

Unique Factorization in $\mathbf{Z}[2^{1/3}]$ A Well-Ordered Approach

PRELIMINARIES

THUE'S LEMMA

1. Let r, m be integers with $m > 0$. Associate to each pair of integers x, y with $0 \leq x, y \leq m^{1/2}$ the residue class of $x - ry \pmod{m}$. By Pigeonhole, two distinct pairs determine the same residue class. Consequently, there are $X, Y \in \mathbf{Z}$, not both zero, with $|X|, |Y| \leq m^{1/2}$ and such that

$$X \equiv rY \pmod{m}.$$

A CRITERION FOR UNIQUE FACTORIZATION

Definition: Let R be a domain. We say $\pi \in R$ is prime if π is nonzero, not a unit, and whenever $\pi \mid ab$ with $a, b \in R$, either $\pi \mid a$ or $\pi \mid b$. (Equivalently, (π) is a nonzero prime ideal of R .)

2. Show: In an integral domain R , every prime is irreducible.

Definition: Let a be a nonzero, nonunit element of a domain R . We call a uniquely factorable if a has a factorization into irreducibles of R and this factorization is unique up to order and unit factors.

3. ("Unique prime factorization" is redundant)
Show: If $a \in R$ has a factorization into primes of R , then a is uniquely factorable.
4. In a domain R , the set of elements possessing a factorization into primes is "downward-closed" under divisibility. Specifically, if a, b are nonzero nonunits of R for which $a \mid b$, and b has a factorization into primes, then a has a factorization into primes.

PRACTICAL RING THEORY

5. Let F be a field and S be a Ring. Show that if there is a surjective homomorphism from F to S , then either S is the zero ring or $F \simeq S$.
6. Let R be a Ring, and let I, J be ideals of R . Let $\bar{J}$ denote the image of J under the natural surjection $R \twoheadrightarrow R/I$, and let $\bar{I}$ denote the image of I under the natural surjection $R \twoheadrightarrow R/J$. Show that $(R/I)/\bar{J} \simeq R/(I+J) \simeq (R/J)/\bar{I}$.

This justifies the claims from both AlgNT lectures and first-year NT lectures that $\mathbf{Z}_p[T]/(T^2+1) \simeq \mathbf{Z}[T]/(p, T^2+1) \simeq \frac{\mathbf{Z}[T]/(T^2+1)}{(p)} \simeq \mathbf{Z}[i]/(p)$.

FIRST STEPS INTO $\mathbf{Z}[2^{1/3}]$

In what follows, we write $\theta = 2^{1/3}$, understanding θ to denote the cube root of 2 in $\mathbf{R}$. We write $\mathbf{Z}[\theta]$ and $\mathbf{Q}[\theta]$ for the subrings of $\mathbf{R}$ obtained by adjoining θ to $\mathbf{Z}$ and $\mathbf{Q}$, respectively; then

$$\mathbf{Z}[\theta] = \mathbf{Z} + \mathbf{Z}\theta + \mathbf{Z}\theta^2, \quad \text{while} \quad \mathbf{Q}[\theta] = \mathbf{Q} + \mathbf{Q}\theta + \mathbf{Q}\theta^2.$$

Note that $\mathbf{Q}[\theta]$ is a field, isomorphic to $\mathbf{Q}[T]/(T^3-2)$.

Let $\omega = e^{2\pi i/3}$. There are three embeddings (injective homomorphisms) of $\mathbf{Q}[\theta]$ into $\mathbf{C}$: we can either keep θ as is (do nothing) or replace θ with either of $\omega\theta$ or $\omega^{-1}\theta$ (the other two complex roots of $T^3 - 2$). We let $\sigma_0, \sigma_1, \sigma_{-1}$ be the corresponding maps; concretely, $\sigma_i: \mathbf{Q}[\theta] \rightarrow \mathbf{C}$ acts by

$$a_0 + a_1\theta + a_2\theta^2 \mapsto a_0 + a_1\omega^i\theta + a_2\omega^{2i}\theta^2.$$

The norm of an $\alpha \in \mathbf{Q}[\theta]$ is defined as the product of the images of α under these three embeddings, i.e., $N\alpha = \prod_{i=-1}^1 \sigma_i(\alpha)$. Explicitly,

$$N(a_0 + a_1\theta + a_2\theta^2) = a_0^3 + 2a_1^3 + 4a_2^3 - 6a_0a_1a_2. \quad (1)$$

We can also write

$$N(a_0 + a_1\theta + a_2\theta^2) = (a_0 + a_1\theta + a_2\theta^2)(a_0^2 - 2a_1a_2 + (2a_2^2 - a_0a_1)\theta + (a_1^2 - a_0a_2)\theta^2). \quad (2)$$

(These identities may be verified by straightforward but tedious calculations.) In particular, (1) shows that the norm maps $\mathbf{Z}[\theta]$ to $\mathbf{Z}$, while (2) implies that $\alpha \mid N\alpha$ (within the ring $\mathbf{Z}[\theta]$) for each $\alpha \in \mathbf{Z}[\theta]$.

7. Prove: $\alpha \in \mathbf{Z}[\theta]$ is a unit $\iff N\alpha = \pm 1$.
8. If every rational integer > 1 has a factorization into primes in $\mathbf{Z}[\theta]$, then $\mathbf{Z}[\theta]$ is a UFD.
9. If every prime of $\mathbf{Z}$ has a factorization into primes of $\mathbf{Z}[\theta]$, then $\mathbf{Z}[\theta]$ is a UFD.

LOOK AND SEE...

We can check “by hand” that the first couple of primes of $\mathbf{Z}$ factor into primes of $\mathbf{Z}[\theta]$.

10. Clearly, $2 = \theta \cdot \theta \cdot \theta$. Verify that $\mathbf{Z}[\theta]/(\theta) \simeq \frac{\mathbf{Z}[T]/(T^3-2)}{(T)} \simeq \mathbf{Z}[T]/(T, T^3-2) \simeq \mathbf{Z}[T]/(2, T) \simeq \mathbf{Z}_2[T]/(T) \simeq \mathbf{Z}_2$. Since $\mathbf{Z}_2$ is a field, θ is prime.
11. Check: $3 = (1 + \theta) \cdot (1 + \theta) \cdot (1 + \theta)\epsilon$ for a unit ϵ of $\mathbf{Z}[\theta]$, and all three factors are prime.

WOP ENTERS THE CHAT

Suppose for a contradiction that there is a prime of $\mathbf{Z}$ that cannot be written as a product of primes of $\mathbf{Z}[\theta]$. Then (drum roll...) there is a least such prime, call it p . At this point we know $p \geq 5$.

Certainly p itself is not prime in $\mathbf{Z}[\theta]$! Hence, $T^3 - 2$ has to factor nontrivially mod p and (as a cubic) has a root in $\mathbf{Z}_p$. Let $r \in \mathbf{Z}$ with $r^3 \equiv 2 \pmod{p}$, and use Thue’s Lemma to choose $X, Y \in \mathbf{Z}$, not both zero, with

$$X \equiv rY \pmod{p}, \quad |X|, |Y| \leq \lfloor p^{1/2} \rfloor.$$

Then p divides $X^3 - 2Y^3$, and the corresponding quotient s satisfies

$$|s| = |X^3 - 2Y^3|/p \leq 3\lfloor p^{1/2} \rfloor^3/p.$$

We can check by hand that this last expression is smaller than p for $p = 5, 7$. And for $p \geq 11$, we have $3\lfloor p^{1/2} \rfloor^3/p < 3p^{1/2} < p$. Therefore, $|s| < p$.

Since $s \neq 0$, $|s|$ factors as a product of primes less than p , each of which is a product of primes in $\mathbf{Z}[\theta]$. Therefore, for some choice of $u = \pm 1$, we have $s = u\lambda_1 \dots \lambda_k$, where each λ_i is a prime in $\mathbf{Z}[\theta]$. Writing $X^3 - 2Y^3 = (X - \theta Y)(X^2 + \theta XY + \theta^2 Y^2)$, we conclude that

$$(X - \theta Y)(X^2 + \theta XY + \theta^2 Y^2) = u p \lambda_1 \dots \lambda_k.$$

12. Show: The factors λ_i can be distributed between the factors on the left so as to obtain nonunits $\pi, \rho \in \mathbf{Z}[\theta]$ satisfying

$$p = \pi\rho, \quad \pi \mid X - \theta Y, \quad \rho \mid X^2 + \theta XY + \theta^2 Y^2.$$

Fix such a pair (π, ρ) for what follows.

13. Let I be the ideal generated by $X - \theta Y$ and p . Then $\mathbf{Z}[\theta]/I \simeq \mathbf{Z}_p$.
14. $I \subseteq (\pi)$, and so there is a natural surjective homomorphism $\mathbf{Z}[\theta]/I \twoheadrightarrow \mathbf{Z}[\theta]/(\pi)$.
15. $\mathbf{Z}[\theta]/(\pi) \simeq \mathbf{Z}_p$, and hence π is prime.
16. Since $\mathbf{Z}[\theta]/(\pi) \simeq \mathbf{Z}_p$, every element of $\mathbf{Z}[\theta]$ is congruent, modulo π , to a rational integer uniquely determined modulo p . What is θ congruent to modulo π ?

CASE I: $T^3 - 2$ SPLITS INTO LINEAR FACTORS MOD p

We suppose in this case that there are $r_1, r_2, r_3 \in \mathbf{Z}$ with

$$T^3 - 2 \equiv (T - r_1)(T - r_2)(T - r_3) \pmod{p}.$$

Running the argument of the last section, taking successively $r = r_1, r_2, r_3$, we obtain three primes π_1, π_2, π_3 dividing p .

17. Show: The r_i are distinct modulo p .
18. No two of the π_i differ by a unit factor.
19. Use norms to show that p is, up to a unit, the product $\pi_1\pi_2\pi_3$. Derive a contradiction to the choice of p .

CASE II: $T^3 - 2$ DOES NOT SPLIT COMPLETELY MOD p

In this case,

$$T^3 - 2 \equiv (T - r)(T^2 + rT + r^2) \pmod{p},$$

where $T^2 + rT + r^2$ is irreducible modulo p .

Let π and ρ be defined as before. We have already seen that π is prime. We now claim that ρ is also prime. As $p = \pi\rho$, we have that p is a product of primes of $\mathbf{Z}[\theta]$, which is again a contradiction.

20. (Re)define I as the ideal generated by p and $X^2 + \theta XY + \theta^2 Y^2$. Show that $\mathbf{Z}[\theta]/I \simeq \mathbf{Z}_p[T]/(T^2 + rT + r^2)$.
21. $I \subseteq (\rho)$, and so there is a natural surjective homomorphism $\mathbf{Z}[\theta]/I \twoheadrightarrow \mathbf{Z}[\theta]/(\rho)$.
22. $\mathbf{Z}[\theta]/(\rho)$ is a field; hence, ρ is prime.

Remark. A “fuddy-duddy” might object to our entire project, on the (factual) grounds that $\mathbf{Z}[2^{1/3}]$ is norm-Euclidean (has a division algorithm where the size function is taken as the absolute value of the norm). If you have division, isn’t all this overkill? Well, it is not easy to show division holds here! More importantly: Our method is rather versatile. For instance, in principle it can be applied to prove unique factorization in $\mathbf{Z}[d^{1/3}]$ (d not a cube) whenever that domain is a UFD. We suspect (but cannot prove) that this happens infinitely often; e.g., it occurs for $d = 2, 3, 5, 6, 23, 29, 33, \dots$. By contrast, results of Cioffari imply that $d = 2, 3$ are the only noncube positive integers d for which $\mathbf{Z}[d^{1/3}]$ is norm-Euclidean.

We briefly indicate the necessary changes to implement the argument for $d = 5$ (the case $d = 3$ is slightly simpler). A (s)light modification to the proof of Thue’s lemma allows us to choose $X \equiv rY \pmod{p}$, $(X, Y) \neq (0, 0)$, with $|X| \leq 5^{1/6}p^{1/2}$, $|Y| \leq p^{1/2}5^{-1/6}$. Then $|X^3 - 5Y^3|/p \leq 2\sqrt{5}p^{1/2}$, which is smaller than p once $p > 20$. Replacing the upper bounds on $|X|, |Y|$ with their integer parts, we in fact handle all $p > 7$. And for $p = 2, 3, 5, 7$, one has (writing $\theta = 5^{1/3}$) prime factorizations

$$\begin{aligned} 2 &= (\theta^2 + 2\theta + 3)(\theta^2 - \theta - 1) \\ 3 &= (\theta - 2) \cdot (\theta - 2) \cdot (\theta - 2)(\text{unit}), \\ 5 &= \theta^3, \\ 7 &= 7. \end{aligned}$$

The WOP portion of the argument is essentially unchanged.