Tsinghua MathCamp 2017
Number Theory Research Projects

Project 1

The goal of this project is to begin to find ways to understand and compensate for the lack of unique factorization in $\mathbf{Z}[\sqrt{-5}]$ and other rings $\mathbf{Z}[\sqrt{d}]$.

Before we even get started, let's think about the unique factorization theorem in $\mathbf{Z}$. If $n \in \mathbf{Z}$ is nonzero then we know n can be written uniquely as $n = up_1^{n_1}p_2n_2 \cdots p_k^{n_k}$ where $u = \pm 1$ and the p_i are positive primes with $p_1 \leq p_2 \leq \cdots \leq p_k$. We can then define the *valuation* of n at p_i to be the number $v_{p_i} = n_i$ to which p_i is raised in the factorization of n. This number is also sometimes called the *multiplicity* of p_i in n.

It is easy to see that for a prime $p \in \mathbf{Z}$ and $m, n \in \mathbf{Z}$ we have

$$v_p(mn) = v_p(m) + v_p(n).$$

In a sense this formula captures the essence of the uniqueness of factorization in $\mathbf{Z}$. It says that if we multiply two integers m and n together, then the number of factors of p in the product mn is the just the number of factors of p in m plus the number of factors of p in n. Compare this with the formula $(1+\sqrt{-5})(1-\sqrt{-5}) = 2 \cdot 3$ in $\mathbf{Z}[\sqrt{-5}]$ where the factor of 2 on the right side of this equation seems to come from nowhere.

Now, as a warm up, let's recall what we know about the primes in $\mathbf{Z}[i]$, where the arithmetic works very well. First of all, we have the unique factorization theorem, which says that given an element $\alpha \in \mathbf{Z}[i]$ which is neither a unit nor 0, there is an essentially unique way to write $\alpha = \pi_1\pi_2 \cdots \pi_k$ where $\pi_1, \pi_2, \ldots, \pi_k$ are each prime in $\mathbf{Z}[i]$. Here "essentially unique" means that the factorization is unique up to reordering the primes and multiplying them by units of $\mathbf{Z}[i]$. So for example, $8-i = (2+i)(3-2i)$ and $8-i = (2+3i)(1-2i)$ but this doesn't violate uniqueness since $1-2i = (-i)(2+i)$ and $2+3i = i(3-2i)$. Recall that two elements of $\mathbf{Z}[i]$ which are unit multiples of each other are called *associates*. So $1-2i$ and $2+i$ are associates.

We have seen

Lemma 1. *Every prime in $\mathbf{Z}[i]$ is an associate of one of the following:*

- *A prime $p \in \mathbf{Z}$ with $p \equiv 3 \pmod 4$*
- *$x+iy$ or $x-iy$ where $x^2+y^2 = p$ is a prime in $\mathbf{Z}$ with $p \equiv 1 \pmod 4$ and $0 < x < y$.*
- *$1+i$*

Moreover, no two primes on this list are associates of each other.

Let's look a little more closely at the second type of primes in the lemma. Let $p \in \mathbf{Z}$ be a prime congruent to 1 modulo 4 and let $p = x^2+y^2$ with $0 < x < y$. So we get two primes in $\mathbf{Z}[i]$, $\pi_1 = x+iy$ and $\pi_2 = x-iy$. Since $x^2+y^2 \equiv 0 \pmod p$ we have $(x/y)^2 \equiv -1 \pmod p$. Let's write s for the value of x/y modulo p. Then $s^2 \equiv -1 \pmod p$. Of course we also have $(-s)^2 \equiv -1 \pmod p$, and $s, -s$ are the only two solutions to the congruence $z^2 \equiv -1 \pmod p$.

Suppose now that you know the value of s, but don't know the values of x or y. For example, let's take $p = 7933$. You can check that $s = 4983$ is a square root of -1 modulo 7933, so there is a (unique) prime $\pi = x + iy$ in $\mathbf{Z}[i]$ with $x^2 + y^2 = 7933$, $0 < x < y$, and $x/y \equiv 4983 \pmod{7933}$. But that doesn't let you immediately figure out x and y. It *does* however give you a way of testing whether any given element $\alpha \in \mathbf{Z}[i]$ is a multiple of $x + iy$:

Problem 1. *Find a way of testing whether an element $\alpha = a+bi \in \mathbf{Z}[i]$ is a multiple of $x + iy$ if all you know are the values of $p = x^2 + y^2$ and $s \equiv x/y \pmod{p}$. In particular, your method* should not *involve finding values of x and y.*

Hint: You might want to start by imagining that you did know x and y and then see if you can rephrase your answer in a way that uses s instead of x and y.

Since we know the unique factorization theorem in $\mathbf{Z}[i]$ we can define v_π for a prime $\pi \in \mathbf{Z}[i]$ just as we did in $\mathbf{Z}$. In particular for nonzero $\alpha \in \mathbf{Z}[i]$ we define $v_\pi(\alpha)$ to be the power to which π, or an associate of π, appears in the prime factorization of α.

Problem 2. *Use your idea from Problem 1 to find a way to compute $v_\pi(\alpha)$ where $\pi = x + iy$ and $\alpha = a + bi$* without *using x and y but instead using only $s \equiv x/y \pmod{p}$.*

Remark 1. *Note that the prime $1 + i$ behaves similarly to the primes we just discussed. Think about how the previous discussion could be applied to $1 + i$.*

Problem 3. *Generalize everything above about $\mathbf{Z}[i]$ (including the lemma) to work for $\mathbf{Z}[\sqrt{-2}]$.*

Hint: For now replace the condition "$p \equiv 1 \pmod{4}$" with the condition "-2 is a square mod p." By the end of the course you'll even be able to replace that condition with a congruence on p, but you might not be able to do that until the end of the third week.

If we now try to carry this out for $\mathbf{Z}[\sqrt{-5}]$ we run into trouble even just listing the primes, since there are numbers like 3 for which -5 is a square but which don't factor in $\mathbf{Z}[\sqrt{-5}]$. The goal of this project is to find a way to work around this problem. With that in mind, let $p \in \mathbf{Z}$ be a prime such that -5 is square modulo p and let s and $-s$ be the square roots of -5 modulo p. Then we wish there were a prime $\pi_{p,s}$ such that $\pi_{p,s} = x + y\sqrt{-5}$ with $x^2 + y^2 = p$ and $(x/y) \equiv s \pmod{p}$. We know that our wish won't always come true, but we can always hope:

Problem 4. *Suppose $p \neq 2, 5$ is a prime in $\mathbf{Z}$ such that -5 is a square modulo p, and let $s, -s$ be the two square roots of -5 modulo p. Generalizing what you did for $\mathbf{Z}[i]$ and $\mathbf{Z}[\sqrt{-2}]$, give a condition on an element $\alpha = a + b\sqrt{-5} \in \mathbf{Z}[\sqrt{-5}]$ that will allow us to test whether or not $\pi_{p,s}$ divides α in $\mathbf{Z}[\sqrt{-5}]$* if *such a prime $\pi_{p,s} = x + y\sqrt{-5}$ with $x^2 + 5y^2 = p$ and $(x/y) \equiv s \pmod{p}$ exists.*

Again, your condition should not make explicit use of x or y, only s, α, and p.

Now for the fun part - even if we can't write $p = x^2 + 5y^2$ with x and y in $\mathbf{Z}$, so that there is no prime $\pi_{p,s}$, we *still* can apply your condition to an element α!

Definition 1. *We'll say that α is a* (p,s)-multiple *if the condition you gave in the previous problem holds for α.*

If we get lucky, and $\pi_{p,s}$ does happen to exist then obviously α is a multiple of $\pi_{p,s}$ if and only if α is a (p,s)-multiple. But it turns out this condition is useful even if there is no prime $\pi_{p,s}$.

Problem 5. *Let $p \neq 2, 5$ be a prime in $\mathbf{Z}$ such that -5 is a square modulo p, and let $s, -s$ be the two square roots of -5 modulo p. Let $\alpha \in \mathbf{Z}[i]$. Prove that p divides α in $\mathbf{Z}[\sqrt{-5}]$ if and only if α is (p,s)-multiple* and *α is a $(p,-s)$-multiple.*

This problem generalizes the fact that if p is an odd integer prime and $p = x^2+y^2$ then for $\alpha \in \mathbf{Z}[i]$ we have p divides α in $\mathbf{Z}[i]$ if and only if $x+yi$ and $x-yi$ both divide α.

Problem 6. *Let $p \neq 2, 5$ be a prime in $\mathbf{Z}$ such that -5 is a square modulo p, and let $s, -s$ be the two square roots of -5 modulo p. Let $\alpha, \beta \in \mathbf{Z}[i]$. Prove that if α is a (p,s)-multiple and β is a $(p,-s)$-multiple, then p divides $\alpha\beta$ in $\mathbf{Z}[\sqrt{-5}]$.*

Note that this problem does not *follow automatically from the previous one. Why not? You might chose to prove a lemma to connect them. (Or you can just prove this result directly without referring to the previous problem).*

Problem 7. *Use your solution to Problem 4 to define $v_{p,s}(\alpha)$ for $\alpha \in \mathbf{Z}[\sqrt{-5}]$. Here again $p \neq 2, 5$ is a prime in $\mathbf{Z}$ such that -5 is a square modulo p and s is a square root of -5 modulo p. In order for your definition to be reasonable, it should have a few good properties. First, it should behave well in the case where there actually* does *exist a prime $\pi_{p,s} = x+y\sqrt{-5} \in \mathbf{Z}[\sqrt{-5}]$ with $x^2+y^2 = p$ and $x/y \equiv s \pmod{p}$. In particular, in that case you should have that $v_{p,s}(\alpha) = k$ where $\pi_{p,s}^k | \alpha$ but $\pi_{p,s}^{k+1} \nmid \alpha$. Secondly, in any case we should have that $v_{p,s}(\alpha\beta) = v_{p,s}(\alpha) + v_{p,s}(\beta)$. Finally, the highest power of p that divides α in $\mathbf{Z}[\sqrt{-5}]$ should be the minimum of $v_{p,s}(\alpha)$ and $v_{p,-s}(\alpha)$. Prove that all of these properties in fact true.*

Problem 8. *Let $p \neq 2, 5$ be a prime in $\mathbf{Z}$ such that -5 is a square modulo p, and let $s, -s$ be the two square roots of -5 modulo p. Find a formula for $v_p(N(\alpha))$ in terms of $v_{p,s}(\alpha)$ and $v_{p,-s}(\alpha)$. Here $N(a)$ is the norm of α and $v_p(N(\alpha))$ is the usual multiplicity of p in $N(\alpha)$ as integers.*

Problem 9. *The situation for $p = 2$ is similar to what we have just been doing, except that there is only one value for s. Generalize everything above to work for $p = 2$ as well. (You'll need to modify some of the statements slightly in the $p = 2$ case.)*

Problem 10. *Let $p \neq 2, 5$ be a prime in $\mathbf{Z}$ such that -5 is a square modulo p and let s be a square root of -5 modulo p. We know that there might not be an element $\pi \in \mathbf{Z}[\sqrt{-5}]$ such that $N(\pi) = p$ and $v_{p,s}(\pi) = 1$. Prove that there always will be a $\pi \in \mathbf{Z}[\sqrt{-5}]$ such that $N(\pi) = p$ or $N(\pi) = 2p$. Prove that this π will be prime.*

Hint: Consider the elements of $\mathbf{Z}[\sqrt{-5}]$ as points in the complex plane and look at just those points that correspond to (p,s)-multiples. Now use Minkowski's theorem.

The primes $p \in \mathbf{Z}$ for which -5 is a square mod p come in two flavors. We'll say p is *visible* if there is an element in $\mathbf{Z}[\sqrt{-5}]$ of norm p and we'll say p is *invisible* if there is no such element. Note that 2 is invisible and 5 is visible.

Problem 11. *Let p, q be primes in $\mathbf{Z}$ such that -5 is a square modulo both p and q. Prove there exists an element of norm pq in $\mathbf{Z}[\sqrt{-5}]$ iff p and q are either both visible or both invisible.*

Problem 12. *Give a complete description of the set of prime elements in* $\mathbf{Z}[\sqrt{-5}]$. *Given an element* $\alpha \in \mathbf{Z}[\sqrt{-5}]$ *describe how to find* all *of the essentially inequivalent factorizations of* α *in* $\mathbf{Z}[\sqrt{-5}]$.

If you've gotten this far, and want to keep going, you should try to extend this to other cases of $\sqrt{-d}$ with $d < 0$. The case of $d = -163$ is especially interesting, but you'll have to be careful about the prime $p = 2$. You can also try looking at positive d - the tricky part there is finding the right way to generalize Problem 10. Have fun with it!

Project 2

The project will let you generalize and extend the description we've given of which integers n can be written in the form $n = x^2 + y^2$.

We'll start with a general definition. A *2-polynomial* is polynomial of the form $f(x, y) = ax^2 + bxy + cy^2$ with $a, b, c \in \mathbf{Z}$. We'll say an integer n is *represented* by $f(x, y)$ if there exist integers x and y such that $n = f(x, y)$. In that case, we also say $f(x, y)$ represents n.

Problem 1

Problem 1.1 Which integers n are represented by $x^2 + 2xy + 2y^2$? That is, for which n do there exist integers x and y such that $n = x^2 + 2xy + 2y^2$?

Here's some suggestions on how you might proceed. First check examples of small n to make a conjecture. Does your conjecture look familiar? Look carefully at the values of x and y that you find for each particular n and see how they relate to the earlier problem you are reminded of by your conjecture.

Problem 1.2 Let $f(x, y) = (x + 2y)^2 + (3x + 5y)^2 = 10x^2 + 34xy + 29y^2$. Which integers n be written as $n = f(x, y) = 10x^2 + 34xy + 29y^2$?

Problem 1.3 Give 3 more examples of 2-polynomials that represent the same integers are the 2-polynomials above.

Problem 1.4 Now you get to generalize. Give a definition for what you think it should mean to say that two 2-polynomials are equivalent. Prove that what you've given is actually an equivalence relation on the set of 2-polynomials .

Note: It is tempting define two 2-polynomials to be equivalent iff and only if they represent the same integers as each other. That isn't an unreasonable definition, but it turns out not to be the most useful. If you use that definition, you'll create more work for yourself later on.

Problem 2

Problem 2.1 Prove that if two 2-polynomials are equivalent then they represent exactly the same integers as each other. If that isn't true for your definitions, then you should go back and revise it!

Problem 2.2 Given a 2-polynomial $f(x, y) = ax^2 + bxy + cy^2$, we'll define the measure of f to be

$$m(f) = b^2 - 4ac.$$

Prove that if f and g are equivalent 2-polynomials then $m(f) = g(f)$. Again, if this isn't true for your definition, you'll need to go back and revise it!

A 2-polynomial with negative measure is called *definite*. If

$$f(x, y) = ax^2 + bxy + cy^2$$

is definite and $a > 0$ we say f is *positive definite*. We'll focus our attention on positive definite 2-polynomials for the rest of this project.

Problem 2.3 Prove that a positive definite 2-polynomial only represents positive integers.

Problem 2.4 Give an example of two positive definite 2-polynomials with the same measure that are *not* equivalent.

Problem 3

Problem 3.1 Consider the 2-polynomial $f(x, y) = 3x^2 + 2xy + 4y^2$. Find a 2-polynomial $g(x, y) = ax^2 + bxy + 4y^2$ with $a < 3$ which is equivalent to $f(x, y)$.

Problem 3.2 Now we're ready for a major result. Let $d < 0$. Prove that there are only finitely many equivalence classes of 2-polynomials with measure d.

Problem 4

Problem 4.1 Prove that any 2-polynomial of measure -4 is equivalent to $x^2 + y^2$.

Problem 4.2 Find a set of representatives of the equivalence classes of 2-polynomials of measure -20. How many are there?

Problem 4.3 Find sets of representative of the equivalence classes of 2-polynomials of measure d for each $0 > d \geq -24$. Note that for some d there are *no* 2-polynomials at all.

Problem 5

Problem 5.1 Prove that if a positive definite 2-polynomial of measure d represents a prime p then d is a square mod p.

Problem 5.2 The converse to the previous problem isn't true. Can you make a conjecture about how to represent p by 2-polynomials if you know d is a square mod p? Can you prove your conjecture?

Problem 5.3 Which integers are of the form $x^2 + 2y^2$? $x^2 + xy + y^2$? $x^2 + 3y^2$? $x^2 + xy + 2y^2$? $x^2+xy+3y^2$? $x^2+xy+5y^2$, $x^2+xy+11y^2$? $x^2+xy+17y^2$? $x^2 + xy + 41y^2$?

Problem 6

Problem 6.1 Make a conjecture about which integers are represented by x^2+5y^2. Prove your conjecture.

Problem 6.2 Make a conjecture about which primes are of the form $x^2 + 14y^2$. This is much trickier than the other examples we've looked at. Prove as much of your conjecture as you can.

Problem 6.3 Make a conjecture about which primes are of the form $x^2 + 23y^2$. This is even trickier than for x^2+14y^2. Can you prove any parts of your conjecture?