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.

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.

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

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

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

$611 = 47 \cdot 13$.

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 $s + t$.

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.

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

Given n and parameter y:

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

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

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

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

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

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

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?

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

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 $n^{o(1)}$.

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):

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

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:

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

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

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

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 $\mathbf{Z}[f_d r]$:
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.

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)

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.

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 $i - jm$.

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

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.

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
$c = n_7a^7 + n_6a^6b + \cdots + n_0b^7$.

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.

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.

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.

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.

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}.

More generally: Choose z.
Compute $\gcd\{c, S\}$ where $S = (\rho_1 - \rho_2)(\rho_2 - \rho_4)\cdots(\rho_z - \rho_{2z})$.

How big does z have to be for all primes $\le y$ to divide S?

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

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

The $p-1$ method

$S_1 = 2^{232792560} - 1$ has prime divisors
3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 53, 61, 67, 71, 73, 79, 89, 97, 103, 109, 113, 127, 131, 137, 151, 157, 181, 191, 199 etc.

These divisors include
70 of the 168 primes $\leq 10^3$;
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: $s = 232792560$
$= \text{lcm}\{1, 2, 3, 4, 5, \ldots, 20\}$
$= 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19.$

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. $c = 8597231219$: ...

$$\begin{aligned}
2^{27} \bmod c &= 134217728;\\
2^{54} \bmod c &= 134217728^2 \bmod n\\
&= 935663516;\\
2^{55} \bmod c &= 1871327032;\\
2^{110} \bmod c &= 1871327032^2 \bmod c\\
&= 1458876811; \ldots;
\end{aligned}$$

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

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. $c = 8597231219$: ...

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

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.

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 $\operatorname{lcm}\{1,2,\ldots,K\}$
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 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 $\le 10^3$;
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 $232792560(3/5,4/5) = (0,1)$.

The elliptic-curve method

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

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 $\leq H$ 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 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.

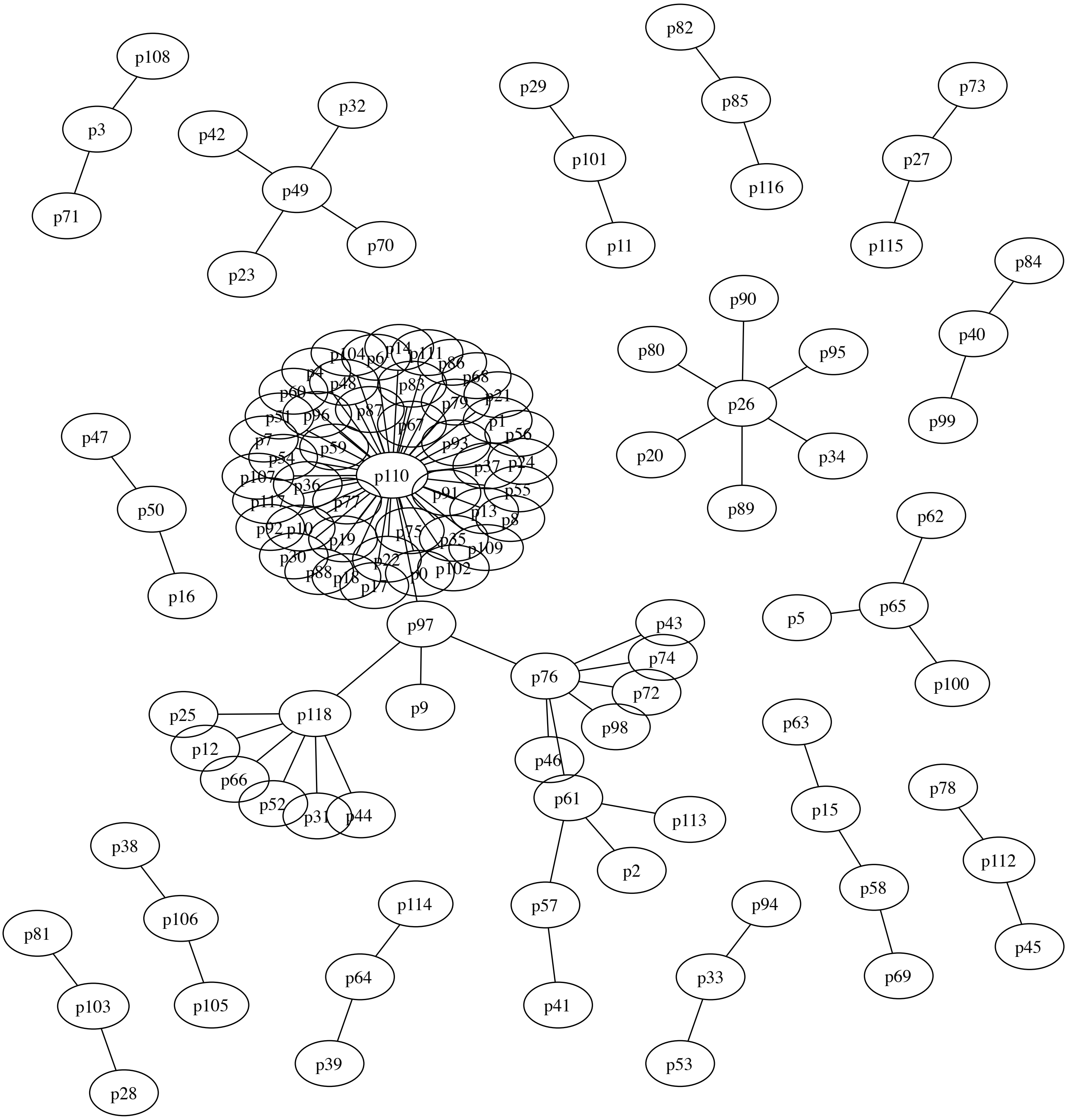
“Almost all of the vulnerable keys were generated by and are used to secure embedded hardware devices such as routers and firewalls, not to secure popular web sites such as your bank or email provider.”

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



Prime p110 appears 46 times

```
c0000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
000000000000000000000000000002f9
```

Prime p110 appears 46 times

```
c0000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
000000000000000000000000000002f9
```

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

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 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 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 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.

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.

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.

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

$n \bmod 2 = 1$

$n \bmod 11 \in \{1, 10\}$

$n \bmod 37 \in \{1, 10, 37\}$

$n \bmod 97 \in \{1, 35, 36, 61, 62, 96\}$

$n \bmod 331 \in \{1, 330\}$

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,

$$n \bmod 2 \cdot 11 \cdot 37 \cdot 97 \cdot 331$$
$$\in \quad \{1, 65537, 4878941,$$
$$8942297, 14367385, 24016035\}$$

Worse,

$n \bmod 2 \cdot 11 \cdot 37 \cdot 97 \cdot 331$
$\in \quad \{1, 65537, 4878941,$
$8942297, 14367385, 24016035\}$

$n \in \left\{65537^i \bmod L \middle| i \in \mathbf{Z}\right\}$
and 65537 has order 6 $\bmod L$.

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
$p, q \in \left\{65537^i \bmod L | i \in \mathbf{Z}\right\}$.

Worse,

$n \bmod 2 \cdot 11 \cdot 37 \cdot 97 \cdot 331$
$\in \quad \{1, 65537, 4878941,$
$8942297, 14367385, 24016035\}$

$n \in \left\{65537^i \bmod L \middle| i \in \mathbf{Z}\right\}$
and 65537 has order 6 $\bmod L$.

If $n = p \cdot q = 65537^i \bmod L$
then likely
$p, q \in \left\{65537^i \bmod L \middle| i \in \mathbf{Z}\right\}$.

There are more congruences
where this holds.
Actually $L = \prod_{\ell < 702, \ell \text{prime}} \ell$.

How do these turn into 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.

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 $p' \in \{65537^i \bmod L | i \in \mathbf{Z}\}$.

Each run is cheap, but there are many options for p', e.g. $65537^i \bmod 23 \in \{\pm 1, \pm 2, \pm 3, \pm 4, \ldots, \pm 9, \pm 10, \pm 11\}$.

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 × 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'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.