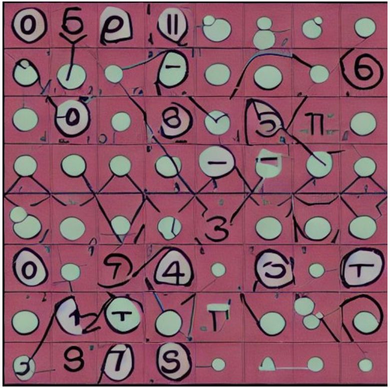
Factoring using multiplicative relations modulo n: a subexponential algorithm inspired by the index calculus

Katherine E. Stange



MathCrypt, August 19th, 2023

Factoring

Well-known problems that are **equivalent** to factoring n:

1. Finding the Euler totient $\varphi(n)$
2. finding the order of elements $g \in (\mathbb{Z}/n\mathbb{Z})^*$ (under ERH; Miller, Shor, Ekerå)

Multiplicative relations modulo n

Factor base $\mathscr{B}$ of b residues $a_1, \ldots, a_b$ modulo n

Multiplicative relations:

$$\prod_{i=1}^{b} a_i^{f_i} = 1$$

Lattice of exponent vectors:

$$\Lambda_{\mathscr{B}} = \left\{ \mathbf{f} = (f_i)_{i=1}^{b} : \prod_{i=1}^{b} a_i^{f_i} = 1 \right\} \subseteq \mathbb{Z}^b.$$

If the residues generate $(\mathbb{Z}/n\mathbb{Z})^*$, then $\Lambda_{\mathscr{B}}$ will have covolume equal to $\varphi(n)$.

The restriction $\Lambda_{\mathscr{B}}|_{S_i}$ of $\Lambda_{\mathscr{B}}$ to i-th coordinate axis S_i has covolume $= \operatorname{ord}(a_i)$.

Equivalently, any generating set for $\Lambda_{\mathscr{B}}|_{S_i}$ will be $\{d_j \mathbf{e}_i\}_j$ where $\gcd(d_j) = \operatorname{ord}(a_i)$.

Main idea

If we can find a generating set for $\Lambda_{\mathscr{B}}|_{S_i}$, we have found $\mathrm{ord}(a_i)$.

And therefore, we factor n.

Approach:

- collect multiplicative relations modulo n, i.e. elements of $\Lambda_{\mathscr{B}} \subseteq \mathbb{Z}^b$
- do linear algebra to obtain elements of $\Lambda_{\mathscr{B}}|_{S_i} \subseteq \mathbb{Z}$

Index Calculus vs. Factoring

Index Calculus $g^x \equiv h \pmod{p}$

Factor base:

$$p_1, p_2, \ldots, p_b$$

Find relations (random x):

$$g^x = \prod_{i=1}^{b} p_i^{f_i} \pmod{p},$$

Linear algebra:

$$x \log(g) = \sum_{i=1}^{b} f_i \log(p_i) \pmod{p-1}$$

Factoring n

Factor base:

$$p_1, p_2, \ldots, p_b$$

Find relations (random x):

$$g^x = \prod_{i=1}^{b} p_i^{f_i} \pmod{n},$$

Linear algebra:

$$x \log(g) = \sum_{i=1}^{b} f_i \log(p_i) \pmod{\varphi(n)}$$

From multiplicative relations to multiplicative order

Let $\mathscr{O}$ be an oracle that provides multiplicative relations modulo n, of length $O(\log n)$ amongst a factor base $\mathscr{B}$.

Theorem

Under the existence of $\mathscr{O}$:

- *there is a Las Vegas algorithm to find the multiplicative order of residues modulo n*
- *with runtime polynomial in $|\mathscr{B}|$ and $\log n$;*
- *with $|\mathscr{B}| + c = O(|\mathscr{B}|)$ calls to $\mathscr{O}$;*
- *and under the Main Hypothesis*[1]*, the probability of success approaches $1 - 1/\zeta(c+1)$.*

[1] coming soon to a slide deck near you!

Algorithm

1. Collect multiplicative relations:

$$g^{x_j} = \prod_{i=1}^{b} p_i^{f_{j,i}} \pmod{n},$$

2. Find relations $\mathbf{b}_t$ between $\mathbf{f}_j = (f_{j,i})_i$ in $\mathbb{Z}$:

$$\sum_{j=1}^{b+c} (\mathbf{b}_t)_j \mathbf{f}_j = 0,$$

3. Compute α_t:

$$\alpha_t := \sum_{j=1}^{b+c} (\mathbf{b}_t)_j x_j.$$

4. Take $\gcd(\alpha_t)$.

Correctness

$$g^{x_j} = \prod_{i=1}^{b} p_i^{f_{j,i}} \pmod{n}, \quad \sum_{j=1}^{b+c} (\mathbf{b}_t)_j \mathbf{f}_j = \mathbf{0},$$

implies that

$$\prod_{j=1}^{b+c} (g^{x_j})^{(\mathbf{b}_t)_j} = 1 \pmod{n}$$

which implies that

$$\alpha_t = \sum_{j=1}^{b+c} (\mathbf{b}_t)_j x_j = 0 \pmod{\operatorname{ord}(g)}$$

Main Hypothesis

The *size* of a relation: logarithm of 1-norm $|\mathbf{f}_i|_1$ of its exponent vector.

(Thus relation vectors whose entries are $< n$ have size $O(\log n)$.)

Let $\Lambda'_{\mathscr{B}} \subseteq \Lambda_{\mathscr{B}}$ be a lattice generated by $|\mathscr{B}| + c$ relations randomly chosen from amongst those in $\Lambda_{\mathscr{B}}$ of size $O(\log n)$.

Main Hypothesis

Then, as $n \to \infty$, the probability that $\Lambda'_{\mathscr{B}}|_{S_i} = \Lambda_{\mathscr{B}}|_{S_i}$ is equal to the probability that $c+1$ random integers (in the sense of natural density) share no common factor, i.e. $1 - 1/\zeta(c+1)$ where ζ is the Riemann zeta function.

Fontein and Wocjan prove this for $n \geq 8b^{\frac{b+1}{2}}$ and $c = b + 1$.

Runtime

$b = |\mathscr{B}|$

- entries of $b \times (b+c)$ matrix are size $O(\log n)$ (integers $< n$)
- computing kernel is polynomial in b and $\log n$
- kernel generators have entries of size polynomial in b and $\log n$
- $O(b)$ GCD operations on integers of this size

$\Rightarrow$ runtime polynomial in b and $\log n$ plus $O(b)$ calls to $\mathscr{O}$.

Factoring Algorithm

Usual notation:

$$L_x(\alpha, \beta) = \exp((\beta + o(1))(\log x)^{\alpha}(\log\log x)^{1-\alpha}).$$

- Relation finding: As for index calculus, time $L_n(1/2, 1)$ with $b = L_n(1/2, 1/2)$.
- Linear algebra is polynomial in b and $\log n$

$\Rightarrow$ full algorithm is subexponential $L_n(1/2, \beta)$ for some β.

Possible optimizations

1. elliptic curve method to remove all prime factors below a bound before attempting this algorithm
2. test for the existence of a non-trivial kernel periodically as we generate relations
3. use a single kernel element, when it is found, to obtain a multiple of $\mathrm{ord}(g)$ and then do further linear algebra modulo that modulus.
4. linear sieve of Coppersmith, Odlyzko and Schroeppel for relation-finding.
5. number field sieve in relation-finding: Gordon

Example

Take $n = 62389$. Factor base of $b = 15$ primes $2 \le p \le 47$. $g = 43$
Goal: 25 relations.
With 188 smoothness tests, we find the relations:

$$43^{55571} = 2^3 \cdot 3^3 \cdot 7 \cdot 29,$$
$$43^{51344} = 5^4,$$
$$43^{1724} = 2 \cdot 5^3 \cdot 7 \cdot 23,$$
$$43^{9399} = 3 \cdot 13 \cdot 37,$$
$$43^{56136} = 2 \cdot 3 \cdot 11^2 \cdot 13,$$
$$43^{53393} = 5^4 \cdot 41,$$
$$43^{24567} = 2^4 \cdot 7 \cdot 23^2,$$
$$43^{2484} = 2 \cdot 3^2 \cdot 13 \cdot 37,$$
$$43^{39818} = 7^2,$$

$$43^{41451} = 2^2 \cdot 5 \cdot 7 \cdot 11^2,$$
$$43^{53596} = 3^3 \cdot 11 \cdot 43,$$
$$43^{12688} = 2^3 \cdot 3 \cdot 7 \cdot 19^2,$$
$$43^{10480} = 2^3 \cdot 3^3 \cdot 5 \cdot 13,$$
$$43^{19831} = 2^8 \cdot 3 \cdot 5 \cdot 11,$$
$$43^{27853} = 2^6 \cdot 3^2 \cdot 5 \cdot 7,$$
$$43^{25154} = 2^5 \cdot 31 \cdot 37,$$
$$43^{9481} = 2^3 \cdot 7 \cdot 11,$$

$$43^{20} = 2^2 \cdot 5^3 \cdot 7^2,$$
$$43^{25418} = 2^5 \cdot 3 \cdot 17 \cdot 19,$$
$$43^{50821} = 5^2 \cdot 41,$$
$$43^{46106} = 2 \cdot 3 \cdot 7 \cdot 11^2,$$
$$43^{14141} = 2 \cdot 3 \cdot 5^2 \cdot 7 \cdot 19,$$
$$43^{26246} = 2 \cdot 3^3 \cdot 5 \cdot 41,$$
$$43^{10795} = 2 \cdot 5^3 \cdot 7 \cdot 11,$$
$$43^{20889} = 5 \cdot 11 \cdot 37,$$

Example

The relation matrix is (cols are relations):

$$
\begin{pmatrix}
3 & 0 & 1 & 0 & 1 & 0 & 4 & 1 & 0 & 2 & 0 & 3 & 3 & 8 & 6 & 5 & 3 & 2 & 5 & 0 & 1 & 1 & 1 & 1 & 0 \\
3 & 0 & 0 & 1 & 1 & 0 & 0 & 2 & 0 & 0 & 3 & 1 & 3 & 1 & 2 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 3 & 0 & 0 \\
0 & 4 & 3 & 0 & 0 & 4 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 3 & 0 & 2 & 0 & 2 & 1 & 3 & 1 \\
1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 2 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 2 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 2 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 2 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}
$$

Example

Rows representing the right kernel:

$$
\begin{pmatrix}
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 12 & 0 & -23 & 3 & 0 & 14 & 18 & 0 & -14 & -13 & 0 \\
0 & 0 & 2 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 7 & 0 & -12 & 1 & 0 & 8 & 10 & 0 & -8 & -8 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 & -1 & 0 & -1 & -1 & 0 & 1 & 2 & -1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 8 & 0 & -15 & 2 & 0 & 8 & 10 & 0 & -8 & -7 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 13 & 0 & -25 & 3 & 0 & 14 & 19 & 0 & -15 & -13 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & 0 & 4 & 0 & -7 & 0 & 0 & 4 & 5 & 0 & -4 & -2 & -1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & -5 & -1 & 0 & 3 & 3 & 0 & -3 & -1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 8 & 0 & -16 & 2 & 0 & 9 & 11 & 0 & -9 & -8 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 2 & 0 & -5 & 1 & 0 & 2 & 3 & -2 & -2 & -1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 6 & 0 & -15 & 3 & 0 & 8 & 11 & 0 & -8 & -8 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 14 & 0 & -27 & 3 & 0 & 16 & 20 & 0 & -16 & -13 & 0
\end{pmatrix}
$$

Example

The corresponding α_k are:

$$1201200,\ 631400,\ -61600,\ 708400,\ 1232000,\ 323400,$$

$$277200,\ 754600,\ 169400,\ 662200,\ 1309000.$$

Their gcd is 15400. We check that

$$43^{15400} = 1, \quad 43^{15400/2} = 51174 \neq \pm 1 \pmod{n}.$$

and therefore taking

$$\gcd(51174 - 1, 62389) = 701$$

reveals a non-trivial factor. In fact, $62389 = 701 \cdot 89$.

Thank you!