A DO-IT-YOURSELF PROOF OF THE $n = 3$ CASE OF FERMAT'S LAST THEOREM

RAVI VAKIL, VAKIL-AT-MATH.MIT.EDU

Fermat's Last Theorem has had a lasting impact on mathematics because the tools and concepts developed in various attempts have turned out to be extraordinarily effective elsewhere in number theory. The culmination of these efforts, Wiles' wonderful proof of the Shimura-Taniyama-Weil conjecture (in the case of semistable elliptic curves), has not just dispatched the most famous conjecture of all time, but also fundamentally changed the landscape of number theory.

Fermat's Last Theorem (Wiles, Taylor-Wiles). If n, x, y, and z are integers with $n \geq 3$ and $x^n + y^n = z^n$, then $xyz = 0$.

When referring to Fermat's Last Theorem for a fixed n, we'll use the short-form FLTn. FLT4 is the easiest case. The second-easiest case, FLT3, is also reasonable enough for the ambitious reader to figure out, although more hints are necessary. Many important ideas come up that figure prominently in number theory, and mathematics in general. I'll summarize these ideas at the very end.

Warning: this is very interactive! You will really have to try all of the problems. If you get stuck, then skip to the next one. Even getting stuck is a good thing (much better than not trying at all), because the seeds of ideas that come up in one problem invariably turn up again in a later one. If you successfully solve most of the problems, congratulations — you've figured out part of one of the most important problems in the history of humankind! (And if you've also proved the $n = 4$ case, then you'll have proved "half" of Fermat's Last Theorem — you'll have proofs for "half" the positive integers n!)

The only advanced background you'll need is some experience with complex numbers. Warmup questions are marked with a W; many of them will be used later, so don't skip them! The questions giving the actual proof are marked with a P. The argument isn't as long as it looks, as you'll see from the summary at the end.

1. Unique factorization

The Unique Factorization Theorem can be written as follows: Any non-zero integer n can be uniquely factored into primes (or irreducibles), up to units (so $(-2) \times 3$ and $2 \times (-3)$ are considered to be the same factorization).

W1. Suppose x, y, z pairwise relatively prime integers, and $xyz = w^2$ for some non-zero integer w. Show that $x = \alpha a^2$, $y = \beta b^2$, $z = \gamma c^2$ for some units α, β, γ, and integers a, b, c. (This may seem an awkward way to phrase this result, but bear with it.) There was no real reason to require w to be non-zero, except to save you the hassle of dealing with the special case $w = 0$ in your proof.

W2. Suppose x, y, z pairwise relatively prime integers, and $xyz = w^3$ for some non-zero integer w. Show that $x = \alpha a^3$, $y = \beta b^3$, $z = \gamma c^3$ for some units α, β, γ, and integers a, b, c.

Because we're dealing with cubes, we can do a little better: the α, β, and γ can be incorporated into the a^3, b^3, and c^3:

W3. Suppose x, y, z pairwise relatively prime integers, and $xyz = w^3$ for some non-zero integer w. Show that $x = a^3$, $y = b^3$, $z = c^3$ for some integers a, b, c.

2. A twist on the integers: F-integers

We'll define a new set of numbers that behaves a lot like the integers. They will be complex numbers. You'll have to recall how to add, subtract, multiply, and divide complex numbers, and take complex conjugates: $\overline{a+bi} = a - bi$. Recall also the definition of the norm $N(z)$ of a complex number z (named after a character on the popular television show "Cheers"):

$$N(a+bi) = (a+bi)\overline{(a+bi)} = a^2 + b^2.$$

You can check that $N(z_1 z_2) = N(z_1)N(z_2)$. The absolute value of a complex number z is $|z| = \sqrt{N(z)}$: $|a+bi| = \sqrt{a^2+b^2}$.

Let $\omega = \frac{-1+i\sqrt{3}}{2}$. ($\omega$ is the Greek letter *omega*.)

W4. Check that $\omega^3 = 1$ and $\omega^2 = -1 - \omega$. Calculate $(1-\omega)(1-\omega^2)$. Show that $(1-\omega^2) = -\omega^2(1-\omega)$, $\overline{\omega} = \omega^2$, and $3 = -\omega^2(1-\omega)^2$. Expand $(x+y)(x+\omega y)(x+\omega^2 y)$. (We'll use all of these later, so make sure to do them!)

Let the set of complex numbers of the form $a + b\omega$ (where a and b are integers) be called F-integers. (This is a non-standard name, so don't use it in public.)

You already know how to add and subtract and multiply them, because they are just complex numbers:

$$\begin{aligned}(a+b\omega)+(c+d\omega) &= (a+c)+(b+d)\omega,\\ (a+b\omega)-(c+d\omega) &= (a-c)+(b-d)\omega.\end{aligned}$$

You can multiply them without translating back to i's, using $\omega^2 = -1-\omega$ (W4). For example, $(a+b\omega)(c+d\omega)$ can be calculated by just expanding out and simplifying:

$$\begin{aligned}(a+b\omega)(c+d\omega) &= ac + ad\omega + bc\omega + bd\omega^2\\ &= ac + (ad+bc)\omega + bd(-1-\omega)\\ &= (ac-bd) + (ad+bc-bd)\omega\end{aligned}$$

You can find norms too:

$$N(a+b\omega) = (a+b\omega)\overline{(a+b\omega)} = (a+b\omega)(a+b\omega^2) = a^2+ab\omega+ab\omega^2+b^2 = a^2+b^2-ab.$$

(Aside: does this remind you of the cosine law with a triangle with sides a and b, and enclosed angle 60 degrees?)

You can picture the F-integers as a triangular grid in the complex plane. (As a reality check you should draw this picture, and label the points 0, 1, -1, 2, ω, ω^2, $1+\omega$, $1+\omega^2$, $1-\omega$, $1-\omega^2$.)

Most things you can do with integers, you can also do with F-integers. For example, while there are two units in the integers, there are actually six units in the F-integers (the F-integers with norm 1). Two F-integers are *associates* if one is a unit times the other.

W5. Find the six units of the F-integers? (Hint: See your picture of the triangular grid.)

An F-integer is *prime* if it isn't a unit, and it is only divisible by its associates and the units. Some of these primes might look surprising to you. For example, 2 is prime, but 3 isn't a prime F-integer, because it factors:

$$3 = (1-\omega)(1-\omega^2).$$

$(1-\omega)$ and $(1-\omega^2)$ are both prime. In fact they are associates — they differ by the unit $-\omega^2$ (see W4). The prime number $1-\omega$ will be a big player in the proof of FLT3.

W6. Show that $2\omega+1 = i\sqrt{3}$ is a prime number that's an associate of $1-\omega$. (Hint: find the unit that associates them.)

W7. Show that $1-\omega$ is prime as follows. If it is composite, and thus factors into two non-units x and y, then $N(x)N(y) = N(1-\omega)$. What are the possible values of $N(x)$ and $N(y)$? Why does one of x and y have to be a unit?

W8. 7 isn't a prime F-number. Can you factor it?

We can use modular arithmetic on F-integers as well. Recall that for two ordinary integers a and b to be congruent modulo n, there must exist an integer r such that $(a-b) = nr$. Congruences for F-integers work exactly the same way: if α and β are two F-integers, then they are congruent modulo the F-integer ν iff there exists an F-integer ρ such that $(\alpha-\beta) = \nu\rho$.

W9. If n is an ordinary integer, check that the F-integers $a+b\omega$ and $c+d\omega$ are congruent modulo n if and only if $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$ as ordinary integers.

W10. Confirm that the two notions of congruence coincide: that is, if a, b, and n are ordinary integers, then $a \equiv b \pmod{n}$ as F-integers if and only if $a \equiv b \pmod{n}$ by the usual notion of congruence.

Therefore, we can speak about congruence without having to specify whether we're talking about congruence as F-integers or about regular congruence: they mean the same thing!

W11. Show that the cube of a F-integer is congruent to an integer modulo 3. (Hint: Expand $(a + b\omega)^3$ and see what you get.)

In other words, $\rho^3 \equiv 0$, 1, or 2 $\pmod 3$ (and not ω, $\omega + 1$, $\omega + 2$, 2ω, $2\omega + 1$, $2\omega + 2 \pmod 3$). (Aside: More generally, if ρ is an F-integer not divisible by $1 - \omega$, then $\rho^3 \equiv \pm 1 \pmod 9$, which can be rewritten $\rho^3 \equiv \pm 1 \pmod{(1 - \omega)^4}$, although we won't need it, [D] p. 104. This should be seen as similar to the fact that if ρ is an integer not divisible by 2, then $\rho^2 \equiv \pm 1 \pmod{2^3}$.)

3. F-integers and unique factorization

F-integers also have unique factorization. In other words, given any F-integer, you can uniquely factor it into primes (up to the 6 units). (This is the only part of the argument that won't be done here.) We say two F-integers are *relatively prime* if they have no common prime factor.

We now have results about factoring cubes into relatively prime terms that are similar to W2 and W3 for integers.

W12. Suppose x, y, z pairwise relatively prime F-integers, and $xyz = w^3$ for some non-zero F-integer w. Show that $x = \alpha a^3$, $y = \beta b^3$, $z = \gamma c^3$ for some F-integers a, b, c and units α, β, γ (i.e. α, β, $\gamma \in \{1, \omega, \omega^2, -1, -\omega, -\omega^2\}$ — oops, I just gave away the answer to W5!). Remember, use unique factorization.

W13. Suppose x, y, z pairwise relatively prime F-integers, and $xyz = w^3$ for some non-zero F-integer w. Show that $x = \alpha a^3$, $y = \beta b^3$, $z = \gamma c^3$ for some F-integers a, b, c, where α, β, and γ are each in the set $\{1, \omega, \omega^2\}$.

4. Fermat's Last Theorem ($n = 3$ case)

You're now ready to begin figuring out the proof! You'll use the warm-ups, but the main ideas about F-integers that you'll need are: comfort with multiplying them, the cubic factorization problem W13, and the prime $1 - \omega$.

Notice that to show FLT3, we need only show that $\pm a^3 \pm b^3 \pm c^3 = 0$ has no solutions in integers a, b, c unless $abc = 0$. (We can pick our signs in any way we wish. Choosing $+$, $+$, $-$ gives FLT3 the way it is usually seen.)

P1. Show that if there is a solution, then there is a solution where a, b, c are pairwise relatively prime. From here on in, we'll assume this is the case.

P2. Show that there are no solutions when none of a, b, c are divisible by 3. (Hint: Look modulo some number. You'll find that 3 won't work. Numbers like 2 and 5 won't help. So what should you try?)

So we can assume one of them is divisible by 3. So we want to show there are no solutions to

$$x^3 + y^3 = (3^m z)^3 \tag{1}$$

where x, y, z are integers, pairwise relatively prime, and not divisible by 3; and m is a non-negative integer. We've already taken care of the case $m = 0$ (P2), so suppose from now on that $m > 0$.

Now $x^3 + y^3 = (x + y)(x + \omega y)(x + \omega^2 y)$ (see W4), which is a factorization in the F-integers! For convenience, let $A = x + y$, $B = x + \omega y$, $C = x + \omega^2 y$. Then A, B, and C multiply to a cube! Could they be pairwise relatively prime? Sadly, they aren't.

P3. Show that the prime number $1 - \omega$ divides A, B, and C as follows. $1 - \omega$ divides 3, which divides A. $1 - \omega$ divides $(x + y)$ and $(\omega - 1)y$, so it divides their sum B. Do something similar with C.

So they aren't pairwise relatively prime. But they're almost as good. Aside from the common factor of $1 - \omega$, they *are* relatively prime.

P4. Show that $x = -\omega(A - \omega^2 B)/(1 - \omega)$ and $y = (A - B)/(1 - \omega)$. Hence if A and B have a common factor on top of $(1 - \omega)$, then x and y would too. Show the analogous fact for the pairs (B, C) and (C, A). This means that $\gcd(A, B) = \gcd(B, C) = \gcd(C, A) = (1 - \omega)$.

P5. We've seen that $x + y = A$ is divisible by 3. Using $ABC = (3^m z)^3$ and the previous question, show that

$$x + y = \eta_0 3^{3m-1} \rho_0^3,\ x + \omega y = \eta_1 (1 - \omega)\rho_1^3,\ x + \omega^2 y = \eta_2 (1 - \omega)\rho_2^3. \tag{2}$$

where each η_i is one of the units 1, ω, ω^2, and ρ_0, ρ_1, ρ_2 are relatively prime F-integers not divisible by the prime $1 - \omega$. (Hint: $x + y$ is divisible by two factors of $(1 - \omega)^2$ from $3 = -\omega^2(1 - \omega)^2$, and $x + \omega y$ and $x + \omega^2 y$ have one factor of $1 - \omega$ from P4. Thus $x + y$ gets the rest of the factors of $(1 - \omega)$, which give 3^{3m-1}. You'll need the same trick as in W13 to show that η_i can be taken to be one of the units 1, ω, ω^2.)

We'll deal with these three equations separately. The third one we can deal with quickly.

P6. Ignore the third equation. (That's the easy part!)

We next deal with the first equation.

P7. Check that $\eta_0 = 1$ by checking that $\frac{\overline{\eta_0}}{\eta_0}$ is a cube, in particular $\frac{\overline{\rho_0}^3}{\rho_0^3}$. Then check that the only units that are cubes are 1 and -1.

P8. Now $x + y = 3^{3m-1}\rho_0^3$. Show that we can assume that ρ_0 is an integer (not just a F-integer). Hint: $\rho_0^3 = 3^{1-3m}(x + y)$ is a real number. If $\rho_0 = s + t\omega$, show — by expanding out — that if ρ_0^3 is real, then $s = t$ or $s = 0$ or $t = 0$. If $t = 0$, then ρ_0 is real. If $s = 0$, then we can replace ρ_0 by ρ_0/ω, which is real (and has the same cube as ρ_0). If $s = t$, then we can replace ρ_0 by $\frac{\rho_0}{\omega^2} = \frac{-\rho_0}{1+\omega}$, which is also real (and also has the same cube as ρ_0).

We've now massaged the equations into:

$$x + y = 3^{3m-1}\rho_0^3, \; x + \omega y = \eta_1(1-\omega)\rho_1^3,$$

where η_1 is 1, ω, or ω^2; ρ_1 is a F-integer; and ρ_0 is an honest-to-goodness integer.

We next deal with the second equation.

P9. Show that $\eta_1 = 1$ as follows. Reduce the equation $x + y + (\omega - 1)y = \eta_1(1-\omega)\rho_1^3$ modulo $3(1-\omega)$. $A = x + y$ is divisible by $9 = 3(1-\omega)(1-\omega^2)$, so is divisible by $3(1-\omega)$. Use this to show that $y \equiv -\eta_1\rho_1^3 \pmod 3$. But $\rho_1^3 \equiv 1$ or $2 \pmod 3$ (from W11; why not 0?), and $y \equiv 1$ or $2 \pmod 3$, so η_1 can't be ω or ω^2.

Let $\rho_1 = a + b\omega$ where a and b are integers.

P10. Show that $x + \omega y = (a^3 + b^3 - 6ab^2 + 3a^2b) + (-a^3 - b^3 + 6a^2b - 3ab^2)\omega$. Hence $x = a^3 + b^3 - 6ab^2 + 3a^2b$ and $y = -a^3 - b^3 + 6a^2b - 3ab^2$.

P11. Show that a, b, and $a - b$ are pairwise relatively prime. (Hint: anything dividing two of them would also have to divide both x and y, which are supposed to be relatively prime.)

P12. Show that there are no solutions with $a = 0$ or $b = 0$ or $a = b$. (Just plug in for x and y, and see that they don't satisfy equation (1)!)

P13. Show that $9ab(a - b) = x + y = 9 \cdot 3^{3(m-1)}\rho_0^3$ from earlier results.

P14. So a, b, and $a - b$ are pairwise relatively prime integers multiplying to the cube of a number $3^{m-1}\rho_0$! Show that this somehow gives a solution to the equation $x_0^3 + y_0^3 = (3^{m-1}z_0)^3$, where x_0, y_0, and z_0 are pairwise relatively prime, and not divisible by 3.

P15. You've now shown that if equation (1) has a solution for some positive integer m, then it has a solution when $m - 1$ as well. You have already shown that it has no solution for $m = 0$ (P2), so finish off the proof!

5. Summary

We summarize the argument to show that it isn't as complicated as it first appears. The first key idea is to generalize the integers to F-integers, and to see that the F-integers have unique factorization. (F-integers in turn can be generalized greatly. Unfortunately, these generalizations rarely have unique factorization — so the F-integers are quite special — and much of modern number theory has been developed to try to deal with this lack of unique factorization.)

Then we return to the problem at hand, using familiar techniques from FLT4, but incorporating the new idea of F-integers. Look at equation (1), $x^3+y^3 = (3^m z)^3$ where m is a non-negative integer, and x, y, z are relatively prime and not divisible by 3. This has no solutions when $m = 0$ (P2). If $m > 0$, we factor the left side in F-integers $(x + y)(x + \omega y)(x + \omega^2 y)$. They aren't relatively prime, but they only have the common factor $1 - \omega$, from which we get the important equations (2):

$$x + y = \eta_0 3^{3m-1} \rho_0^3,\ x + \omega y = \eta_1 (1 - \omega) \rho_1^3,\ x + \omega^2 y = \eta_2 (1 - \omega) \rho_2^3.$$

We forget the third. In the first, we show that $\eta_0 = 1$ (by showing that $\frac{\overline{\eta_0}}{\eta_0} = \frac{\overline{\rho_0^3}}{\rho_0^3}$ is a cube, P7), and then show that we can take ρ_0 to be an integer. In the second, we show that $\eta_1 = 1$ by considering the equation modulo $3(1 - \omega)$. Finally, we let $\rho_1 = a + b\omega$, work out x and y in terms of a and b, and then substitute in the equation for $x + y$, getting a solution to (1) with m one less.

Many ideas introduced here turn out be fundamentally important in number theory, in particular the ideas of F-integers (which are generalized greatly), unique factorization, the complex numbers (and the geometry of F-integers in the complex numbers), the importance of the prime $1 - \omega$, and the idea of "descent" (in this case, taking a hypothetical solution to (1) for some m, and producing a solution to (1) with m one less).

If you've gotten this far, and successfully proved the $n = 3$ case of Fermat's Last Theorem, well done! Reach over your shoulder and pat yourself on the back.

Acknowledgements. This is essentially the article [FLT3], edited to apply to fit with the Mathcamp talks. Suggestions from Dave Savitt of Harvard University greatly improved the presentation. The form of this proof comes from the excellent book [Wa], especially Ex. 9.5 p. 183, although the exposition has be changed significantly. Another proof is given in [D] (pp. 96–104), where Gauss' original proof that FLT3 holds even when x, y, and z are F-integers is given. The term "F-integers" is non-standard; F-integers are usually called Eisenstein numbers.

References

[D] H. Dörrie, *100 Great Problems of Elementary Mathematics: Their History and Solution*, Dover: New York, 1965.

[FLT4] R. Vakil, *A Do-It-Yourself Proof of the $n = 4$ Case of Fermat's Last Theorem*, in *Crux Mathematicorum with Mathematical Mayhem*, I can't remember which issue (ask me later).

[FLT3] R. Vakil, *A Do-It-Yourself Proof of the $n = 3$ Case of Fermat's Last Theorem*, in **Crux Mathematicorum with Mathematical Mayhem**, I can't remember which issue.

[UF] R. Vakil, *Unique factorization, Funny Dice, the 2-Square Theorem, and FLT3*, to appear next issue. In this article, we'll discuss unique factorization in variants of the integers, and use it to i) fill in the last proof of FLT3, ii) find a funny pair of dice that gives the same outcome as a usual pair of dice, iii) solve the famous problem: find all integers that can be expressed as a sum of 2 square.

[Wa] L. Washington, *Cyclotomic Fields*, Graduate Texts in Mathematics vol. 83, Springer-Verlag: New York, 1982.