operatorname{lcm}\{1,2,\ldots,K\}}-1 \bmod c$.

Similar time spent on trial division finds far fewer primes for large H.

Safe primes

This means numbe
to factor if their fa
have smooth $p_i -$

To construct hard
avoid such factors

ANSI does recomm
using "safe primes
primes of the form
when generating R

This does not help
NFS nor against th
algorithms.

$\}$:

0^5.

?

$0\}$:

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 c produce $2^{\operatorname{lcm}\{1,2,\ldots,K\}}-1 \bmod c$.

Similar time spent on trial division finds far fewer primes for large H.

Safe primes

This means numbers are eas
to factor if their factors p_i
have smooth p_i-1.

To construct hard instances
avoid such factors – that's i

ANSI does recommend
using "safe primes", i.e.,
primes of the form $2p'+1$
when generating RSA modu

This does not help against t
NFS nor against the followi
algorithms.

Plausible conjecture: if K is $\exp\sqrt{\left(\frac{1}{2}+o(1)\right)\log H \log\log H}$ then $p-1$ divides $\text{lcm}\{1,2,\ldots,K\}$ 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 $2^{\text{lcm}\{1,2,\ldots,K\}}-1$ with probability $1/K^{1+o(1)}$.

$(1.4\ldots+o(1))K$ squarings mod c produce $2^{\text{lcm}\{1,2,\ldots,K\}}-1 \bmod c$.

Similar time spent on trial division finds far fewer primes for large H.

Safe primes

This means numbers are easy to factor if their factors p_i have smooth $p_i - 1$.

To construct hard instances avoid such factors – that's it?

ANSI does recommend using "safe primes", i.e., primes of the form $2p'+1$ when generating RSA moduli.

This does not help against the NFS nor against the following algorithms.

e conjecture: if K is

$\frac{}{2} + o(1)\big)\log H \log\log H$
1 divides $\mathrm{lcm}\{1, 2, \ldots, K\}$
$^{1+o(1)}$ primes $p \le H$.
$p - 1$ is replaced by
2 in $\mathbf{F}_p^*$.

rm random prime $p \le H$
$2^{\mathrm{lcm}\{1,2,\ldots,K\}} - 1$
bability $1/K^{1+o(1)}$.

$+ o(1))K$ squarings mod c
$2^{\mathrm{lcm}\{1,2,\ldots,K\}} - 1 \bmod c$.

time spent on trial division
fewer primes for large H.

Safe primes

This means numbers are easy to factor if their factors p_i have smooth $p_i - 1$.

To construct hard instances avoid such factors – that's it?

ANSI does recommend using "safe primes", i.e., primes of the form $2p' + 1$ when generating RSA moduli.

This does not help against the NFS nor against the following algorithms.

The $p +$

(1982 W

Define (

2327925

$(3/5, 4/$

The inte
is divisib
82 of th
223 of t
455 of t
720 of t
etc.

re: if K is

og $H \log\log H$

lcm$\{1, 2, \ldots, K\}$

mes $p \leq H$.

eplaced by

m prime $p \leq H$

$K\} - 1$

$/K^{1+o(1)}$.

squarings mod c

$,K\} - 1 \bmod c$.

on trial division

mes for large H.

Safe primes

This means numbers are easy to factor if their factors p_i have smooth $p_i - 1$.

To construct hard instances avoid such factors – that's it?

ANSI does recommend using "safe primes", i.e., primes of the form $2p' + 1$ when generating RSA moduli.

This does not help against the NFS nor against the following algorithms.

The $p + 1$ factoriz

(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.

s

g H

$\ldots, K\}$

H.

$\leq H$

mod c

od c.

ivision

ge H.

Safe primes

This means numbers are easy to factor if their factors p_i have smooth $p_i - 1$.

To construct hard instances avoid such factors – that's it?

ANSI does recommend using "safe primes", i.e., primes of the form $2p' + 1$ when generating RSA moduli.

This does not help against the NFS nor against the following algorithms.

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 $\leq 10^3$;
223 of the primes $\leq 10^4$;
455 of the primes $\leq 10^5$;
720 of the primes $\leq 10^6$;
etc.

Safe primes

This means numbers are easy to factor if their factors p_i have smooth $p_i - 1$.

To construct hard instances avoid such factors – that's it?

ANSI does recommend using "safe primes", i.e., primes of the form $2p' + 1$ when generating RSA moduli.

This does not help against the NFS nor against the following algorithms.

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.

mes

ans numbers are easy
r if their factors p_i
ooth $p_i - 1$.

truct hard instances
ch factors – that's it?

pes recommend
afe primes", i.e.,
of the form $2p' + 1$
nerating RSA moduli.

es not help against the
r against the following
ms.

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 $\leq 10^3$;
223 of the primes $\leq 10^4$;
455 of the primes $\leq 10^5$;
720 of the primes $\leq 10^6$;
etc.

Given ar
compute
and com
hoping t

Many p'
are foun

If -1 is
and $p+$
then 5^{23}

Proof: p
$(4/5 + 3$
so $(p +$
in the gr
so 23279

ers are easy
actors p_i
1.

instances
– that's it?

mend
", i.e.,
$2p' + 1$
RSA moduli.

o against the
he following

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 c
compute $5^{23279256}$
and compute gcd
hoping to factor c

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: $p \equiv 3 \pmod{}$ (m
$(4/5 + 3i/5)^p = 4$
so $(p + 1)(3/5, 4/$
in the group Clock
so 232792560(3/5

sy

t?

li.

he

ng

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 c, compute $5^{232792560} X$ mod c and compute gcd with c, hoping to factor c.

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 23279256 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 $232792560(3/5, 4/5) = ($

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 c, compute $5^{232792560} X \bmod c$ and compute gcd with c, hoping to factor c.

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 $(4/5 + 3i/5)^p = 4/5 - 3i/5$ and so $(p+1)(3/5, 4/5) = (0, 1)$ in the group Clock($\mathbf{F}_p$) so $232792560(3/5, 4/5) = (0, 1)$.

1 factorization method

Williams)

$X, Y) \in \mathbf{Q} \times \mathbf{Q}$ as the

560th 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 c,
compute $5^{232792560} X \bmod c$
and compute gcd with c,
hoping to factor c.

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
$(4/5 + 3i/5)^p = 4/5 - 3i/5$ and
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

Stage 1:

compute

$s = \mathrm{lcm}$

Stage 2:

$B_1 < q_1$

compute

If order

(same cu

divides s

$R_i = (0,$

Compute

ation method

$\times$ **Q** as the
iple of
group Clock(**Q**).

$5^{232792560}X$

$\leq 10^3$;
$\leq 10^4$;
$\leq 10^5$;
$\leq 10^6$;

Given an integer c,
compute $5^{232792560}X \bmod c$
and compute gcd with c,
hoping to factor c.

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
$(4/5 + 3i/5)^p = 4/5 - 3i/5$ and
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

Stage 1: Point P
compute $R = sP$
$s = \mathrm{lcm}\{2, 3, \ldots,$

Stage 2: Small pri
$B_1 < q_1, \ldots, q_k \leq$
compute $R_i = q_i R$

If order of P on E
(same curve, reduc
divides sq_i, then
$R_i = (0, 1)$ (using

Compute gcd$\{c, \prod$

hod

he

k($\mathbf{Q}$).

X

Given an integer c, compute $5^{232792560}X \bmod c$ and compute gcd with c, hoping to factor c.

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 $(4/5+3i/5)^p = 4/5-3i/5$ and 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

Stage 1: Point P on E over compute $R = sP$ for $s = \operatorname{lcm}\{2,3,\ldots,B_1\}$.

Stage 2: Small primes $B_1 < q_1, \ldots, q_k \le B_2$ compute $R_i = q_i R$.

If order of P on $E/\mathbf{F}_{p_i}$ (same curve, reduce mod p_i divides sq_i, then $R_i = (0,1)$ (using Edwards)

Compute $\gcd\{c, \prod y(R_i)\}$.

Given an integer c,
compute $5^{232792560}X \bmod c$
and compute gcd with c,
hoping to factor c.

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
$(4/5 + 3i/5)^p = 4/5 - 3i/5$ and
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

Stage 1: Point P on E over $\mathbf{Z}/c$,
compute $R = sP$ for
$s = \text{lcm}\{2, 3, \ldots, B_1\}$.

Stage 2: Small primes
$B_1 < q_1, \ldots, q_k \leq B_2$
compute $R_i = q_i R$.

If order of P on $E/\mathbf{F}_{p_i}$
(same curve, reduce mod p_i)
divides sq_i, then
$R_i = (0, 1)$ (using Edwards).

Compute $\gcd\{c, \prod y(R_i)\}$.

n integer c,
e $5^{232792560}X \bmod c$
npute gcd with c,
to factor c.

s not found by $\mathbf{F}_p^*$
d by Clock($\mathbf{F}_p$).

not a square mod p
1 divides 232792560
$^{32792560}X \bmod p = 0$.

$p \equiv 3 \pmod 4$, so
$3i/5)^p = 4/5 - 3i/5$ and
$1)(3/5, 4/5) = (0, 1)$
roup Clock($\mathbf{F}_p$)
$92560(3/5, 4/5) = (0, 1)$.

The elliptic-curve method

Stage 1: Point P on E over $\mathbf{Z}/c$,
compute $R = sP$ for
$s = \operatorname{lcm}\{2, 3, \ldots, B_1\}$.

Stage 2: Small primes
$B_1 < q_1, \ldots, q_k \le B_2$
compute $R_i = q_i R$.

If order of P on $E/\mathbf{F}_{p_i}$
(same curve, reduce mod p_i)
divides sq_i, then
$R_i = (0, 1)$ (using Edwards).

Compute $\gcd\{c, \prod y(R_i)\}$.

Good ne
All prim
reasonab

Order of
$\in [p+1$
If a curv

Plausible
exp $\sqrt{(}$
then, for
a uniform
has char

Find p u
$\le B_1^{2+o(}$
Time su

c,

${}^{0}X \bmod c$

with c,

nd by $\mathbf{F}_p^*$

$x(\mathbf{F}_p)$.

are mod p

232792560

$\bmod p = 0$.

od 4), so

$/5 - 3i/5$ and

$5) = (0, 1)$

$x(\mathbf{F}_p)$

$, 4/5) = (0, 1)$.

The elliptic-curve method

Stage 1: Point P on E over $\mathbf{Z}/c$, compute $R = sP$ for $s = \operatorname{lcm}\{2, 3, \ldots, B_1\}$.

Stage 2: Small primes $B_1 < q_1, \ldots, q_k \le B_2$ compute $R_i = q_i R$.

If order of P on $E/\mathbf{F}_{p_i}$ (same curve, reduce mod p_i) divides sq_i, then $R_i = (0, 1)$ (using Edwards).

Compute $\gcd\{c, \prod y(R_i)\}$.

Good news (for th

All primes $\le H$ fo

reasonable numbe

Order of elliptic-cu

$\in [p + 1 - 2\sqrt{p}, p$

If a curve fails, try

Plausible conjectu

$\exp \sqrt{\left(\frac{1}{2} + o(1)\right) \mathrm{lo}}$

then, for each prim

a uniform random

has chance $\ge 1/B$

Find p using, $\le B$

$\le B_1^{2+o(1)}$ squarin

Time subexponent

c

0

.

and

)

$0, 1)$.

The elliptic-curve method

Stage 1: Point P on E over $\mathbf{Z}/c$, compute $R = sP$ for $s = \operatorname{lcm}\{2, 3, \ldots, B_1\}$.

Stage 2: Small primes $B_1 < q_1, \ldots, q_k \le B_2$ compute $R_i = q_i R$.

If order of P on $E/\mathbf{F}_{p_i}$ (same curve, reduce mod p_i) divides sq_i, then $R_i = (0, 1)$ (using Edwards).

Compute $\gcd\{c, \prod y(R_i)\}$.

Good news (for the attacker

All primes $\le H$ found after

reasonable number of curves

Order of elliptic-curve group

$\in [p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{}$

If a curve fails, try another.

Plausible conjecture: if B_1 i

$\exp \sqrt{\left(\frac{1}{2} + o(1)\right) \log H \log \mathrm{lo}}$

then, for each prime $p \le H$,

a uniform random curve mo

has chance $\ge 1/B_1^{1+o(1)}$ to

Find p using, $\le B_1^{1+o(1)}$ cur

$\le B_1^{2+o(1)}$ squarings.

Time subexponential in H.

The elliptic-curve method

Stage 1: Point P on E over $\mathbf{Z}/c$, compute $R = sP$ for $s = \operatorname{lcm}\{2, 3, \ldots, B_1\}$.

Stage 2: Small primes $B_1 < q_1, \ldots, q_k \le B_2$ compute $R_i = q_i R$.

If order of P on $E/\mathbf{F}_{p_i}$ (same curve, reduce mod p_i) divides sq_i, then $R_i = (0, 1)$ (using Edwards).

Compute $\gcd\{c, \prod y(R_i)\}$.

Good news (for the attacker): *All* primes $\le H$ found after reasonable number of curves.

Order of elliptic-curve group $\in [p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}]$. If a curve fails, try another.

Plausible conjecture: if B_1 is $\exp\sqrt{\left(\frac{1}{2} + o(1)\right)\log H \log\log H}$ then, for each prime $p \le H$, a uniform random curve mod p has chance $\ge 1/B_1^{1+o(1)}$ to find p.

Find p using, $\le B_1^{1+o(1)}$ curves; $\le B_1^{2+o(1)}$ squarings. Time subexponential in H.

otic-curve method

Point P on E over $\mathbf{Z}/c$,

e $R = sP$ for

$\{2, 3, \ldots, B_1\}$.

Small primes

$, \ldots, q_k \le B_2$

e $R_i = q_i R$.

of P on $E/\mathbf{F}_{p_i}$

urve, reduce mod p_i)

sq_i, then

$, 1)$ (using Edwards).

e $\gcd\{c, \prod y(R_i)\}$.

Good news (for the attacker):
All primes $\le H$ found after
reasonable number of curves.

Order of elliptic-curve group
$\in [p+1-2\sqrt{p}, p+1+2\sqrt{p}]$.
If a curve fails, try another.

Plausible conjecture: if B_1 is
$\exp\sqrt{\left(\frac{1}{2}+o(1)\right)\log H \log\log H}$
then, for each prime $p \le H$,
a uniform random curve mod p
has chance $\ge 1/B_1^{1+o(1)}$ to find p.

Find p using, $\le B_1^{1+o(1)}$ curves;
$\le B_1^{2+o(1)}$ squarings.
Time subexponential in H.

Bad RSA

2004 Ba

checked

found 2

2012.02.

Augier–E

“Ron wa

(Crypto

SSL/PG

distinct

those,

thanks t

method

on E over $\mathbf{Z}/c$,
for
$B_1\}$.

mes
B_2
R.

$/\mathbf{F}_{p_i}$
ce mod p_i)

Edwards).

$y(R_i)\}$.

Good news (for the attacker):
All primes $\le H$ found after
reasonable number of curves.

Order of elliptic-curve group
$\in [p+1-2\sqrt{p}, p+1+2\sqrt{p}]$.
If a curve fails, try another.

Plausible conjecture: if B_1 is
$\exp\sqrt{\left(\frac{1}{2}+o(1)\right)\log H \log\log H}$
then, for each prime $p \le H$,
a uniform random curve mod p
has chance $\ge 1/B_1^{1+o(1)}$ to find p.

Find p using, $\le B_1^{1+o(1)}$ curves;
$\le B_1^{2+o(1)}$ squarings.
Time subexponential in H.

Bad RSA random

2004 Bauer–Lauri
checked 18000 PG
found 2 keys shari

2012.02.14 Lenstr
Augier–Bos–Klein
"Ron was wrong,
(Crypto 2012): ch
SSL/PGP RSA ke
distinct keys; fact
those,
thanks to shared p

$\mathbf{Z}/c$,

)

.

Good news (for the attacker):
All primes $\leq H$ found after
reasonable number of curves.

Order of elliptic-curve group
$\in [p+1-2\sqrt{p}, p+1+2\sqrt{p}]$.
If a curve fails, try another.

Plausible conjecture: if B_1 is
$\exp\sqrt{\left(\frac{1}{2}+o(1)\right)\log H \log\log H}$
then, for each prime $p \leq H$,
a uniform random curve mod p
has chance $\geq 1/B_1^{1+o(1)}$ to find p.

Find p using, $\leq B_1^{1+o(1)}$ curves;
$\leq B_1^{2+o(1)}$ squarings.
Time subexponential in H.

Bad RSA randomness

2004 Bauer–Laurie:
checked 18000 PGP RSA ke
found 2 keys sharing a facto

2012.02.14 Lenstra–Hughes–
Augier–Bos–Kleinjung–Wach
“Ron was wrong, Whit is rig
(Crypto 2012): checked 7 ·
SSL/PGP RSA keys; found
distinct keys; factored 1272
those,
thanks to shared prime facto

Good news (for the attacker):
All primes $\le H$ found after reasonable number of curves.

Order of elliptic-curve group $\in [p+1-2\sqrt{p}, p+1+2\sqrt{p}]$.
If a curve fails, try another.

Plausible conjecture: if B_1 is $\exp\sqrt{\left(\frac{1}{2}+o(1)\right)\log H \log\log H}$ then, for each prime $p \le H$, a uniform random curve mod p has chance $\ge 1/B_1^{1+o(1)}$ to find p.

Find p using, $\le B_1^{1+o(1)}$ curves; $\le B_1^{2+o(1)}$ squarings.
Time subexponential in H.

<u>Bad RSA randomness</u>

2004 Bauer–Laurie:
checked 18000 PGP RSA keys; found 2 keys sharing a factor.

2012.02.14 Lenstra–Hughes–Augier–Bos–Kleinjung–Wachter "Ron was wrong, Whit is right" (Crypto 2012): checked $7 \cdot 10^6$ SSL/PGP RSA keys; found $6 \cdot 10^6$ distinct keys; factored 12720 of those,
thanks to shared prime factors.

ews (for the attacker):
es $\leq H$ found after
ble number of curves.

f elliptic-curve group
$- 2\sqrt{p}, p + 1 + 2\sqrt{p}]$.
ve fails, try another.

e conjecture: if B_1 is
$+ o(1)) \log H \log \log H$
r each prime $p \leq H$,
m random curve mod p
nce $\geq 1/B_1^{1+o(1)}$ to find p.
using, $\leq B_1^{1+o(1)}$ curves;
$^{(1)}$ squarings.
bexponential in H.

Bad RSA randomness

2004 Bauer–Laurie:
checked 18000 PGP RSA keys;
found 2 keys sharing a factor.

2012.02.14 Lenstra–Hughes–
Augier–Bos–Kleinjung–Wachter
"Ron was wrong, Whit is right"
(Crypto 2012): checked $7 \cdot 10^6$
SSL/PGP RSA keys; found $6 \cdot 10^6$
distinct keys; factored 12720 of
those,
thanks to shared prime factors.

2012.02.
Durumer
announc
2012):
checked
keys; fac
2422 SS

"Almost
were ger
secure e
such as
to secure
as your

e attacker):
und after
r of curves.

urve group
$+ 1 + 2\sqrt{p}]$.
another.

re: if B_1 is
og H log log H
me $p \le H$,
curve mod p
$_1^{1+o(1)}$ to find p.
$_1^{1+o(1)}$ curves;
gs.
tial in H.

Bad RSA randomness

2004 Bauer–Laurie:
checked 18000 PGP RSA keys;
found 2 keys sharing a factor.

2012.02.14 Lenstra–Hughes–Augier–Bos–Kleinjung–Wachter
"Ron was wrong, Whit is right"
(Crypto 2012): checked $7 \cdot 10^6$
SSL/PGP RSA keys; found $6 \cdot 10^6$
distinct keys; factored 12720 of
those,
thanks to shared prime factors.

2012.02.17 Hening
Durumeric–Wustro
announcement (US
2012):
checked $>10^7$ SSL
keys; factored 248
2422 SSH host key

"Almost all of the
were generated by
secure embedded
such as routers an
to secure popular
as your bank or en

r):

s.

o

$\sqrt{p}$].

s

g H

d p

find p.

ves;

Bad RSA randomness

2004 Bauer–Laurie:
checked 18000 PGP RSA keys;
found 2 keys sharing a factor.

2012.02.14 Lenstra–Hughes–Augier–Bos–Kleinjung–Wachter "Ron was wrong, Whit is right" (Crypto 2012): checked $7 \cdot 10^6$ SSL/PGP RSA keys; found $6 \cdot 10^6$ distinct keys; factored 12720 of those,
thanks to shared prime factors.

2012.02.17 Heninger–Durumeric–Wustrow–Halder announcement (USENIX Sec 2012):
checked $>10^7$ SSL/SSH RS keys; factored 24816 SSL ke 2422 SSH host keys.

"Almost all of the vulnerable were generated by and are u secure embedded hardware such as routers and firewalls to secure popular web sites as your bank or email provid

Bad RSA randomness

2004 Bauer–Laurie:
checked 18000 PGP RSA keys;
found 2 keys sharing a factor.

2012.02.14 Lenstra–Hughes–Augier–Bos–Kleinjung–Wachter "Ron was wrong, Whit is right" (Crypto 2012): checked $7 \cdot 10^6$ SSL/PGP RSA keys; found $6 \cdot 10^6$ distinct keys; factored 12720 of those,
thanks to shared prime factors.

2012.02.17 Heninger–Durumeric–Wustrow–Halderman announcement (USENIX Security 2012):
checked $>10^7$ SSL/SSH RSA keys; factored 24816 SSL keys, 2422 SSH host keys.

"Almost all of the vulnerable keys were generated by and are used to secure embedded hardware devices such as routers and firewalls, not to secure popular web sites such as your bank or email provider."

A randomness

uer–Laurie:
18000 PGP RSA keys;
keys sharing a factor.

.14 Lenstra–Hughes–
Bos–Kleinjung–Wachter
as wrong, Whit is right"
2012): checked $7 \cdot 10^6$
P RSA keys; found $6 \cdot 10^6$
keys; factored 12720 of

o shared prime factors.

2012.02.17 Heninger–Durumeric–Wustrow–Halderman announcement (USENIX Security 2012):
checked $>10^7$ SSL/SSH RSA keys; factored 24816 SSL keys, 2422 SSH host keys.

"Almost all of the vulnerable keys were generated by and are used to secure embedded hardware devices such as routers and firewalls, not to secure popular web sites such as your bank or email provider."

These co
$p_1 q_1$, p_2
$p_4 q_2$, p_5
and thus
Obvious
Faster:

Nice foll
Do this
Online d

These w
certified
should h
But: stu

ness

e:
GP RSA keys;
ng a factor.

a–Hughes–
ung–Wachter
Whit is right"
hecked $7 \cdot 10^6$
ys; found $6 \cdot 10^6$
ored 12720 of

prime factors.

2012.02.17 Heninger–Durumeric–Wustrow–Halderman announcement (USENIX Security 2012):
checked $>10^7$ SSL/SSH RSA keys; factored 24816 SSL keys, 2422 SSH host keys.

"Almost all of the vulnerable keys were generated by and are used to secure embedded hardware devices such as routers and firewalls, not to secure popular web sites such as your bank or email provider."

These computatio
$p_1q_1, p_2q_2, p_3q_3,$
$p_4q_2, p_5q_5, p_6q_6;$
and thus also p_2 a
Obvious:GCD com
Faster: scaled rem

Nice follow-up pro
Do this with Taiwa
Online data base o

These were genera
certified smart car
should have good
But: student brok

eys;
or.
–
nter
ght"
10^6
$6 \cdot 10^6$
0 of
ors.

2012.02.17 Heninger–Durumeric–Wustrow–Halderman announcement (USENIX Security 2012):
checked $>10^7$ SSL/SSH RSA keys; factored 24816 SSL keys, 2422 SSH host keys.

"Almost all of the vulnerable keys were generated by and are used to secure embedded hardware devices such as routers and firewalls, not to secure popular web sites such as your bank or email provider."

These computations find q_2
$p_1 q_1$, $p_2 q_2$, $p_3 q_3$,
$p_4 q_2$, $p_5 q_5$, $p_6 q_6$;
and thus also p_2 and p_4.
Obvious:GCD computation.
Faster: scaled remainder tre

Nice follow-up project:
Do this with Taiwan citizen
Online data base of RSA key

These were generated on
certified smart cards;
should have good randomne
But: student broke 103 keys

2012.02.17 Heninger–Durumeric–Wustrow–Halderman announcement (USENIX Security 2012):
checked $>10^7$ SSL/SSH RSA keys; factored 24816 SSL keys, 2422 SSH host keys.

"Almost all of the vulnerable keys were generated by and are used to secure embedded hardware devices such as routers and firewalls, not to secure popular web sites such as your bank or email provider."

These computations find q_2 in
$p_1 q_1$, $p_2 q_2$, $p_3 q_3$,
$p_4 q_2$, $p_5 q_5$, $p_6 q_6$;
and thus also p_2 and p_4.
Obvious:GCD computation.
Faster: scaled remainder trees.

Nice follow-up project:
Do this with Taiwan citizen cards.
Online data base of RSA keys.

These were generated on
certified smart cards;
should have good randomness.
But: student broke 103 keys.

.17 Heninger–
ric–Wustrow–Halderman
ement (USENIX Security

$>10^7$ SSL/SSH RSA
ctored 24816 SSL keys,
H host keys.

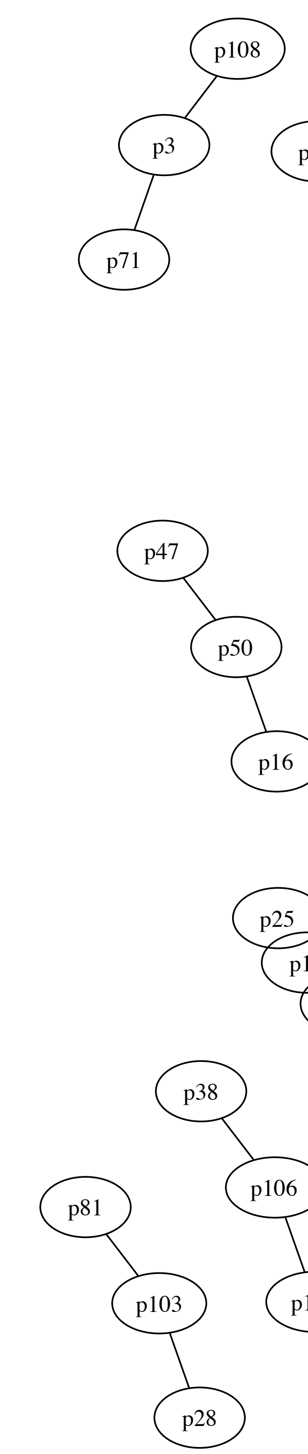
all of the vulnerable keys
nerated by and are used to
mbedded hardware devices
routers and firewalls, not
e popular web sites such
bank or email provider."

These computations find q_2 in
$p_1 q_1, p_2 q_2, p_3 q_3,$
$p_4 q_2, p_5 q_5, p_6 q_6;$
and thus also p_2 and p_4.
Obvious:GCD computation.
Faster: scaled remainder trees.

Nice follow-up project:
Do this with Taiwan citizen cards.
Online data base of RSA keys.

These were generated on
certified smart cards;
should have good randomness.
But: student broke 103 keys.

Closer lo



ger–
ow–Halderman
SENIX Security

L/SSH RSA
16 SSL keys,
ys.

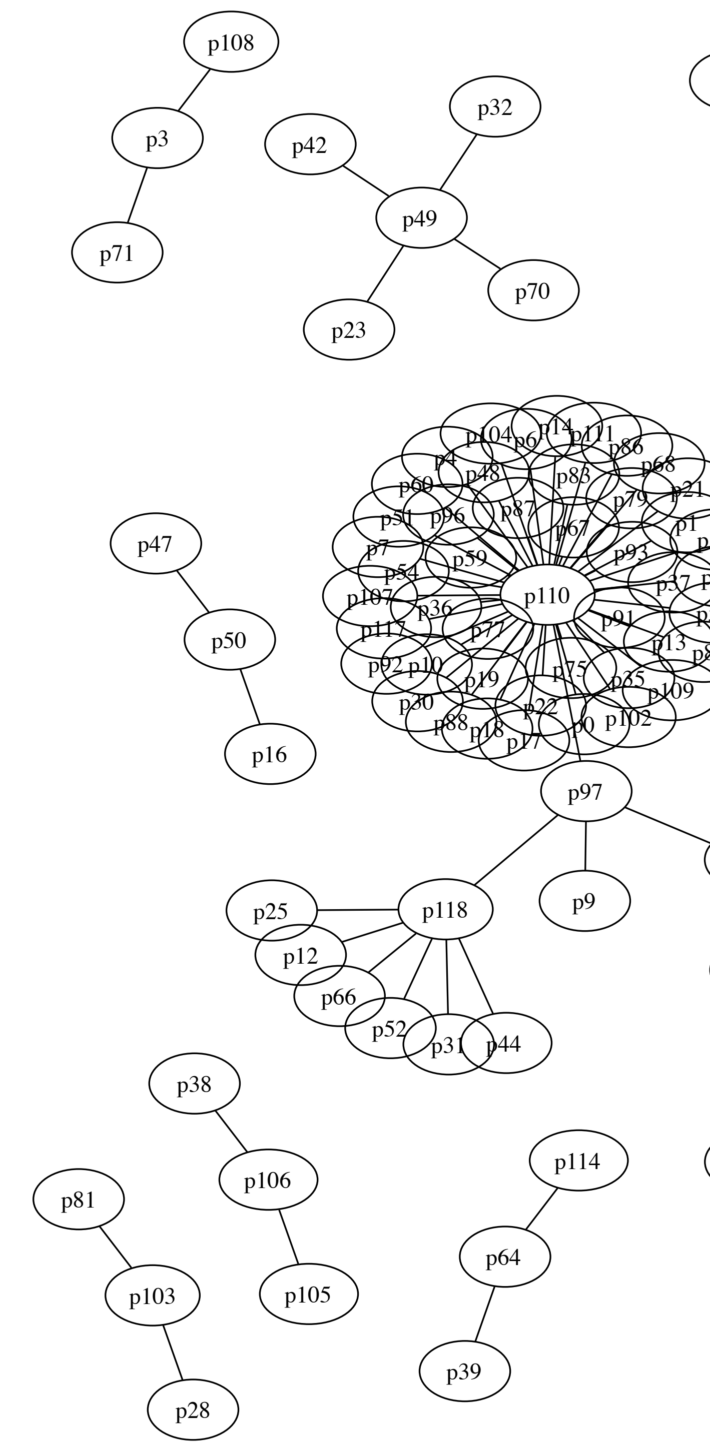
vulnerable keys
and are used to
hardware devices
d firewalls, not
web sites such
mail provider.”

These computations find q_2 in
$p_1 q_1, p_2 q_2, p_3 q_3,$
$p_4 q_2, p_5 q_5, p_6 q_6;$
and thus also p_2 and p_4.
Obvious:GCD computation.
Faster: scaled remainder trees.

Nice follow-up project:
Do this with Taiwan citizen cards.
Online data base of RSA keys.

These were generated on
certified smart cards;
should have good randomness.
But: student broke 103 keys.

Closer look at the



rman
curity

A
ys,

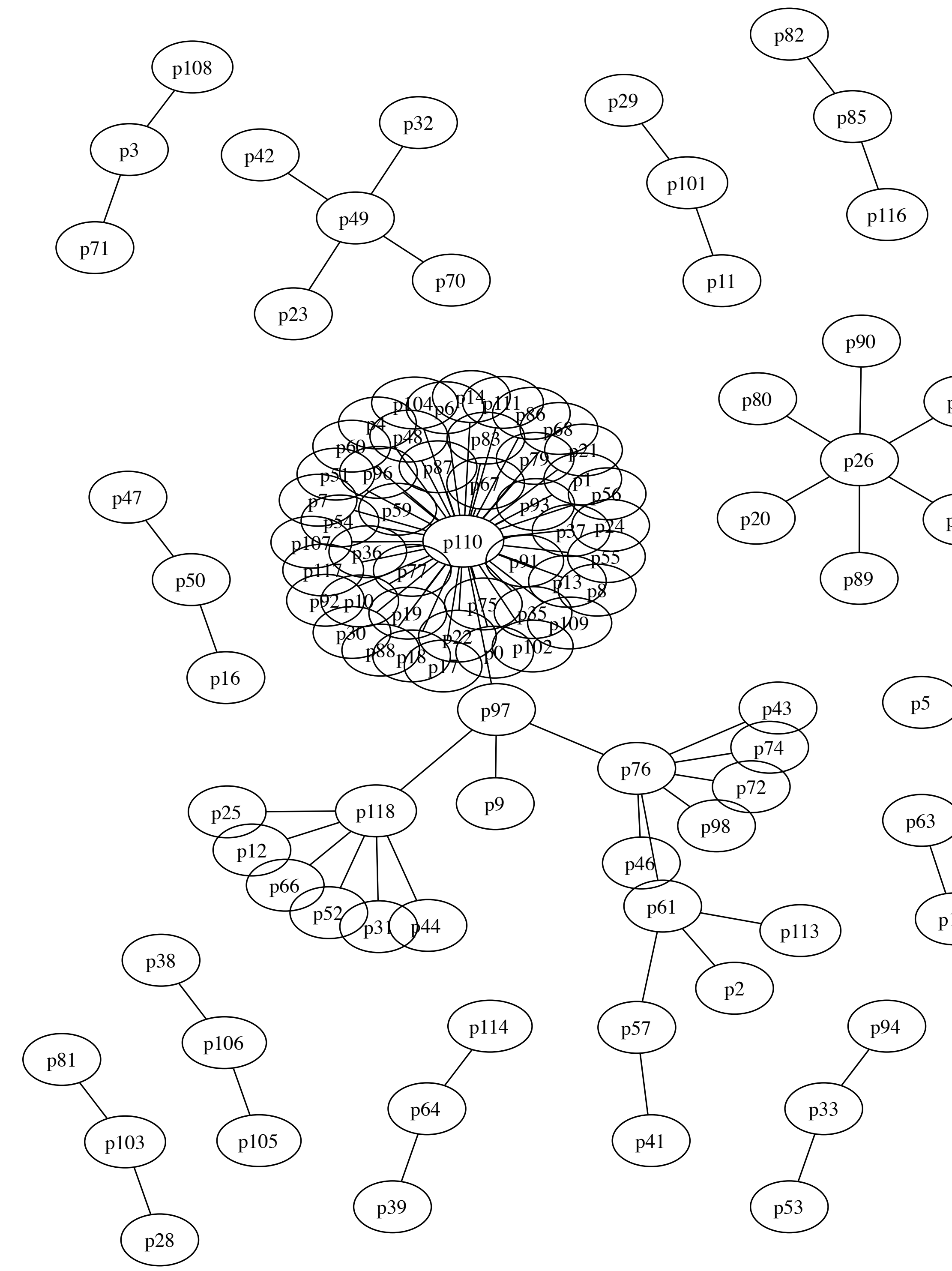
e keys
sed to
devices
, not
such
ler.”

These computations find q_2 in
$p_1 q_1, p_2 q_2, p_3 q_3,$
$p_4 q_2, p_5 q_5, p_6 q_6;$
and thus also p_2 and p_4.
Obvious:GCD computation.
Faster: scaled remainder trees.

Nice follow-up project:
Do this with Taiwan citizen cards.
Online data base of RSA keys.

These were generated on
certified smart cards;
should have good randomness.
But: student broke 103 keys.

Closer look at the 119 prime



These computations find q_2 in

$p_1 q_1, p_2 q_2, p_3 q_3,$

$p_4 q_2, p_5 q_5, p_6 q_6;$

and thus also p_2 and p_4.

Obvious:GCD computation.

Faster: scaled remainder trees.

Nice follow-up project:

Do this with Taiwan citizen cards.

Online data base of RSA keys.

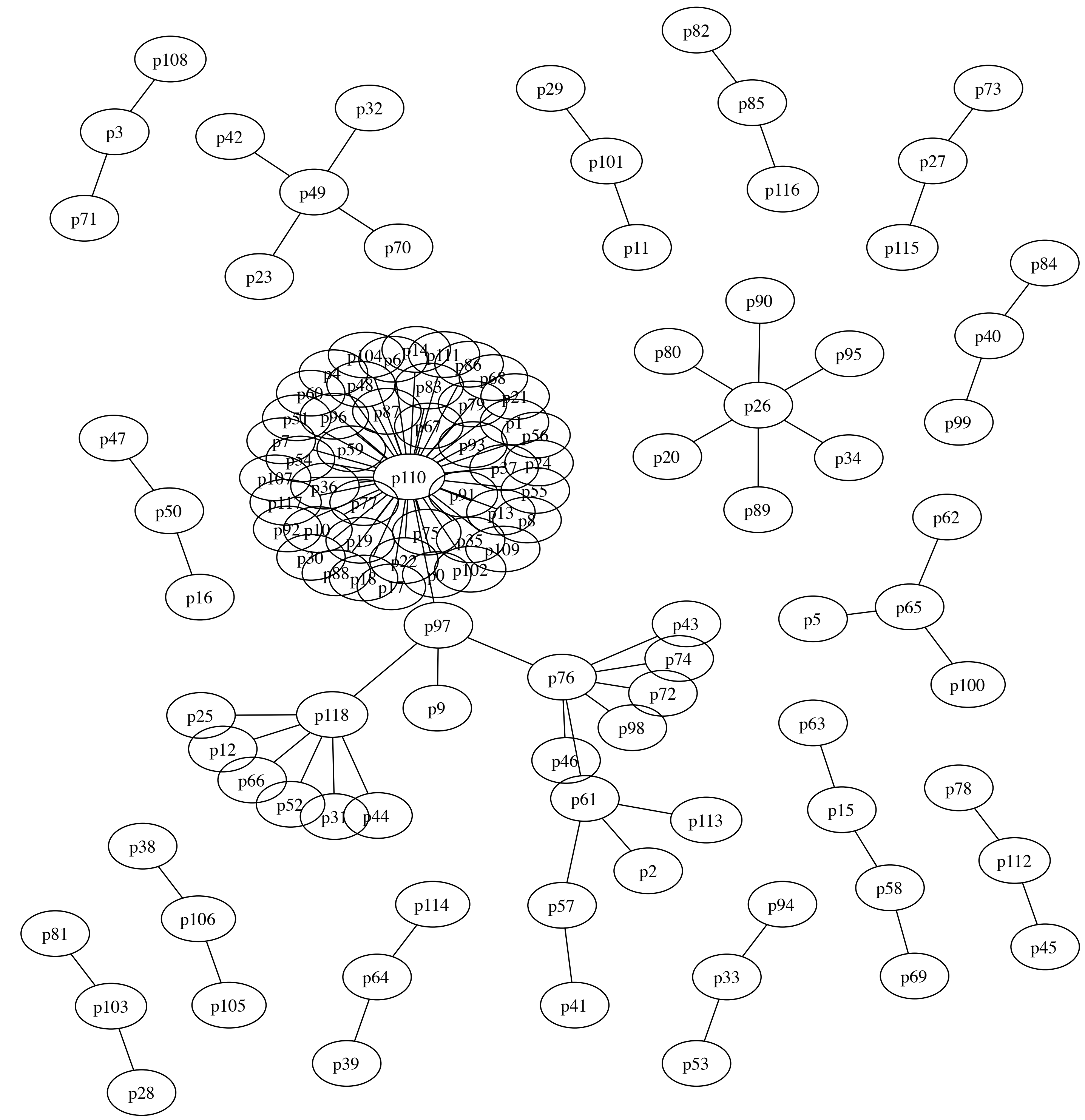
These were generated on

certified smart cards;

should have good randomness.

But: student broke 103 keys.

Closer look at the 119 primes



omputations find q_2 in

q_2, $p_3 q_3$,

q_5, $p_6 q_6$;

s also p_2 and p_4.

:GCD computation.

scaled remainder trees.

ow-up project:

with Taiwan citizen cards.

lata base of RSA keys.

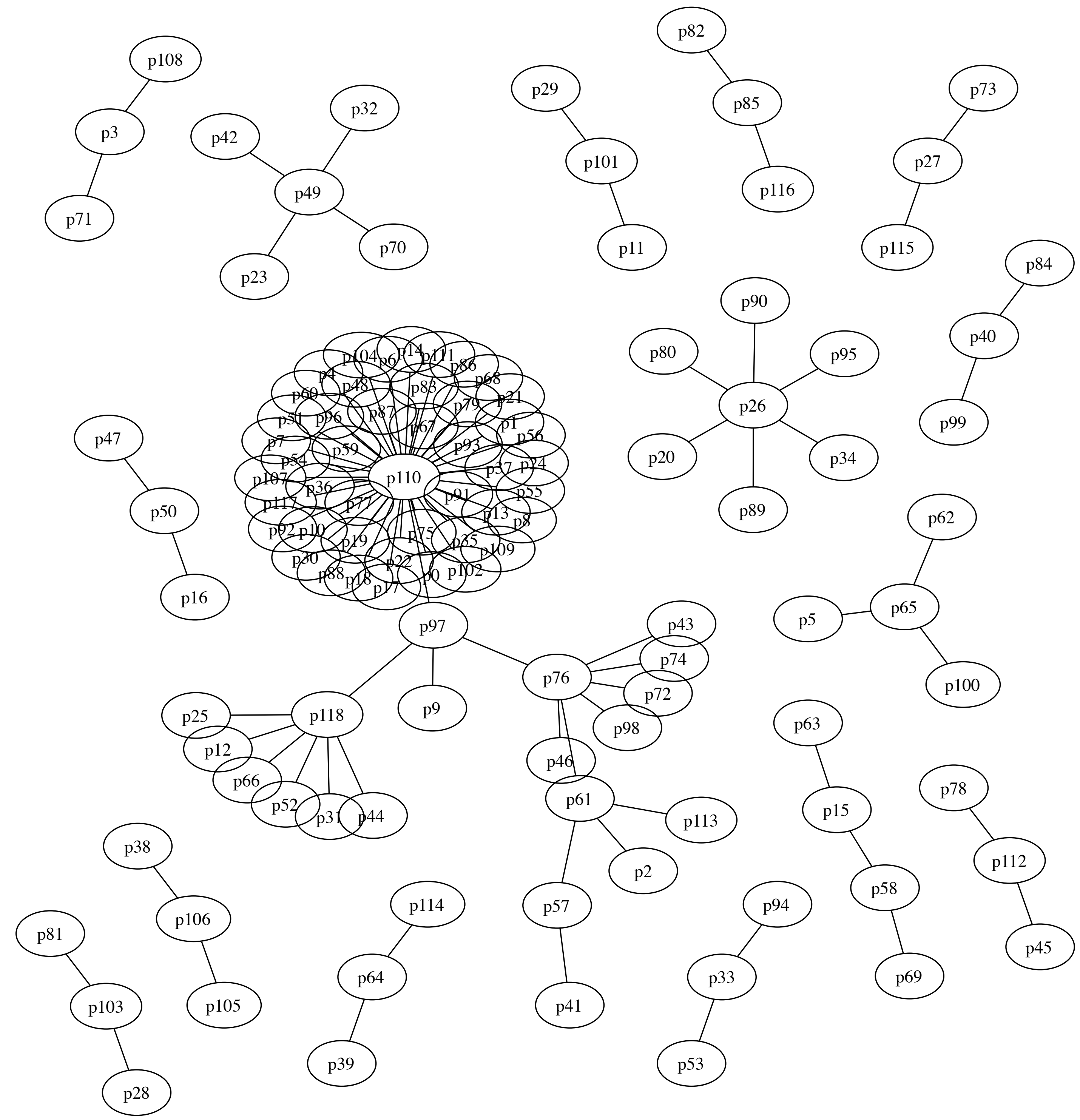
ere generated on

smart cards;

ave good randomness.

udent broke 103 keys.

Closer look at the 119 primes



Prime p

c00000000

00000000

00000000

00000000

ns find q_2 in

nd p_4.

nputation.

nainder trees.

ject:

an citizen cards.

of RSA keys.

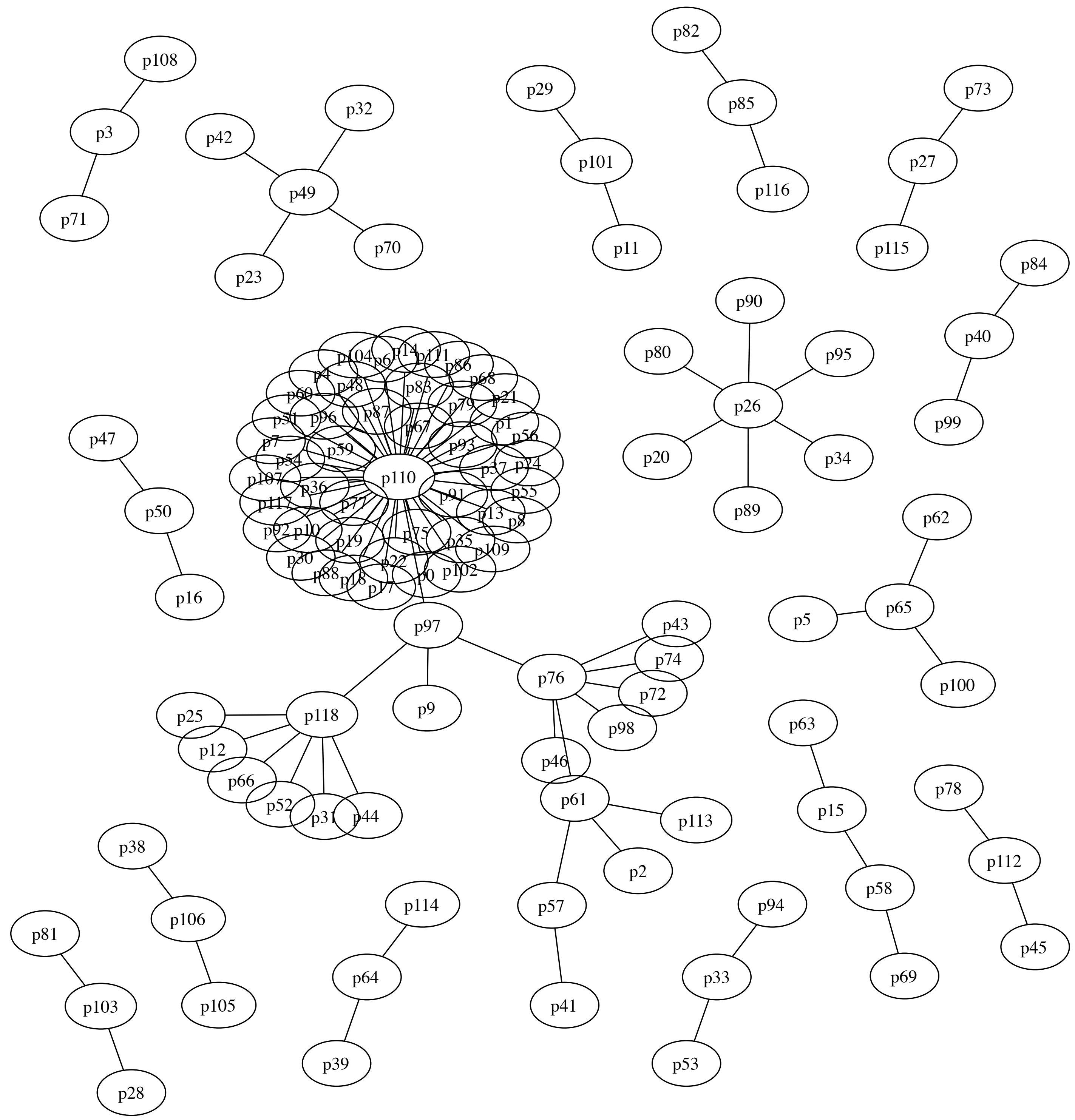
ated on

ds;

randomness.

e 103 keys.

Closer look at the 119 primes



Prime p110 appea

c0000000000000000

0000000000000000

0000000000000000

0000000000000000

in

es.

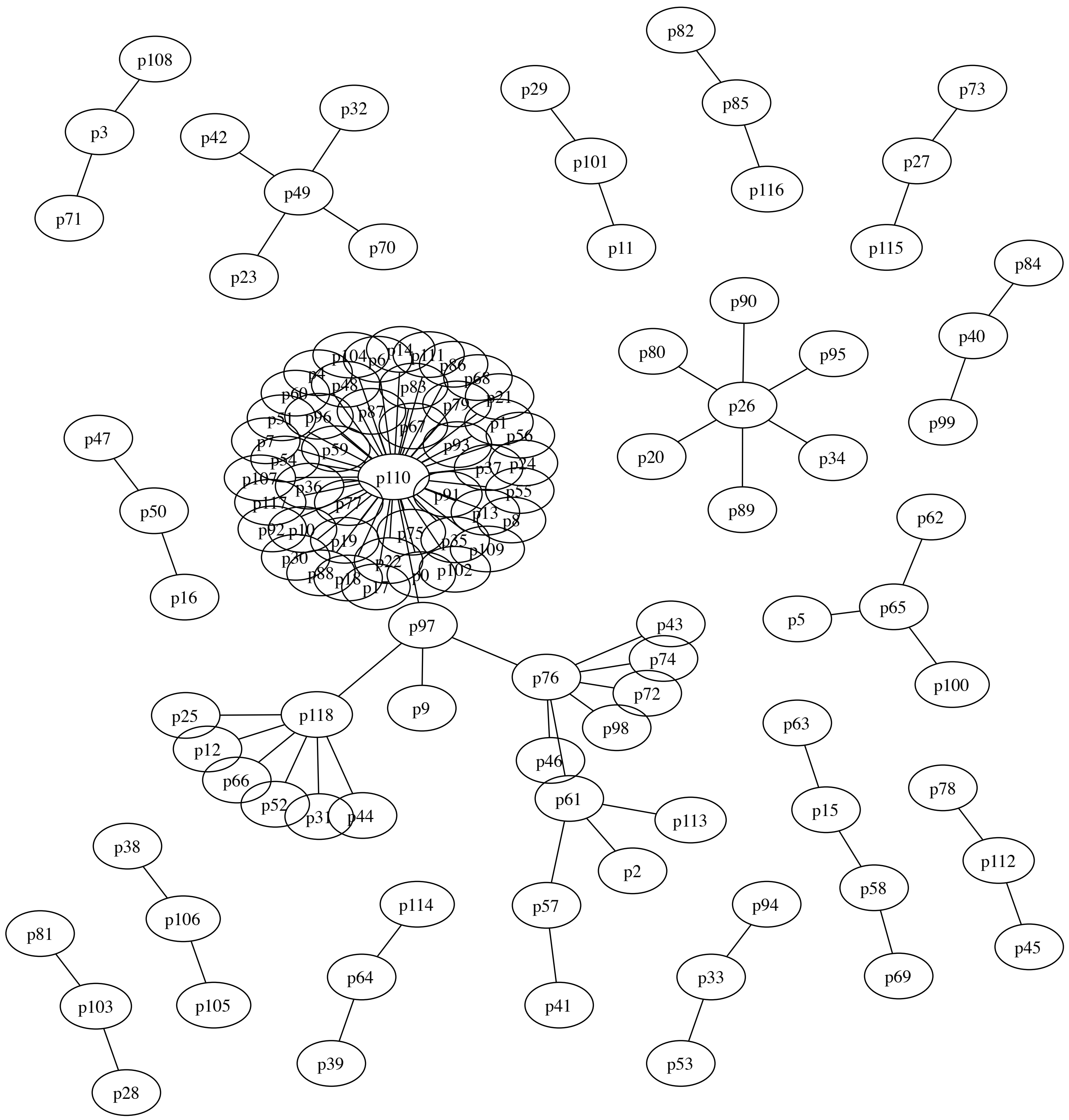
cards.

ys.

ss.

s.

Closer look at the 119 primes



Prime p110 appears 46 time

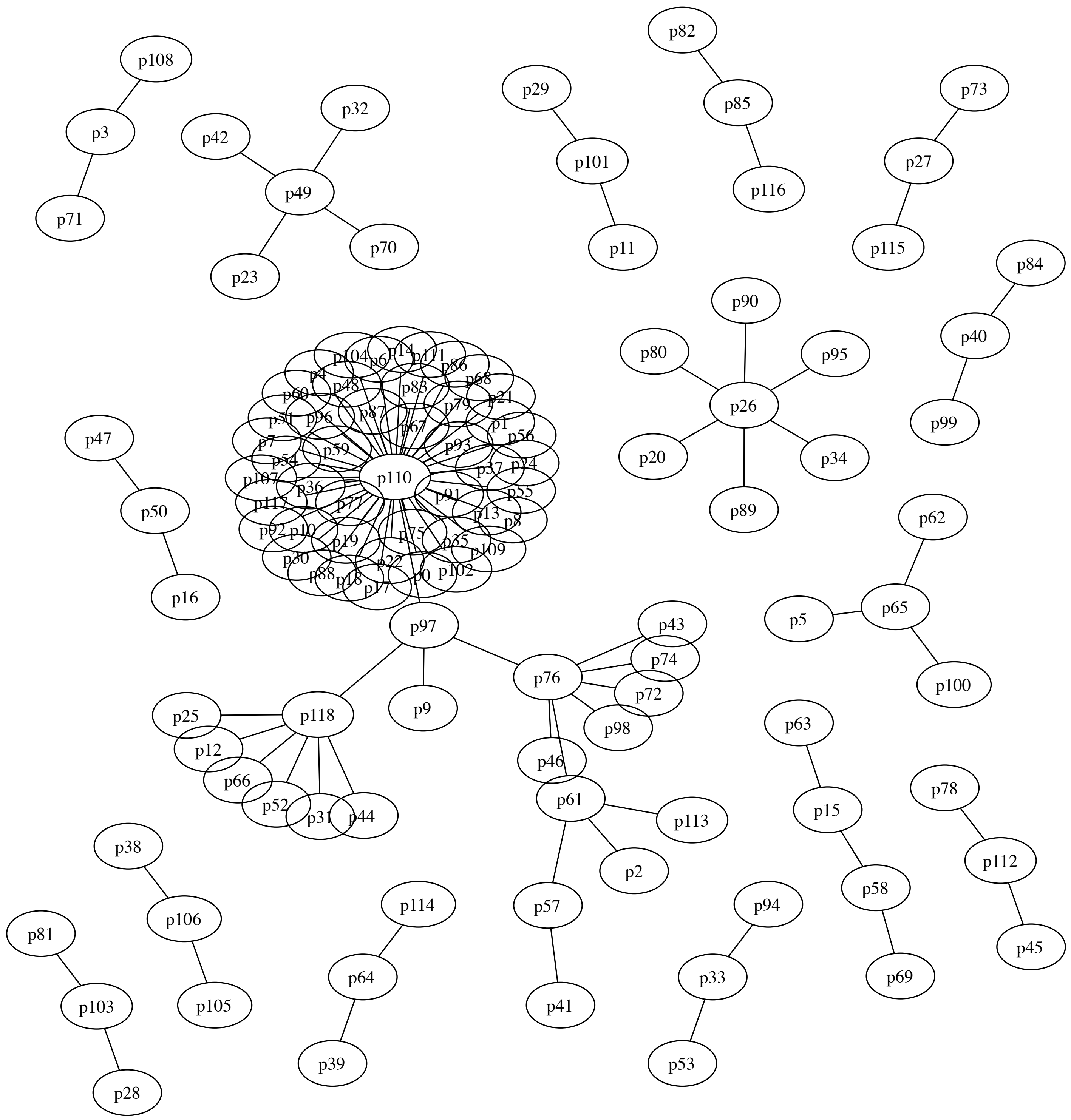
c00000000000000000000000000000

000000000000000000000000000000

000000000000000000000000000000

000000000000000000000000000000

Closer look at the 119 primes



Prime p110 appears 46 times

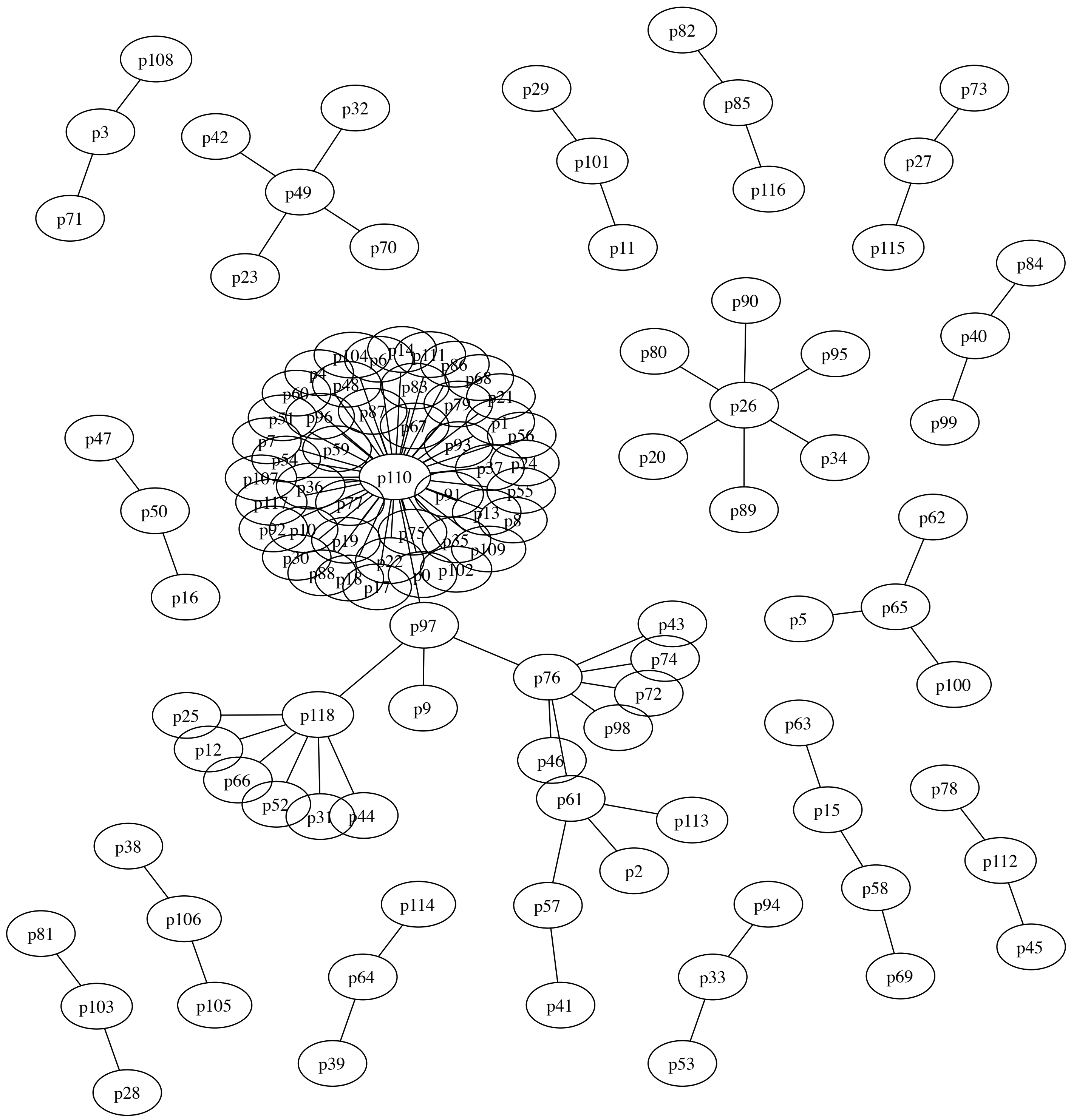
c0000000000000000000000000000000

00000000000000000000000000000000

00000000000000000000000000000000

000000000000000000000000000002f9

Closer look at the 119 primes

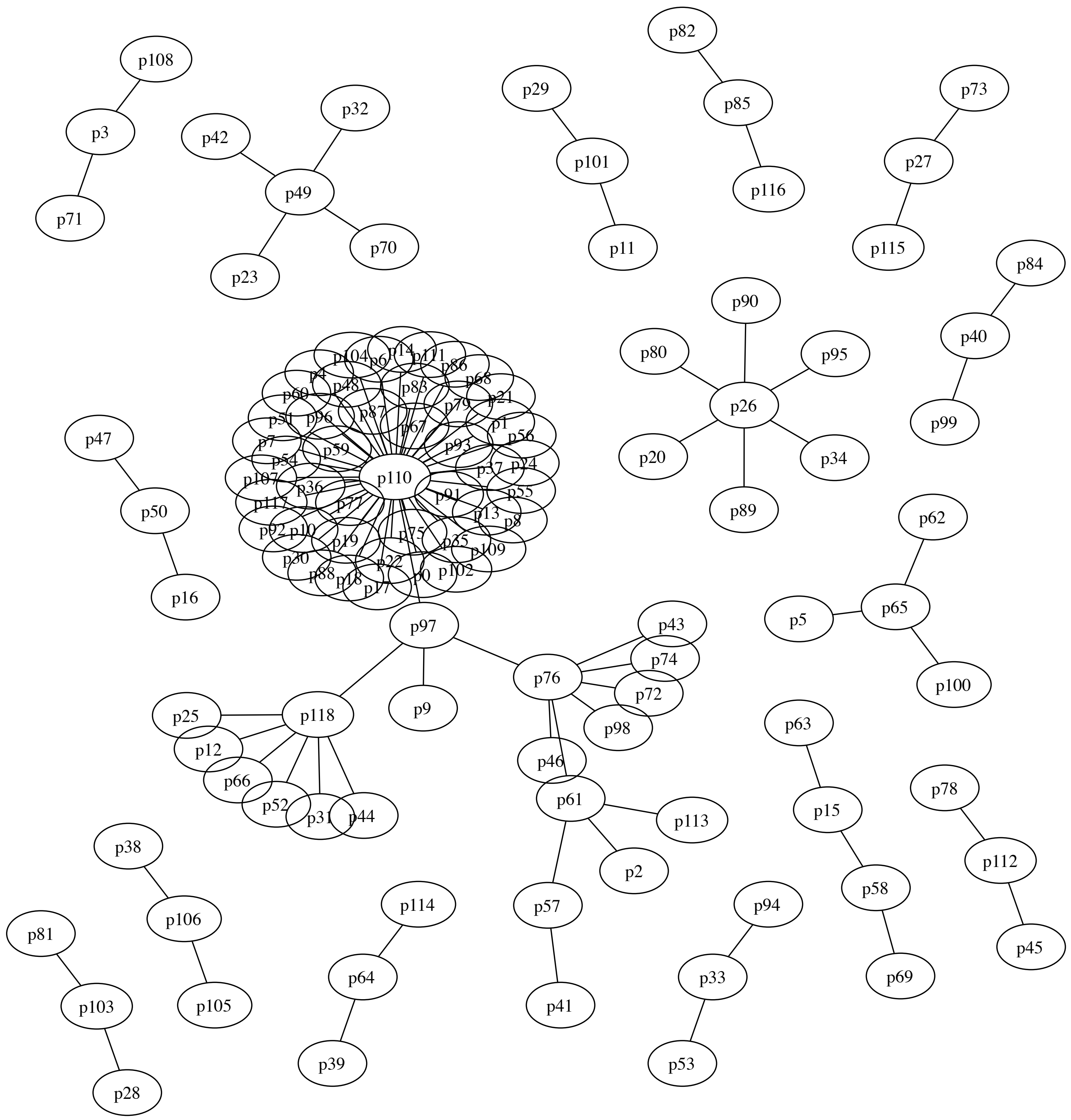


Prime p110 appears 46 times

```
c0000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
000000000000000000000000000002f9
```

which is the next prime after $2^{511} + 2^{510}$.

Closer look at the 119 primes



Prime p110 appears 46 times

c0000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
000000000000000000000000000002f9

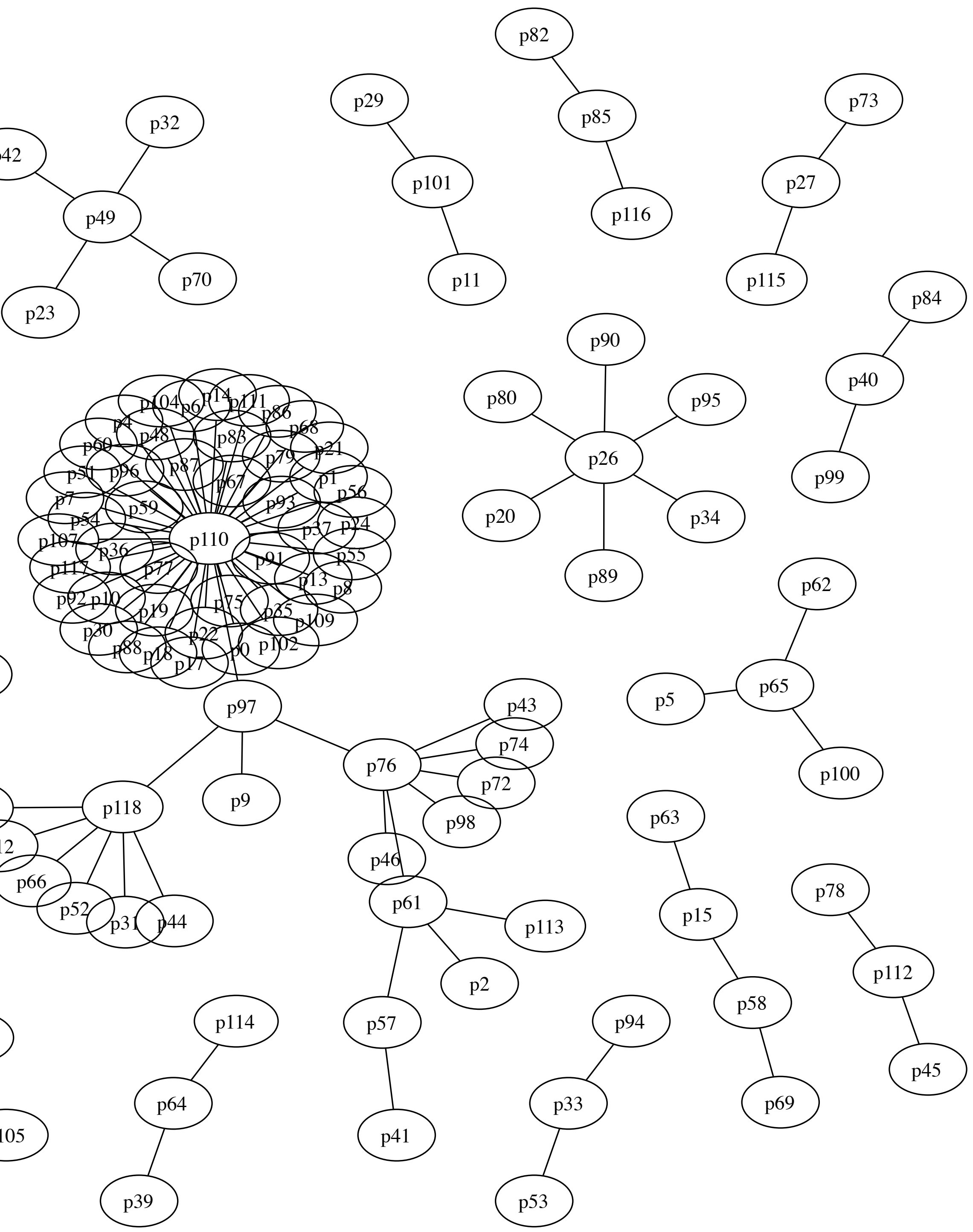
which is the next prime after $2^{511} + 2^{510}$.

Next up

c9242492249292499249492449242492
24929249924949244924249224929249
92494924492424922492924992494924
492424922492924992494924492424e5

Several other factors exhibit such a pattern.

ook at the 119 primes



Prime p110 appears 46 times

`c0000000000000000000000000000000`

`00000000000000000000000000000000`

`00000000000000000000000000000000`

`000000000000000000000000000002f9`

which is the next prime after $2^{511} + 2^{510}$.

Next up

`c9242492249292499249492449242492`

`24929249924949244924249224929249`

`92494924492424922492924992494924`

`492424922492924992494924492424e5`

Several other factors exhibit such a pattern.

Prime ge

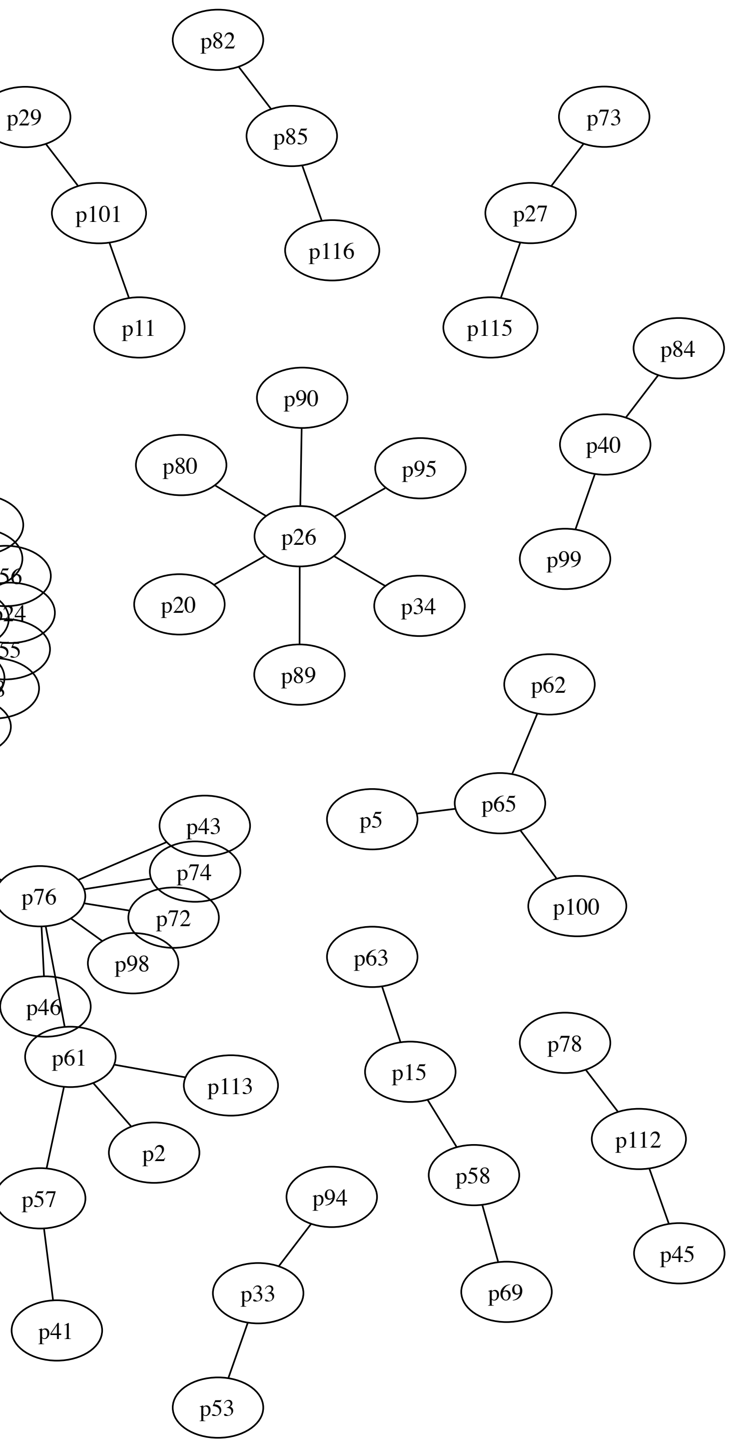
Choose a

3, 5, or

more tha

to exact

119 primes



Prime p110 appears 46 times

```
c0000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
000000000000000000000000000002f9
```

which is the next prime after $2^{511} + 2^{510}$.

Next up

```
c9242492249292499249492449242492
24929249924949244924249224929249
92494924492424922492924992494924
4924249224929249924949244924 24e5
```

Several other factors exhibit such a pattern.

Prime generation

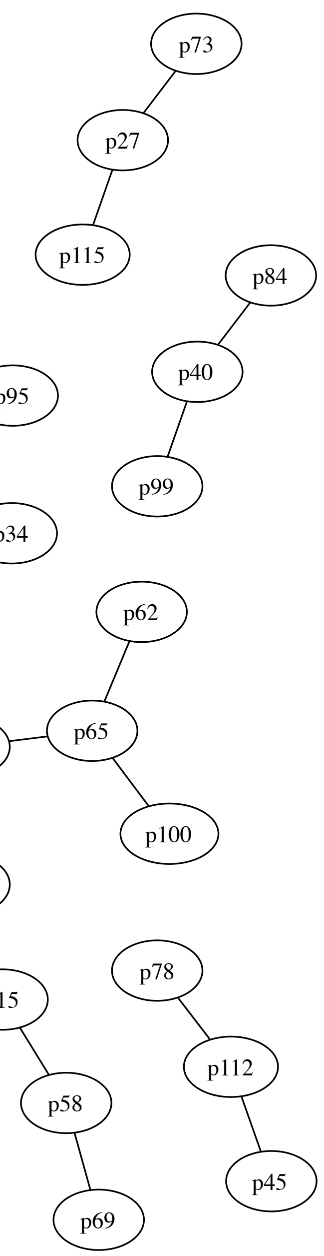
Choose a bit patte

3, 5, or 7 bits, rep

more than 512 bit

to exactly 512 bits

es



Prime p110 appears 46 times

```
c0000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
000000000000000000000000000002f9
```

which is the next prime after $2^{511} + 2^{510}$.

Next up

```
c9242492249292499249492449242492
24929249924949244924249224929249
92494924492424922492924992494924
4924249224929249924949244924 24e5
```

Several other factors exhibit such a pattern.

Prime generation

Choose a bit pattern of leng
3, 5, or 7 bits, repeat it to c
more than 512 bits, and trun
to exactly 512 bits.

Prime p110 appears 46 times

c0000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
000000000000000000000000000002f9

which is the next prime after $2^{511} + 2^{510}$.

Next up

c9242492249292499249492449242492
24929249924949244924249224929249
92494924492424922492924992494924
492424922492924992494924492424e5

Several other factors exhibit such a pattern.

Prime generation

Choose a bit pattern of length 1, 3, 5, or 7 bits, repeat it to cover more than 512 bits, and truncate to exactly 512 bits.

Prime p110 appears 46 times

`c0000000000000000000000000000000`

`00000000000000000000000000000000`

`00000000000000000000000000000000`

`000000000000000000000000000002f9`

which is the next prime after $2^{511} + 2^{510}$.

Next up

`c9242492249292499249492449242492`

`24929249924949244924249224929249`

`92494924492424922492924992494924`

`4924249224929249924949244924 24e5`

Several other factors exhibit such a pattern.

Prime generation

Choose a bit pattern of length 1, 3, 5, or 7 bits, repeat it to cover more than 512 bits, and truncate to exactly 512 bits.

For every 32-bit word, swap the lower and upper 16 bits.

Prime p110 appears 46 times

```
c0000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
000000000000000000000000000002f9
```

which is the next prime after $2^{511} + 2^{510}$.

Next up

```
c9242492249292499249492449242492
24929249924949244924249224929249
92494924492424922492924992494924
492424922492924992494924492424e5
```

Several other factors exhibit such a pattern.

Prime generation

Choose a bit pattern of length 1, 3, 5, or 7 bits, repeat it to cover more than 512 bits, and truncate to exactly 512 bits.

For every 32-bit word, swap the lower and upper 16 bits.

Fix the most significant two bits to 11.

Prime p110 appears 46 times

```
c0000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
000000000000000000000000000002f9
```

which is the next prime after $2^{511} + 2^{510}$.

Next up

```
c92424922492924992494924492424 92
24929249924949244924249224929249
92494924492424922492924992494924
4924249224929249924949244924 24e5
```

Several other factors exhibit such a pattern.

Prime generation

Choose a bit pattern of length 1, 3, 5, or 7 bits, repeat it to cover more than 512 bits, and truncate to exactly 512 bits.

For every 32-bit word, swap the lower and upper 16 bits.

Fix the most significant two bits to 11.

Find the next prime greater than or equal to this number.

110 appears 46 times

```
000000000000000000000000
000000000000000000000000
000000000000000000000000
0000000000000000000002f9
```

the next prime after

510
.

```
249292499249492449242492
924949244924249224929249
492424922492924992494924
2492924992494924492424e5
```

other factors exhibit such

n.

Prime generation

Choose a bit pattern of length 1, 3, 5, or 7 bits, repeat it to cover more than 512 bits, and truncate to exactly 512 bits.

For every 32-bit word, swap the lower and upper 16 bits.

Fix the most significant two bits to 11.

Find the next prime greater than or equal to this number.

Factorin

Choose

3, 5, or

more tha

to exact

For every

lower an

Fix the

to 11.

Find the

or equal

rs 46 times

0000000000000

0000000000000

0000000000000

000000000002f9

prime after

494924492424 92

24249224929249

92924992494924

494924492424e5

ors exhibit such

Prime generation

Choose a bit pattern of length 1, 3, 5, or 7 bits, repeat it to cover more than 512 bits, and truncate to exactly 512 bits.
For every 32-bit word, swap the lower and upper 16 bits.
Fix the most significant two bits to 11.
Find the next prime greater than or equal to this number.

Factoring by trial d

Choose a bit patte
3, 5, or 7 bits, rep
more than 512 bit
to exactly 512 bits
For every 32-bit w
lower and upper 1
Fix the most signi
to 11.
Find the next prim
or equal to this nu

es

0000

0000

0000

02f9

r

2492

9249

4924

24e5

such

Prime generation

Choose a bit pattern of length 1, 3, 5, or 7 bits, repeat it to cover more than 512 bits, and truncate to exactly 512 bits.
For every 32-bit word, swap the lower and upper 16 bits.
Fix the most significant two bits to 11.
Find the next prime greater than or equal to this number.

Factoring by trial division

Choose a bit pattern of leng
3, 5, or 7 bits, repeat it to c
more than 512 bits, and trur
to exactly 512 bits.
For every 32-bit word, swap
lower and upper 16 bits.
Fix the most significant two
to 11.
Find the next prime greater
or equal to this number.

Prime generation

Choose a bit pattern of length 1, 3, 5, or 7 bits, repeat it to cover more than 512 bits, and truncate to exactly 512 bits.
For every 32-bit word, swap the lower and upper 16 bits.
Fix the most significant two bits to 11.
Find the next prime greater than or equal to this number.

Factoring by trial division

Choose a bit pattern of length 1, 3, 5, or 7 bits, repeat it to cover more than 512 bits, and truncate to exactly 512 bits.
For every 32-bit word, swap the lower and upper 16 bits.
Fix the most significant two bits to 11.
Find the next prime greater than or equal to this number.

Prime generation

Choose a bit pattern of length 1, 3, 5, or 7 bits, repeat it to cover more than 512 bits, and truncate to exactly 512 bits.
For every 32-bit word, swap the lower and upper 16 bits.
Fix the most significant two bits to 11.
Find the next prime greater than or equal to this number.

Factoring by trial division

Choose a bit pattern of length 1, 3, 5, or 7 bits, repeat it to cover more than 512 bits, and truncate to exactly 512 bits.
For every 32-bit word, swap the lower and upper 16 bits.
Fix the most significant two bits to 11.
Find the next prime greater than or equal to this number.

Do this for any pattern:
0,1,001,010,011,100,101,110
00001,00010,00011,00100,00101,...

eneration

a bit pattern of length 1,
7 bits, repeat it to cover
an 512 bits, and truncate
ly 512 bits.
y 32-bit word, swap the
d upper 16 bits.
most significant two bits

e next prime greater than
to this number.

Factoring by trial division

Choose a bit pattern of length 1, 3, 5, or 7 bits, repeat it to cover more than 512 bits, and truncate to exactly 512 bits.
For every 32-bit word, swap the lower and upper 16 bits.
Fix the most significant two bits to 11.
Find the next prime greater than or equal to this number.

Do this for any pattern:
0,1,001,010,011,100,101,110
00001,00010,00011,00100,00101,. . .

Computi
moduli,

ern of length 1,
eat it to cover
s, and truncate
s.
ord, swap the
6 bits.
ficant two bits

ne greater than
umber.

Factoring by trial division

Choose a bit pattern of length 1, 3, 5, or 7 bits, repeat it to cover more than 512 bits, and truncate to exactly 512 bits.
For every 32-bit word, swap the lower and upper 16 bits.
Fix the most significant two bits to 11.
Find the next prime greater than or equal to this number.

Do this for any pattern:
0,1,001,010,011,100,101,110
00001,00010,00011,00100,00101,. . .

Computing GCDs
moduli, of which 1

Factoring by trial division

Choose a bit pattern of length 1, 3, 5, or 7 bits, repeat it to cover more than 512 bits, and truncate to exactly 512 bits.
For every 32-bit word, swap the lower and upper 16 bits.
Fix the most significant two bits to 11.
Find the next prime greater than or equal to this number.

Do this for any pattern:
0,1,001,010,011,100,101,110
00001,00010,00011,00100,00101,...

Computing GCDs factored 1
moduli, of which 18 were ne

Factoring by trial division

Choose a bit pattern of length 1, 3, 5, or 7 bits, repeat it to cover more than 512 bits, and truncate to exactly 512 bits.
For every 32-bit word, swap the lower and upper 16 bits.
Fix the most significant two bits to 11.
Find the next prime greater than or equal to this number.

Do this for any pattern:
0,1,001,010,011,100,101,110
00001,00010,00011,00100,00101,. . .

Computing GCDs factored 105 moduli, of which 18 were new.

Factoring by trial division

Choose a bit pattern of length 1, 3, 5, or 7 bits, repeat it to cover more than 512 bits, and truncate to exactly 512 bits.
For every 32-bit word, swap the lower and upper 16 bits.
Fix the most significant two bits to 11.
Find the next prime greater than or equal to this number.

Do this for any pattern:
0,1,001,010,011,100,101,110
00001,00010,00011,00100,00101,. . .

Computing GCDs factored 105 moduli, of which 18 were new.

Breaking RSA-1024
by "trial division".
Factored 4 more keys using patterns of length 9.

Factoring by trial division

Choose a bit pattern of length 1, 3, 5, or 7 bits, repeat it to cover more than 512 bits, and truncate to exactly 512 bits.
For every 32-bit word, swap the lower and upper 16 bits.
Fix the most significant two bits to 11.
Find the next prime greater than or equal to this number.

Do this for any pattern:
0,1,001,010,011,100,101,110
00001,00010,00011,00100,00101,...

Computing GCDs factored 105 moduli, of which 18 were new.

Breaking RSA-1024 by "trial division".
Factored 4 more keys using patterns of length 9.

More factors by studying other keys and using lattices.
"Factoring RSA keys from certified smart cards: Coppersmith in the wild"
(with D.J. Bernstein, Y.-A. Chang, C.-M. Cheng, L.-P. Chou, N. Heninger, N. van Someren)
http://smartfacts.cr.yp.to/

g by trial division

a bit pattern of length 1,
7 bits, repeat it to cover
an 512 bits, and truncate
ly 512 bits.
y 32-bit word, swap the
d upper 16 bits.
most significant two bits

next prime greater than
to this number.

for any pattern:
010,011,100,101,110
0010,00011,00100,00101,. . .

Computing GCDs factored 105 moduli, of which 18 were new.

Breaking RSA-1024 by "trial division".
Factored 4 more keys using patterns of length 9.

More factors by studying other keys and using lattices.
"Factoring RSA keys from certified smart cards: Coppersmith in the wild"
(with D.J. Bernstein, Y.-A. Chang, C.-M. Cheng, L.-P. Chou, N. Heninger, N. van Someren)
http://smartfacts.cr.yp.to/

Bad RSA

M. Nem
D. Kline
All RSA
Infineon
n mod 2
n mod 1
n mod 3
n mod 9
n mod 3

division

ern of length 1,
eat it to cover
s, and truncate
s.
ord, swap the
6 bits.
ficant two bits

ne greater than
umber.

ttern:
00,101,110
1,00100,00101,. . .

Computing GCDs factored 105 moduli, of which 18 were new.

Breaking RSA-1024
by "trial division".
Factored 4 more keys using patterns of length 9.

More factors by studying other keys and using lattices.
"Factoring RSA keys from certified smart cards: Coppersmith in the wild"
(with D.J. Bernstein, Y.-A. Chang, C.-M. Cheng, L.-P. Chou, N. Heninger, N. van Someren)
http://smartfacts.cr.yp.to/

Bad RSA random

M. Nemec, M. Sys
D. Klinec, V. Mat
All RSA keys gene
Infineon smart car
$n \bmod 2 = 1$
$n \bmod 11 \in \{1, 10$
$n \bmod 37 \in \{1, 10$
$n \bmod 97 \in \{1, 35$
$n \bmod 331 \in \{1, 3$

th 1,
cover
ncate

the

bits

than

0
0101,. . .

Computing GCDs factored 105 moduli, of which 18 were new.

Breaking RSA-1024 by “trial division”. Factored 4 more keys using patterns of length 9.

More factors by studying other keys and using lattices. “Factoring RSA keys from certified smart cards: Coppersmith in the wild” (with D.J. Bernstein, Y.-A. Chang, C.-M. Cheng, L.-P. Chou, N. Heninger, N. van Someren)
http://smartfacts.cr.yp.to/

Bad RSA randomness 2017

M. Nemec, M. Sys, P. Svend
D. Klinec, V. Matyas

All RSA keys generated by s
Infineon smart cards satisfy

$n \bmod 2 = 1$

$n \bmod 11 \in \{1, 10\}$

$n \bmod 37 \in \{1, 10, 37\}$

$n \bmod 97 \in \{1, 35, 36, 61, 62$

$n \bmod 331 \in \{1, 330\}$

Computing GCDs factored 105 moduli, of which 18 were new.

Breaking RSA-1024 by “trial division”. Factored 4 more keys using patterns of length 9.

More factors by studying other keys and using lattices. “Factoring RSA keys from certified smart cards: Coppersmith in the wild” (with D.J. Bernstein, Y.-A. Chang, C.-M. Cheng, L.-P. Chou, N. Heninger, N. van Someren) http://smartfacts.cr.yp.to/

Bad RSA randomness 2017 – ROCA

M. Nemec, M. Sys, P. Svenda, D. Klinec, V. Matyas

All RSA keys generated by some Infineon smart cards satisfy

$n \bmod 2 = 1$

$n \bmod 11 \in \{1, 10\}$

$n \bmod 37 \in \{1, 10, 37\}$

$n \bmod 97 \in \{1, 35, 36, 61, 62, 96\}$

$n \bmod 331 \in \{1, 330\}$

Computing GCDs factored 105 moduli, of which 18 were new.

Breaking RSA-1024 by "trial division". Factored 4 more keys using patterns of length 9.

More factors by studying other keys and using lattices. "Factoring RSA keys from certified smart cards: Coppersmith in the wild" (with D.J. Bernstein, Y.-A. Chang, C.-M. Cheng, L.-P. Chou, N. Heninger, N. van Someren) http://smartfacts.cr.yp.to/

Bad RSA randomness 2017 – ROCA

M. Nemec, M. Sys, P. Svenda, D. Klinec, V. Matyas

All RSA keys generated by some Infineon smart cards satisfy

$n \bmod 2 = 1$

$n \bmod 11 \in \{1, 10\}$

$n \bmod 37 \in \{1, 10, 37\}$

$n \bmod 97 \in \{1, 35, 36, 61, 62, 96\}$

$n \bmod 331 \in \{1, 330\}$

These give $1 \cdot 2 \cdot 3 \cdot 6 \cdot 2 = 72$ possibilities of $n \bmod L$, where $L = 2 \cdot 11 \cdot 37 \cdot 97 \cdot 331$, instead of $1 \cdot 10 \cdot 36 \cdot 96 \cdot 330 = 11404800$

ing GCDs factored 105
of which 18 were new.

g RSA-1024
division".
l 4 more keys using
of length 9.

ctors by studying other
l using lattices.
ng RSA keys from
smart cards:
mith in the wild"
J. Bernstein, Y.-A.
C.-M. Cheng, L.-P. Chou,
nger, N. van Someren)
martfacts.cr.yp.to/

Bad RSA randomness 2017 – ROCA

M. Nemec, M. Sys, P. Svenda,
D. Klinec, V. Matyas

All RSA keys generated by some Infineon smart cards satisfy

$n \bmod 2 = 1$
$n \bmod 11 \in \{1, 10\}$
$n \bmod 37 \in \{1, 10, 37\}$
$n \bmod 97 \in \{1, 35, 36, 61, 62, 96\}$
$n \bmod 331 \in \{1, 330\}$

These give $1 \cdot 2 \cdot 3 \cdot 6 \cdot 2 = 72$ possibilities of $n \bmod L$, where $L = 2 \cdot 11 \cdot 37 \cdot 97 \cdot 331$, instead of $1 \cdot 10 \cdot 36 \cdot 96 \cdot 330 = 11404800$

Worse,
$n \bmod 2$
$\in \{1, 6$
8942297

factored 105
18 were new.
24

eys using
9.

udying other
tices.
eys from
ds:
e wild"
ein, Y.-A.
ng, L.-P. Chou,
an Someren)
cr.yp.to/

Bad RSA randomness 2017 – ROCA

M. Nemec, M. Sys, P. Svenda,
D. Klinec, V. Matyas
All RSA keys generated by some
Infineon smart cards satisfy

$n \bmod 2 = 1$
$n \bmod 11 \in \{1, 10\}$
$n \bmod 37 \in \{1, 10, 37\}$
$n \bmod 97 \in \{1, 35, 36, 61, 62, 96\}$
$n \bmod 331 \in \{1, 330\}$

These give $1 \cdot 2 \cdot 3 \cdot 6 \cdot 2 = 72$
possibilities of $n \bmod L$, where
$L = 2 \cdot 11 \cdot 37 \cdot 97 \cdot 331$, instead of
$1 \cdot 10 \cdot 36 \cdot 96 \cdot 330 = 11404800$

Worse,
$n \bmod 2 \cdot 11 \cdot 37 \cdot$ 9
$\in \{1, 65537, 487$
$8942297, 1436738$

105

ew.

her

Chou,

en)

Bad RSA randomness 2017 – ROCA

M. Nemec, M. Sys, P. Svenda,
D. Klinec, V. Matyas

All RSA keys generated by some Infineon smart cards satisfy

$n \bmod 2 = 1$

$n \bmod 11 \in \{1, 10\}$

$n \bmod 37 \in \{1, 10, 37\}$

$n \bmod 97 \in \{1, 35, 36, 61, 62, 96\}$

$n \bmod 331 \in \{1, 330\}$

These give $1 \cdot 2 \cdot 3 \cdot 6 \cdot 2 = 72$ possibilities of $n \bmod L$, where $L = 2 \cdot 11 \cdot 37 \cdot 97 \cdot 331$, instead of $1 \cdot 10 \cdot 36 \cdot 96 \cdot 330 = 11404800$

Worse,

$n \bmod 2 \cdot 11 \cdot 37 \cdot 97 \cdot 331$

$\in \{1, 65537, 4878941,$

$8942297, 14367385, 2401603$

Bad RSA randomness 2017 – ROCA

M. Nemec, M. Sys, P. Svenda,
D. Klinec, V. Matyas

All RSA keys generated by some Infineon smart cards satisfy

$n \bmod 2 = 1$

$n \bmod 11 \in \{1, 10\}$

$n \bmod 37 \in \{1, 10, 37\}$

$n \bmod 97 \in \{1, 35, 36, 61, 62, 96\}$

$n \bmod 331 \in \{1, 330\}$

These give $1 \cdot 2 \cdot 3 \cdot 6 \cdot 2 = 72$ possibilities of $n \bmod L$, where $L = 2 \cdot 11 \cdot 37 \cdot 97 \cdot 331$, instead of $1 \cdot 10 \cdot 36 \cdot 96 \cdot 330 = 11404800$

Worse,

$n \bmod 2 \cdot 11 \cdot 37 \cdot 97 \cdot 331$

$\in \quad \{1, 65537, 4878941,$
$8942297, 14367385, 24016035\}$

Bad RSA randomness 2017 – ROCA

M. Nemec, M. Sys, P. Svenda,
D. Klinec, V. Matyas
All RSA keys generated by some Infineon smart cards satisfy
$n \bmod 2 = 1$
$n \bmod 11 \in \{1, 10\}$
$n \bmod 37 \in \{1, 10, 37\}$
$n \bmod 97 \in \{1, 35, 36, 61, 62, 96\}$
$n \bmod 331 \in \{1, 330\}$

These give $1 \cdot 2 \cdot 3 \cdot 6 \cdot 2 = 72$ possibilities of $n \bmod L$, where $L = 2 \cdot 11 \cdot 37 \cdot 97 \cdot 331$, instead of $1 \cdot 10 \cdot 36 \cdot 96 \cdot 330 = 11404800$

Worse,

$n \bmod 2 \cdot 11 \cdot 37 \cdot 97 \cdot 331$
$\in \quad \{1, 65537, 4878941,$
$8942297, 14367385, 24016035\}$

$n \in \left\{65537^i \bmod L | i \in \mathbf{Z}\right\}$
and 65537 has order 6 mod L.

Bad RSA randomness 2017 – ROCA

M. Nemec, M. Sys, P. Svenda,
D. Klinec, V. Matyas

All RSA keys generated by some Infineon smart cards satisfy

$n \bmod 2 = 1$

$n \bmod 11 \in \{1, 10\}$

$n \bmod 37 \in \{1, 10, 37\}$

$n \bmod 97 \in \{1, 35, 36, 61, 62, 96\}$

$n \bmod 331 \in \{1, 330\}$

These give $1 \cdot 2 \cdot 3 \cdot 6 \cdot 2 = 72$ possibilities of $n \bmod L$, where $L = 2 \cdot 11 \cdot 37 \cdot 97 \cdot 331$, instead of $1 \cdot 10 \cdot 36 \cdot 96 \cdot 330 = 11404800$

Worse,

$n \bmod 2 \cdot 11 \cdot 37 \cdot 97 \cdot 331$
$\in \{1, 65537, 4878941, 8942297, 14367385, 24016035\}$

$n \in \left\{65537^i \bmod L | i \in \mathbf{Z}\right\}$
and 65537 has order 6 mod L.

If $n = p \cdot q = 65537^i \bmod L$ then likely
$p, q \in \left\{65537^i \bmod L | i \in \mathbf{Z}\right\}$.

Bad RSA randomness 2017 – ROCA

M. Nemec, M. Sys, P. Svenda, D. Klinec, V. Matyas

All RSA keys generated by some Infineon smart cards satisfy

$n \bmod 2 = 1$

$n \bmod 11 \in \{1, 10\}$

$n \bmod 37 \in \{1, 10, 37\}$

$n \bmod 97 \in \{1, 35, 36, 61, 62, 96\}$

$n \bmod 331 \in \{1, 330\}$

These give $1 \cdot 2 \cdot 3 \cdot 6 \cdot 2 = 72$ possibilities of $n \bmod L$, where $L = 2 \cdot 11 \cdot 37 \cdot 97 \cdot 331$, instead of $1 \cdot 10 \cdot 36 \cdot 96 \cdot 330 = 11404800$

Worse,

$n \bmod 2 \cdot 11 \cdot 37 \cdot 97 \cdot 331$
$\in \quad \{1, 65537, 4878941, 8942297, 14367385, 24016035\}$

$n \in \left\{65537^i \bmod L | i \in \mathbf{Z}\right\}$ and 65537 has order 6 mod L.

If $n = p \cdot q = 65537^i \bmod L$ then likely $p, q \in \left\{65537^i \bmod L | i \in \mathbf{Z}\right\}$.

There are more congruences where this holds.
Actually $L = \prod_{\ell < 702, \ell \text{prime}} \ell$.

A randomness 2017 – ROCA

ec, M. Sys, P. Svenda,
c, V. Matyas
keys generated by some
smart cards satisfy
$= 1$
$1 \in \{1, 10\}$
$7 \in \{1, 10, 37\}$
$7 \in \{1, 35, 36, 61, 62, 96\}$
$31 \in \{1, 330\}$

ive $1 \cdot 2 \cdot 3 \cdot 6 \cdot 2 = 72$
ties of $n \bmod L$, where
$11 \cdot 37 \cdot 97 \cdot 331$, instead of
$6 \cdot 96 \cdot 330 = 11404800$

Worse,
$n \bmod 2 \cdot 11 \cdot 37 \cdot 97 \cdot 331$
$\in \{1, 65537, 4878941,$
$8942297, 14367385, 24016035\}$

$n \in \left\{65537^i \bmod L | i \in \mathbf{Z}\right\}$
and 65537 has order 6 $\bmod L$.

If $n = p \cdot q = 65537^i \bmod L$
then likely
$p, q \in \left\{65537^i \bmod L | i \in \mathbf{Z}\right\}$.

There are more congruences
where this holds.
Actually $L = \prod_{\ell < 702, \ell \text{prime}} \ell$.

How do

$\log_2 L \approx$
so $p = p$
where p
$\gcd\{k, L$
is rando
Same fo

nes 2017 – ROCA

s, P. Svenda,
yas
erated by some
ds satisfy

}
, 37}
, 36, 61, 62, 96}
30}

3 · 6 · 2 = 72
nod L, where
· 331, instead of
0 = 11404800

Worse,

$n \bmod 2 \cdot 11 \cdot 37 \cdot 97 \cdot 331$
$\in \quad \{1, 65537, 4878941,$
$8942297, 14367385, 24016035\}$

$n \in \left\{65537^i \bmod L | i \in \mathbf{Z}\right\}$
and 65537 has order 6 $\bmod L$.

If $n = p \cdot q = 65537^i \bmod L$
then likely
$p, q \in \left\{65537^i \bmod L | i \in \mathbf{Z}\right\}$.

There are more congruences
where this holds.
Actually $L = \prod_{\ell < 702, \ell \text{prime}} \ell$.

How do these turn

$\log_2 L \approx 971$ and
so $p = p' + k \cdot L$,
where $p \equiv p' \bmod$
$\gcd\{k, L\} = 1$ and
is random so that
Same for q.

– ROCA

da,

some

2, 96}

72

ere

tead of

800

Worse,

$n \bmod 2 \cdot 11 \cdot 37 \cdot 97 \cdot 331$
$\in \quad \{1, 65537, 4878941,$
$8942297, 14367385, 24016035\}$

$n \in \left\{65537^i \bmod L | i \in \mathbf{Z}\right\}$
and 65537 has order 6 $\bmod L$.

If $n = p \cdot q = 65537^i \bmod L$
then likely
$p, q \in \left\{65537^i \bmod L | i \in \mathbf{Z}\right\}$.

There are more congruences
where this holds.
Actually $L = \prod_{\ell < 702, \ell \text{prime}} \ell$.

How do these turn into prim

$\log_2 L \approx 971$ and $\log_2 p = 1$
so $p = p' + k \cdot L$,
where $p \equiv p' \bmod L$, and k v
$\gcd\{k, L\} = 1$ and $\log_2 k \approx$
is random so that p is prime
Same for q.

Worse,

$n \bmod 2 \cdot 11 \cdot 37 \cdot 97 \cdot 331$

$\in \quad \{1, 65537, 4878941,$

$8942297, 14367385, 24016035\}$

$n \in \left\{65537^i \bmod L | i \in \mathbf{Z}\right\}$

and 65537 has order 6 $\bmod L$.

If $n = p \cdot q = 65537^i \bmod L$

then likely

$p, q \in \left\{65537^i \bmod L | i \in \mathbf{Z}\right\}$.

There are more congruences

where this holds.

Actually $L = \prod_{\ell < 702, \ell \text{prime}} \ell$.

<u>How do these turn into primes?</u>

$\log_2 L \approx 971$ and $\log_2 p = 1024$,

so $p = p' + k \cdot L$,

where $p \equiv p' \bmod L$, and k with

$\gcd\{k, L\} = 1$ and $\log_2 k \approx 53$

is random so that p is prime.

Same for q.

Worse,

$n \bmod 2 \cdot 11 \cdot 37 \cdot 97 \cdot 331$
$\in \quad \{1, 65537, 4878941,$
$8942297, 14367385, 24016035\}$

$n \in \left\{65537^i \bmod L | i \in \mathbf{Z}\right\}$
and 65537 has order 6 $\bmod L$.

If $n = p \cdot q = 65537^i \bmod L$
then likely
$p, q \in \left\{65537^i \bmod L | i \in \mathbf{Z}\right\}$.

There are more congruences
where this holds.
Actually $L = \prod_{\ell < 702, \ell \text{prime}} \ell$.

<u>How do these turn into primes?</u>

$\log_2 L \approx 971$ and $\log_2 p = 1024$,
so $p = p' + k \cdot L$,
where $p \equiv p' \bmod L$, and k with
$\gcd\{k, L\} = 1$ and $\log_2 k \approx 53$
is random so that p is prime.
Same for q.

Lenstra's "Divisors in Residue
Classes" finds prime factors of
the form $p = u + k \cdot L$
efficiently if $L \geq n^{1/3}$.
Coppersmith, Howgrave-Graham,
and Nagaraj work for $L \geq n^{1/4}$.

$\log_2 L > 970 > 683 > 2048/3$.

$\cdot 11 \cdot 37 \cdot 97 \cdot 331$

$55537, 4878941,$

$, 14367385, 24016035\}$

$537^i \bmod L | i \in \mathbf{Z}\}$

37 has order 6 mod L.

$\cdot q = 65537^i \bmod L$

ely

$65537^i \bmod L | i \in \mathbf{Z}\}$.

re more congruences

his holds.

$L = \prod_{\ell < 702, \ell \text{prime}} \ell$.

How do these turn into primes?

$\log_2 L \approx 971$ and $\log_2 p = 1024$, so $p = p' + k \cdot L$, where $p \equiv p' \bmod L$, and k with $\gcd\{k, L\} = 1$ and $\log_2 k \approx 53$ is random so that p is prime. Same for q.

Lenstra's "Divisors in Residue Classes" finds prime factors of the form $p = u + k \cdot L$ efficiently if $L \geq n^{1/3}$. Coppersmith, Howgrave-Graham, and Nagaraj work for $L \geq n^{1/4}$.

$\log_2 L > 970 > 683 > 2048/3$.

Full atta

Run Len

$\{65537^i$

Each rur

there are

p', e.g.

$\{\pm 1, \pm 2$

$97 \cdot 331$
$8941,$
$5, 24016035\}$

$L|i \in \mathbf{Z}\big\}$
ler 6 mod L.

$37^i \bmod L$

d $L|i \in \mathbf{Z}\big\}$.

ongruences

$_{702,\ell \text{prime}}\,\ell$.

How do these turn into primes?

$\log_2 L \approx 971$ and $\log_2 p = 1024$,
so $p = p' + k \cdot L$,
where $p \equiv p' \bmod L$, and k with $\gcd\{k, L\} = 1$ and $\log_2 k \approx 53$ is random so that p is prime.
Same for q.

Lenstra's "Divisors in Residue Classes" finds prime factors of the form $p = u + k \cdot L$ efficiently if $L \geq n^{1/3}$.
Coppersmith, Howgrave-Graham, and Nagaraj work for $L \geq n^{1/4}$.

$\log_2 L > 970 > 683 > 2048/3$.

Full attack

Run Lensta for all
$\big\{65537^i \bmod L|i \in$
Each run is cheap,
there are many op
p', e.g. 65537^i mo
$\{\pm 1, \pm 2, \pm 3, \pm 4, .$

$35\}$

L.

$\}$.

How do these turn into primes?

$\log_2 L \approx 971$ and $\log_2 p = 1024$,
so $p = p' + k \cdot L$,
where $p \equiv p' \bmod L$, and k with
$\gcd\{k, L\} = 1$ and $\log_2 k \approx 53$
is random so that p is prime.
Same for q.

Lenstra's "Divisors in Residue Classes" finds prime factors of the form $p = u + k \cdot L$ efficiently if $L \geq n^{1/3}$.
Coppersmith, Howgrave-Graham, and Nagaraj work for $L \geq n^{1/4}$.

$\log_2 L > 970 > 683 > 2048/3$.

Full attack

Run Lensta for all $p' \in \left\{65537^i \bmod L | i \in \mathbf{Z}\right\}$.

Each run is cheap, but there are many options for p', e.g. $65537^i \bmod 23 \in \{\pm 1, \pm 2, \pm 3, \pm 4, \ldots, \pm 9, \pm$

How do these turn into primes?

$\log_2 L \approx 971$ and $\log_2 p = 1024$,
so $p = p' + k \cdot L$,
where $p \equiv p' \bmod L$, and k with
$\gcd\{k, L\} = 1$ and $\log_2 k \approx 53$
is random so that p is prime.
Same for q.

Lenstra's "Divisors in Residue Classes" finds prime factors of the form $p = u + k \cdot L$ efficiently if $L \geq n^{1/3}$.
Coppersmith, Howgrave-Graham, and Nagaraj work for $L \geq n^{1/4}$.

$\log_2 L > 970 > 683 > 2048/3$.

Full attack

Run Lensta for all $p' \in \left\{65537^i \bmod L | i \in \mathbf{Z}\right\}$.

Each run is cheap, but there are many options for p', e.g. $65537^i \bmod 23 \in \{\pm1, \pm2, \pm3, \pm4, \ldots, \pm9, \pm10, \pm11\}$.

How do these turn into primes?

$\log_2 L \approx 971$ and $\log_2 p = 1024$,
so $p = p' + k \cdot L$,
where $p \equiv p' \bmod L$, and k with
$\gcd\{k, L\} = 1$ and $\log_2 k \approx 53$
is random so that p is prime.
Same for q.

Lenstra's "Divisors in Residue Classes" finds prime factors of the form $p = u + k \cdot L$ efficiently if $L \geq n^{1/3}$.
Coppersmith, Howgrave-Graham, and Nagaraj work for $L \geq n^{1/4}$.

$\log_2 L > 970 > 683 > 2048/3$.

Full attack

Run Lensta for all $p' \in \left\{65537^i \bmod L | i \in \mathbf{Z}\right\}$.

Each run is cheap, but there are many options for p', e.g. $65537^i \bmod 23 \in \{\pm 1, \pm 2, \pm 3, \pm 4, \ldots, \pm 9, \pm 10, \pm 11\}$.

But L is much larger than needed.
So use $L' | L$ which minimizes number of choices $\times$ runtime.

these turn into primes?

971 and $\log_2 p = 1024$,
$p' + k \cdot L$,
$\equiv p' \bmod L$, and k with
$\} = 1$ and $\log_2 k \approx 53$
m so that p is prime.
r q.

s "Divisors in Residue
finds prime factors of
$p = u + k \cdot L$
y if $L \geq n^{1/3}$.
mith, Howgrave-Graham,
garaj work for $L \geq n^{1/4}$.

$970 > 683 > 2048/3$.

Full attack

Run Lensta for all $p' \in \{65537^i \bmod L | i \in \mathbf{Z}\}$.

Each run is cheap, but there are many options for p', e.g. $65537^i \bmod 23 \in \{\pm1, \pm2, \pm3, \pm4, \ldots, \pm9, \pm10, \pm11\}$.

But L is much larger than needed. So use $L'|L$ which minimizes number of choices $\times$ runtime.

What we

It would
p' as
$p' \equiv 2^{r_1}$
$p' \equiv 3^{r_2}$
$p' \equiv 3^{r_3}$
$p' \equiv 2^{r_4}$
$p' \equiv 2^{r_5}$
with r_i
reconstru

Note: 2
so this g
$2 \cdot 4 \cdot 6 \cdot$

n into primes?

$\log_2 p = 1024$,

L, and k with

$\log_2 k \approx 53$

p is prime.

s in Residue

ne factors of

$k \cdot L$

$^{1/3}$.

wgrave-Graham,

for $L \geq n^{1/4}$.

$3 > 2048/3$.

Full attack

Run Lensta for all $p' \in \left\{65537^i \bmod L | i \in \mathbf{Z}\right\}$.

Each run is cheap, but there are many options for p', e.g. $65537^i \bmod 23 \in \{\pm 1, \pm 2, \pm 3, \pm 4, \ldots, \pm 9, \pm 10, \pm 11\}$.

But L is much larger than needed. So use $L'|L$ which minimizes number of choices $\times$ runtime.

What went wrong

It would have been

p' as

$p' \equiv 2^{r_1} \bmod 3$

$p' \equiv 3^{r_2} \bmod 5$

$p' \equiv 3^{r_3} \bmod 7$

$p' \equiv 2^{r_4} \bmod 11$

$p' \equiv 2^{r_5} \bmod 13$

with r_i random ar

reconstructed usin

Note: 2 and 3 are

so this gives

$2 \cdot 4 \cdot 6 \cdot 10 \cdot 12 =$

nes?

024,

with
53
e.

ue
of

ham,
$1/4$.

/3.

Full attack

Run Lensta for all $p' \in \left\{65537^i \bmod L \middle| i \in \mathbf{Z}\right\}$.

Each run is cheap, but there are many options for p', e.g. $65537^i \bmod 23 \in \{\pm 1, \pm 2, \pm 3, \pm 4, \ldots, \pm 9, \pm 10, \pm 11\}$.

But L is much larger than needed. So use $L'|L$ which minimizes number of choices $\times$ runtime.

What went wrong here?

It would have been OK to c
p' as
$p' \equiv 2^{r_1} \bmod 3$
$p' \equiv 3^{r_2} \bmod 5$
$p' \equiv 3^{r_3} \bmod 7$
$p' \equiv 2^{r_4} \bmod 11$
$p' \equiv 2^{r_5} \bmod 13$
with r_i random and p' reconstructed using CRT.

Note: 2 and 3 are generator
so this gives
$2 \cdot 4 \cdot 6 \cdot 10 \cdot 12 = 5760$ opti

Full attack

Run Lensta for all $p' \in \{65537^i \bmod L | i \in \mathbf{Z}\}$.

Each run is cheap, but there are many options for p', e.g. $65537^i \bmod 23 \in \{\pm 1, \pm 2, \pm 3, \pm 4, \ldots, \pm 9, \pm 10, \pm 11\}$.

But L is much larger than needed. So use $L' | L$ which minimizes number of choices $\times$ runtime.

What went wrong here?

It would have been OK to choose p' as

$p' \equiv 2^{r_1} \bmod 3$

$p' \equiv 3^{r_2} \bmod 5$

$p' \equiv 3^{r_3} \bmod 7$

$p' \equiv 2^{r_4} \bmod 11$

$p' \equiv 2^{r_5} \bmod 13$

with r_i random and p' reconstructed using CRT.

Note: 2 and 3 are generators, so this gives $2 \cdot 4 \cdot 6 \cdot 10 \cdot 12 = 5760$ options.

ck

sta for all $p' \in$
$\bmod L | i \in \mathbf{Z}\}$.

n is cheap, but
e many options for
$65537^i \bmod 23 \in$
$2, \pm 3, \pm 4, \ldots, \pm 9, \pm 10, \pm 11\}$.

much larger than needed.
$L' | L$ which minimizes
of choices $\times$ runtime.

What went wrong here?

It would have been OK to choose p' as

$p' \equiv 2^{r_1} \bmod 3$
$p' \equiv 3^{r_2} \bmod 5$
$p' \equiv 3^{r_3} \bmod 7$
$p' \equiv 2^{r_4} \bmod 11$
$p' \equiv 2^{r_5} \bmod 13$

with r_i random and p' reconstructed using CRT.

Note: 2 and 3 are generators, so this gives $2 \cdot 4 \cdot 6 \cdot 10 \cdot 12 = 5760$ options.

It would
but wors
to choos
$p' \equiv 2^{r_1}$
$p' \equiv 2^{r_2}$
$p' \equiv 2^{r_3}$
$p' \equiv 2^{r_4}$
$p' \equiv 2^{r_5}$
with r_i
reconstru

Note: 2
this give
$2 \cdot 4 \cdot 3 \cdot$

$p' \in$
$\in \mathbf{Z}\}$.
, but
tions for
od 23 $\in$
$\ldots, \pm 9, \pm 10, \pm 11\}$.

ger than needed.
minimizes
$\times$ runtime.

What went wrong here?

It would have been OK to choose p' as
$p' \equiv 2^{r_1} \bmod 3$
$p' \equiv 3^{r_2} \bmod 5$
$p' \equiv 3^{r_3} \bmod 7$
$p' \equiv 2^{r_4} \bmod 11$
$p' \equiv 2^{r_5} \bmod 13$
with r_i random and p' reconstructed using CRT.

Note: 2 and 3 are generators, so this gives $2 \cdot 4 \cdot 6 \cdot 10 \cdot 12 = 5760$ options.

It would have OK'
but worse
to choose p' as
$p' \equiv 2^{r_1} \bmod 3$
$p' \equiv 2^{r_2} \bmod 5$
$p' \equiv 2^{r_3} \bmod 7$
$p' \equiv 2^{r_4} \bmod 11$
$p' \equiv 2^{r_5} \bmod 13$
with r_i random ar
reconstructed usin

Note: 2 is not alw
this gives only
$2 \cdot 4 \cdot 3 \cdot 10 \cdot 12 =$

$10, \pm 11\}$.

eeded.

s

e.

What went wrong here?

It would have been OK to choose
p' as
$p' \equiv 2^{r_1} \bmod 3$
$p' \equiv 3^{r_2} \bmod 5$
$p' \equiv 3^{r_3} \bmod 7$
$p' \equiv 2^{r_4} \bmod 11$
$p' \equiv 2^{r_5} \bmod 13$
with r_i random and p'
reconstructed using CRT.

Note: 2 and 3 are generators,
so this gives
$2 \cdot 4 \cdot 6 \cdot 10 \cdot 12 = 5760$ options.

It would have OK'ish
but worse
to choose p' as
$p' \equiv 2^{r_1} \bmod 3$
$p' \equiv 2^{r_2} \bmod 5$
$p' \equiv 2^{r_3} \bmod 7$
$p' \equiv 2^{r_4} \bmod 11$
$p' \equiv 2^{r_5} \bmod 13$
with r_i random and p'
reconstructed using CRT.

Note: 2 is not always a gene
this gives only
$2 \cdot 4 \cdot 3 \cdot 10 \cdot 12 = 2880$ opti

What went wrong here?

It would have been OK to choose
p' as
$p' \equiv 2^{r_1} \bmod 3$
$p' \equiv 3^{r_2} \bmod 5$
$p' \equiv 3^{r_3} \bmod 7$
$p' \equiv 2^{r_4} \bmod 11$
$p' \equiv 2^{r_5} \bmod 13$
with r_i random and p'
reconstructed using CRT.

Note: 2 and 3 are generators,
so this gives
$2 \cdot 4 \cdot 6 \cdot 10 \cdot 12 = 5760$ options.

It would have OK'ish
but worse
to choose p' as
$p' \equiv 2^{r_1} \bmod 3$
$p' \equiv 2^{r_2} \bmod 5$
$p' \equiv 2^{r_3} \bmod 7$
$p' \equiv 2^{r_4} \bmod 11$
$p' \equiv 2^{r_5} \bmod 13$
with r_i random and p'
reconstructed using CRT.

Note: 2 is not always a generator,
this gives only
$2 \cdot 4 \cdot 3 \cdot 10 \cdot 12 = 2880$ options.

ent wrong here?

have been OK to choose

mod 3

mod 5

mod 7

mod 11

mod 13

random and p'

ucted using CRT.

and 3 are generators,

gives

$10 \cdot 12 = 5760$ options.

It would have OK'ish

but worse

to choose p' as

$p' \equiv 2^{r_1} \bmod 3$

$p' \equiv 2^{r_2} \bmod 5$

$p' \equiv 2^{r_3} \bmod 7$

$p' \equiv 2^{r_4} \bmod 11$

$p' \equiv 2^{r_5} \bmod 13$

with r_i random and p'

reconstructed using CRT.

Note: 2 is not always a generator,

this gives only

$2 \cdot 4 \cdot 3 \cdot 10 \cdot 12 = 2880$ options.

It is real

to replac

exponen

$p' \equiv 547$

with r r

Note:

The orde

modulo

are 2,4,6

are linke

Instead

this give

options.

here?

n OK to choose

nd p'

g CRT.

generators,

5760 options.

It would have OK'ish

but worse

to choose p' as

$p' \equiv 2^{r_1} \bmod 3$

$p' \equiv 2^{r_2} \bmod 5$

$p' \equiv 2^{r_3} \bmod 7$

$p' \equiv 2^{r_4} \bmod 11$

$p' \equiv 2^{r_5} \bmod 13$

with r_i random and p'

reconstructed using CRT.

Note: 2 is not always a generator,

this gives only

$2 \cdot 4 \cdot 3 \cdot 10 \cdot 12 = 2880$ options.

It is really bad

to replace this by

exponentiation and

$p' \equiv 5477^r \bmod 3$

with r random.

Note:

The orders of 547

modulo 3,5,7,11, a

are 2,4,6,2, and 6,

are linked.

Instead of $2 \cdot 4 \cdot 6$

this gives lcm$\{2, 4$

options.

hoose

rs,

ons.

It would have OK'ish
but worse
to choose p' as
$p' \equiv 2^{r_1} \bmod 3$
$p' \equiv 2^{r_2} \bmod 5$
$p' \equiv 2^{r_3} \bmod 7$
$p' \equiv 2^{r_4} \bmod 11$
$p' \equiv 2^{r_5} \bmod 13$
with r_i random and p'
reconstructed using CRT.

Note: 2 is not always a generator,
this gives only
$2 \cdot 4 \cdot 3 \cdot 10 \cdot 12 = 2880$ options.

It is really bad
to replace this by a single
exponentiation and choose p
$p' \equiv 5477^r \bmod 3 \cdot 5 \cdot 7 \cdot 11$
with r random.

Note:
The orders of 5477
modulo 3,5,7,11, and 13
are 2,4,6,2, and 6, but the p
are linked.

Instead of $2 \cdot 4 \cdot 6 \cdot 2 \cdot 6 =$
this gives $\text{lcm}\{2, 4, 6, 2, 6\} =$
options.

It would have OK'ish
but worse
to choose p' as

$p' \equiv 2^{r_1} \bmod 3$
$p' \equiv 2^{r_2} \bmod 5$
$p' \equiv 2^{r_3} \bmod 7$
$p' \equiv 2^{r_4} \bmod 11$
$p' \equiv 2^{r_5} \bmod 13$

with r_i random and p'
reconstructed using CRT.

Note: 2 is not always a generator,
this gives only
$2 \cdot 4 \cdot 3 \cdot 10 \cdot 12 = 2880$ options.

It is really bad
to replace this by a single
exponentiation and choose p' as
$p' \equiv 5477^r \bmod 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$
with r random.

Note:
The orders of 5477
modulo 3,5,7,11, and 13
are 2,4,6,2, and 6, but the powers
are linked.

Instead of $2 \cdot 4 \cdot 6 \cdot 2 \cdot 6 = 576$
this gives $\operatorname{lcm}\{2, 4, 6, 2, 6\} = 12$
options.