Factoring into coprimes

D. J. Bernstein
University of Illinois at Chicago

Does $91^{1952681} 119^{1513335} 221^{634643}$ equal $1547^{1708632} 6898073^{439346}$?

Each side has logarithm ≈ 19466590.674872.

Which integers (a, b, c, d, e) satisfy $91^a 119^b 221^c = 1547^d 6898073^e$?

$91 = 7 \cdot 13$; $119 = 7 \cdot 17$;

$221 = 13 \cdot 17$; $1547 = 7 \cdot 13 \cdot 17$;

$6898073 = 7^4 \cdot 13^2 \cdot 17$.

$$(a, b, c, d, e) \mapsto$$
$$91^a 119^b 221^c 1547^{-d} 6898073^{-e} =$$
$$7^{a+b-d-4e} 13^{a+c-d-2e} 17^{b+c-d-e}.$$

Kernel is generated by

$(1, 1, 1, 2, 0)$ and $(3, 2, 0, 1, 1)$.

General algorithm

Given integers $e_1, \ldots, e_k$ and positive integers $s_1, \ldots, s_k$:

$s_1^{e_1} \cdots s_k^{e_k} = 1$ if and only if $e_1 \operatorname{ord}_q s_1 + \cdots + e_k \operatorname{ord}_q s_k = 0$ for all primes q dividing $s_1 \cdots s_k$.

Problem: Often difficult to find q's.

Solution: Find coprime base P for $\{s_1, \ldots, s_k\}$ with $1 \notin P$.

Coprime means $\gcd\left\{q, q'\right\} = 1$ for all $q, q' \in P$ with $q \neq q'$.

Base means each s_j is a product of powers of elements of P.

Then $s_1^{e_1} \cdots s_k^{e_k} = 1$ if and only if $e_1 \operatorname{ord}_q s_1 + \cdots + e_k \operatorname{ord}_q s_k = 0$ for all $q \in P$.

Can find coprime base
by iterating $(a, b) \mapsto (a/g, g, b/g)$
where $g = \gcd\{a, b\}$.

1547							6898073
1	1547						4459
1	17		91				49
1	17	1	91				49
1	17	1	13		7		7
1	17	1	13	1	7		7
1	17	1	13	1	1	7	1

$\mathrm{cb}\{1547, 6898073\} = \{17, 13, 7\}$.

Can factor S into coprimes
in quadratic time.
(Bach, Driscoll, Shallit 1990)

- Given a, b: compute $\operatorname{cb}\{a, b\}$.
- Given a, Q, with Q coprime: compute $\operatorname{cb}(\{a\} \cup Q)$.
- Given S: compute $\operatorname{cb} S$.
- Given S, P: factor S using P.

An example of **factor refinement**:

Given squarefree $g \in (\mathbf{Z}/2)[x]$.
Want to factor g.

One way: Find basis $h_1, h_2, \ldots$
for $\left\{h \in (\mathbf{Z}/2)[x] : (gh)' = h^2\right\}$.
Then $\operatorname{cb}\{g, h_1, h_2, \ldots\}$ contains
all irreducible divisors of g.

(Niederreiter 1993)

Ideal arithmetic in number rings

Monic irreducible $\varphi \in \mathbf{Z}[x]$.
Want to handle ideals of $\mathbf{Z}[x]/\varphi$.

Represent ideal M as
$\left\{\mathbf{Z}_q M : q \in P\right\}$ with P coprime.

Compress $\mathbf{Z}_q M$ as if q were prime.

(Bernstein)

Fast arithmetic

In time $O(n \log n \log \log n)$
can multiply n-digit numbers.
(Schönhage, Strassen 1971)

Or divide n-digit numbers.
(Cook; Sieveking; Kung; Brent)

In time $O(n(\log n)^2 \log \log n)$
can find gcd of n-digit numbers.
(Lehmer; Knuth; Schönhage)

Need more for fast cb:

5	48828125
1 5	9765625
1 1 5	1953125
1 1 1 5	390625
1 1 1 1 5	78125
1 1 1 1 1 5	15625
1 1 1 1 1 1 5	3125
1 1 1 1 1 1 1 5	625
1 1 1 1 1 1 1 1 5	125
1 1 1 1 1 1 1 1 1 5	25
1 1 1 1 1 1 1 1 1 1 5	5
1 1 1 1 1 1 1 1 1 1 1 5	1

If $a = 5^e$ and $b = 5^f$ then
$\text{cb}\{a, b\} = \{5^{\gcd\{e,f\}}\} - \{1\}$.

$(a/g, g, b/g)$ for $g = \gcd\{a, b\}$ is
$(5^{e-f}, 5^f, 1)$ or $(1, 5^e, 5^{f-e})$.

$(e, f) \mapsto (e - f, f)$ or $(e, f - e)$
is Euclid's original gcd algorithm.
Sometimes very slow.

Better: Subtract $2^j f$ from e if e is between $2^j f$ and $2^{j+1} f$.

Can do this to exponents with fast combination of multiplication, division, gcd.

For example: $\min\{e, 64f\}$ from $c_1 = \gcd\{a, b^2\}$, $c_2 = \gcd\{a, c_1^2\}$, $c_3 = \gcd\{a, c_2^2\}$, $c_4 = \gcd\{a, c_3^2\}$, $c_5 = \gcd\{a, c_4^2\}$, $c_6 = \gcd\{a, c_5^2\}$.

Given coprime sets P, Q,
to quickly compute $\operatorname{cb}(P \cup Q)$:

Replace Q with Q' such that
$\operatorname{cb}(P \cup Q) = \operatorname{cb}(P \cup Q')$;
Q' has $O(n \log n)$ digits;
and Q' has $O(\log n)$ elements.

Insert Q' one element at a time.

If $Q = \{q_{00}, q_{01}, \ldots, q_{15}\}$ then

$$
\begin{aligned}
Q' = \{ & q_{00}q_{02}q_{04}q_{06}q_{08}q_{10}q_{12}q_{14}, \\
& q_{01}q_{03}q_{05}q_{07}q_{09}q_{11}q_{13}q_{15}, \\
& q_{00}q_{01}q_{04}q_{05}q_{08}q_{09}q_{12}q_{13}, \\
& q_{02}q_{03}q_{06}q_{07}q_{10}q_{11}q_{14}q_{15}, \\
& q_{00}q_{01}q_{02}q_{03}q_{08}q_{09}q_{10}q_{11}, \\
& q_{04}q_{05}q_{06}q_{07}q_{12}q_{13}q_{14}q_{15}, \\
& q_{00}q_{01}q_{02}q_{03}q_{04}q_{05}q_{06}q_{07}, \\
& q_{08}q_{09}q_{10}q_{11}q_{12}q_{13}q_{14}q_{15}\}.
\end{aligned}
$$

Can compute $\operatorname{cb} S$ given S in time $n(\log n)^{O(1)}$.

Given coprime base P for S, can factor S over P in time $n(\log n)^{O(1)}$.

Same for any ~~freakoid~~ free coid with fast arithmetic.

(Bernstein)

Decomposing perfect powers

Given integer $c > 1$ with $c < 2^n$.
Want largest integer k
such that c is a kth power.

Find integer r_k within 0.9 of $c^{1/k}$
for $1 \le k < n$.

Can check if $(r_k)^k = c$ for each k
in total time $e^{O(\sqrt{\log n \log\log n})} n$.
(Bernstein)

Time $n(\log n)^{O(1)}$ using fast factorization into coprimes:

Compute $P = \text{cb}\,\{r_1, r_2, \ldots\}$.

c is a kth power if and only if k divides $\text{ord}_q\, c$ for each $q \in P$. Largest k is $\gcd\left\{\text{ord}_q\, c : q \in P\right\}$.

(Lenstra, Pila)