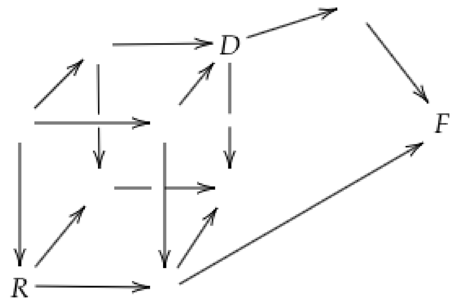

A proof of Fermat's Last Theorem for n=3

Danila Kurganov

Imperial College London

Introduction

The easy-to-state Fermat's Last Theorem (there are no non-zero solutions to $x^n + y^n = z^n$ over $\mathbb{Z}$, for $n > 2$) has motivated and eluded the greatest of mathematicians for centuries. We exhibit the power of abstraction by proving it for $n = 3$, referencing [1] throughout.

Rings

First, the definition of **rings**.

Definition. A non-empty set R equipped with two binary operations $+$ and $\cdot$ is said to be a **ring** if R is an abelian group on $+$, and $\cdot$ is associative as well as distributive over $+$.

Definitions. A **commutative ring** is a ring where $\cdot$ is commutative. A **commutative ring with unity** is a commutative ring which additionally has a multiplicative identity element, e. Finally, for our analysis, a **domain** is a commutative ring with unity where it holds that if $a \cdot b = z$, then $a = z$ or $b = z$.

Example We see that $\mathbb{Z}$ is a domain.

Divisibility in Commutative Rings

Working with rings other than $\mathbb{Z}$ give us more options. We therefore find it useful to define divisibility in rings. Let R be a *commutative* ring, with $a, b \in R$.

Definitions. a **divides** b (denoted by a | b) if and only if $\exists c \in R$ such that $a \cdot c = b$. Further, $d \in R$ is the **greatest common divisor** of a and b if d divides a and b, and all other divisors of a and b also divide d.

We introduce corresponding number-theoretic definition to commutative rings *with unity*:

Definitions. $u \in R$ is a **unit** if and only if $\exists v \in R$ such that $uv = e$, where e is the multiplicative identity in R. a, b are **associates** if and only if there exists a unit u such that $a = ub$. An element $\pi \in R$ is **irreducible** if and only if π is not a zero or unit element, and from $\pi = a \cdot b$, it follows that either a or b is a unit. An element $\pi \in R$ is **prime** if and only if π is not a zero or unit element, and from $\pi | ab$ it follows that $\pi | a$ or $\pi | b$.

Notation. We denote $\mathbb{X}[x]$ by $\{u + vx : u, v \in \mathbb{X}\}$, where $\mathbb{X}$ is a ring, and x is a chosen element.

Definition. Let $\alpha = a + b\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$. We define the **norm** of α by $N(\alpha) = |a^2 - db^2|$. For sake of conciseness, we admit $N(ab) = N(a)N(b)$. Note that $N : \mathbb{Q}[\sqrt{d}] \to \mathbb{Z}^+ \cup \{0\}$.

Lemma 2. The set $\{(a + b\sqrt{-3})/2\}$, where $a, b \in \mathbb{Z}$ and a, b are both even or odd is a ring, and its only units are the sixth roots of unity.

Proof. $(a + b\sqrt{-3})/2 \cdot (c + d\sqrt{-3})/2 = 1 \overset{\text{norm}}{\Rightarrow} (a^2 + 3b^2) \cdot (c^2 + 3d^2) = 16 \overset{parity}{\Rightarrow} (a^2 + 3b^2) = 4$, which gives all sixth roots of unity.

Euclidean Rings and FTA

The Fundamental Theorem of Arithmetic (FTA) is key to many number-theoretic proofs, so we seek to generalise it outside of $\mathbb{Z}$. Unfortunately, not all rings follow FTA!

Example. Unique factorisation does not hold in $\mathbb{Z}[\sqrt{-3}]$. In fact, $4 = 2 \cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3})$, giving two distinct decompositions into products of irreducibles.

Proof. $1 + \sqrt{-3}$ is non-zero nor a unit. Furthermore, $1+\sqrt{-3} = (a+b\sqrt{-3})(c+d\sqrt{-3}) \overset{\text{norm}}{\Rightarrow} 4 = (a^2+3b^2)(c^2+3d^2)$. By considering solutions in $\mathbb{Z}$, we see that we must have $(\pm 1 + 0\sqrt{-3})$ as a unit factor. Similarly, 2 is non-zero nor a unit, and similar analysis shows it is irreducible in $\mathbb{Z}[\sqrt{-3}]$.

Proving FTA requires the Euclidean division algorithm. Taking inspiration, we define:

Definition. R is a **Euclidean Ring** if and only if R is a domain and there exists a function, $\delta : R \backslash \{z\} \to \mathbb{Z}^+ \cup \{z\}$ such that:

1) For all non-zero $a, b \in R$, $\delta(a) \leq \delta(ab)$.
2) Let $a, b \in R$ with $b \neq z$, then $\exists m, r \in R$ such that $a = mb + r$ where either (i) $r = 0$ or (ii) $r \neq 0$ and $\delta(r) < \delta(b)$.

Several ER Lemmas

We first need several lemmas:

Lemma 3. Let R be ER. Then it must contain an additive (z) and multiplicative (e) identity. **Proof.** Observe the quantifiers found in the axioms.

Lemma 4. Let R be ER, with $a, b \in R$, not both z. Let $c = gcd(a, b)$. Then there exist $s, t \in R$ such that $as + bt = c$.

Proof. Consider $S = \{ma + nb : m, n \in R\}$. Lemma 3 admits S is non-empty. Find $m_0, n_0 \in R$ such that $c = m_0a + n_0b$, $\delta(c)$ minimised. We also let $w = m_1a + n_1b$ be arbitrary.

By **ER(2)** there exist $k, r \in R$ such that $w = kc + r$. So $r = w - kc = (m_1 - km_0)a + (n_1 - kn_0)b \in S$, so $r = 0$, but then $w = kc$.

Hence c is a common divisor of all elements in S, notably a and b. Suppose R has another common divisor, c_1, then $c_1 | a, c_1 | b \Rightarrow c_1 | m_0a + n_0b$. But this is c, so as other common divisors divide c we conclude that $gcd(a, b) = c$.

Lemma 5. $\mathbb{Z}[\rho]$ with $\delta(u + v\rho) = (u + v\rho)(v + v\rho^2)$ is ER.

Proof. Directly comparing with the definition, $\delta(u + v\rho) = (u + v\rho)(u + v\rho^2) = z\overline{z} = |z|^2$ we know $||$ satisfies condition (I).

For condition (II), let $a = u + v\rho, b = s + t\rho \neq 0 \in \mathbb{Z}[\rho]$. Then $a/b = (u + v\rho)/(s + t/\rho) = l + m\rho$ for suitable $l, m \in \mathbb{Q}$.

We find $L, M \in \mathbb{Z}$ such that $|L - l|, |M - m| \leq 1/2$, and denote $K = (l - L)\rho + (m - M)\rho$, noting that $\delta(K) < 1$ by triangle inequality.

But since $a/b = (L + M\rho) + K, a = (L + M\rho)b + Kb \in \mathbb{Z}[\rho]$, and so we find that $\delta(Kb) = |K|^2\delta(b) < \delta(b)$ as is needed.

FTA for ERs

Now we can prove a generalised FTA!

Theorem 1. Let R be an ER. If $\pi \in R$ is irreducible then π is prime. Hence elements of R can be uniquely factorised.

Proof. We must show that if $\pi | bc$ then $\pi | b$ or $\pi | c$. So let $b, c \in R$ be arbitrary with $\pi | bc$.

If $\pi \nmid b$, then the only common divisors to π and b are units, one of which is e. Hence, $gcd(\pi, b) = e$.

By Lemma 4, there must therefore exist $s, t \in R$ such that $s\pi + tb = e$. But then $s\pi c + tbc = c$, so clearly $\pi | c$.

Theorem 2. Let R be ER and let a be a non-zero non-unit in R. *If* $a = \pi_1\pi_2 \dots \pi_m = \pi'_1\pi'_2 \dots \pi'_n$ where the π_i and π_j are irreducibles *then* $m = n$ and the π_i and π_j can be paired off such that the paired elements are associates. So elements of R can be uniquely factorised.

Proof. We provide a proof by contradiction. Of the contradictory elements, choose $a \in R$ such that m is a small as possible.

Since $a = \pi_1\pi_2 \dots \pi_m$, π_m is irreducible, so by Theorem 1, π_m is prime. Hence, $pi_m | \pi'_1\pi'_2 \dots \pi'_n \Rightarrow \pi_m | \pi'_j$ for some j. But π_m and π'_j are irreducible, so they are associates, and so we have that $\pi'_j = u\pi_m$ for some unit u. We now consider $a = b\pi_m$.

$b = \pi_1\pi_2 \dots \pi_{m-1} = \pi'_1 \dots \pi'_{j-1}(u\pi'_{j+1}) \dots \pi_n$.

Due to minimality, the factors of b *must* be able to pair off as associates, and so not only does $m = n$, but a is no longer a contradictory element! Contradiction!

This completes the result. We now have the required abstraction for FLT.

Some final lemmas

But first we must derive some tools:

Lemma 6. Suppose there exist coprime $\alpha, \beta, \gamma \in \mathbb{Z}[\rho]$ which satisfy $x^3 + y^3 + z^3 = 0$. Further suppose that $\pi = 1 - \rho | \alpha$ and $3 | \pi^2$. Then there exist $c, d \in \mathbb{Z}$ such that $\beta\rho^c \equiv \pm 1 \pmod 3$ and $\gamma\rho^d \equiv \pm 1 \pmod 3$ in $\mathbb{Z}[\rho]$.

Proof. Due to symmetry we simply need to show the result for β alone. Let $\beta = x + y\rho \in \mathbb{Z}[\rho] \Rightarrow \beta = u + v\pi$ for some $u, v \in \mathbb{Z}$. Since $\pi \nmid \beta \in \mathbb{Z}[\rho]$, $3 \nmid u \in \mathbb{Z}$, and so $u \equiv \pm 1 \pmod 3 \in \mathbb{Z}$.

Considering $\mathbb{Z}[\rho]$, suppose $\beta = 1 + v\pi$. Then $\beta\rho^f = (1 + v\pi)(1 - \pi)^f \equiv 1 + (v - f)\pi \pmod 3$. Alternatively, $\beta = -1 + v\pi$ gives $\beta\rho^f = (-1 + v\pi)(1 - \pi)^f \equiv (-1 + v\pi)(1 - f\pi) \equiv -1 - (v + f)\pi \pmod 3$.

In either case, $v = \pm f$ does the trick, so we are done.

Lemma 7. If the norm of a number in $\mathbb{Z}[\rho]$ is prime, then it is irreducible.

Proof. Note the co-domain of the norm function. The corresponding ring is ER, so it follow that primes are irreducible in $\mathbb{Z}[\rho]$.

Corollary 1. $1 - \rho$ is irreducible in $\mathbb{Z}[\rho]$. **Proof.** $\delta(1 - \rho) = 3$ which is prime.

FLT for case 3

We are now ready.

Theorem 3. Fermat's Last Theorem is true for the third case in $\mathbb{Z}[\rho]$, and hence in $\mathbb{Z}$.

Proof. Suppose there is a solution $(\alpha, \beta, \gamma) \in \mathbb{Z}[\rho]$ satisfying $x^3 + y^3 + z^3 = 0$. We further suppose these elements have no common prime factor, as otherwise we can divide through by this factor. We now derive a key result about α.

Setting $a = \beta + \gamma, b = \gamma + \alpha, c = \alpha + \beta$ we see that: $-\rho^2\pi^2 = 3$, so $\pi | 3$ gives us $\pi | 24abc = (a + b + c)^3$. Due to Corollary 1, $\pi^3 | 24abc$.

If $\pi^3 | 24$ then $\pi^3 | 24 - 3^3 = -3 = \rho^2\pi^2$. But then $\pi | \rho^2$, contradicting Lemma 2 which says that ρ is unit. Hence $\pi^3 | abc$.

We set $\pi | a \Rightarrow \pi | a^3$ which shows with our contradictory FLT assumption that $\pi | \alpha, \pi \nmid \beta$, and $\pi \nmid \gamma$.

We now derive key results about β and γ.

Using the facts that $(\beta\rho^c)^3 = \beta^3$ and $(\gamma\rho^c)^3 = \gamma^3$ with Lemma 6, we deduce that $\beta, \gamma \equiv \pm 1 \pmod 3$.

If $\beta \equiv \gamma \equiv \pm 1 \pmod 3$ then $\beta^3 + \gamma^3 \equiv \pm 1 \pmod 3$. $\pi | \alpha$ so $\pi | \alpha^3 + \beta^3 + \gamma^3$, giving us a contradiction as then $\pi | \pm 1$.

Thus, assume that with appropriate $\lambda, \mu \in \mathbb{Z}[\rho]$, $\beta = 1 + 3\lambda, \gamma = -1 + 3\mu$.

Hence we see that $3^2 | \beta^3 + \gamma^3$, and so $\pi^4 | \beta^3 + \gamma^3$ as $3 | \pi$.

With these deductions, we can now find another solution.

Let $A = (\beta + \gamma\rho)/\pi, B = (\beta\rho + \gamma)/\pi, andC = (\beta + \gamma)\rho^2/\pi$.

We note that $A + B + C = 0$ and $ABC = (\beta^3 + \gamma^3)/\pi^3$, giving us $\pi | ABC$ and $\pi^3 | ABC$.

Since $gcd(\beta, \gamma) = 1$ and both can be written as a linear combination of A and B, $gcd(A, B) = 1$. Hence A, B, C are all coprime in $\mathbb{Z}[\rho]$. We deduce that A, B, C are all cubes, so WLOG have $\pi | C$.

Further, have $A = u_1\phi^3, B = u_2\chi^3, C = u_3\psi^3$. So $u_1\phi^3 + u_2\chi^3 + u_3\psi^3 = 0$, giving us $\phi^3 + u_4\chi^3 \equiv 0 \pmod{\pi^3}$.

By analysing the possibilities, we have that $\phi^3, \chi^3 \equiv \pm 1$. Hence, $0 \equiv \phi^3 + u_4\chi^3 \equiv \pm 1 \pm u_4$ and so with Lemma 2 we have $u_1 = \pm u_2$.

Since $u_1u_2u_3$ is a unit and a cube, $u_3 = \pm u_1$. We therefore arrive at $\phi^3 + (\pm\chi)^3 + (\pm\psi)^3 = 0$, a new (!) solution, and $(\phi\chi\psi)^3 = (\beta^3 + \gamma^3)/\pi^3 = (\pm\alpha/\pi)^3$.

A valid solution must have some divisor of π. But our method removes them(!) - eventually, a contradiction!

A conclusion

The abstract method allows us to simplify and generalise properties previously unrealised onto FLT.

References

[1] R.B.J.T Allenby. Rings, Fields, and Groups: An introduction to Abstract Algebra E. Arnold, 1983.