Scientific Research Publishing

Advances in Pure Mathematics, 2020, 10, 114-124
https://www.scirp.org/journal/apm
ISSN Online: 2160-0384
ISSN Print: 2160-0368

On Conditional Probabilities of Factoring Quadratics

Thomas Beatty, Gabriela von Linden

Department of Mathematics, Florida Gulf Coast University, Fort Myers, FL, USA
Email: tbeatty@fgcu.edu, gaby.vonlinden@gmail.com

How to cite this paper: Beatty, T. and von Linden, G. (2020) On Conditional Probabilities of Factoring Quadratics. *Advances in Pure Mathematics*, **10**, 114-124.
https://doi.org/10.4236/apm.2020.103008

Received: January 30, 2020
Accepted: March 16, 2020
Published: March 19, 2020

Abstract

Factoring quadratics over $\mathbb{Z}$ is a staple of introductory algebra and textbooks tend to create the impression that doable factorizations are fairly common. To the contrary, if coefficients of a general quadratic are selected randomly without restriction, the probability that a factorization exists is zero. We achieve a specific quantification of the probability of factoring quadratics by taking a new approach that considers the absolute size of coefficients to be a parameter n. This restriction allows us to make relative likelihood estimates based on finite sample spaces. Our probability estimates are then conditioned on the size parameter n and the behavior of the conditional estimates may be studied as the parameter is varied. Specifically, we enumerate how many formal factored expressions could possibly correspond to a quadratic for a given size parameter. The conditional probability of factorization as a function of n is just the ratio of this enumeration to the total number of possible quadratics consistent with n. This approach is patterned after the well-known case where factorizations are carried out over a finite field. We review the finite field method as background for our method of dealing with $\mathbb{Z}[x]$. The monic case is developed independently of the general case because it is simpler and the resulting probability estimating formula is more accurate. We conclude with a comparison of our theoretical probability estimates with exact data generated by a computer search for factorable quadratics corresponding to various parameter values.

Keywords

Factorization, Polynomial, Quadratic, Integers, Rational Numbers, Monic, Modular Arithmetic, Conditional Probability

1. Introduction

This paper presents the preliminary results of a broader program to estimate the

probabilities of factoring more general polynomials over $\mathbb{Z}$. We anticipate that subsequent research will develop along the lines suggested by the quadratic case investigated here, specifically by using the method of parameterizing the maximum absolute value of coefficients and correlating the conditional probabilities of factorization with the size of the parameter.

The probability that a given general quadratic $\alpha x^2+\beta x+\gamma \in \mathbb{Z}[x]$ can be factored depends heavily on the commensurability of the coefficients [1] [2] [3]. Loosely speaking, if the coefficients are all about the same size in absolute value, and that size is small, the existence of a factorization is relatively more likely than otherwise. Our intention is to quantify this phenomenon. Dealing with the infinite number of choices available for coefficients is a problem. We sidestep this obstacle by adapting the method used to determine the probability of factorization of quadratics over finite fields. Briefly, we establish a cutoff, or size parameter n, for the absolute value of any coefficients appearing in any of the quadratics we wish to study. This makes the number of quadratics under consideration finite as well as the number of formal factored expressions that could possibly yield such a quadratic. Then the classical probability is just the ratio of the number of admissible factored expressions to the total number of quadratics which conform to the cutoff. This probability $P(n)$ is, of course, a conditional probability given that the coefficients do not exceed n in absolute value. So the infinite character of the problem is initially made finitary where calculations can be done and then can be recovered by allowing n to approach infinity.

We consider three cases, the first of which, factoring quadratics over finite fields, is well-known [4]. For factoring quadratics over $\mathbb{Z}$, we split the discussion into two parts: 1) the monic case, and 2) the general case. For simplicity we consider quadratics in $\mathbb{Z}[x]$ that have non-negative roots.

Figure 1 shows factorization probabilities calculated by the computer search. Currently we have no formula that estimates the case $ax^2+bx+c \in \mathbb{Z}[x]$ with $\alpha \neq 0$ other than curve fitting. The trend in the graph in **Figure 1** is borne out by the following proposition.

Proposition 0

If $a,b,c \in \mathbb{Z}$ are selected randomly without restriction, then the probability of factoring ax^2+bx+c over $\mathbb{Z}$ is zero.

Proof. Suppose we are given ax^2+bx+c with $a,b,c \in \mathbb{Z}$ selected at random. This quadratic factors over $\mathbb{Q}$, hence $\mathbb{Z}$ by Gauss' Lemma, if the discriminant $\Delta = b^2-4ac$ is a perfect square. We ask what is the probability that Δ is a perfect square if a and b have been selected and c is provisionally allowed to range over $[-n,n]$ for some $n \in \mathbb{N}$. Then there are $2n+1$ possible values of Δ spread over an interval of length $|8an|$. The largest possible number of perfect squares in such an interval would occur when none of the interval intersected the open left half line and where the arithmetic density of squares was the greatest. This would occur if the interval were exactly $[0,|8an|]$. The number of squares in this interval does not exceed $\sqrt{|8an|}$. The classical probability that

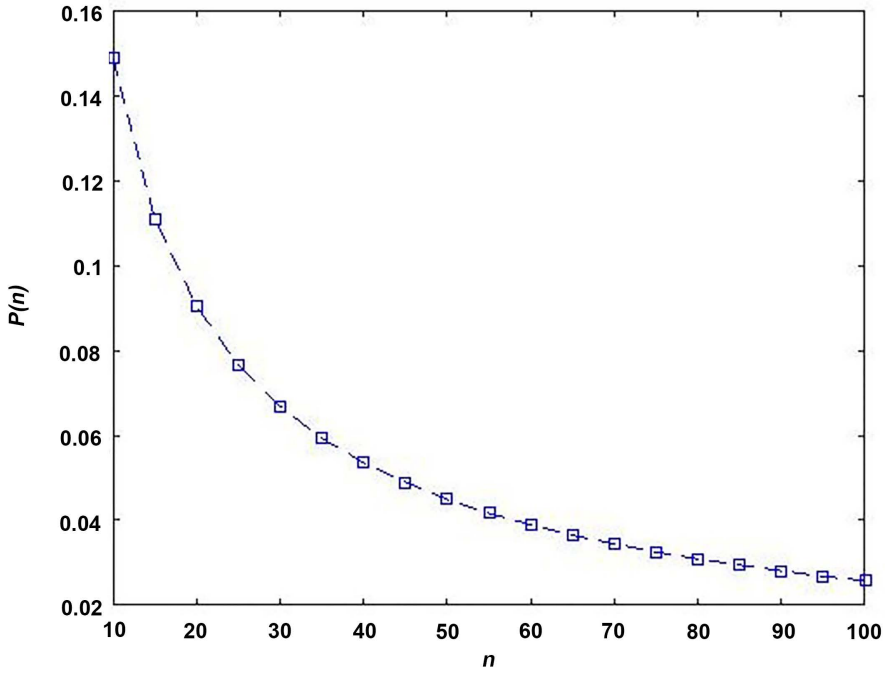

Figure 1. $P(n)$ is the probability of factoring ax^2+bx+c with $|a|,|b|,|c|\le n$.

one of these squares coincides with a value of Δ is therefore no more than $\frac{\sqrt{|8an|}}{2n+1}<\sqrt{2}|a|\frac{1}{\sqrt{n}}$. As the provisional restriction that $c\in[-n,n]$ is relaxed by allowing $n\to\infty$, we see $\sqrt{2}|a|\frac{1}{\sqrt{n}}\to 0$. It follows that the probability that Δ is a perfect square, and therefore ax^2+bx+c is factorable over $\mathbb{Z}$, is zero in the limit, which corresponds to no restrictions at all on *c*. Since this is true for any triple (a,b,c), the proposition is established.

We wish to have a more granular understanding of the way in which factorability depends on commensurability of coefficients. Our approach to this question is motivated by solving the factorization probability problem in the context of finite fields, which we review below.

2. Factoring Over $GF\left(p^n\right)$

Suppose we are given a random monic quadratic over the finite field $GF(p)$. What is the likelihood that it factors [5]?

2.1. Proposition 1

If $f(x)=x^2+\alpha x+\beta$ and $\alpha,\beta\in GF(p)$, then the probability P_p of factoring $f(x)$ over $GF(p)$ is $\frac{1}{2}+\frac{1}{2p}$.

Proof. There are p^2 possible pairs of coefficients, hence p^2 distinct quadratics. On the other hand, if *f* factors as $(x-r_1)(x-r_2)$, then there are *p* facto-

rizations where $r_1 = r_2$ and $\binom{p}{2}$ distinct factorizations where $r_1 \neq r_2$, allowing for interchanging the factors. P_p is the ratio of possible factorizations to possible quadratics, so $P_p = \dfrac{p + \dfrac{p(p-1)}{2}}{p^2} = \dfrac{1}{2} + \dfrac{1}{2p}$.

Now let us generalize to an arbitrary quadratic.

2.2. Corollary 1-1

If $f(x) = \lambda x^2 + \alpha x + \beta$ and $\lambda(\neq 0), \alpha, \beta \in GF(p)$, then the probability P_p of factoring $f(x)$ over $GF(p)$ is $\dfrac{1}{2} + \dfrac{1}{2p}$.

Proof. Evidently there are $(p-1)p^2$ possible triples of coefficients, but we can mimic the above proof by rewriting $f(x) = \lambda\left(x^2 + \lambda^{-1}\alpha x + \lambda^{-1}\beta\right) = \lambda\left(x^2 + \alpha' x + \beta'\right)$. Now the possible factorizations would look like $\lambda(x - r_1)(x - r_2)$. Once again, the probability of factoring a random quadratic, not necessarily monic, would be

$$P_p = \frac{(p-1)\left(\dfrac{p^2 + p}{2}\right)}{(p-1)p^2} = \frac{1}{2} + \frac{1}{2p}.$$

2.3. Corollary 1-2

If $f(x) = \lambda x^2 + \alpha x + \beta$ and $\lambda(\neq 0), \alpha, \beta \in GF\left(p^n\right)$, then the probability P_{p^n} of factoring $f(x)$ over $GF\left(p^n\right)$ is $\dfrac{1}{2} + \dfrac{1}{2p^n}$.

Proof. Following the proof for the preceding, we have $\left(p^n - 1\right)p^{2n}$ possible triples of coefficients, and $\left(p^n - 1\right)\left[p^n + \dfrac{p^n\left(p^n - 1\right)}{2}\right] = \left(p^n - 1\right)\left(\dfrac{p^{2n} + p^n}{2}\right)$ possible factorizations. Hence $P_{p^n} = \dfrac{\left(p^n - 1\right)\left(\dfrac{p^{2n} + p^n}{2}\right)}{\left(p^n - 1\right)p^{2n}} = \dfrac{1}{2} + \dfrac{1}{2p^n}$.

2.4. Corollary 1-3

The limit as $p \to \infty$ of the probability P_{p^n} of factoring a quadratic over $GF\left(p^n\right)$ is $\dfrac{1}{2}$.

Proof. This follows immediately from the fact that the limit as $p \to \infty$ of the expression in Corollary 1-2 is independent of *n*.

The situation we see embodied in Proposition 1 and its corollaries is somewhat unexpected (at least the first time it is considered) and in any case very different from factoring over $\mathbb{Z}$. It is a mildly entertaining exercise in experimen-

tal mathematics to choose a large prime p and ask a computer algebra system to factor several random quadratics with large coefficients modulo p. Superficially, since p is large, it seems that the chances for a factorization would be about the same as if the factorization were to be done over $\mathbb{Z}$, namely poor. But in the long run, about half of the test examples result in factorizations. Although it would defeat the whole purpose of our discussion of the enumeration method for factorization probabilities in the finite field case, a short proof of Proposition 1 can be gotten directly from number theory. The quadratic equation $x^2+\alpha x+\beta=0$ can be simplified by completing the square, leaving a constant on the right hand side. Among the $p-1$ non-zero least residues modulo p, exactly $\frac{p-1}{2}$ are quadratic residues. The constant needs to be a quadratic residue so that roots can be found to construct a factorization. Zero is always a quadratic residue, so there are $\frac{p-1}{2}+1=\frac{p+1}{2}$ quadratic residues in all. On the other hand, there are p least residues modulo p, hence the probability that a randomly chosen least residue is in fact a quadratic residue is $\frac{p+1}{2p}=\frac{1}{2}+\frac{1}{2p}$ as above.

3. Factoring Over $\mathbb{Z}$-Monic Case

We would like to adapt the same argument for factoring over $\mathbb{Z}$ as we used for finite fields, namely counting up the number of possible distinct factorizations and dividing by the number of distinct quadratic expressions to get a probability of being able to factor. Since $\mathbb{Z}$ is infinite this plan is immediately hobbled [6]. Consider the polynomial x^2+ax+1, where α is random. There are only two hopes for factorization: $\alpha=\pm 2$. Yet there are infinitely many choices for α, so the probability of factorization is evidently zero. To salvage any insight from this state of affairs, we have to content ourselves with a conditional probability based on limiting how "random" a random quadratic can be. A reasonable choice is to insist that its coefficients be commensurable with its possible zeroes. Clearly $x^2+37x+1$ does not have this property, which is informal at the moment, but which will soon be made precise. On the other hand, both x^2+x+1 and x^2+2x+1 seem to have it. In one case there is a factorization, in the other not. This conditional probability will be based on a relative likelihood calculation where the commensurability condition is quantified by a parameter. As the parameter increases, the commensurability decreases, and the probability of factorization will tend to zero. The point of our approach is to model the detailed behavior of this process. To introduce the specifics in a simple context, we first consider monic quadratics with the restriction that they have non-negative roots.

Let us define a "window of feasibility" $W(n)$ in the plane as the rectangle of grid points $[0,n+1]\times[0,n]\subset\mathbb{Z}^2$. Suppose we are given a random $p(x)\in\mathbb{Z}[x]$ of the form $x^2-\alpha x+\beta$ with $\alpha,\beta\geq 0$ and $\beta\leq n$. If $p(x)$ factors as

$(x-r_1)(x-r_2)$ both roots are nonnegative and $\alpha = r_1 + r_2$ and $\beta = r_1 r_2$. If $\beta > 0$ these conditions imply that $\alpha \le n+1$, and in the event $\beta = 0$ we impose this condition arbitrarily to ensure that all $p(x)$ satisfying these conditions can be mapped in the obvious way to $(\alpha, \beta) \in W(n)$. At the moment we have every point in $W(n)$ as the image of some $p(x)$ with $\alpha, \beta \ge 0$. Clearly this is a bijective mapping. We call $W(n)$ a window of feasibility since any $p(x)$ with $0 < \beta \le n$ and $\alpha > n+1$ is necessarily impossible to factor. The motivation for constructing the window is to exclude those cases which overwhelm ordinary probability calculations. A quadratic inside the window may or may not be factorable, but if not, the reason will not be due to incommensurability of coefficients. Figure 2 shows this situation.

Note that a grid point of the form $(\alpha, 0)$ corresponds to the quadratic $x^2 - \alpha x = x(x-\alpha)$, so factorization is always possible. A grid point of the form $(0, \beta)$, provided $\beta > 0$ corresponds to the quadratic $x^2 + \beta$, which never factors.

Now denote by $F(n)$ the grid points in $W(n)$ corresponding to factorable polynomials. A factorable quadratic mapped to (α, β) must have $\alpha = r_1 + r_2$ and $\beta = r_1 r_2$ for some r_1, r_2. Let us then plot pairs of roots on the $W(n)$ grid and define $\phi(r_1, r_2) = (\alpha, \beta)$ as the mapping that associates a root pair to the quadratic which factors with those roots. We will see shortly that there are substantial limitations on which points in $W(n)$ can be root pairs. In other words,

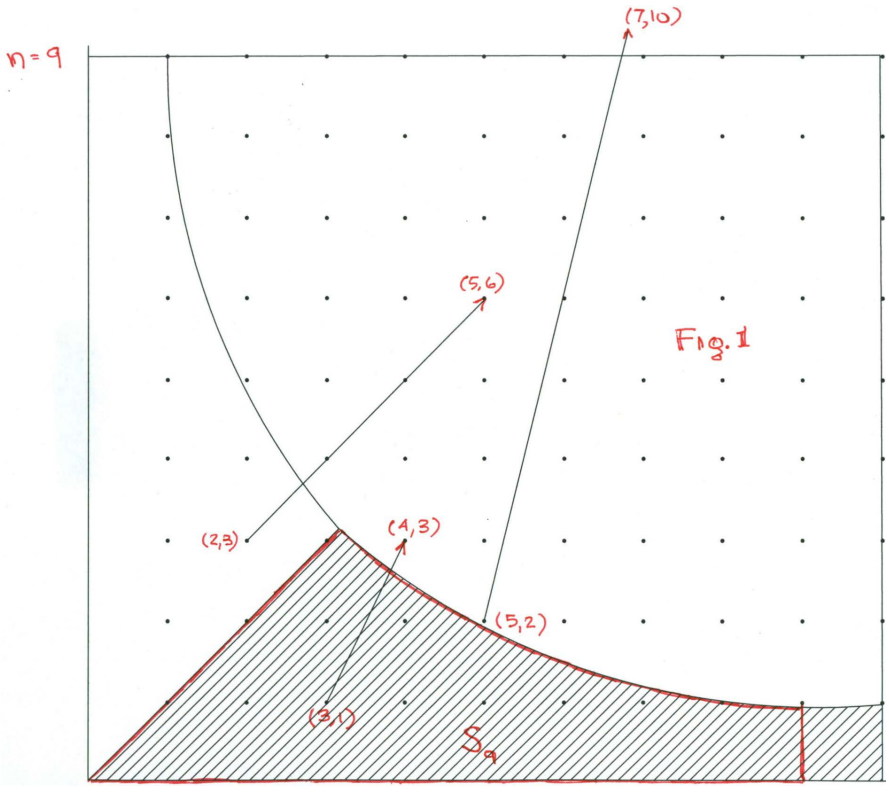

Figure 2. Window of Feasibility for $n = 9$. Grid points in shaded area are possible root pairs.

the domain of ϕ will be relatively small, so surjectivity will clearly be out of the question. We would like ϕ to be injective, and since $\phi(r_1,r_2)=\phi(r_2,r_1)$ we impose the condition $r_2 \le r_1$ without loss of generality. Graphically, this amounts to eliminating all root pairs strictly above the line $r_2 = r_1$. Now $W(n)\setminus\{(r_1,r_2): r_2 \le r_1\}$ is still not $F(n)$ since there is another important condition on the root pairs, namely $r_1 r_2 \le n$. The only admissible root pair grid points whenever $r_2 > 0$ are also below the hyperbola $r_2 = \frac{n}{r_1}$. This is also true trivially if $r_2 = 0$ so the hyperbola is an upper bound for all root pairs corresponding to factorable quadratics. Now we estimate the number of points in $F(n)$ by calculating the area inside the region of the plane defined by the line $r_2 = 0$, the line $r_2 = r_1$, and the hyperbola $r_2 = \frac{n}{r_1}$. The area of this region is $A = \int_0^{\sqrt{n}} (r_1)\mathrm{d}r_1 + \int_{\sqrt{n}}^{n+1} \left(\frac{n}{r_1}\right)\mathrm{d}r_1 = \frac{n\ln n + 3n}{2}$. We estimate the number of grid points in $F(n)$ by assuming one grid point per unit of area. This estimate is asymptotically exact. Now $W(n)$ has $(n+1)(n+2)$ total grid points. Finally, our conditional probability estimate is $\frac{n\ln n + 3n}{2(n+1)(n+2)}$. We have proved:

3.1. Proposition 2

Given a random quadratic in $\mathbb{Z}[x]$ of the form $x^2 - \alpha x + \beta$, where $\alpha, \beta \ge 0$, the approximate probability $P(n)$ of factorization, subject to the conditions $\alpha \le n+1$ and $\beta \le n$ for fixed $n \in \mathbb{N}$, is given by $P(n) = \frac{n\ln n + 3n}{2(n+1)(n+2)}$.

3.2. Corollary 2-1

With the notation of Proposition 2, $P(n)$ is asymptotically $\frac{\ln n}{2n}$.

Proof. Divide numerator and denominator of $\frac{n\ln n + 3n}{2(n+1)(n+2)}$ by n to get $\frac{\ln n + 3}{2\left(n+3+\frac{2}{n}\right)}$. Note that for large n we have $\ln n \gg 3$ and $n \gg 3 + \frac{2}{n}$. Hence $n \gg 1$ implies $P(n) \approx \frac{\ln n}{2n}$.

Unsurprisingly, letting $n \to \infty$ corresponds to α and β being chosen completely arbitrarily and we confirm that $\lim_{n\to\infty} P(n) = 0$ by L'Hôpital's rule. The rate at which the likelihood of factorization declines is $P'(n) \approx -\frac{\ln n}{2n^2}$ for large n, as would be expected.

For perspective, if $n = 440$, the corresponding likelihood of factorability $P(440) \approx 1\%$.

4. Factoring over $\mathbb{Z}$-General Case

Consider the lattice cube $L(n)=[0,n]^3 \subset \mathbb{Z}^3$ as the three-dimensional analog of the preceding window of feasibility. The general quadratic [7] $p(x)=\alpha x^2-\beta x+\gamma \in \mathbb{Z}[x]$ with $\alpha>0, \beta, \gamma \geq 0$ can be associated injectively with the point $(\alpha,\beta,\gamma) \in L(n)$ provided $\max\{\alpha,\beta,\gamma\} \leq n$. Since $\alpha \neq 0$, there are $(n-1)n^2$ grid points in $L(n)$ which represent distinct quadratics of this type. We would like to estimate the number of these which are factorable so that we can calculate the conditional probability $P(n)$ of factorability in the manner of the finite field and monic cases above. Suppose $p(x)$ does factor in $\mathbb{Z}$ as $(ax-b)(cx-d)$, with $a,c>0$ and $b,d \geq 0$. Note that the greatest common divisor of α,β and γ does not appear as a separate factor but is considered to be bundled into the term $(ax-b)$. Then $\alpha=ac$, $\beta=bc+ad$, and $\gamma=bd$. Since the maximum α is *n*, it follows that admissible pairs (a,c) would satisfy $c \leq \frac{n}{a}$. As in the monic case, we embed $\mathbb{Z}^2$ in $\mathbb{R}^2$, calculate the appropriate area under the given hyperbola, and then assume one grid point (admissible pair) per unit of area with the understanding that this is asymptotically correct. The area in the first quadrant of the *ac* plane is $\int_1^n \frac{n(\delta a)}{a}-n=n\ln n-n=n(\ln n-1)$. Since the maximum γ is *n*, but either *b* or *d* (or both) could be zero, the appropriate area in the first quadrant of the *bd* plane would be $\int_1^n \frac{n(\delta b)}{b}+n=n\ln n+n=n(\ln n+1)$. Evidently there are $[n(\ln n-1)]\cdot[n(\ln n+1)]=n^2\left((\ln n)^2-1\right)=F(n)$ expressions of the form $(ax-b)(cx-d)$ which could factor the quadratic $\alpha x^2-\beta x+\gamma$ subject to the constraints imposed on those coefficients. Certainly not every point in $L(n)$ corresponds to a factorable quadratic, but we can be assured that any points which are associated with a factorable quadratic have a factorization counted by $F(n)$. Since the factor pairs commute, we divide $F(n)$ by two and it follows that the conditional probability of factorization is estimated by

$$P(n)=\frac{F(n)}{2n^3}=\frac{n^2\left((\ln n)^2-1\right)}{2n^3}=\frac{(\ln n)^2-1}{2n}.$$

We have proved:

4.1. Proposition 3

Given a random quadratic in $\mathbb{Z}[x]$ of the form $\alpha x^2-\beta x+\gamma$, where $\alpha>0, \beta, \gamma \geq 0$ and $\max\{\alpha,\beta,\gamma\} \leq n$, an estimate for the probability $P(n)$ of factorization is given by $P(n)=\frac{(\ln n)^2-1}{2n}$.

4.2. Corollary 3-1

With the notation of Proposition 3, $P(n)$ is asymptotically $\frac{(\ln n)^2}{n}$.

Table 1. Actual vs. Calculated-Monic Case.

n	Calc	Actual
10	0.200	0.197
20	0.128	0.121
30	0.097	0.089
40	0.078	0.070
50	0.065	0.058
1000	0.005	*
∞	0	*

n = coefficient bound; Calc = calculated $P(n)$; Actual = actual $P(n)$ by computer check.

Table 2. Actual vs. Calculated-General Case.

n	Calc	Actual
10	0.215	0.149
20	0.199	0.190
30	0.176	0.067
40	0.158	0.054
50	0.143	0.045
1000	0.023	*
∞	0	*

n = coefficient bound; Calc = calculated $P(n)$; Actual = actual $P(n)$ by computer check.

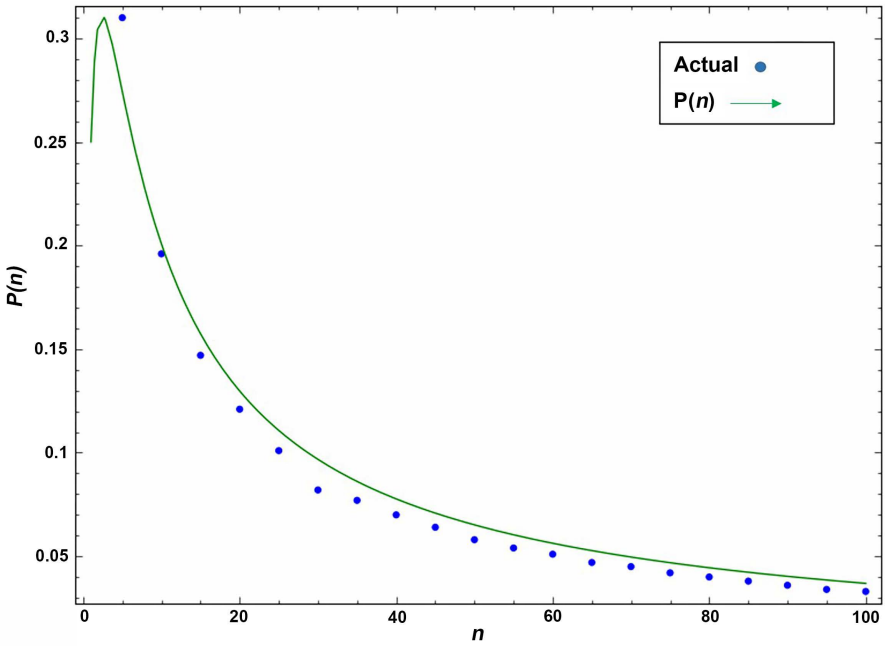

Figure 3. Probability of factoring $P(n)$ vs. absolute coefficient bound n actual vs. calculated.

Proof. For $n \gg e$, $\frac{(\ln n)^2 - 1}{2n} \approx \frac{(\ln n)^2}{2n}$.

As expected, $\lim_{n\to\infty} P(n) = 0$ again by L'Hôpital's rule.

5. Summary & Conclusions

We have described two methods for estimating the conditional probability that a random quadratic in $\mathbb{Z}[x]$ with non-negative bounded coefficients can be factored as a function of the bounding parameter. The simpler case is based on mapping monic quadratics injectively to a two-dimensional lattice in $\mathbb{Z}^2$ and enumerating the formal expressions that could possibly represent factorizations of them. The ratio of the number of admissible formal factorizations to the total number of points in the lattice defines the conditional probability of factorization for the given coefficient bound. The more complicated case involves mapping general quadratics to a three-dimensional lattice in $\mathbb{Z}^3$ and reprising the calculation for the two-dimensional case. Both methods have their provenance in the problem of calculating the likelihood that a quadratic over a finite field may be factored. In the case of finite fields, only a finite number of polynomials are possible and only a finite number of factorizations can be written, making the calculation a simple ratio. This fails, of course, for $\mathbb{Z}$, but the point of our method is to resurrect the utility of finiteness by imposing a size limitation on coefficients [8].

Table 1 presents a comparison of values from the monic formula for conditional probability given by Proposition 2 with a computer generated census of factorable monic quadratics. There is reasonably close agreement, even for small n. The computer algorithm works by simply checking to see if the quadratic formula yields a rational number. Recall if a polynomial in $\mathbb{Z}[x]$ factors over $\mathbb{Q}$, then it factors over $\mathbb{Z}$.

Table 2 recaps a similar comparison for the general quadratics in Proposition 3. For the sake of simplicity we have ignored double counting certain factored expressions arising from symmetries (for example if $a = c$). This overstates the calculated probability of factorization, especially for small n, so we may regard $P(n)$ in this case as an upper bound for the true probability. In any case, our formula establishes $P(\infty) = 0$.

Below in Figure 3 a graph of the calculated $P(n)$ versus n is shown as the continuous curve. The separate data points correspond to Table 1. The expected feature that $\lim_{n\to\infty} P(n) = 0$ is also evident.

To close on a philosophical note, although factorization of random quadratics over $\mathbb{Z}$ has been shown to be a progressively futile exercise, practicing pattern recognition with doable examples for small n is a worthwhile exercise that no doubt pays dividends elsewhere in mathematics.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Burton, D. (2005) Elementary Number Theory. McGraw-Hill Higher Education, Inc., New York, NY.

[2] Dummit, D.S. and Foote, R.M. (2014) Abstract Algebra. 3rd Edition, John Wiley and Sons, Inc., Hoboken, NJ.

[3] Gallian, J. (2010) Contemporary Abstract Algebra. 7th Edition, Cengage Learning.

[4] Morandi, P. (1996) Field and Galois Theory. Springer, Berlin. https://doi.org/10.1007/978-1-4612-4040-2

[5] Lenstra, A., Lenstra, H. and Lovász, L. (1982) Factoring Polynomials with Rational Coefficients. *Mathematische Annalen*, **261**, 515-534. https://doi.org/10.1007/BF01457454

[6] Miller, V.S. (1992) Factoring Polynomials via Relation-Finding. In: Dolev, D., Galil, Z. and Rodeh, M., Eds., *Theory of Computing and Systems ISTCS* 1992, Lecture Notes in Computer Science, Vol. 601, Springer, Berlin, Heidelberg.

[7] Hart, W., Hoeij, M. and Novocin, A. (2011) Practical Polynomial Factoring in Polynomial Time. *Proceedings of the International Symposium on Symbolic and Algebraic Computation* (*ISSAC*), San Jose, CA, 163-170. https://doi.org/10.1145/1993886.1993914

[8] Ostrowski, A.M. (1975) On Multiplication and Factorization of Polynomials I, *Aequationes Mathematicae*, **13**, 201-228. https://doi.org/10.1007/BF01836524