UNIQUE FACTORIZATION AND FERMAT'S LAST THEOREM
HOMEWORK 1

Problem 1 (Pythagorean Triples). In this problem you will find all Pythagorean triples, i.e., all integer solutions to the equation

$$x^2 + y^2 = z^2$$

with $xyz \neq 0$. The solution will be used in the next problem, but you can skip this problem if you like since it's tangential to the lectures (although it's really quite pretty). Given such a solution (x, y, z), we can write $(x/z)^2 + (y/z)^2 = 1$, and hence $(x/z, y/z)$ is a point on the unit circle

$$S^1 = \{\vec{v} \in \mathbf{R}^2 \ : \ |\vec{v}| = 1\}$$

with rational (**Q**-valued) coordinates; such a point is called a *rational point*. So our first step will be to determine all of the rational points on S^1. In order to do this, we will define an invertible map between $\mathbf{R}$ and $S^1 \setminus \{N\}$, where $N = (0, 1)$ is the "north pole".

(i) Define $\varphi : \mathbf{R} \to S^1 \setminus \{N\}$ as follows. Given $t \in \mathbf{R}$, let L be the line through $(t, 0)$ and N. Prove that L intersects S^1 in exactly one other point

$$(x, y) = \left(\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1}\right).$$

Set $\varphi(t) = (x, y)$. Prove that φ is bijective (one-to-one and onto), and calculate $\varphi^{-1}(x, y)$ for $(x, y) \in S^1 \setminus \{N\}$. Show that φ^{-1} takes rational points on $S^1 \setminus \{N\}$ to rational numbers, so that φ restricts to a bijection between **Q** and the set of rational points on $S^1 \setminus \{N\}$.

(ii) Let (x, y, z) be a Pythagorean triple. Briefly explain why, when classifying Pythagorean triples, we may assume that x, y, z are pairwise coprime (that is, the greatest common divisor of any two is 1). Such a triple is called *primitive*. Assuming therefore that (x, y, z) is primitive, prove that exactly one of x, y is even, and that z is odd (hint: examine the equation $x^2 + y^2 \equiv z^2 \pmod 4$).

(iii) Again let (x, y, z) be a primitive Pythagorean triple, and assume that x is even, so that y and z are odd. As $(x/z)^2 + (y/z)^2 = 1$, we have from part (i) that there exists $t = p/q$ such that $(x/z, y/z) = \varphi(t)$. Rewriting, we have

$$\frac{x}{z} = \frac{2pq}{p^2+q^2} \qquad \frac{y}{z} = \frac{p^2-q^2}{p^2+q^2}.$$

We may of course assume that p and q are coprime. Prove that p and q have opposite parity (i.e. that one is odd and the other is even), and that $2pq$ is prime to $p^2 + q^2$. Conclude that

(1.1)
$$x = 2pq \qquad y = p^2 - q^2 \qquad z = p^2 + q^2.$$

(iv) Conversely, prove that if p and q are relatively prime nonzero integers with opposite parity, and if we define (x, y, z) using the equations (1.1), then (x, y, z) is a primitive Pythagorean triple.

Problem 2 (Fermat's Last Theorem for $n = 4$). In this problem you will prove that there are no solutions to the equation

$$x^4 + y^4 = z^2 \tag{2.1}$$

in nonzero integers x, y, z. This implies that Fermat's Last Theorem is true for $n = 4$ (why?). Note that if there exists a solution to (2.1), then there exists such a solution with $x, y, z > 0$.

(i) Let (x, y, z) be a solution to (2.1) with $x, y, z > 0$, and assume that with $z \geq 1$ is *minimal* among all such solutions. Show that x, y, z are pairwise coprime. As $(x^2)^2 + (y^2)^2 = z^2$, we may apply Problem 1. After possibly permuting x and y, we can find coprime nonzero integers p, q of opposite parity such that

$$x^2 = 2pq \quad y^2 = p^2 - q^2 \quad z = p^2 + q^2.$$

We may assume that p and q are positive. By examining the above equations modulo 4, show that q is is even, say $q = 2q'$. Prove that p and q' are squares, say $p = a^2$ and $q' = b^2$.

(ii) Show that y is prime to p and q. Applying Problem 1 to the equation $y^2 + q^2 = p^2$, we get that there are relatively prime nonzero c, d such that

$$y = c^2 - d^2 \quad q = 2cd \quad p = c^2 + d^2. \tag{2.2}$$

Show that c and d are again squares, say $c = x'^2$ and $d = y'^2$.

(iii) Since $p = a^2$, the equation (2.2) gives an equation $a^2 = x'^4 + y'^4$. Show that $a < z$, contradicting the minimality of z.

The above method of choosing a minimal solution to an equation, then showing that there must exist a smaller solution, was invented by Fermat, and is known as *infinite descent*. (Fermat would have chosen any solution and found a smaller one, then remarked that such a pattern could not continue indefinitely.) In fact the above argument is based on Fermat's own proof of this fact.

Problem 3 (Roots of Unity). In this problem you will prove some of the basic properties of the roots of unity. Let $n \geq 2$ be an integer.

(i) Prove that there are exactly n complex numbers ζ such that $\zeta^n = 1$. Such a complex number is called an *nth root of unity*.

(ii) Let $\boldsymbol{\mu}_n = \{\zeta \in \mathbf{C} : \zeta^n = 1\}$. Prove that $\boldsymbol{\mu}_n$ is a group under multiplication of complex numbers. In other words, show that:
   (1) $1 \in \boldsymbol{\mu}_n$,
   (2) if $\zeta, \zeta' \in \boldsymbol{\mu}_n$ then $\zeta\zeta' \in \boldsymbol{\mu}_n$, and
   (3) if $\zeta \in \boldsymbol{\mu}_n$ then $\zeta^{-1} \in \boldsymbol{\mu}_n$.

(iii) Show that $\boldsymbol{\mu}_n$ is a *cyclic* group. In other words, show that there exists $\zeta \in \boldsymbol{\mu}_n$ such that

$$\boldsymbol{\mu}_n = \{1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\}.$$

(iv) An nth root of unity ζ as in (iii) is called a *generator*. How many generators does $\boldsymbol{\mu}_n$ have? Write them all down.

(v) Factor the bivariate polynomial $X^n + Y^n$ as a product of homogeneous linear polynomials (polynomials of the form $aX + bY$ for $a, b \in \mathbf{C}$).

Problem 4 (Prime Factorization). This problem is meant to make you think carefully about how to prove the existence and uniqueness of prime factorization of ordinary integers, since we will soon be factoring more interesting numbers.

(1) Show that any positive integer a can be written as a product $p_1 \cdots p_n$ of (not necessarily distinct) prime numbers.

(2) In class we showed, using only division with remainder, that if p is a prime number and $p|ab$, then $p|a$ or $p|b$. Using only this fact, prove that the prime factorization in (i) is unique, in that if

$$a = p_1 \cdots p_n = q_1 \cdots q_m$$

where the p_i, q_j are (not necessarily distinct) prime numbers, then $n = m$ and one can reorder $(p_1, \ldots, p_n)$ to obtain $(q_1, \ldots, q_n)$.