ERIC WEISSTEIN'S world of MATHEMATICS
SEARCH
INDEX BY SUBJECT
- Algebra
- Applied Mathematics
- Calculus and Analysis
- Discrete Mathematics
- Foundations of Mathematics
- Geometry
- History and Terminology
- Number Theory
- Probability and Statistics
- Recreational Mathematics
- Topology

ALPHABETICAL INDEX

- ABOUT THIS SITE
- AUTHOR'S NOTE
- FAQs
- WHAT'S NEW
- RANDOM ENTRY
- BE A CONTRIBUTOR
- SIGN THE GUESTBOOK
- EMAIL COMMENTS
- HOW CAN I HELP?
- TERMS OF USE

ERIC'S OTHER SITES

- ORDER BOOK HERE
- ORDER BOOK FROM AMAZON.COM

Number Theory ▸ Factors ▾

Dixon's Factorization Method

In order to find integers *x* and *y* such that

$$x^2 \equiv y^2 \pmod{n} \tag{1}$$

(a modified form of Fermat's factorization method), in which case there is a 50% chance that $\mathrm{GCD}(n, x-y)$ is a factor of *n*, choose a random integer r_i, compute

$$g(r_i) \equiv {r_i}^2 \pmod{n}, \tag{2}$$

and try to factor $g(r_i)$. If $g(r_i)$ is not easily factorable (up to some small trial divisor *d*), try another r_i. In practice, the trial *r*s are usually taken to be $\lfloor\sqrt{n}\rfloor + k$, with *k* = 1, 2, ..., which allows the quadratic sieve factorization method to be used. Continue finding and factoring $g(r_i)$s until $N \equiv \pi d$ are found, where π is the prime counting function. Now for each $g(r_i)$, write

$$g(r_i) = {p_{1i}}^{a_{1i}} {p_{2i}}^{a_{2i}} \cdots {p_{Ni}}^{a_{Ni}}, \tag{3}$$

and form the exponent vector

$$\mathbf{v}(r_i) = \begin{bmatrix} a_{1i} \\ a_{2i} \\ \vdots \\ a_{Ni} \end{bmatrix}. \tag{4}$$

Now, if a_{ki} are even for any *k*, then $g(r_i)$ is a square number and we have found a solution to (1). If not, look for a linear combination $\sum_i c_i \mathbf{v}(r_i)$ such that the elements are all even, i.e.,

$$c_1 \begin{bmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{N1} \end{bmatrix} + c_2 \begin{bmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{N2} \end{bmatrix} + \ldots + c_N \begin{bmatrix} a_{1N} \\ a_{2N} \\ \vdots \\ a_{NN} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \pmod{2} \tag{5}$$

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1N} \\ a_{21} & a_{22} & \cdots & a_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ a_{N1} & a_{N2} & \cdots & a_{NN} \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_N \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \pmod{2}. \tag{6}$$

Since this must be solved only mod 2, the problem can be simplified by replacing the a_{ij} s with

$$b_{ij} = \begin{cases} 0 & \text{for } a_{ij} \text{ even} \\ 1 & \text{for } a_{ij} \text{ odd.} \end{cases} \tag{7}$$

Gaussian elimination can then be used to solve

$$\mathbf{bc} = \mathbf{z} \tag{8}$$

for **c**, where **z** is a vector equal to $\mathbf{0}$ (mod 2). Once **c** is known, then we have

$$\prod_k g(r_k) \equiv \prod_k {r_k}^2 \pmod{n}, \tag{9}$$

where the products are taken over all *k* for which $c_k = 1$. Both sides are

perfect squares, so we have a 50% chance that this yields a nontrivial factor of *n*. If it does not, then we proceed to a different **z** and repeat the procedure. There is no guarantee that this method will yield a factor, but in practice it produces factors faster than any method using trial divisors. It is especially amenable to parallel processing, since each processor can work on a different value of *r*.

References

Bressoud, D. M. *Factorization and Prime Testing*. New York: Springer-Verlag, pp. 102-104, 1989.

Dixon, J. D. "Asymptotically Fast Factorization of Integers." *Math. Comput.* **36**, 255-260, 1981.

Lenstra, A. K. and Lenstra, H. W. Jr. "Algorithms in Number Theory." In *Handbook of Theoretical Computer Science, Volume A: Algorithms and Complexity* (Ed. J. van Leeuwen).

New York: Elsevier, pp. 673-715, 1990.

Pomerance, C. "A Tale of Two Sieves." *Not. Amer. Math. Soc.* **43**, 1473-1485, 1996.

Author: Eric W. Weisstein