The number-field sieve

Finding small factors of integers

Speed of the number-field sieve

Proving primality in polynomial time

D. J. Bernstein
University of Illinois at Chicago

Problem: Completely factor 31415926535897932 3.

Eventually find that $31415926535897932 3 = 317213509 \cdot 990371647$.

Factorization completed? Yes: $317213509, 990371647$ are prime.

“Prove it!”

Next 15 slides are
the world's longest proof
that 317213509 is prime.

Exercise: Do the same for
990371647.

First step: 3391 is prime.

Proof: 3391 is not divisible by 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58. Note that $59^2 = 3481 > 3391$.

Next: Define $n = 317213509$.
Then n is not divisible by any prime < 3364.

Proof: n is not divisible by
2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12,
13, 14, 15, 16, 17, 18, 19, 20, 21,
22, 23, 24, 25, 26, 27, 28, 29, 30,
31, 32, 33, 34, 35, 36, 37, 38, 39,
40, 41, 42, 43, 44, 45, 46, 47, 48,
49, 50, 51, 52, 53, 54, 55, 56, 57,
58, 59, 60, 61, 62, 63, 64, 65, 66,
67, 68, 69, 70, 71, 72, $\ldots$, 3363.

Define p as the smallest prime divisor of n.

Then $p \geq 3364$.

In other words:
In $\mathbf{F}_p[x]$, the polynomials $x-1, x-2, \ldots, x-3364$ are distinct.

Unique factorization: The product $(x-1)^{e_1} \cdots (x-3364)^{e_{3364}}$ in $\mathbf{F}_p[x]$ determines the vector $(e_1, \ldots, e_{3364})$.

Next:

n is a primitive root modulo 3391;
i.e., has order 3390 modulo 3391.

Proof:

$n \bmod 3391 = 2414 \neq 1$;
$n^2 \bmod 3391 = 1658 \neq 1$;
$n^3 \bmod 3391 = 1032 \neq 1$;
$n^4 \bmod 3391 = 2254 \neq 1$;
$\vdots$
$n^{3389} \bmod 3391 = 2558 \neq 1$;
$n^{3390} \bmod 3391 = 1$.

Next:

$(x-1)^n = x^n - 1$

in the ring $(\mathbf{Z}/n)[x]/(x^{3391}-1)$.

Proof:

$(x-1)^2 = x^2 + 317213507x + 1;$

$\vdots$

$$(x-1)^{158606754} = 7406606x^{3390} + \cdots;$$

$$(x-1)^{317213508} = 93545x^{3390} + \cdots;$$

$$(x-1)^{317213509} = x^{2414} + 317213508 = x^{n \bmod 3391} - 1.$$

Next:

$(x-2)^n = x^n - 2$

in the ring $(\mathbf{Z}/n)[x]/(x^{3391}-1)$.

Proof:

$(x-2)^2 = x^2 + 317213505x + 4$;

$\vdots$

$$(x-2)^{158606754}$$
$$= 114354286x^{3390} + \cdots;$$

$$(x-2)^{317213508}$$
$$= 164442849x^{3390} + \cdots;$$

$$(x-2)^{317213509}$$
$$= x^{2414} + 317213507$$
$$= x^{n \bmod 3391} - 2.$$

More exponentiations:

$(x-3)^n = x^n - 3,$

$(x-4)^n = x^n - 4,$

$(x-5)^n = x^n - 5,$

$(x-6)^n = x^n - 6,$

$(x-7)^n = x^n - 7,$

$(x-8)^n = x^n - 8,$

$(x-9)^n = x^n - 9,$

$(x-10)^n = x^n - 10,$

$(x-11)^n = x^n - 11,$

$(x-12)^n = x^n - 12,$

$(x-13)^n = x^n - 13,$

$(x-14)^n = x^n - 14,$

$(x-15)^n = x^n - 15,$

$(x-16)^n = x^n - 16,$

$(x-17)^n = x^n - 17,$

$(x-18)^n = x^n - 18$

Last exponentiation:

$(x - 3364)^n = x^n - 3364$

in the ring $(\mathbf{Z}/n)[x]/(x^{3391} - 1)$.

Proof:

$\vdots$

$$(x - 3364)^{158606754} = 261799987x^{3390} + \cdots;$$

$$(x - 3364)^{317213508} = 196658336x^{3390} + \cdots;$$

$$(x - 3364)^{317213509} = x^{2414} + 317210145 = x^{n \bmod 3391} - 3364.$$

Now play with equations.

p divides n
so $(x - a)^n = x^n - a$
in $\mathbf{F}_p[x]/(x^{3391} - 1)$
for each $a \in \{1, 2, \ldots, 3364\}$.

For each integer $i \geq 0$,
substitute x^{n^i} for x:
$(x^{n^i} - a)^n = x^{n^{i+1}} - a$ in
$\mathbf{F}_p[x]/((x^{n^i})^{3391} - 1)$,
hence in $\mathbf{F}_p[x]/(x^{3391} - 1)$.

By induction $(x - a)^{n^i} = x^{n^i} - a$
in $\mathbf{F}_p[x]/(x^{3391} - 1)$.

For each integer $j \ge 0$,
apply Fermat's little theorem:
$(x-a)^{n^i p^j} = (x^{n^i} - a)^{p^j} = x^{n^i p^j} - a$ in $\mathbf{F}_p[x]/(x^{3391}-1)$.

Define $h \in \mathbf{F}_p[x]$ as the smallest irreducible polynomial dividing $(x^{3391}-1)/(x-1)$.

Then $(x-a)^{n^i p^j} = x^{n^i p^j} - a$ in the field $\mathbf{F}_p[x]/h$.

Have $x^{3391} = 1$ in $\mathbf{F}_p[x]/h$,
so x has order 1 or 3391.

Can x have order 1 in $\mathbf{F}_p[x]/h$?
If so then h divides $x-1$ in $\mathbf{F}_p[x]$
so h^2 divides $x^{3391}-1$ in $\mathbf{F}_p[x]$.
But $x^{3391}-1$ is squarefree in $\mathbf{F}_p[x]$
since $3391 \neq 0$ in $\mathbf{F}_p$.
Contradiction.

Thus x has order 3391 in $\mathbf{F}_p[x]/h$.

Recall that $n \bmod 3391 \neq 1$.
Thus $x^n \neq x$ in $\mathbf{F}_p[x]/h$.

Thus $(x-a)^n = x^n - a \neq x - a$
in $\mathbf{F}_p[x]/h$.

Thus $x-a$ is nonzero in $\mathbf{F}_p[x]/h$.

For each subset

$T \subseteq \{1, 2, \ldots, 3364\}$

define $\pi_T \in \mathbf{F}_p[x]$

by $\pi_T = \prod_{a \in T}(x - a)$.

e.g. $\pi_{\{6,9\}} = (x - 6)(x - 9)$.

Each π_T has degree ≤ 3364.

Critical equation in $\mathbf{F}_p[x]/h$:

$\pi_T^{n^i p^j} =$

$\prod_{a \in T}(x - a)^{n^i p^j} =$

$\prod_{a \in T}(x^{n^i p^j} - a) =$

$\pi_T(x^{n^i p^j})$.

Assume $\pi_T = \pi_U$ in $\mathbf{F}_p[x]/h$.

Then $\pi_T^{n^i p^j} = \pi_U^{n^i p^j}$ in $\mathbf{F}_p[x]/h$
so $\pi_T(x^{n^i p^j}) = \pi_U(x^{n^i p^j})$
in $\mathbf{F}_p[x]/h$.

Thus $x^{n^i p^j}$ is a root in $\mathbf{F}_p[x]/h$
of the polynomial $\pi_T - \pi_U$.

Thus $\pi_T - \pi_U$ has
3390 distinct roots in $\mathbf{F}_p[x]/h$.
But $\pi_T - \pi_U$ has degree ≤ 3364.
Hence $\pi_T = \pi_U$.

By unique factorization, $T = U$.

There are 2^{3364} subsets T. The 2^{3364} polys $\pi_T = \prod_{a\in T}(x-a)$ are all different in $\mathbf{F}_p[x]/h$.

Consider the products $n^i p^j$ with $i, j \in \{0, 1, \ldots, 58\}$. Have $1 \le n^i p^j \le (2^{29})^{58+58} = 2^{3364}$.

There are $59^2 = 3481$ pairs (i, j). Products mod 3391 must collide: $n^i p^j \bmod 3391 = n^k p^\ell \bmod 3391$ with $(i, j) \ne (k, \ell)$. Have $|n^i p^j - n^k p^\ell| \le 2^{3364} - 1$.

In $\mathbf{F}_p[x]/h$ have $\pi_T^{n^i p^j} = \pi_T(x^{n^i p^j}) = \pi_T(x^{n^k p^\ell}) = \pi_T^{n^k p^\ell}$ so $\pi_T^{n^i p^j - n^k p^\ell} = 1$.

If $n^i p^j - n^k p^\ell \neq 0$: Number of $(n^i p^j - n^k p^\ell)$th roots of 1 in a field is at most $2^{3364} - 1$, contradiction.

Thus $n^i p^j = n^k p^\ell$.
If $i = k$ then $p^j = p^\ell$ so $(i, j) = (k, \ell)$, contradiction.
Thus n is a power of p.

None of $n^{1/2}, n^{1/3}, \ldots, n^{1/29}$ are integers, so $n = p$.

We'll see that
every prime n has
a similar primality proof.

Can find and verify the proof
using $(\lg n)^{O(1)}$ bit operations.
No randomness required.
No conjectures required.

The proof is
much slower than trial division
for n as small as 317213509,
but it scales surprisingly well
to larger values of n.

One complication:

We *believe* that, for each $n \geq 2$, there is a prime q in
$[4\lceil \lg n \rceil^2 + 3, O((\lg n)^2)]$
for which n is a primitive root.

But we don't know how to prove that q exists.

So we loosen the q requirements.
Then easy to prove that q exists.
Compensate with slightly more work in the rest of the proof.

Given integer $n > 1$:

Find smallest prime number q that does not divide $n(n-1)(n^2-1)(n^3-1)\cdots(n^{4\lceil \lg n\rceil^2}-1)$; i.e., such that n has order $> 4\lceil \lg n\rceil^2$ modulo q.

How? For each small integer p, check primality by trial division, and inspect powers of n modulo p. Fast since q is small.

Conjecture: $q \in O((\lg n)^2)$.
Theorem: $q \in O((\lg n)^5)$.

How to prove $q \in O((\lg n)^5)$?

Prime-number theorem says that $\prod_{p \leq k} p \approx \exp k$.

Weak, relatively easy to prove: $\prod_{p \leq k} p$ grows exponentially.

In particular, have $\prod_{p \leq k} p > n(n-1)(n^2-1)(n^3-1)\cdots(n^{4\lceil \lg n \rceil^2}-1)$
for some $k \in O((\lg n)^5)$.
So $n(n-1)(n^2-1)(n^3-1)\cdots(n^{4\lceil \lg n \rceil^2}-1)$ can't be divisible by all $p \leq k$.

Compute $\beta = 2 \lceil \lg n \rceil \lfloor \sqrt{q-1} \rfloor$.

Conjecture: $\beta \in O((\lg n)^2)$.
Theorem: $\beta \in O((\lg n)^{3.5})$.

Enumerate primes $< \beta$.
If n equals a prime $< \beta$,
stop: n is prime. Otherwise,
if n is divisible by a prime $< \beta$,
stop: n is composite.

Assume from now on
that n is not divisible
by any of the primes $< \beta$.

Define p as the smallest prime divisor of n.

Evidently $p \geq \beta$.

In $\mathbf{F}_p[x]$, the polynomials
$x - 1, x - 2, \ldots, x - \beta$
are distinct.

Unique factorization: The product
$(x - 1)^{e_1} \cdots (x - \beta)^{e_\beta}$
in $\mathbf{F}_p[x]$ determines
the vector $(e_1, \ldots, e_\beta)$.

Define
$G = \{n^i p^j \bmod q : i \geq 0, j \geq 0\}$
and $\gamma = 2\lceil \lg n \rceil \lfloor \sqrt{\#G} \rfloor$.

Then $n^{2\lfloor \sqrt{\#G} \rfloor} \leq 2^\gamma$.

$0 \notin G$ so $\#G \leq q - 1$
and $\gamma \leq 2\lceil \lg n \rceil \lfloor \sqrt{q-1} \rfloor = \beta$.

G includes all $n^i \bmod q$
so $\#G > 4\lceil \lg n \rceil^2$ and
$\gamma \leq 2\lceil \lg n \rceil \sqrt{\#G} < \#G$.

For each $a \in \{1, 2, \ldots, \beta\}$ check whether $(x - a)^n = x^n - a$ in the ring $(\mathbf{Z}/n)[x]/(x^q - 1)$.

These exponentiations take $\le \beta(q(\lg n)^2)^{1+o(1)}$ bit operations.
Conjecture: $\le (\lg n)^{6+o(1)}$.
Theorem: $\le (\lg n)^{10.5+o(1)}$.
Slow arithmetic: $\le (\lg n)^{16.5+o(1)}$.

If $(x - a)^n \ne x^n - a$, stop: n is composite.

Assume from now on that $(x - a)^n = x^n - a$ for each $a \in \{1, 2, \ldots, \beta\}$.

Play with equations as before.

$(x-a)^{n^i p^j} = (x^{n^i} - a)^{p^j} = x^{n^i p^j} - a$ in $\mathbf{F}_p[x]/(x^q - 1)$ for each $a \in \{1, 2, \ldots, \beta\}$, each $i \geq 0$, each $j \geq 0$.

Define $h \in \mathbf{F}_p[x]$ as the smallest irreducible polynomial dividing $(x^q - 1)/(x - 1)$.

$(x-a)^{n^i p^j} = x^{n^i p^j} - a$
in the field $\mathbf{F}_p[x]/h$.
x has order q in $\mathbf{F}_p[x]/h$.
$x - a$ is nonzero in $\mathbf{F}_p[x]/h$.

For each subset $T \subseteq \{1, 2, \ldots, \gamma\}$
define $\pi_T \in \mathbf{F}_p[x]$
by $\pi_T = \prod_{a \in T}(x - a)$.

Each π_T has degree $\le \gamma$.

Critical equation in $\mathbf{F}_p[x]/h$:
$\pi_T^{n^i p^j} =$
$\prod_{a \in T}(x - a)^{n^i p^j} =$
$\prod_{a \in T}(x^{n^i p^j} - a) =$
$\pi_T(x^{n^i p^j})$.

Assume $\pi_T = \pi_U$ in $\mathbf{F}_p[x]/h$.

Then $\pi_T^{n^i p^j} = \pi_U^{n^i p^j}$ in $\mathbf{F}_p[x]/h$
so $\pi_T(x^{n^i p^j}) = \pi_U(x^{n^i p^j})$
in $\mathbf{F}_p[x]/h$.

Thus $x^{n^i p^j}$ is a root in $\mathbf{F}_p[x]/h$
of the polynomial $\pi_T - \pi_U$.

Thus $\pi_T - \pi_U$ has
$\#G$ distinct roots in $\mathbf{F}_p[x]/h$.
But $\deg(\pi_T - \pi_U) \le \gamma < \#G$.
Hence $\pi_T = \pi_U$.

By unique factorization, $T = U$.

There are 2^γ subsets T. The 2^γ polys $\pi_T = \prod_{a \in T}(x - a)$ are all different in $\mathbf{F}_p[x]/h$.

Consider the products $n^i p^j$ with $i, j \in \{0, 1, \ldots, \lfloor \sqrt{\#G} \rfloor\}$. Have $1 \le n^i p^j \le n^{2\lfloor \sqrt{\#G} \rfloor} \le 2^\gamma$.

There are $> \#G$ pairs (i, j). Products mod q must collide: $n^i p^j \bmod q = n^k p^\ell \bmod q$ with $(i, j) \ne (k, \ell)$. Have $|n^i p^j - n^k p^\ell| \le 2^\gamma - 1$.

In $\mathbf{F}_p[x]/h$ have $\pi_T^{n^i p^j} =$

$\pi_T(x^{n^i p^j}) = \pi_T(x^{n^k p^\ell}) = \pi_T^{n^k p^\ell}$

so $\pi_T^{n^i p^j - n^k p^\ell} = 1$.

If $n^i p^j - n^k p^\ell \neq 0$: Number of $(n^i p^j - n^k p^\ell)$th roots of 1 in a field is at most $2^\gamma - 1$, contradiction.

Thus $n^i p^j = n^k p^\ell$.
If $i = k$ then $p^j = p^\ell$ so $(i, j) = (k, \ell)$, contradiction.
Thus n is a power of p.

Finally check whether n is a square, cube, etc. If so, stop: n is composite.

Otherwise $n = p$ so n is prime.

Done! Have proven primality of n, or have proven compositeness of n.

Length of proof,
including all computations,
is $(\lg n)^{O(1)}$.
Conjecture: $\le (\lg n)^{6+o(1)}$.
Theorem: $\le (\lg n)^{10.5+o(1)}$.
Easiest theorem: $\le (\lg n)^{16.5+o(1)}$.
Bottleneck is the exponentiations.

Appendix: exponential growth

Weak prime-number theorem:
$\prod_{1<p\le 2k} p \ge 2^{2k}/(2k+1)(2k)^{\sqrt{2k}}$.

Proof: What is $\operatorname{ord}_p \binom{2k}{k}$?

0 if $p > 2k$.
≤ 1 if $\sqrt{2k} < p \le 2k$.
$\le (\lg 2k)/\lg p$ if $1 < p \le \sqrt{2k}$.

Thus $2^{2k}/(2k+1) \le \binom{2k}{k} \le$
$(\prod_{\sqrt{2k}<p\le 2k} p)\prod_{p\le\sqrt{2k}} 2k \le$
$(\prod_{1<p\le 2k} p)(2k)^{\sqrt{2k}}$.