Bézout's Identity

P. Reany

July 23, 2022

Abstract

Herein is a clever proof to a fundamental theorem of number theory. There are heuristics to glean from this proof. Introducing the *well-tempered set*.

1 Introduction

As I see it, there are six major principles of number theory:

The Principle of Mathematical Induction
Fundamental Theorem of Arithmetic
The Division Algorithm
The Well-Ordering Principle
Axiom of Choice
Bézout's Identity

These six principles are not just useful in number theory; just try to do group theory without them.

This paper states and proves Bézout's Identity,[1] namely, that if $a, b \in \mathbb{Z}\backslash\{0\}$ and $d \equiv (a, b) =$ GCD(a,b),[2] then there exist integers $x, y \in \mathbb{Z}$ such that

$$ax + by = d\,. \tag{1}$$

The proof offered below is nonconstructive[3] and explicitly uses the Division Algorithm and the Well-Ordering Principle, of which I will state the simplest versions that I require.

The *Division Algorithm* claims that if $j, k \in \mathbb{Z}^+$ with $j \leq k$, then there exists $q \in \mathbb{Z}^+$ (q is called the 'quotient') and an $r \in \mathbb{Z}^+ \cup \{0\}$ (r is called the 'remainder'), such that

$$k = jq + r\,, \tag{2}$$

where $r < j$. If $r = 0$, then we say that 'j divides k', and write it as $j \,|\, k$.

The *Well-Ordering Principle* claims that every non-empty set of positive integers contains a least element. Let Σ be a set of integers, at least one of which is positive. Let S be the subset of Σ of all positive elements of Σ. What this principle claims is that **there exists** an element $a \in S$ such that if $x \in S$ then $a \leq x$.

[1] Not the Bézout's Theorem.

[2] The GCD, or greatest common divisior, of two integers is the greatest positive integer that divides them both evenly.

[3] The proof will show existence, but will not solve for the unknown integers.

2 A useful lemma

Let $g, h \in \mathbb{Z}^+$.
If $g \,|\, h$ and $h \,|\, g$, then $g = h$.

The proof is left to the reader.

3 Setting up the Well-Tempered Set

Given a, b (not both zero) $\in \mathbb{Z}$, let Σ be defined as

$$\Sigma = \{ax + by \,|\, x, y \in \mathbb{Z}\}\,. \tag{3}$$

Since we want to apply the Well-Ordering Principle, we'd better make sure that for any choices of a and b, consistent with their given constraints, that Σ has at least one positive element. That's easy to do: For any a, choose $x = a$, and for any b, choose $y = b$ (remember that we're assuming that at least one of a, b is different from 0). Therefore, $a^2 + b^2 \in \Sigma$, but $a^2 + b^2 > 0$.

Clearly, the set Σ has been carefully chosen for this proof. For if Bézout's Identity is true, then $d = (a, b)$ is in Σ, and we just need to find a way to prove it. This leads us to a heuristic I call the *well-tempered set* construction:

> If you're going to construct a set that will contain all the solutions you're looking for, the set should be the 'smallest' set you can think of that will contain the solution/s, if it/they exist, yet large enough to meet all the conditions of all the lemmas you want to employ in your proof.

A couple comments might be helpful here: First, don't strain your brain for the absolute smallest set — just get within the ballpark. On the other hand, don't go overboard the other way by using the set of all sets. Second, don't fear defining infinite sets, as we did to define Σ. You might find a clever way to define a finite set that works as well, but it would come with extra conditions that would probably complicate working with it, yet gain no greater insight from it. The trick is to find the set that has the fewest number of defining properties.

4 Solution

Let S be the subset of Σ that contains all the positive elements of Σ. Let ℓ be the smallest positive element of S (the existence of ℓ is established by the Well-Ordering Principle). Then, in accordance with how the elements of $S \subset \Sigma$ are defined in (3), there exist integers $\overline{x}, \overline{y}$ (whose values we do not need to know), such that

$$\ell = a\overline{x} + b\overline{y}\,. \tag{4}$$

My first task is to show that ℓ divides both a and b. Let's start with a. (The Logic: Either ℓ divides a, or it doesn't.) If $\ell \nmid a$, then, by the Division Algorithm, there exist positive integers q_a and $0 < r_a < \ell$,[4] such that

$$a = \ell q_a + r_a\,. \tag{5}$$

But we can solve this for r_a and use (4) to get that

$$r_a = a - \ell q_a = a(1 - q_a\overline{x}) + b(-q_a\overline{y}) \in S\,. \tag{6}$$

Thus, ℓ is the smallest integer in S, yet $r_a \in S$ and $r_a < \ell$. This is a contradiction, proving that $r_a = 0$, hence $\ell \,|\, a$. And by the same logic, $\ell \,|\, b$.

[4] We must insist that $r_a > 0$ or we allow the case $\ell | a$, which we're trying to avoid at the moment.

Now, since every common divisor of a and b is also a divisor of $d = (a, b)$, then $\ell \,|\, d$. If we could show by the 'useful lemma' above that $d \,|\, \ell$, then we would know that $d = \ell$.

We know that d is a common divisor of both a and b. Hence, there exist $k_a, k_b \in \mathbb{Z}^+$ such that

$$a = dk_a \quad \text{and} \quad b = dk_b \,. \tag{7}$$

So, from (4),

$$\ell = dk_a\overline{x} + dk_b\overline{y} = d(k_a\overline{x} + k_b\overline{y}) \,. \tag{8}$$

Since $k_a\overline{x} + k_b\overline{y} \in \mathbb{Z}$, then $d \,|\, \ell$, which, combined with $\ell \,|\, d$, implies that $d = \ell$.[5] Hence, $d \in \Sigma$, and therefore it can be written as

$$d = (a, b) = a\overline{x} + b\overline{y} \,, \tag{9}$$

for some $\overline{x}$, $\overline{y} \in \mathbb{Z}$. And we're done.

5 Conclusion

Proofs like this one give me the feeling of a stage magician pulling a rabbit out of a hat. Yet, the founding principles of this stage act seem unremarkable to me: The Division Algorithm, the Well-Ordering Principle, and the right to define sets ad hoc for a given problem.

[5] We need not be concerned that $k_a\overline{x} + k_b\overline{y} = 0$ because ℓ is assumed to be positive.