A GEOMETRIC APPROACH TO INTEGER FACTORIZATION

Dmitry I. Khomovsky
Lomonosov Moscow State University
khomovskij@physics.msu.ru

Received: , Revised: , Accepted: , Published:

Abstract
We give a geometric approach to integer factorization. This approach is based on special approximations of segments of the curve that is represented by \( y = \frac{n}{x} \), where \( n \) is the integer whose factorization we need.

1. Introduction
Let \( n = xy \) be an odd integer and \( x, y \) be its nontrivial factors. It is known that \( n \) can be represented as the difference of two squares:

\[
    n = \left( \frac{x + y}{2} \right)^2 - \left( \frac{x - y}{2} \right)^2. \tag{1}
\]

This property is used in Fermat’s factorization method, which is based on searching for the representation of an odd integer as \( n = a^2 - b^2 \). To find such a representation we need to take values of \( a \geq \lceil \sqrt{n} \rceil \) and determine whether \( a^2 - n \) is a perfect square. Fermat’s method is the most efficient when there is a factor near \( \sqrt{n} \). It is used in the so-called multiplier improvement that was applied by Sherman Lehman in [1]. The main idea of this improvement consists in searching for a multiplier \( r < n^{1/3} \) such that \( rn \) has a factor near \( \sqrt{rn} \). Lehman’s algorithm has worst-case running time \( O(n^{1/3}) \). Although the above methods are rarely used for practical purposes, the ideas underlying them are a part of more efficient methods for factoring integers.

We only give some references that allow the reader to become familiar with existing methods (see [2, 3, 4, 5]).

In this paper, we propose one approach to factorization of integers which has a simple geometric interpretation. This approach allows us to look at Fermat’s factorization method and similar methods from a different angle.
2. The main theorem

Let $C$ be a plane curve defined by an equation $f(x, y) = 0$ in Cartesian coordinates, where $f : \mathbb{R}^2 \to \mathbb{R}$. The following theorem gives a method for finding solutions of the Diophantine equation $f(x, y) = 0$, in other words integral points on $C$.

**Theorem 1.** Let $f$, $g$ be functions from $\mathbb{R}^2$ to $\mathbb{R}$, and $g$ such that $g(x, y) \in \mathbb{Z}$ if $x, y \in \mathbb{Z}$. If for any integer $k$ from $a \leq k \leq b$, where $a, b \in \mathbb{Z}$, the system of equations $f(x, y) = 0$, $g(x, y) = k$ does not have an integer solution, then the Diophantine equation $f(x, y) = 0$ does not have solutions on $A = \{(x, y) : a \leq g(x, y) \leq b\}$.

**Proof.** Suppose that the equation $f(x, y) = 0$ has an integer solution $(x_0, y_0)$ that belongs to the set $A$. Since $x_0, y_0$ are integers, $g(x_0, y_0)$ is also an integer, moreover, we have $a \leq g(x_0, y_0) \leq b$. But this contradicts the theorem conditions. $\square$

The geometric meaning of the above result is revealed in the following reasoning. To find integral points on a smooth segment of the curve $C$ or to show that they do not exist, we locally approximate $C$ by another curve with the equation $g(x, y) = 0$, and $g$ must be such that $g(x, y) \in \mathbb{Z}$ if $x, y \in \mathbb{Z}$. After this, we look for integer solutions of the system $f(x, y) = 0$, $g(x, y) = k$ for $a \leq k \leq b$, where $a, b$ are chosen so that the segment considered belongs to $A$.

3. Factoring integers

We consider the curve $C$ represented by the explicit equation $y = n/x$ with $x > 0$. This curve is related to the problem of factoring $n$. At $x = \sqrt{n}$ the tangent to $C$ is represented by $y = -x + 2\sqrt{n}$. If we take $y = -x + \lfloor 2\sqrt{n} \rfloor$, then the corresponding line lies under the positive branch of $C$, and the function $g(x, y) = x + y - \lfloor 2\sqrt{n} \rfloor$ satisfies the conditions of Theorem 1. Therefore, if we consider the system $y = n/x$, $y = -x + \lfloor 2\sqrt{n} \rfloor + k$ for $0 \leq k \leq b$ and if $n$ has a divisor $p$ in the interval

$$\frac{1}{2} \left( \lfloor 2\sqrt{n} \rfloor + b + 1 - \sqrt{\lfloor 2\sqrt{n} \rfloor + b + 1} - 4n \right) < p \leq \sqrt{n},$$

then we can find this divisor. To determine whether the above system has integer solutions it is sufficient to check whether $(\lfloor 2\sqrt{n} \rfloor + k)^2 - 4n$ is a perfect square. Since $n$ is odd, we may only consider the system for $k$ such that $\lfloor 2\sqrt{n} \rfloor + k$ is even. Also, if some additional information on divisors of $n$ is known, it can be used to reduce the number of values of $k$ that need to be checked in the interval $0 \leq k \leq b$.

For example, divisors of the Fermat numbers $F_m = 2^{2^m} + 1$ $(m \geq 2)$ are of the form $r \cdot 2^{m+2} + 1$, which was established by Euler and Lucas. Then for $F_m = pq$ we can show that $p + q \equiv 2 \mod 2^{2(m+2)}$. Thus, we need to check only values of $k$ such that $k \equiv 2 - \lfloor \sqrt{F_m} \rfloor \mod 2^{2(m+2)}$. 


Note that the above-described factorization method is exactly Fermat’s method. Indeed, let us consider the term \((x + y)/2\) on the right-hand side of the formula \([1]\). Its smallest possible value is \(\sqrt{n}\), since \(y = n/x\). Therefore, the choice of integer values of this term is equivalent to the choice of \(\ell\) in \(y = -x + 2[\sqrt{n}] + 2\ell\). The following illustration reveals the geometrical meaning of the method.

![Figure 1: Graphic illustration of Fermat’s method.](image)

**Remark.** We can consider an approximation of segments of \(C\) by osculating circles. At the point \((x_0, n/x_0)\), the osculating circle is given by

\[
\left( x - \frac{n^2 + 3x_0^4}{2x_0^3} \right)^2 + \left( y - \frac{3n^2 + x_0^4}{2nx_0} \right)^2 = \frac{(x_0^4 + n^2)^3}{4n^2x_0^6}.
\]

At \(x_0 = \sqrt{n}\) we have \((x - 2\sqrt{n})^2 + (y - 2\sqrt{n})^2 = 2n\). The solution of the system\(^1\)

\[(x - [2\sqrt{n}])^2 + (y - [2\sqrt{n}])^2 = 2n = 2([\sqrt{n} - [2\sqrt{n}])^2 - 2n] + k, y = n/x\]

shows that for large \(n\) and small \(b\) if we examine the system for all integers \(k\) from \(1 \leq k \leq b\), then the interval in which we are looking for divisors has the length approximately equal to \(2(bn)^{1/4}\). This is no better than \(2(b^2n)^{1/4}\) in Fermat’s method.

### 3.1. Using the Taylor series

The first-degree Taylor polynomial of the function \(n/x\) at \(x = \sqrt{n/s} (s \in \mathbb{Z}^+)\) is \(-sx + 2\sqrt{sn}\). Since the coefficients of the polynomial \(g(x, y) = y + sx - [2\sqrt{sn}]\) are integers, then \(g(x, y)\) can be used to search for divisors of \(n\) in a neighborhood of \(\sqrt{n/s}\) (see Theorem 1). It can be shown that for large \(n\) we can check for divisors the interval with the length approximately equal to \(2(b^2n/s^3)^{1/4}\) by making \(b\) steps. Here, by one step we mean checking the existence of integer solutions of \(n/x + sx - [2\sqrt{sn}] = k\). We see that for \(s \geq n^{1/3}\), i.e., for \(x \leq n^{1/3}\), the first-order approximation is inefficient.

---

\(^1\)For simplicity, we can consider the system \((x - 2\sqrt{n})^2 + (y - 2\sqrt{n})^2 = 2n + k, y = n/x\).
Now we consider the second-degree Taylor polynomial of the function \( n/x \) at \( x = (n/s)^{1/3} \) (\( s \in \mathbb{Z}^+ \)). It is equal to \( sx^2 - 3(s^2 n)^{1/3} x + 3(sn^2)^{1/3} \). The polynomial \( g(x, y) = y - sx^2 + [3(s^2 n)^{1/3}] x - [3(sn^2)^{1/3}] \) with integer coefficients can be used to search for divisors of \( n \) in a neighborhood of \((n/s)^{1/3}\). We need to use the equation

\[
\frac{n}{x} - sx^2 + [3(s^2 n)^{1/3}] x - [3(sn^2)^{1/3}] = \left[ \left[ 3(s^2 n)^{1/3} \right] (n/s)^{1/3} - \left[ 3(sn^2)^{1/3} \right] \right] + k.
\]

(4)

If for integers \( k = 1, 2, \ldots, b \) we answer the question whether there exists an integer solution of (4), then the length of the interval that we have checked for divisors \((n/s)^{1/3}\) in order to answer the question whether (4) has an integer root, we should check the interval is to the right of the point \((n/s)^{1/3}\). Thus, from Figure 2 we see that this is realized, when we solve the equation (4). Thus, the following figure is an illustration of the search for divisors of \( n \) in a neighborhood of \( n^{1/3} \).

![Figure 2: The second-order approximation of \( n/x \) at \( x = n^{1/3} \).](image)

The polynomial \( f(x) = x^2 - [3n^{1/3}] x + [3n^{2/3}] + \left[ \left[ 3n^{1/3} \right] n^{1/3} - \left[ 3n^{2/3} \right] \right] \).

As can be seen from the estimate of the length of the interval, the second-order approximation is inefficient for \( s \geq n^{1/4} \), which is equivalent to \( x \leq n^{1/4} \).

**Remark.** The cubic equation \( ax^3 + bx^2 + cx + d = 0 \) with integer coefficients has one integer root and two complex conjugate roots only if \(-\Delta\) is a perfect square, where \( \Delta = 18abcd - 4b^3d + b^2c^2 - 4ac^3 - 27a^2d^2 \) is the discriminant of the equation. From Figure 2 we see that this is realized, when we solve the equation (4). Thus, in order to answer the question whether (4) has an integer root, we should check its discriminant before solving it.

By analogy with the previous reasoning, we have

\[
\frac{n}{x} + sx^3 - \left[ 4(s^3 n)^{1/4} \right] x^2 + \left[ 6(s^2 n^2)^{1/4} \right] x - \left[ 4(sn^3)^{1/4} \right] = C + k,
\]

(5)

where

\[
C = \left[ 2(sn^3)^{1/4} - \left[ 4(s^3 n)^{1/4} \right] (n/s)^{1/2} + \left[ 6(s^2 n^2)^{1/4} \right] (n/s)^{1/4} - \left[ 4(sn^3)^{1/4} \right] \right],
\]

(6)
for divisors in a neighborhood of \((n/s)^{1/4}\). The estimate of the length of the interval corresponding to \(b\) steps is \(2(b^4n/s^5)^{1/16}\). Finally, the equation for divisors of \(n\) in a neighborhood of \((n/s)^{1/4}\) is:

\[
n/x + (-1)^m s x^{m-1} + \sum_{i=1}^{m-1} (-1)^{m-i} \left[\binom{m}{i} (s^{m-i} n^i)^{1/m}\right] x^{m-1-i} = C + k,
\]

where

\[
C = \left[ (1 + (-1)^m) (sn^{m-1})^{1/m} + \sum_{i=1}^{m-1} (-1)^{m-i} \left[\binom{m}{i} (s^{m-i} n^i)^{1/m}\right] (n/s)^{(m-i)/m} \right].
\]

So far we have considered the case \(s \in \mathbb{Z}^+\), but (8) can be used for rational \(s = h/t\) if \(k\) is replaced by \(k/t\). We put \(s = 1/t \ (t \in \mathbb{Z}^+)\) in (4) and replace \(k\) by \(k/t\), then we obtain the equation for divisors of \(n\) in a neighborhood of \((nt)^{1/3}\). In this case the length of the interval corresponding to \(b\) steps is \((b^3tn)^{1/9}\). On the other hand, if we use the first-order approximation of divisors of \(n\) at \(x = (nt)^{1/3}\), then the length of the interval is \(2(bt)^{1/2}\). Comparing the obtained estimates with each other, we can answer the question: at what values of \(x\) is the first-order approximation more efficient? To answer it, we need to solve the following inequality \(2(bt)^{1/2} > (b^3tn)^{1/9}\).

If we put \(b = 1\), i.e., we make only one check, then we get \(t > (n/2^9)^{2/7}\). Finally, we have \(x > (n/4)^{3/7}\). The result should be considered approximate.

**Remark.** If we use (7) at \(x = n^{1/m}\), the interval for divisors is proportional to \(n^{1/m^2}\). The following question arises: is there such an approximation of \(C\) at an arbitrary point \(x = n^e \ (0 < e < 1/2)\) which gives the length of the interval that is proportional to \(x^e\)?

### 3.2. Lehman-like methods

Let \(r\) be a positive integer. The search for divisors of \(rn\) in a neighborhood of \(\sqrt{rn}\) can be carried out using the equation \(rn/x + x - (2\sqrt{rn}) = k \ (k \in \mathbb{Z}^+)\). It has the solutions \(x = (A + \sqrt{A^2 - 4rn})/2\), where \(A = [2\sqrt{rn}] + k\), which are integer if \(A^2 - 4rn\) is a perfect square. As it was shown, the length of the interval corresponding to \(b\) steps \((k = 1, 2, \ldots, b)\) is equal to \(2(b^2rn)^{1/4}\). We see that if \(b = \left[n^{1/6}/(4\sqrt{r})\right]\), then the length is greater than or equal to \(n^{1/3}\). The relationship between the above and Lehman’s method becomes clear if one looks at the version of Lehman’s algorithm in [6].

Let us agree that if we apply the multiplier improvement using an approximation of \(rn/x\) at \(x = u(rn)\), where \(u : \mathbb{R} \to \mathbb{R}\), then we will call it a divisors trap related to the function \(u\). In these terms, Lehman’s method is based on the trap related to \(u(\omega) = \sqrt{\omega}\). We can modify this method by using another trap with the function \(v(\omega) = \omega^{1/3}\). So if large \(n\) has a divisor near \(n^{1/3}\), then it will fall into the latter
trap with a smaller value of $r$. In other words, the more traps the smaller the value of the multiplier at which a divisor of composite $n$ will be found. This idea and formulas \(^7\), \(^8\) can be used to obtain efficient factorization algorithms.

**Acknowledgments.** I thank my school math teacher Ms. Nadezhda P. Vlasova.

**References**

[1] R. S. Lehman, Factoring large integers, *Mathematics of Computation* **28**,126 (1974), 637-646.

[2] A. K. Lenstra, Integer factoring, *Designs, codes and cryptography* **19**,2 (2000), 101-128.

[3] R. P. Brent, Parallel algorithms for integer factorisation, *Number theory and cryptography* **154** (1990), 26-37.

[4] G. Hiary, A deterministic algorithm for integer factorization, *Mathematics of Computation* **85**,300 (2016), 2065-2069.

[5] M. Agrawal, N. Saxena, and S. S. Srivastava, Integer factoring using small algebraic dependencies. LIPs-Leibniz International Proceedings in Informatics. Vol. 58. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2016.

[6] R. Crandall, and C. B. Pomerance, *Prime numbers: a computational perspective*. Vol. 182. Springer Science & Business Media, 2006.