Math 4527 (Number Theory 2)

Lecture #29 of 37 $\sim$ March 31, 2021

Factorization in $\mathcal{O}_{\sqrt{-3}}$ + Diophantine Equations

- Factorization in $\mathcal{O}_{\sqrt{-3}}$
- Applications to Diophantine Equations

This material represents §8.3.2-8.3.3 from the course notes.

Factorization in $\mathcal{O}_{\sqrt{-3}}$, I

Since $\mathcal{O}_{\sqrt{-3}} = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ is also a Euclidean domain, we can analyze factorizations in this ring using essentially the same techniques we used for $\mathbb{Z}[i]$ and for $\mathbb{Z}[\sqrt{-2}]$.

- Things are slightly complicated by the fact that the generator for the ring is $\frac{1+\sqrt{-3}}{2}$ rather than $\sqrt{-3}$, but it is not especially difficult to handle this minor change.
- We also have more units in $\mathcal{O}_{\sqrt{-3}}$: specifically, it contains the sixth roots of unity, which are the elements $\frac{\pm 1 \pm \sqrt{-3}}{2}$ and ± 1.
- One helpful aspect of these extra units is that every element is associate to one of the form $a + b\sqrt{-3}$ with $a, b \in \mathbb{Z}$.
- Explicitly, if $\alpha = \frac{c+d\sqrt{-3}}{2}$ with c, d odd has $c \equiv d \bmod 4$, then $\alpha \cdot \frac{1-\sqrt{-3}}{2}$ has integer coefficients, while if $c \equiv d + 2 \bmod 4$ then $\alpha \cdot \frac{1+\sqrt{-3}}{2}$ has integer coefficients.

Factorization in $\mathcal{O}_{\sqrt{-3}}$, II

Now we can identify the irreducible elements in $\mathcal{O}_{\sqrt{-3}}$:

Theorem (Irreducibles in $\mathcal{O}_{\sqrt{-3}}$)

Up to associates, the irreducible elements in $\mathcal{O}_{\sqrt{-3}}$ are as follows:

1. *The element $\sqrt{-3}$ (of norm 3).*
2. *The primes $p \in \mathbb{Z}$ congruent to 2 modulo 3 (of norm p^2).*
3. *The distinct irreducible factors $a + b\sqrt{-3}$ and $a - b\sqrt{-3}$ (each of norm p) of $p = a^2 + 3b^2$ where $p \in \mathbb{Z}$ is congruent to 1 modulo 3.*

Factorization in $\mathcal{O}_{\sqrt{-3}}$, III

Proof:

- Since $\mathbb{Z}[i]$ is Euclidean, we may equivalently find the ideal factors of the ideals (p) for integer primes p, which we may do by factoring $q(x) = x^2 - x + 1$ modulo p.
- For $p = 3$, we have $x^2 - x + 1 \equiv (x-2)^2 \pmod{p}$, so we obtain the ideal factorization $(3) = (\omega - 2)^2 = (\sqrt{-3})^2$, yielding the element factorization $3 = -(\sqrt{-3})^2$.
- For $p \equiv 2$ mod 3, the polynomial $x^2 - x + 1$ is irreducible modulo p. For $p = 2$ this can be checked directly, and for odd p, by quadratic reciprocity we have $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{3}\right)(-1)^{-(p-1)/2} = \left(\frac{p}{3}\right)$. When $p \equiv 2$ mod 3, this last Legendre symbol is -1, and so -3 is not a square modulo p. Since the roots of $x^2 - x + 1$ are $\frac{1 \pm \sqrt{-3}}{2}$, this means $x^2 - x + 1$ has no roots hence is irreducible modulo p. Thus, the ideal (p) is prime, as is the element p.

Factorization in $\mathcal{O}_{\sqrt{-3}}$, IV

Proof (continued):

- For $p \equiv 1 \bmod 3$, we instead have $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = 1$: thus -3 is a square modulo p, so $x^2 - x + 1$ factors mod p.
- If the factorization is $x^2 - x + 1 \equiv (x - r)(x - 1 + r) \pmod{p}$, the ideal factorization is $(p) = (p, \omega - r) \cdot (p, \omega - 1 + r)$.
- Since $\mathcal{O}_{\sqrt{-3}}$ is a PID, the ideal $(p, \omega - r) = (a + b\sqrt{-3})$ for some a, b that we can compute by applying the Euclidean algorithm to p and $\omega - r$. Its conjugate is then $(p, \omega - 1 + r) = (a - b\sqrt{-3})$.
- This yields the ideal factorization $(p) = (a + b\sqrt{-3})(a - b\sqrt{-3})$ and so we get the element factorization $p = (a + b\sqrt{-3})(a - b\sqrt{-3})$ up to a unit factor, which by rescaling we may assume is 1. This means $p = (a + b\sqrt{-3})(a - b\sqrt{-3}) = a^2 + 3b^2$, and we have $N(a + b\sqrt{-3}) = a^2 + 3b^2 = p = N(a - b\sqrt{-3})$.

Factorization in $\mathcal{O}_{\sqrt{-3}}$, V

We can then compute element factorizations just as before:

- First, find the prime factorization of $N(a + b\sqrt{-3}) = a^2 + 3b^2$ over the integers $\mathbb{Z}$, and write down a list of all (rational) primes $p \in \mathbb{Z}$ dividing $N(a + b\sqrt{-3})$.
- Second, for each p on the list, find the factorization of p in the ring $\mathcal{O}_{\sqrt{-D}}$, which we can do by referring to the lists above, and then solving $p = a^2 + 3b^2$ in integers a, b whenever this equation has a solution.
- We can find this factorization by inspection for small p, and for large p we can find a solution by solving the quadratic $r^2 \equiv -3 \pmod{p}$ and then using the Euclidean algorithm to compute the gcd $a + b\sqrt{-3}$ of p and $\sqrt{-3} + r$ in $\mathcal{O}_{\sqrt{-3}}$.
- Finally, use trial division to determine which irreducible elements divide $a + b\sqrt{-3}$ in $\mathcal{O}_{\sqrt{-3}}$ and to which powers.

Factorization in $\mathcal{O}_{\sqrt{-3}}$, VI

<u>Example</u>: Find the prime factorization of $27 - \sqrt{-3}$ in $\mathcal{O}_{\sqrt{-3}}$.

Factorization in $\mathcal{O}_{\sqrt{-3}}$, VI

Example: Find the prime factorization of $27 - \sqrt{-3}$ in $\mathcal{O}_{\sqrt{-3}}$.

- We compute $N(27 - \sqrt{-3}) = 27^2 + 3 \cdot 1^2 = 2^2 \cdot 3 \cdot 61$, so the primes dividing the norm are 2, 3, and 61.
- Over $\mathcal{O}_{\sqrt{-3}}$, the element 2 is prime, and we also can find the factorizations $3 = 0 + 3 \cdot 1^2 = -\sqrt{-3}^2$ and $61 = 7^2 + 3 \cdot 2^2 = (7 + 2\sqrt{-3})(7 - 2\sqrt{-3})$.
- Now we just do trial division to find the correct powers of each of these elements dividing $47 + 32\sqrt{-2}$: we get one factor of 2, one factor of $\sqrt{-3}$, and one of $7 \pm 2\sqrt{-3}$.
- Doing the trial division yields the factorization $27 - \sqrt{-3} = \dfrac{-1 - \sqrt{-3}}{2} \cdot 2 \cdot \sqrt{-3} \cdot (7 + 2\sqrt{-3})$.

Factorization in $\mathcal{O}_{\sqrt{-3}}$, VII

We can also describe the integers that can be represented by the two quadratic forms $a^2 + ab + b^2$ and $a^2 + 3b^2$:

Theorem (Integers of the Form $a^2 + ab + b^2$ and $a^2 + 3b^2$)

Let n be a positive integer, and write $n = 3^k p_1^{n_1} \cdots p_k^{n_k} q_1^{m_1} \cdots q_d^{m_d}$, where $p_1, \cdots, p_k$ are distinct primes congruent to 1 modulo 3 and $q_1, \cdots, q_d$ are distinct primes congruent to 2 modulo 3. Then n can be written in the form $a^2 + ab + b^2$ for integers a, b if and only if it can be written in the form $a^2 + 3b^2$, if and only if all the m_i are even. Furthermore, in this case, the number of ordered pairs of integers (A, B) such that $n = A^2 + AB + B^2$ is equal to $6(n_1 + 1)(n_2 + 1) \cdots (n_k + 1)$.

Factorization in $\mathcal{O}_{\sqrt{-3}}$, VIII

Proof:

- The question of whether n can be written as $n = A^2 + AB + B^2$ is equivalent to the question of whether n is the norm of an element $A + B\omega \in \mathcal{O}_{\sqrt{-3}}$ where $\omega = \frac{1+\sqrt{-3}}{2}$.
- Write $A + B\omega = \rho_1 \rho_2 \cdots \rho_r$ as a product of irreducibles (unique up to units), and take norms to obtain $n = N(\rho_1) \cdot N(\rho_2) \cdot \cdots \cdot N(\rho_r)$.
- By the classification of primes in $\mathcal{O}_{\sqrt{-3}}$, if ρ is irreducible in $\mathcal{O}_{\sqrt{-3}}$, then $N(\rho)$ is either 3, a prime congruent to 1 modulo 3, or the square of a prime congruent to 2 modulo 3.
- Hence there exists such a choice of ρ_i with $n = \prod N(\rho_i)$ if and only if all the m_i are even.
- For representations $a^2 + 3b^2$, we simply observe that every irreducible element in $\mathcal{O}_{\sqrt{-3}}$ is associate to one in $\mathbb{Z}[\sqrt{-3}]$, so all statements about representability also hold for $a^2 + 3b^2$.

Factorization in $\mathcal{O}_{\sqrt{-3}}$, IX

Proof (continued):

- For the counting, since the factorization of $A + B\omega$ is unique, to find the number of possible pairs (A, B), we need only count the number of ways to select terms for $A + B\omega$ and $A + B\overline{\omega}$ from the factorization of n over $\mathcal{O}_{\sqrt{-3}}$, which is $n = (-1)^k(\sqrt{-3})^{2k}(\pi_1\overline{\pi_1})^{n_1}\cdots(\pi_k\overline{\pi_k})^{n_k}q_1^{m_1}\cdots q_d^{m_d}$.
- Up to associates, we must choose $A + B\omega = (\sqrt{-3})^k(\pi_1^{a_1}\overline{\pi_1}^{b_1})\cdots(\pi_k^{a_k}\overline{\pi_k}^{b_k})q_1^{m_1/2}\cdots q_d^{m_d/2}$, where $a_i + b_i = n_i$ for each $1 \le i \le k$.
- Since there are $n_i + 1$ ways to choose the pair (a_i, b_i), and 6 ways to multiply $A + B\omega$ by a unit, the total number of ways to write n as $A^2 + AB + B^2$ is $6(n_1 + 1)\cdots(n_k + 1)$, as claimed.

Factorization in $\mathcal{O}_{\sqrt{-3}}$, X

Example: Determine whether 21, 101, and 292 can be written in the form $a^2 + 3b^2$ for integers a and b.

Factorization in $\mathcal{O}_{\sqrt{-3}}$, X

Example: Determine whether 21, 101, and 292 can be written in the form $a^2 + 3b^2$ for integers a and b.

- We have $21 = 3 \cdot 7$. Since all of the primes are either 3 or congruent to 1 modulo 3, 21 is of the form $a^2 + 3b^2$.
- The integer 101 is prime and congruent to 2 modulo 3. Therefore, it cannot be written in the form $a^2 + 3b^2$.
- We have $292 = 2^2 \cdot 73$. Since 73 is congruent to 1 modulo 3 and since 2 occurs to an even power, 292 is of the form $a^2 + 3b^2$.

Some More Diophantine Equations, I

Example: Find all integer solutions to the Diophantine equation $x^2 + y^2 = z^5$ where x and y are relatively prime.

Some More Diophantine Equations, I

Example: Find all integer solutions to the Diophantine equation $x^2 + y^2 = z^5$ where x and y are relatively prime.

- Since squares are 0 or 1 modulo 4, one of x, y must be odd and the other is even, and also z is odd.
- Now factor the equation inside $\mathbb{Z}[i]$, which as we have shown is a unique factorization domain, as $(x+iy)(x-iy) = z^5$.
- Claim: $x + iy$ and $x - iy$ are relatively prime inside $\mathbb{Z}[i]$.
- To see this, observe that any common divisor must necessarily divide the sum $2x$ and the difference $2iy$, but since x and y are relatively prime integers, this means that the gcd must divide $2 = -i(1+i)^2$. Thus the only possible Gaussian prime divisor of the gcd is $1 + i$, but $1 + i$ does not divide $x + iy$ because x and y have opposite parity.

Some More Diophantine Equations, II

Example: Find all integer solutions to the Diophantine equation $x^2 + y^2 = z^5$ where x and y are relatively prime.

- So, with $(x + iy)(x - iy) = z^5$, we just showed $x + iy$ and $x - iy$ are relatively prime inside $\mathbb{Z}[i]$. Since their product is a fifth power (namely, z^5) and $\mathbb{Z}[i]$ is a UFD, this means that each term must be a fifth power up to a unit factor.
- But since the only units are $\pm 1, \pm i$ and these are all fifth powers (of themselves), we must have $x+iy = (a+bi)^5 = (a^5-10a^3b^2+5b^4)+(5a^4b-10a^2b^3+b^5)i$. Then the conjugate $x - iy$ is $(a - bi)^5$, and $z^5 = (x + iy)(x - iy) = (a^2 + b^2)^5$.
- Since all such tuples work, the solutions are of the form $(x, y, z) = (a^5 - 10a^3b^2 + 5b^4,\ 5a^4b - 10a^2b^3 + b^5,\ a^2 + b^2)$ for relatively prime integers a and b.

Some More Diophantine Equations, III

Example: Show that the only integer solutions to the Diophantine equation $y^2 = x^3 - 2$ are $(3, \pm 5)$.

Some More Diophantine Equations, III

Example: Show that the only integer solutions to the Diophantine equation $y^2 = x^3 - 2$ are $(3, \pm 5)$.

- First, observe that y must be odd, for if y were even then we would $x^3 \equiv 2 \pmod 4$, which is impossible.
- Now we rearrange the equation and factor it inside $\mathbb{Z}[\sqrt{-2}]$ as $(y + \sqrt{-2})(y - \sqrt{-2}) = x^3$.
- Claim: $y + \sqrt{-2}$ and $y - \sqrt{-2}$ are relatively prime in $\mathbb{Z}[\sqrt{-2}]$.
- To see this, observe that any common divisor must divide $(y + \sqrt{-2}) - (y - \sqrt{-2}) = 2\sqrt{-2} = -(\sqrt{-2})^3$, so the only possible irreducible factor of the difference is $\sqrt{-2}$.
- But $y + \sqrt{-2}$ cannot be divisible by $\sqrt{-2}$ since this would require y to be even.
- Thus, $y + \sqrt{-2}$ and $y - \sqrt{-2}$ are relatively prime.

Some More Diophantine Equations, IV

Example: Show that the only integer solutions to the Diophantine equation $y^2 = x^3 - 2$ are $(3, \pm 5)$.

- We showed $y + \sqrt{-2}$ and $y - \sqrt{-2}$ are relatively prime.
- Since their product is a cube (namely, x^3) and $\mathbb{Z}[\sqrt{-2}]$ is a UFD, this means that each term must be a cube up to a unit factor. But since the only units are ± 1 and these are both cubes, we must have $y + \sqrt{-2} = (a + b\sqrt{-2})^3 = (a^3 - 6ab^2) + (3a^2 b - 2b^3)\sqrt{-2}$, which requires $3a^2 b - 2b^3 = 1$.
- Factoring yields $b(3a^2 - 2b^2) = 1$ and so since a, b are integers, we see that $b = \pm 1$ and then $3a^2 = 2 \pm 1$, which has the two solutions $(a, b) = (\pm 1, -1)$.
- Then $y = a^3 - 6ab^2 = \pm 5$ and then $x = 3$, and so we obtain the solutions $(x, y) = (3, \pm 5)$ as claimed.

Some More Diophantine Equations, V

Example: Show that the Diophantine equation $4y^2 = x^3 - 3$ has no integer solutions.

Some More Diophantine Equations, V

Example: Show that the Diophantine equation $4y^2 = x^3 - 3$ has no integer solutions.

- First note that y cannot be divisible by 3, since then x would also have to be divisible by 3, but in that case $3 = x^3 - 4y^2$ would be divisible by 9, impossible.
- Now rearrange the equation and factor it inside the UFD $\mathcal{O}_{\sqrt{-3}}$ as $(2y + \sqrt{-3})(2y - \sqrt{-3}) = x^3$.
- Any common divisor of $2y + \sqrt{-3}$ and $2y - \sqrt{-3}$ must divide their difference $2\sqrt{-3}$, which is the product of the irreducible elements $\sqrt{-3}$ and 2. Clearly 2 cannot divide $2y + \sqrt{-3}$, and $\sqrt{-3}$ cannot divide it either because y is not divisible by 3.
- Therefore, $2y + \sqrt{-3}$ and $2y - \sqrt{-3}$ are relatively prime.

Some More Diophantine Equations, VI

Example: Show that the Diophantine equation $4y^2 = x^3 - 3$ has no integer solutions.

- We've shown $2y + \sqrt{-3}$ and $2y - \sqrt{-3}$ are relatively prime.
- Since their product is a cube and $\mathcal{O}_{\sqrt{-3}}$ is a UFD, this means that each term must be a cube up to a unit factor.
- By rescaling and conjugating if necessary, we either have $2y + \sqrt{-3} = (a + b\sqrt{-3})^3$ or $(2y + \sqrt{-3}) \cdot \frac{-1+\sqrt{-3}}{2} = (a + b\sqrt{-3})^3$ for some $a, b \in \mathbb{Z}$. However, the second case cannot occur, because the coefficients of the product on the LHS are not integers.
- So we must have $2y + \sqrt{-3} = (a + b\sqrt{-3})^3$. Expanding and comparing coefficients of $\sqrt{-3}$ yields $1 = 3a^2b - 3b^3$, which is impossible since the right-hand side is a multiple of 3.
- Thus, there are no integer solutions, as claimed.

Some More Diophantine Equations, VII

We can, with a nontrivial amount of work, also establish the $n = 3$ case of Fermat's conjecture, which was first settled by Euler.

For convenience in organizing the proof, we first establish a lemma (which is itself another example of solving a Diophantine equation):

Lemma (Cubes of the Form $m^2 + 3n^2$)

Suppose that m, n are relatively prime integers of opposite parity. If $m^2 + 3n^2 = r^3$, then there exist positive integers a and b with $m = a^3 - 9ab^2$ and $n = 3a^2b - 3b^3$.

The expressions for m and n come from comparing coefficients in $m + n\sqrt{-3} = (a + b\sqrt{-3})^3$.

Some More Diophantine Equations, VIII

Proof:

- Let m, n be relatively prime, opposite parity, $m^2 + 3n^2 = r^3$.
- First, if $3|m$ so that $m = 3k$, then we obtain $9k^2 + 3n^2 = r^3$: this forces $3|r$, but then dividing by 3 shows that $n^3 = (r/3)^3 - 3k^2$ so that 3 would also divide n, which is impossible. Thus, $3 \nmid m$.
- Now factor the equation $m^2 + 3n^2 = r^3$ in $\mathcal{O}_{\sqrt{-3}}$ as $(m + n\sqrt{-3})(m - n\sqrt{-3}) = r^3$.
- Any common divisor of $m + n\sqrt{-3}$ and $m - n\sqrt{-3}$ must also divide $2m$ and $2n\sqrt{-3}$, and since m, n are relatively prime, this means the common divisor must divide $2\sqrt{-3}$.
- Since 2 and $\sqrt{-3}$ are irreducible in $\mathcal{O}_{\sqrt{-3}}$, we can see 2 does not divide $m + n\sqrt{-3}$ because m, n have opposite parities, and $\sqrt{-3}$ does not divide $m + n\sqrt{-3}$ because $3 \nmid m$.

Some More Diophantine Equations, IX

Proof (continued):

- So, $m+n\sqrt{-3}$ and $m-n\sqrt{-3}$ are relatively prime.
- Then since $\mathcal{O}_{\sqrt{-3}}$ is a UFD, we see that $m+n\sqrt{-3}$ must be a unit times a cube: say $m+n\sqrt{-3} = u\cdot(a+b\sqrt{-3})^3$. By negating, conjugating, and replacing $a+b\sqrt{-3}$ with an associate as necessary, we may assume $a, b \in \mathbb{Z}$ and that the unit u is either 1 or $\frac{-1+\sqrt{-3}}{2}$.
- However, if $m+n\sqrt{-3} = \frac{-1+\sqrt{-3}}{2}\cdot(a+b\sqrt{-3})^3$ then since m, n are integers, both a and b must be odd. But then $(-1+\sqrt{-3})(a+b\sqrt{-3})$ has integer coefficients that are even, as does $(a+b\sqrt{-3})^2$, so the product $m+n\sqrt{-3}$ would have both m and n even, contrary to assumption.
- Therefore, we must have $m+n\sqrt{-3} = (a+b\sqrt{-3})^3 = (a^3-9ab^2)+(3a^2b-3b^3)\sqrt{-3}$ and so $m = a^3-9ab^2$ and $n = 3a^2b-3b^3$, as claimed.

Some More Diophantine Equations, X

We can now essentially give Euler's treatment of the $n = 3$ case of Fermat's equation:

Theorem (Euler's $p = 3$ Case of Fermat's Theorem)

There are no solutions to the Diophantine equation $x^3 + y^3 = z^3$ with $xyz \neq 0$.

As with the $n = 4$ case that we did a month and a half ago, the idea is to use a descent argument: by assuming there is a nontrivial solution, we will construct a smaller solution, which yields a contradiction if we assume that we start with the solution having the minimal possible $|z|$.

Some More Diophantine Equations, XI

Proof:

- Assume $x, y, z \neq 0$ and suppose we have a solution to the equation with $|z|$ minimal.
- If two of x, y, z are divisible by a prime p then the third must be also, in which case we could divide x, y, z by p and obtain a smaller solution.
- Thus, without loss of generality, we may assume x, y, z are relatively prime, and so two are odd and the other is even.
- By rearranging and negating, suppose that x and y are odd and relatively prime. Set $x + y = 2p$ and $x - y = 2q$, so that $x = p + q$ and $y = p - q$, where p, q are necessarily relatively prime of opposite parity. We then obtain a factorization $z^3 = x^3 + y^3 = (x + y)(x^2 - xy + y^2) = 2p \cdot (p^2 + 3q^2)$.
- We now proceed in two cases: where $3 \nmid p$ and where $3|p$.

Some More Diophantine Equations, XII

Proof (Case $3 \nmid p$, Start):

- Suppose $3 \nmid p$. Since $p^2 + 3q^2$ is odd, any common divisor of $2p$ and $p^2 + 3q^2$ necessarily divides p and $p^2 + 3q^2$, hence also divides p and $3q^2$. Furthermore, since $3 \nmid p$ this means any common divisor of p and $3q^2$ divides both p and q^2, but these elements are relatively prime.
- Thus, $2p$ and $p^2 + 3q^2$ are relatively prime, so since their product is a cube, each must be a cube up to a unit factor in $\mathbb{Z}$, hence are actually cubes.
- By the lemma, we then have $p = a^3 - 9ab^2$ and $q = 3a^2b - 3b^3$ for some $a, b \in \mathbb{Z}$, and we also know $2p = 2a(a - 3b)(a + 3b)$ is a cube.

Some More Diophantine Equations, XIII

Proof (Case $3 \nmid p$, Finish):

- We have $p = a^3 - 9ab^2$ and $q = 3a^2b - 3b^3$ for some $a, b \in \mathbb{Z}$, and $2p = 2a(a-3b)(a+3b)$ is a cube.
- We see that $2a$, $a - 3b$, $a + 3b$ must be pairwise relatively prime, since any common divisor would necessarily divide $2a$ and $6b$ hence divide 6, but a cannot be divisible by 3 (since then p, q would both be divisible by 3) and a, b cannot have the same parity (since then both p, q would be even).
- Therefore, since their product is a cube in $\mathbb{Z}$, each of $2a$, $a - 3b$, and $a + 3b$ must be a cube in $\mathbb{Z}$. But then if $2a = z_1^3$, $a - 3b = x_1^3$, and $a + 3b = y_1^3$, we have $x_1^3 + y_1^3 = z_1^3$, and clearly we also have $0 < |z_1| < |a| < |r| < |z|$.
- We have therefore found a solution to the equation with a smaller value of z, which is a contradiction.

Some More Diophantine Equations, XIV

Proof (Case $3|p$, Start):

- The case $3|p$ is similar: write $p = 3s$ and note q, s are relatively prime of opposite parity with $z^3 = 18s \cdot (3s^2 + q^2)$.
- Since q cannot be divisible by 3 and $3s^2 + q^2$ is odd, any common divisor of $18s$ and $3s^2 + q^2$ must divide s and $3s^2 + q^2$ hence divides s and q^2, but these are relatively prime.
- Thus $18s$ and $3s^2 + q^2$ are relatively prime, so they are each cubes.
- By the lemma again, we have $q = a^3 - 9ab^2$ and $s = 3a^2b - 3b^3$, where $18s = 3^3 \cdot 2b(a-b)(a+b)$ is a perfect cube.

Some More Diophantine Equations, XV

Proof (Case $3|p$, Finish):

- We have $q = a^3 - 9ab^2$ and $s = 3a^2b - 3b^3$, where $18s = 3^3 \cdot 2b(a-b)(a+b)$ is a perfect cube.
- Like before, any common divisor of any pair of $2b$, $a-b$, $a+b$ must divide $2a$ and $2b$ hence divide 2, but a, b must have opposite parity since otherwise q, s would both be even.
- Thus, $2b$, $a-b$, and $a+b$ are all perfect cubes. But then if $a+b = z_1^3$, $a-b = x_1^3$, and $2b = y_1^3$, we have $x_1^3 + y_1^3 = z_1^3$, and clearly we also have $0 < |z_1| = |a+b| < |s| < |z|$.
- We have again found a solution to the equation with a smaller value of z, which is a contradiction. Since we have reached a contradiction in both cases, we are done.

Summary

We characterized the primes in $\mathcal{O}_{\sqrt{-3}}$, described how to compute factorizations in $\mathcal{O}_{\sqrt{-3}}$, and characterized the integers of the form $a^2 + ab + b^2$ and $a^2 + 3b^2$.

We solved some Diophantine equations using factorization in quadratic integer rings.

We established that the Fermat equation $x^3 + y^3 = z^3$ has no nontrivial integer solutions.

Next lecture: Cubic reciprocity.