MATH7421 Problems Week 1

Solving Integer Problems using Commutative Rings

Some of the exercises below are meant to provide more tasters of the power of Algebraic Number Theory, as in Chapter 1 of the notes. The rest of the exercises tie up some of the loose ends in some of the arguments that we saw there. Since we haven't yet explored the full theory, you might find some of these tricky! However, trying to do them now will allow you to develop familiarity with the basic techniques and applications. You should return to these exercises later when you know more!

1. At the beginning of the notes we saw our first application of Algebraic Number Theory...we used the ring $\mathbb{Z}[\sqrt{-2}]$ and it's nice properties to find all integer solutions to the equation $y^2 = x^3 - 2$. Let's explore the integer solutions of a similar equation.

   (a) Show that there cannot exist a cube number that is exactly one more than a positive square number, i.e. the only integer solution to the equation $x^3 - y^2 = 1$ is $(x, y) = (1, 0)$.
   (Hint: Factor the equation over the ring $\mathbb{Z}[i]$ and use the properties given in the notes)

   (b) Is there a square number that is exactly one more than a positive cube number?

2. Verify the following claims about Pythagorean Triples from the notes:

   (a) If $x^2 + y^2 = z^2$ with $\gcd(x, y, z) = 1$ then $(x + iy)$ and $(x - iy)$ are coprime in $\mathbb{Z}[i]$
   (Hint: If $\alpha, \beta \in \mathbb{Z}[i]$ satisfy $\alpha|\beta$ then the integer $|\alpha|^2$ must divide the integer $|\beta|^2$).

   (b) Show that for every $k, s, t \in \mathbb{Z}$ with $k > 0$ and $s > t > 0$ the triple of integers:

   $$(x, y, z) = (k(s^2 - t^2), 2kst, k(s^2 + t^2))$$

   is a Pythagorean Triple.

3. Let p be an odd prime. In order to prove that a prime $p \equiv 1 \bmod 4$ is a sum of two squares, we needed to find $x \in \mathbb{Z}$ such that $x^2 \equiv -1 \bmod p$. Let's prove that this congruence has a solution!

   (a) Prove Wilson's Theorem, i.e. that $(p - 1)! \equiv -1 \bmod p$.
   (Hint: Every integer $1 \leq a \leq p - 1$ has a unique multiplicative inverse mod p. Use this to cancel terms from the product).

   (b) Use Wilson's Theorem to show that if $p \equiv 1 \bmod 4$ then the congruence $x^2 \equiv -1 \bmod 4$ has a solution. (Hint: Try the value $x = \left(\frac{p-1}{2}\right)!$).

4. In the notes we saw that a prime p is a sum of two squares if and only if p is reducible in $\mathbb{Z}[i]$, which happens if and only if $p = 2$ or $p \equiv 1 \bmod 4$. In this question we will prove the stronger statement that an integer $n \geq 1$ is sum of two squares if and only if every prime $p|n$ such that $p = 3 \bmod 4$ divides n to an even power.

   (a) Suppose that $n \geq 1$ and $n = x^2 + y^2$ for some $x, y \in \mathbb{Z}$. Show that if $p|n$ and $p \equiv 3 \bmod 4$ then actually $p^2|n$.

   (Hint: Factor the RHS and use the fact that p is irreducible in $\mathbb{Z}[i]$).

   (b) Show that $1 \leq \frac{n}{p^2} < n$ is also a sum of two squares. Hence use strong induction to prove the forward claim, i.e. if n is a sum of two squares then every prime $p|n$ such that $p \equiv 3 \bmod 4$ divides n to an even power.

   (c) Show that if $m, n \geq 1$ are both sums of two squares then so is their product mn.

   (d) Use this to show the reverse claim, i.e. if every prime $p|n$ such that $p \equiv 3 \bmod 4$ divides n to an even power then n is a sum of two squares.

5. Let p be an odd prime such that $p \equiv 1, 3 \bmod 8$. It's then a fact that the congruence $x^2 \equiv -2 \bmod p$ has a solution (if you know about Legendre symbols and Quadratic Reciprocity then you should be able to prove this!).

   Use this fact to show that a prime p can be written as $p = x^2 + 2y^2$ if and only if $p = 2$ or $p \equiv 1, 3 \bmod 8$.

   (Hint: Adapt the proof in the notes but use the ring $\mathbb{Z}[\sqrt{-2}]$ instead. Assume for now that this ring has unique factorisation (as mentioned in the notes)).

6. Let $N \geq 1$. Based on the limited evidence so far, you might be tempted (as Euler was!) to conjecture that a prime p can be written as $p = x^2 + Ny^2$ if and only if there is a solution to the congruence $x^2 \equiv -N \bmod p$. However, this is not true!

   (Although more advanced techniques in Algebraic Number Theory can be used to completely solve this problem).

   (a) Show that there is a solution to the congruence $x^2 \equiv -5 \bmod 3$, but that 3 cannot be written as $x^2 + 5y^2$.

   (b) Show that 3 is irreducible in the ring $\mathbb{Z}[\sqrt{-5}]$.

   (Hint: the units in $\mathbb{Z}[\sqrt{-5}]$ are ± 1 and these are exactly the solutions to $|\alpha|^2 = 1$).

   (c) What is the issue? Where does the proof in the notes go wrong?

7. (a) In the notes we saw that (x, y) is an integer solution to the Pell eqution $x^2 - 2y^2 = \pm 1$ if and only if $x + y\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ is a unit. Given that the units of this ring are all of the form $\pm(1 + \sqrt{2})^n$ for $n \in \mathbb{Z}$, show that all solutions to this Pell equation are of the form $(\pm a, \pm b)$, where (a, b) is a term in the recursion $(a_{n+1}, b_{n+1}) = (a_n + 2b_n, a_n + b_n)$ with starting value $(a_0, b_0) = (1, 0)$.

   (b) Use this recursion to compute four positive integer solutions to the equation.

Polynomials, Roots and Irreducibility

1. (a) Prove the Rational Root Test, i.e. if $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n \in \mathbb{Z}[x]$ is non-zero then every rational root $a = \frac{b}{c} \in \mathbb{Q}$ satisfies $b \mid a_0$ and $c \mid a_n$.

   (b) Show that the polynomial $x^3 + 3x + 1 \in \mathbb{Q}[x]$ has no rational roots. Is it irreducible?

   (c) Show that the polynomial $x^4 - 4 \in \mathbb{Q}[x]$ has no rational roots. Is it irreducible?

2. Let $f(x) \in \mathbb{Z}[x]$ be monic. Show that every rational root of $f(x)$ is an integer.

3. Let $f(x) \in \mathbb{Z}[x]$ be monic and suppose that there exists a factorisation $f(x) = g(x)h(x)$ with $g(x), h(x) \in \mathbb{Q}[x]$ also monic. Show that actually $g(x), h(x) \in \mathbb{Z}[x]$.

   (Hint: Read the proof of Gauss' Lemma, how do the pairs of polynomials $g(x), h(x)$ and $s(x), t(x)$ compare?).

4. Use Eisenstein's Criterion to show that the following polynomials are irreducible over $\mathbb{Q}$:

   (a) $x^5 + 14x^4 - 35x^3 + 70x^2 + 28x - 56$.

   (b) $9x^3 - 11x + 44$

5. (a) Let $f(x) \in \mathbb{Q}[x]$. Show that $f(x)$ is reducible if and only if $f(x + a)$ is reducible for every $a \in \mathbb{Q}$.

   (b) Hence show that the polynomial $x^4 + 4x + 1 \in \mathbb{Q}[x]$ is irreducible. (Hint: We know that $\phi_p(x) = \frac{x^p-1}{x-1}$. Is there a nice linear substitution you can use?)

6. Let p be prime and consider the polynomial $f_p(x) = x^p - 1 \in \mathbb{Q}[x]$.

   (a) Show that $f_p(x) = (x - 1)(x^{p-1} + x^{p-2} + ... + x + 1)$, so that $f_p(x)$ is reducible.

   (b) Show that the factor $\phi_p(x) = x^{p-1} + x^{p-2} + ... + x + 1 \in \mathbb{Q}[x]$ is irreducible.
   (Hint: Eisenstein's Criterion).

   (c) Is it true that $x^{n-1} + x^{n-2} + ... + x + 1 \in \mathbb{Q}[x]$ is irreducible for every $n \geq 2$?

7. Show that a non-constant irreducible polynomial $f(x) \in \mathbb{Q}[x]$ cannot have a repeated root in $\mathbb{C}$. (Hint: Consider the factorisation of $f(x)$ and the derivative $f'(x)$)