

Sums Talk: Unique Factorization and Diophantine Approximation

Vijay Sookdeo

April 12, 2007

The following is a talk I gave to the Society of Undergraduate Math Students during the fall semester of 2004.

1 Introduction

A Diophantine equation is an equation where we look for either integer or rational solutions. For example, we call $x^2 - 5y^2 = 1$ a Diophantine equation when we are only interested in integer solutions. Another example is the famous equation of Fermat's 'last theorem', $x^n + y^n = z^n$. We will be looking at the two equations $x^2 + 2 = y^3$ and $x^2 + 19 = y^3$ and how unique factorization plays an important role in solving them.

For positive integers a and b we have the following notation and definition:

- $a|b$ (reads a divides b) means $an = b$ for some integer n .
- p is a *prime number* means if $a|p$ then $a = 1$ or $a = p$
- $\gcd(a, b)$ denotes the greatest common divisor of a and b .

2 Prime Number Property

A prime number p has the 'remarkable' property that if it divides the product of two numbers, then it must divide one of them.

Theorem 1. (Prime Number Property) *For integers a and b , if $p|ab$ then $p|a$ or $p|b$.*

This property is remarkable because it is equivalent to unique factorization of integers. Essentially, we can obtain unique factorization from the prime number property, and vice versa.

Theorem 2. *PNP is equivalent to unique factorization.*

Proof. (prime number property \Rightarrow unique factorization) Clearly $n = 2$ factors uniquely. Assume for all $n \leq k$ we have unique factorization. Suppose $k + 1 = p_1 \cdot p_2 \cdots p_m = q_1 \cdot q_2 \cdots q_r$ are two factorizations of $k + 1$. Then $p_1 | q_1 \cdot q_2 \cdots q_r$ and by the PNP we have $p_1 | q_1$, so $p_1 = q_1$ by definition since $p_1 \neq 1$. Therefore $p_2 \cdot p_3 \cdots p_m = q_2 \cdot q_3 \cdots q_r$ is a factorization of a number $\leq k$ and by our induction hypothesis, this factorization is unique. So $m = r$ and $p_i = q_i$.

(unique factorization \Rightarrow prime number property) If $p | ab$ then p occurs in the factorization of ab . By unique factorization, ab contains only those prime factors which are also prime factors of a and b . Therefore, p is a prime factor of a or b . \square

Before proceeding to the proof of the prime number property, here are two applications. The first is a generalization of the theorem that $\sqrt{2}$ is irrational and the second will play a key role in solving diophantine equations.

Corollary 1. *If m is square-free (i.e. m is not divisible by p^2 for any prime p) then \sqrt{m} is irrational.*

Proof. Supposing the \sqrt{m} is rational, we can write $\sqrt{m} = \frac{a}{b}$ with $\gcd(a, b) = 1$. Rewrite this as $mb^2 = a^2$ and take any prime $p | a$. Then $p^2 | mb^2 = a^2$. Since $\gcd(a, b) = 1$, we have $p \nmid b$ and so the prime number theorem tells us $p | m$. Therefore $p^2 | m$ and this contradicts the fact that m is squarefree. So m cannot be rational. \square

Corollary 2. *If $\gcd(a, b) = 1$ and ab is a square then a is a square and b is a square.*

Proof. Suppose $\gcd(a, b) = 1$ and $ab = n^2$. If $p | a$ then $p | n^2$, and by the prime number property $p | n$. Therefore $p^2 | n^2$ and this implies $p^2 | ab$. Since $\gcd(a, b) = 1$ we have $p^2 \nmid b$ and so $p^2 | a$. Hence every prime factor of a is a square, so a is a square. Similarly for b . \square

Notice that in our proof, there is nothing special about ab being a square. A similar result holds if ab is a cube or fourth power, etc. Interestingly, the proof of the prime number property relies on the division/Euclidean algorithm: For integers a and $b > 0$, there exists integers r and q such that $a = bq + r$ with $0 \leq |r| < b$. Rewriting the statement as $\frac{a}{b} = q + \frac{r}{b}$ we see that this is dividing a by b to obtain a quotient q and remainder r . A geometric way to convince yourself of this fact is to note that multiples of b divide the line into intervals. When dividing a by b , we simply locate the interval containing a . The first multiple less than a tells us the quotient, and the remainder is what I add to this multiple to get a . Notice an important feature of the remainder is that it is less than the divisor b , i.e. less than the size of the interval.

(put pic here)

We will use the Euclidean algorithm to prove a lemma from which the prime number property follows:

Lemma 1. *If $\gcd(a, b) = d$ then there exists integers x and y such that $ax + by = d$*

Proof. Set $S = \{ax + by | x, y \text{ are integers}\}$. It's easy to see S is closed under addition and integer multiplication. Such a set is called an *ideal* of $\mathbb{Z} = \{\text{set of integers}\}$. Take the smallest positive element of S , say $d = ax + by$. Now, every divisor of a and b must also divide d . It suffices to show that $d|a$ and $d|b$. By Euclidean algorithm, $a = dq + r$ with $0 \leq |r| < d$. Note that $a \in S$ since $a = a \cdot 1 + b \cdot 0$ and $dq \in S$. So $|r| = |a - dq| \in S$ and since d is the smallest positive element of S , we must have $r = 0$. Therefore $d|a$ and similarly $d|b$. \square

We are now prepared to give a proof of the prime number property.

Proof. (Prime Number Property) Suppose $p|ab$, then $\gcd(p, a) = p$ or $\gcd(p, a) = 1$. If $\gcd(p, a) = p$ then $p|a$ and we are done. If $\gcd(p, a) = 1$ then the lemma gives $px + ay = 1$. Multiplying by b we have $pbx + aby = b$. Since p divides both terms on the left-hand side of the equation, we must have $p|b$. \square

3 Diophantine Equation

Why is the prime number property important in solving Diophantine equations. Here's a claim by Fermat(1657): 27 is the only cube exceeding a square by 2. This can be expressed as saying that $y = 3$ is the only solution to

$$y^3 = x^2 + 2$$

Euler found a very clever solution to this problem.

Euler's Proof(1770):

Since we have the factorization $x^2 + 2 = (x - \sqrt{-2})(x + \sqrt{-2})$, Euler's brilliant idea was to look at expression of the form $\alpha = a + b\sqrt{-2}$, where a and b are integers. Today we write $\mathbb{Z}[\sqrt{-2}]$ to denote the set of such expressions. Euler noticed that many of the properties of integers are shared by $\mathbb{Z}[\sqrt{-2}]$. For example, $\mathbb{Z}[\sqrt{-2}]$ is closed under addition and multiplication:

$$\begin{aligned} \alpha + \beta &= (a + b)\sqrt{-2} + (c + d\sqrt{-2}) = (a + c) + (b + d)\sqrt{-2} \\ \alpha\beta &= (a + b\sqrt{-2})(c + d\sqrt{-2}) = (ac - 2bd) + (ad + bc)\sqrt{-2} \end{aligned}$$

The number $0 = 0 + 0 \cdot \sqrt{-2}$ plays the role of an additive identity and $1 = 1 + 0 \cdot \sqrt{-2}$ plays the role of a multiplicative identity. For $\alpha, \beta \in \mathbb{Z}[\sqrt{-2}]$, we can say $\alpha|\beta$ if there exist a γ such that $\alpha\gamma = \beta$. Similarly, we can say π is a prime if $\alpha|\pi$ implies $\alpha = 1$ or $\alpha = \pi$. Seeing such great similarities, Euler assumes corollary 2: For $\alpha, \beta \in \mathbb{Z}[\sqrt{-2}]$ if $\gcd(\alpha, \beta) = 1$ and $\alpha\beta$ is a square or cube, etc then α and β are squares or cubes, etc.

He then explicitly shows $\gcd(x - \sqrt{-2}, x + \sqrt{-2}) = 1$. And since the product of $x - \sqrt{-2}$ and $x + \sqrt{-2}$ is a cube, we must have:

$$\begin{aligned} x + \sqrt{-2} &= (a + b\sqrt{-2})^3 \\ &= (a^3 - 6ab^2) + (3a^2b - 2b^3)\sqrt{-2} \end{aligned}$$

Therefore,

$$x = a^3 - 6ab^2 \text{ and } 1 = (3a^2b - 2b^3) = b(3a^2 - 2b^2)$$

The second equation above implies $b = \pm 1$, and so $a = \pm 1$ which gives $x = \pm 5$. Using these values for x , we see that the only solution occurs when $y^3 = 5^2 + 2$, or $y = 27$.

Let us use this method to solve another diophantine equation: $y^3 = x^2 + 19$
Factoring in $\mathbb{Z}[\sqrt{-19}]$ to get

$$y^3 = (x - \sqrt{-19})(x + \sqrt{-19})$$

We can argue that $\gcd(x - \sqrt{-19}, x + \sqrt{-19}) = 1$, and as before we would obtain:

$$\begin{aligned} x + \sqrt{-19} &= (a + b\sqrt{-19})^3 \\ &= (a^3 - 57ab^2) + (3a^2b - 19b^3)\sqrt{-19} \end{aligned}$$

Solving for x ,

$$x = a^3 - 57ab^2 \text{ and } 1 = (3a^2b - 19b^3) = b(3a^2 - 19b^2)$$

So we get $b = \pm 1 \implies 3a^2 - 19 = \pm 1 \implies 3a^2 = 20$ or $3a^2 = 18$. This gives no integer solutions for x , and we therefore conclude that there are no integer solutions to the equation $y^3 = x^2 + 19$. However, we can easily check that $x = \pm 18$ and $y = 7$ are solutions. What went wrong in $\mathbb{Z}[\sqrt{-19}]$ that didn't go wrong in $\mathbb{Z}[\sqrt{-2}]$?

It turns out we have unique factorization in $\mathbb{Z}[\sqrt{-2}]$ which will allow us to prove the analogy to corollary 2. However, unique factorization fails in $\mathbb{Z}[\sqrt{-19}]$. We can see this by observing $20 = (1 - \sqrt{-19})(1 + \sqrt{-19}) = 2^2 \cdot 5$ where it can be shown that $2, 5, 1 - \sqrt{-19}$, and $1 + \sqrt{-19}$ are *primes* in $\mathbb{Z}[\sqrt{-19}]$. Therefore, we cannot prove an analogous corollary 2 in $\mathbb{Z}[\sqrt{-19}]$, and so our method of solving was $y^3 = x^2 + 19$ doomed from the start.

4 $\mathbb{Z}[\sqrt{-2}]$ is a UFD

How do we show that $\mathbb{Z}[\sqrt{-2}]$ is a unique factorization domain. We may use the integer as a guide. If we can obtain a Euclidean algorithm for $\mathbb{Z}[\sqrt{-2}]$

then we can establish a prime number property and this is equivalent to unique factorization. The question therefore become, is it possible to have a Euclidean algorithm for $\mathbb{Z}[\sqrt{-2}]$? Notice that the important feature of the Euclidean algorithm for the integers is the *size* of the remainder - we require the remainder to have size less than the divisor. To start, we need to define a way to measure the size of the elements in $\mathbb{Z}[\sqrt{-2}]$.

We can write $\alpha = a + b\sqrt{-2} = a + bi\sqrt{2}$ and thus we can view $\mathbb{Z}[\sqrt{-2}]$ as a grid in the complex plane. We can then measure the size of elements of $\mathbb{Z}[\sqrt{-2}]$ as we would any complex number. We take distance $|\alpha|$ to be the distance from the origin.

(put pic here)

The question now becomes: Do we have for $\alpha, \beta \in \mathbb{Z}[\sqrt{-2}]$, the existence of ρ and μ such that $\alpha = \beta\mu + \rho$ with $0 \leq |\rho| < |\beta|$? The best way to obtain an answer is to think geometrically. The multiples of any β in $\mathbb{Z}[\sqrt{-2}]$ are at the corners of a lattice of rectangles in the complex plane (i.e. multiples of β tessellate the plane with rectangles where a multiple is at each corner of a rectangle). For example, the four multiples $0, \beta, \sqrt{-2}\beta$, and $(1 + \sqrt{-2}\beta)$ are on the corners of the following rectangle:

(put pic here)

To divide α by β , we look for the rectangle which contains α . The quotient μ would be the corner nearest to α (i.e. the multiple of β closest to α) and the size of the remainder would be the distance from the μ to α .

(put pic here)

Notice the maximum distance from the corners is $\frac{1}{2}\sqrt{2|\beta|^2 + |\beta|^2} < \sqrt{\frac{3}{4}}|\beta| < |\beta|$. Therefore the size of the remainder cannot exceed the size of the divisor, and hence we have a Euclidean algorithm. So we can prove the prime divisor property and obtain unique factorization for $\mathbb{Z}[\sqrt{-2}]$.

This same sort of geometrical reasoning shows that $\mathbb{Z}[\sqrt{-19}]$ cannot have a Euclidean algorithm. The rectangles which are formed by multiples of β are too "stretched out" in this case.

(put pic here)

We see that the maximum distance from the corners is $\frac{1}{2}\sqrt{19|\beta|^2 + |\beta|^2} = \sqrt{5}|\beta| > |\beta|$. So the size of the remainder can be bigger than the size of the divisor and we can therefore have no Euclidean algorithm for $\mathbb{Z}[\sqrt{-19}]$.

5 Conclusion

When you are solving Diophantine equation by factoring over some domain, it is important to know when you have unique factorization. Lame gave a famous false proof by trying to solve Fermat's last theorem by factoring $x^n = y^n - z^n$ in $\mathbb{Z}[\zeta_n]$ as

$$x^n = (y - z)(y - \zeta_n z)(y - \zeta_n^2 z) \cdots (y - \zeta_n^{n-1} z)$$

where n is prime and ζ_n is a primitive n -th root of unity. He then used similar arguments to conclude that the only solutions to $x^n = y^n - z^n$ when $n \geq 3$ are

the trivial ones. However, Lamé ignored unique factorization and it was realized by Kummer that the proof is incorrect since unique factorization fails in some of the domains $\mathbb{Z}[\zeta_n]$. (The first time this happens is when $n = 23$.) Kummer tried to restore unique factorization in $\mathbb{Z}[\zeta_n]$ and in doing so he introduced the concept of an “ideal number” and was able to prove Fermat’s last theorem for a large class of numbers. Dedekind later improved Kummer’s idea (ideal numbers are now called ideals due to Dedekind) and thus gave rise to modern algebraic number theory.

We were able to show that $\mathbb{Z}[\sqrt{-2}]$ has unique factorization by showing it has a Euclidean algorithm. Is this a necessary condition for unique factorization? That is, does the lack of a Euclidean algorithm indicate the lack of unique factorization? The answer is no! There are unique factorization domains with no Euclidean algorithm. There is a much stronger method of determining whether or not a domain (specifically, a Dedekind domain) has unique factorization that involves computing the numbers of elements in a “class group.” We can associate a finite group to every Dedekind domain, and unique factorization is equivalent to saying this group has one element.