Maximizing the Number of Lattice Points on a Strictly Convex Curve

Brandon Rafal Epstein

under the direction of
Hong Wang
Department of Mathematics
Massachusetts Institute of Technology

Research Science Institute
1 October 2015

Abstract

We obtain an upper bound for the maximum number of integral lattice points on the graph of a twice differentiable convex function $f : [0, N] \to [0, N^\gamma]$, where $\gamma > 0$ by generalizing an argument for $\gamma = 1$ to all γ between $\frac{1}{2}$ and 2. This method was based on the asymptotes of sums involving the Euler totient function, which we extended to prove the general case. Moreover, we also strengthen upper bounds for smooth convex functions $f : [0, N] \to [0, N]$ with restrictions on higher derivatives. Specifically, we tighten an upper bound on the number of lattice points on a curve with positive first, second, and third derivatives by modifying a method of Bombieri and Pila. We also examine the problem of finding the maximal number of lattice points on a smooth convex curve $y = f(x)$, subject to the condition $1 < f''(x) < 2$. We conjecture that this maximum is attained for the curve $y = \frac{3}{4}x^2$, which has $2\sqrt{\frac{N}{3}} - O(1)$ lattice points. Finding the number of lattice points on curves has a large number of applications, including prime factorization, which is used in modern cryptography to create secure one-way systems for which it is difficult to decode messages without the proper key. Another application is the approximation of the area under a curve. Though this problem may be solved with numerical integration, approximating the area uses less computing power to produce reasonably accurate measures while saving time.

Summary

Modern cryptography often incorporates mathematical techniques that blend disparate fields of mathematics (like elliptic curves and prime factorization) with computer science as people try to improve their cryptographical systems' security against hackers who in turn try to develop more powerful algorithms to crack them. Specifically, the techniques involving prime factorization are useful because multiplying prime numbers takes much less time than factoring the product of two large primes. They can be thought of as finding *lattice points*, or points with integer coordinates, on a rectangular hyperbola. Quickly counting lattice points can thus hold great importance to cryptography.

A function's derivative represents the instantaneous rate of change of that function. A function is *strictly convex* if it has a non-vanishing (non-zero) second derivative in a certain range, and it is *differentiable* if its derivatives up to a certain order are continuous. The area bounded by a given differentiable, strictly convex curve in a plane can be estimated by counting lattice points inside the curve. These approximations, however, are often rendered imprecise as a result of the presence of lattice points on the curve. We can improve the estimates by finding tighter upper bounds on the number of lattice points on the curve. We examined the maximum number of lattice points a function's graph can contain on a grid of large integer dimensions under different restrictions on the derivatives. For instance, we can require non-zero third derivatives or second derivatives within a certain range. We observed the maximum number of lattice points on convex functions mapping a large interval to another large interval of the same length under certain conditions on the derivatives. We also investigated the general case of a convex function mapping a large interval to another large interval of a different length. In fact, the general case is analogous to the specific one when the larger interval's size is shorter than the square of the smaller interval's size.

The results of this paper reduce the time complexity of calculating the lattice points on a curve under certain conditions. Since factorization is very slow compared to multiplication, the findings may be able to help reduce the time needed to crack a factorization-based cryptographical system.

1 Introduction

We find the number of lattice points, or points with integer coordinates, on a twice differentiable convex function $f : [0, N] \to [0, N^\gamma]$ for some $\gamma > 0$. This problem is motivated by measurements of area under convex curves. Huxley [1] mentions many such approximations involving counting points under a curve. For example, one measure divides the xy-plane into a grid of squares of side length $\frac{1}{M}$. The area is then approximately equal to the combined area of the squares with their bottom-left corners inside the curve. Alternatively, one can count the number of squares with their centers inside the curve. These approximations are hindered by the presence of lattice points on the curves. If we can obtain a stronger upper bound for the number of lattice points on the curve, we can get more accurate approximations to the area contained by the curve.

To find the upper bound, we use techniques from number theory and calculus. For any points $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ in $\mathbb{Z}^2$, the *discrete slope* β is defined as

$$\beta = \frac{y_Q - y_P}{x_Q - x_P}.$$

We study the number of discrete slopes between consecutive lattice points on the graphs—that is, points P and Q such that there is no lattice point on the curve between P and Q—within a bounding box, primarily because the slopes themselves are monotonically increasing as a result of the convex function's positive second derivative. Maximizing the number of discrete slopes also maximizes the number of lattice points because in general the number of lattice points is one greater than the number of discrete slopes.

Some notation must be defined to find the solution to this problem. For a positive integer L, Euler's totient function $\phi(L)$ is defined as the number of positive integers less than or equal to L that are coprime with L. Also, we denote the *greatest common factor* of two positive integers a and b as (a, b).

Smooth functions are functions that have continuous derivatives to the second order. Examples include exponential and polynomial functions. Consider a smooth function $y(x)$ and a sufficiently large integer N. The box bounded by the x and y axes and the lines $x = N$ and $y = N$ contains $(N + 1)^2$ lattice points. We find how many of these lattice points the smooth function can pass through given that the function's second derivative is not equal to zero for any x such that $0 \leq x \leq N$. Without loss of generality, we can consider only the case where the second derivative is positive because, if the second derivative is continuous, it is either always positive, always negative, or somewhere zero. Functions with a purely negative second derivative can be negated to obtain a function with a positive second derivative (shifting upward N spaces to ensure that the same area of the function is within the bounding box).

Huxley [2] and others have found bounds on the number of lattice points on a curve of the form $O\left(N^K(\log N)^\Lambda\right)$ under various conditions of differentiability. For example, van der Corput [3] proved that the number of lattice points was bounded above by $O\left(N^{\frac{2}{3}}\right)$ for a twice differentiable curve, and Huxley [4] found that a three times differentiable curve has a number of lattice points bounded above by $O\left(N^{\frac{7}{11}}(\log N)^{\frac{47}{22}}\right)$. They used methods involving approximating curves with polygons and with transformations of other curves known as *resonance curves.*

In section 3, we investigate a possible maximal case for the number of lattice points on the graph of a function with second derivative strictly between 1 and 2. In section 4, we prove an upper bound to the number of lattice points on the graph of a function $f : [0, N] \to [0, N^\gamma]$. In section 5, we improve an upper bound on the number of lattice points on the graph of a function with strictly positive first, second, and third derivatives.

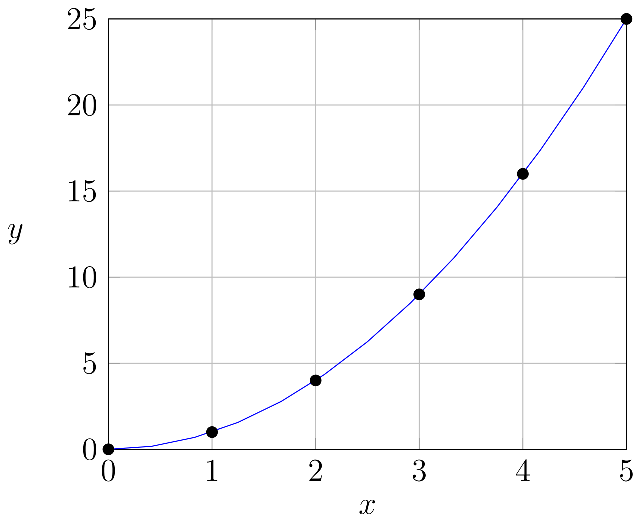

Figure 1: The graph of $y = x^2$ for $N = 25$. There are six lattice points, which is one more than $\sqrt{25}$. As N grows, this difference becomes negligible.

2 Preliminary upper bounds

In this paper, we focus on the cases where the second derivative is nonvanishing, but the upper bound for the general case of a smooth function is $N + 1$ points and is achieved by the function $y = x$. In the case of $y = x$, the curve contains the lattice points $(0, 0), (1, 1), (2, 2), ..., (N, N)$.

The number $N + 1$ is an upper bound for all functions. Were there more lattice points on the curve, it would no longer be a function because—by necessity—there would have to be at least two points with the same x-value. But we must also consider that the function, by the conditions of the problem, cannot have a second derivative equal to zero for any x from 0 to N. The aforementioned $y = x$ has a second derivative equal to zero. Another function that passes through $N + 1$ lattice points is $y = \sin{(\pi x)} + 1$. However, it also has several points with zero second derivative. Both of these functions, therefore, violate the second condition. The function $y = x^2$ does not violate the conditions. It has $\left\lfloor \sqrt{N} \right\rfloor + 1$ lattice points, as shown in Figure 1.

3 The $N \times N$ case

Jarník [5] proved the number of lattice points on a smooth convex curve is bounded above by $2^{\frac{2}{3}}N^{\frac{2}{3}}$. His proof is summarized below.

Let R be some value such that more than half the changes in y between consecutive points are greater than R, and let S be the number of lattice points on the curve. Then

$$N \geq \sum_{i=1}^{\lfloor \frac{S}{2} \rfloor} y_{i+1} - y_i \geq \frac{RS}{2}.$$

To maximize R, we set $R = \frac{2N}{S}$. Then, half the differences should be smaller than $\frac{2N}{S}$ in both the x and y directions. Therefore,

$$S \leq \left(\frac{2N}{S}\right)^2,$$

and isolating S we obtain

$$S \leq \sqrt[3]{(2N)^2} = 2^{\frac{2}{3}}N^{\frac{2}{3}}.$$

The proof of the strict upper bound is known [5] and summarized below. For two consecutive lattice points, p and q respectively are the differences in the x and y coordinates. We calculate the strict upper bound by finding the number of discrete slopes $\frac{p}{q}$ possible such that $p, q \in \mathbb{Z}$ and $p, q \leq x$ for some positive integer x. Next, we compare it to N, which is the sum of the values of p and equivalently of the values of q.

First, to each pair of integers p and q, henceforth denoted $\langle p, q \rangle$, we associate the slope $\frac{q}{p}$. There are some repeated slopes, so to minimize the size of the differences we choose only p and q such that $(p, q) = 1$. If $(p, q) = r$, then we obtain the slope $\frac{q}{p}$, which we can also obtain for the pair $\langle \frac{p}{r}, \frac{q}{r} \rangle$. Let us set q equal to an integer $L > 2$ and consider all values of p less than q with $(p, q) = 1$. Then the number of pairs of p and q for $q = L$ is $\phi(L)$. An example for $L = 12$ is shown in Table 1.

p	q	$\frac{q}{p}$
1	12	12
5	12	$\frac{12}{5}$
7	12	$\frac{12}{7}$
11	12	$\frac{12}{11}$

Table 1: The values of p and q and corresponding slopes for $L = 12$. Note that we must also consider each slope's reciprocal.

Lemma 1. *Let N be a sufficiently large integer and $f : [0, N] \to [0, N]$ be a smooth function such that $f'' > 0$ and for which the number of lattice points on its graph is maximized. Then the differences between the coordinates of consecutive lattice points in the x and y directions do not exceed $\sqrt[3]{\frac{N\pi^2}{3}}$. [5]*

Proof. We note that, to maximize the number of differences between coordinates on the graph, the sum of the differences should be maximized. This is achieved if the sum equals N. We calculate the sum of the p values in two parts for each L. We can group the positive integers from 1 to $L-1$ in pairs that add to L. Since only $\phi(L)$ of these integers are coprime with L, there are $\frac{\phi(L)}{2}$ such pairs, so these integers add to $\frac{L\phi(L)}{2}$. We are also considering the reciprocals of these slopes; therefore, we must also calculate the sum of the values of q. Because these values all equal L and there are $\phi(L)$ of them, they add up to $L\phi(L)$. Adding the two results yields $\frac{3L\phi(L)}{2}$.

For example, in the case of $L = 2$, we obtain only $\langle 1, 2\rangle$, and the sum is 3, in agreement with the above.

We take the sum of these values for all $L \geq 2$ and add 1 because the pair $\langle 1, 1\rangle$ yields a single slope of 1.

We thus have

$$N \leq \sum_{k=2}^{x} \frac{3k\phi(k)}{2} + 1,$$

From [6], we see that the latter sum is asymptotically equivalent to $\frac{3}{\pi^2}x^3$.

Note that we do not arrive at integer values of x for every N. We arrive at an x between two consecutive integers T and $T+1$, so we need to subtract a number of differences less than $\frac{3T\phi(T)}{2} = O(T^2)$, which is negligible compared to $\frac{3}{\pi^2}x^3$ for sufficiently large x.

Isolating x in terms of N, we obtain

$$x \leq \sqrt[3]{\frac{N\pi^2}{3}}.$$

□

Theorem 1. *Let N be a large integer and $f : [0, N] \to [0, N]$ be a smooth function such that $f'' > 0$. The number of lattice points on the graph of f is bounded above by $2\sqrt[3]{\frac{3}{\pi^2}}N^{\frac{2}{3}}$. [5]*

Proof. Since there are $\phi(L)$ pairs, there must be $2\phi(L)$ slopes because each pair yields two slopes. As above, the pair $\langle 1, 1\rangle$ yields a single slope of 1, so we now have a formula for the number of slopes

$$S = 2\sum_{i=2}^{x} \phi(i) + 1$$

which, for large x, grows as $\frac{3}{\pi^2}x^2$ [7].

From these formulae we can find a bound for S in terms of N:

$$S \leq 2\sqrt[3]{\frac{3}{\pi^2}}N^{\frac{2}{3}}.$$

□

We can impose further restrictions on the second derivative. For example, it is possible to restrict it to a certain range, like $1 < f''(x) < 2$.

We will consider curves with a constant non-zero second derivative, i.e., parabolas. The number of lattice points that a parabola of the form $y = \frac{a}{bc^2}x^2$ contains, for sufficiently large N and $a, b, c \in \mathbb{Z}, (a, bc^2) = 1$, can be derived as follows:

Take $y = N$, then $N = \frac{a}{bc^2}x^2$. Isolating x, we obtain $x = b\sqrt{\frac{cN}{a}}$. However, only lattice points with x-coordinates that are multiples of bc can be on the curve. Otherwise, the y-coordinate is not an integer.

Dividing x by bc yields

$$\frac{x}{bc} = \frac{b\sqrt{\frac{cN}{a}}}{bc} = \sqrt{\frac{N}{ac}}.$$

For N sufficiently large, we can use the symmetry of the parabola to shift it right enough spaces such that at most twice as many points fit on the curve.

Therefore, we have

$$2\sqrt{\frac{N}{ac}}$$

lattice points, with an error term in $O(1)$.

So the maximum number of lattice points possible with a constant second derivative under the given restrictions is $2\sqrt{\frac{N}{3}}$. This can be achieved with $y = \frac{3}{4}x^2$.

4 The $N \times N^\gamma$ case

The general case of lattice points on a function $f : [0, N] \to [0, N^\gamma]$ for some $\gamma > 0$ can be further separated into different cases. First, we can consider the case of $\gamma \geq 2$. For this case, we can choose the function $f(x) = x^2$ and obtain exactly $N+1$ lattice points—the absolute maximum because that is the largest number of x-coordinates.

We also consider the case where $\gamma \leq \frac{1}{2}$. In this case, the upper limit on the number of lattice points is $2N^\gamma$. If there were any more lattice points on the curve, by the pigeonhole principle, there would have to be three with the same y coordinate and therefore on the same line. Since a strictly convex curve cannot have three collinear points, the curve can only have $2N^\gamma$ lattice points.

The case where $\frac{1}{2} < \gamma < 2$ can be solved in much the same way as the specific case of $\gamma = 1$.

Let a and b be positive integers for which $p \leq a$ and $q \leq b$ for every difference in consecutive lattice points' coordinates p and q. First, we calculate the number of slopes that are possible.

Lemma 2. *Let a and b be two positive integers such that the differences between the coordinates of consecutive lattice points in the xy-plane are positive and do not exceed a in the x direction or b in the y direction, and the discrete slopes are monotonically increasing. Then there are at most $\frac{6ab}{\pi^2}$ lattice points.*

Proof. The number of slopes S is

$$S = \sum_{1 \leq p \leq a} \sum_{\substack{1 \leq q \leq b \\ (p,q)=1}} 1.$$

The number of positive integers less than or equal to A that are relatively prime with B grows as $\frac{A\phi(B)}{B}$, so we arrive at the following sum

$$S = \sum_{1 \leq p \leq a} \frac{b\phi(p)}{p} \sim b \sum_{1 \leq p \leq a} \frac{\phi(p)}{p}.$$

As in [7], the sum $\sum_{k=1}^{x} \frac{\phi(k)}{k}$ grows as $\frac{6x}{\pi^2}$.

Therefore, $S \sim \frac{6ab}{\pi^2}$.

□

Theorem 2. *Let N be a sufficiently large integer, suppose that $\frac{1}{2} < \gamma < 2$, and let $f : [0, N] \to [0, N^\gamma]$ be a smooth function such that $f'' > 0$. The number of lattice points on the graph of f is bounded above by $2\sqrt[3]{\frac{3}{\pi^2}}N^{\frac{\gamma+1}{3}}$.*

Proof. To calculate ab with respect to N and γ we must add up all values of p that are possible (that is, such that p and q are coprime and $p \leq a$ and $q \leq b$). Therefore, we have the sums

$$N = \sum_{1 \leq p \leq a} \sum_{\substack{1 \leq q \leq b \\ (p,q)=1}} p = \sum_{1 \leq p \leq a} p \sum_{\substack{1 \leq q \leq b \\ (p,q)=1}} 1, \tag{1}$$

$$N^\gamma = \sum_{1 \leq q \leq b} \sum_{\substack{1 \leq p \leq a \\ (p,q)=1}} q = \sum_{1 \leq q \leq b} q \sum_{\substack{1 \leq p \leq a \\ (p,q)=1}} 1. \tag{2}$$

We consider (1), the first sum. (The second sum is calculated in an analogous manner.) Using the asymptotic estimate $\sum_{k=1}^{x} \frac{\phi(k)}{k} \sim \frac{6x}{\pi^2}$, we find that

$$N = \sum_{1 \leq p \leq a} b\phi(p) = b \sum_{1 \leq p \leq a} \phi(p) \sim \frac{3a^2 b}{\pi^2}.$$

The second sum, (2), is similarly

$$N^\gamma \sim \frac{3ab^2}{\pi^2}.$$

To solve for ab, we multiply the sums together to yield

$$N^{\gamma+1} \sim \frac{9a^3 b^3}{\pi^4}.$$

Isolating ab, we obtain

$$ab \sim \sqrt[3]{\frac{\pi^4}{9}} N^{\frac{\gamma+1}{3}}.$$

Substituting this into the formula for $S = \frac{6ab}{\pi^2}$ that we obtained earlier, we arrive at

$$S \sim \frac{6\sqrt[3]{\frac{\pi^4}{9}} N^{\frac{\gamma+1}{3}}}{\pi^2} = 2\sqrt[3]{\frac{3}{\pi^2}} N^{\frac{\gamma+1}{3}}. \qquad \square$$

5 Restricted third derivative

A three times differentiable convex function with $f^{(3)} > 0$ should have N^β lattice points, where $\frac{1}{2} \leq \beta \leq \frac{3}{5}$ [8]. It is conjectured that $\beta = \frac{1}{2}$, and considering $y = N - \sqrt{N-x}$ shows that $\beta = \frac{1}{2}$ is best possible [9].

The following proof is structured similarly to that given in [10].

Let $f(x) \in C^3([0, N]), 0 \leq x \leq N$. We are interested in the integral lattice points on the graph of $f(x)$. Let $P_1, \ldots, P_S$ be these points, arranged in order of increasing x-coordinates.

Let $d \geq 1$ be an integer. Define a finite sequence of integers n_ℓ inductively by the following:

- $n_0 = 1$
- if $n_{\ell-1}$ has been defined, and if there is an integer z such that the points P_i for $n_{\ell-1} \leq i < z$ lie on some algebraic curve of degree at most d but the points P_i for $n_{\ell-1} \leq i \leq z$ do not, then define $n_\ell = z$. Otherwise, the sequence terminates with $n_{\ell-1}$.

Suppose that the sequence n_ℓ has $m+1$ elements. Let $D = \frac{1}{2}(d+1)(d+2)$. Then any $D-1$ points in the plane lie on some algebraic curve of degree at most d. Therefore, $n_\ell - n_{\ell-1} \geq D - 1$.

Let J_d denote the set of ordered pairs $j = (j_1, j_2)$ such that $j_1, j_2 \in \mathbb{Z}$ and $0 \leq j_1 + j_2 \leq d$. We have $|J_d| = D$.

If P is a point with coordinates (x,y), we write $P^j = P^{(j_1,j_2)} := x^{j_1}y^{j_2}$.

Lemma 3. *Suppose $f \in C^{D-1}([0,N])$ and $d \geq 1$. Let x_i be the x-coordinate of point P_i. The sequence n_ℓ defined as above satisfies*

$$\left|x_{n_{\ell+1}} - x_{n_\ell}\right| \geq ||f||_{D-1}^{-\frac{4}{3(d+3)}} D^{-\frac{8(d-3)}{3d(d+3)}} D!^{-\frac{8}{d(d+1)(d+2)(d+3)}} N^{1-\frac{8}{3(d+3)}}.$$

Proof. Bombieri and Pila proved in [10] that the matrix $\left(P_i^j\right)_{\substack{n_\ell \leq i \leq n_{\ell+1} \\ j \in J_d}}$ has rank at most D. Hence, there is a subset $I \in \{n_\ell, \ldots, n_{\ell+1}\}$ of cardinality D such that $\Delta := \det\left(P_i^j\right)_{\substack{i \in I \\ j \in J_d}}$ is non-zero.

Since Δ is clearly an integer, we can conclude that $|\Delta| \geq 1$. We can use another formula, also given in [10], that

$$|\det\left(f_j(x_i)\right)| \leq |V\left(x_1, \ldots, x_n\right)| \, n! N^{-\frac{n(n-3)}{2}} ||f_1||_{n-1} \cdots ||f_n||_{n-1}$$

with $n = D$, the previously defined x_i for $i \in I$, $V\left(x_1, \ldots, x_n\right)$ being the Vandermonde determinant of $x_1, \ldots, x_n$, and f_i the functions $x^{j_1} f(x)^{j_2}$ for $(j_1, j_2) \in J_d$ in some order.

We obtain

$$|V\left(x_i; i \in I\right)| \leq \left|x_{n_{\ell+1}} - x_{n_\ell}\right|^{\frac{D(D+1)}{2}}$$

and (1) gives us:

$$|\Delta| \leq \left|x_{n_{\ell+1}} - x_{n_\ell}\right|^{\frac{D(D-1)}{2}} N^{-\frac{D(D-3)}{2}} D! \prod_{j \in J_d} (DN)^{j_1+j_2-1} ||f||_{D-1}^{j_2}.$$

Bombieri and Pila use a weaker inequality that replaces $D!$ with D^D to obtain a weaker upper bound. Instead, we allow the $D!$ to remain in the equation, and we obtain stronger results:

$$|\Delta| \leq \left(\frac{\left|x_{n_{\ell+1}} - x_{n_\ell}\right|}{N}\right)^{\frac{D(D-1)}{2}} D^{\frac{D(d-3)}{3}} D! N^{\frac{dD}{3}} ||f||_{D-1}^{\frac{dD}{6}}.$$

However, since $|\Delta| \geq 1$, we have

$$\left|x_{n_{\ell+1}} - x_{n_\ell}\right| \geq ||f||_{D-1}^{-\frac{4}{3(d+3)}} D^{-\frac{8(d-3)}{3d(d+3)}} D!^{-\frac{8}{d(d+1)(d+2)(d+3)}} N^{1-\frac{8}{3(d+3)}}.$$

□

Since $D^{\frac{8(d-3)}{3d(d+3)}} D!^{\frac{8}{d(d+1)(d+2)(d+3)}} < 2.03$ for every d, we now obtain:

Main Lemma. *Suppose $d \geq 1$ and $f \in C^{D-1}([0, N])$, with D defined as above. Then the integral lattice points on the graph of $f(x), x \in [0, N]$ lie on the union of not more than*

$$2.03 \left(||f||_{D-1}^{\frac{1}{2}} N\right)^{\frac{8}{3(d+3)}} + 1$$

real algebraic curves of degree at most d.

Remark. *The bound in the general case of J being the set of ordered pairs $j = (j_1, j_2)$ such that $x^{j_1} y^{j_2} \in M$ for M a set of monomials of cardinality D, $p := \sum_{j \in J} j_1 + j_2$, and $q := \sum_{j \in J} j_2$ should be*

$$\left(D^{p-D} D! ||f||_{D-1}^{q}\right)^{\frac{2}{D(D-1)}} N^{\frac{2p}{D(D-1)}} + 1.$$

The factor $\left(\frac{D!}{D^D}\right)^{\frac{2}{D(D-1)}}$ approaches 1 as d increases, so the difference is most pronounced for sufficiently small values of d.

6 Discussion

The analysis of lattice points on a curve has several applications to other fields. For example, some cryptographical methods involve multiplying two large prime numbers, p and q, to obtain a large semiprime, $n = pq$ [11]. This pair is equivalent to the point (p, q) on the curve $y = \frac{n}{x}$. Finding lattice points on hyperbolae of the form $y = \frac{l}{x}$ for positive integer l is equivalent to finding factors of l. An efficient way to find lattice points on such a curve would make it easier to factor a semiprime number. De Loera [11] mentions a method originally proven by Jacobi that states that dividing the number of lattice points within a 4-ball of radius r by 8 is equivalent to finding the sum of the factors of r that are not divisible by 4.

The reason this process is important to cryptography is that multiplying two numbers takes comparatively little time, but factoring a large integer can take a lot longer, particularly if it is the product of only two large prime numbers. No known efficient algorithm has yet been found to factor a large semiprime. Therefore, in public-key cryptography, the large semiprime number can be given as a public key, and the prime numbers are the private key. The private key is used to decrypt messages sent to the recipient as well as to provide a signature identifying the recipient. Similarly, the public key, which can be revealed openly with little risk of cryptographical insecurity, encrypts messages and verifies signatures. The main principle is that the private key, which performs the more secure functions, can be used to easily determine the public key, but using the public key to find the private key is more difficult. This lends importance to finding processes, known as *one-way functions*, that are easy to perform but whose reverse processes are not—if such functions even exist. Factorization is conjectured to be an example of a one-way function.

Counting lattice points on a curve is related to several unsolved problems in mathematics that involve counting lattice points in the interior of a curve. The Gauss circle problem involves calculating the number of lattice points inside a circle with a large integral radius R. The number of lattice points is $\pi R^2 + O\left(R^{\frac{131}{208}}\right)$ [2]. It is conjectured that the error term is actually $O\left(R^{\frac{1}{2}}\right)$. The related Dirichlet divisor problem entails counting lattice points bounded by a hyperbola $y = \frac{n}{x}$. The number of lattice points is $n \log n + (2\gamma - 1)n + O\left(n^{\frac{131}{416}}\right)$, but the error term is conjectured to be $O\left(n^{\frac{1}{4}}\right)$ [2]. The Dirichlet divisor problem is equivalent to finding the asymptotic behavior of the divisor summatory function—the function $\sum_{x=1}^{n} d(x)$, where $d(x)$ is the number of distinct divisors of x.

Counting lattice points on a curve can also help with approximations of area. Although the problem of finding a curve's exact area is solved with integration, the process can be computationally taxing. Conversely, approximating a curve's area by using lattice points is more efficient and can lead to reasonably close estimates even with low-power computers. This conserves time when performing large calculations of area.

7 Conclusion

We calculated an upper bound for the number of lattice points in the graph of a convex function $f : [0, N] \to [0, N^\gamma]$ for large integer N and all $\gamma > 0$ in terms of N and γ. This upper bound was equal to $\min\left(2N^\gamma, 2\sqrt[3]{\frac{3}{\pi^2}}N^{\frac{\gamma+1}{3}}, N\right)$. We also strengthened previous bounds on the number of lattice points on a function $f : [0, N] \to [0, N]$ with positive first-, second-, and third-order derivatives and conjectured that the maximum number of lattice points on a curve with a second derivative strictly between 1 and 2 is $2\sqrt{N}3-O(1)$, achieved with $\frac{3}{4}x^2$. In the future, it is possible to research functions with multivariate input. For example, we may examine the number of lattice points $(x, y, z) \in \mathbb{Z}^3$ on a function $f : [0, N] \times [0, N] \to [0, N]$ whose Hessian matrix is positive definite.

8 Acknowledgments

I would like to thank Hong Wang of the Massachusetts Institute of Technology Department of Mathematics for teaching, guiding, and encouraging me throughout my research. Furthermore, I wish to acknowledge Dr. John Rickert of the Rose-Hulman Institute of Technology for all of his vital assistance and advice with my project and presentation. I am grateful to Dr. Tanya Khovanova of the Massachusetts Institute of Technology Department of Mathematics for her invaluable direction and ideas. In addition, I wish to thank the Massachusetts Institute of Technology Department of Mathematics coordinators, namely Prof. Ankur Moitra and Prof. David Jerison, for their insight and inspiration. I would also like to extend my thanks to Dr. Tatiana Portnaya of the State University of New York at Stony Brook for her enlightening conversations and guidance with the paper-writing. Lastly, I would like to express my eternal gratitude to the Research Science Institute and the Center for Excellence in Education and my sponsors, Mr. Gregory M. Gunn, Dr. David Shaw, Mr. and Mrs. Roger Pellegrini, Dr. David Cheng, Mr. Joshua Revitz, Mr. Kalani Oshiro, the Honorable Joseph I. Lieberman, Mr. Henry Gong and Dr. Liming Gong, and Mr. and Mrs. Sigmund Wissner-Gross, for providing me with this amazing opportunity to conduct my research.

References

[1] M. N. Huxley. International congress of mathematicians. In *Area, Lattice Points and Exponential Sums*, page 413, 1990.

[2] M. N. Huxley. Exponential sums and lattice points iii. *Proceedings of the London Mathematical Society*, 87:591–609, 11 2003.

[3] J. G. van der Corput. Over de roosterpunten in het platte vlak:(de beteekenis van de methoden van voronoi en pfeiffer). 1919.

[4] M. N. Huxley. Exponential sums and lattice points. *Proceedings of the London Mathematical Society*, s3-60(3):471–502, 1990.

[5] V. Jarník. über die gitterpunkte auf konvexen kurven. *Mathematische Zeitschrift*, 24(1):500–518, 1926.

[6] N. J. A. Sloane. http://oeis.org/A011755. Sum{k=1..n} k*phi(k).

[7] A. Walfisz. Weylsche exponentialsummen in der neueren zahlentheorie. *Zeitschrift für Angewandte Mathematik und Mechanik*, 1963.

[8] H. P. F. Swinnerton-Dyer. The number of lattice points on a convex curve. *Journal of Number Theory*, 6(2):128–135, 1974.

[9] W. M. Schmidt. Integer points on curves and surfaces. *Monatshefte für Mathematik*, 99(1):45–72, 1985.

[10] E. Bombieri and J. Pila. The number of integral points on arcs and ovals. *Duke Math. J.*, 59(2):337–357, 10 1989.

[11] J. A. D. Loera. The many aspects of counting lattice points in polytopes. *Mathematische Semesterberichte*, 52:175–195, 2005.