

MATH 4400/6400
HOMEWORK 1
DUE 1/24/08

Instructions: Math 6400 students should do all the problems. Math 4400 students should do the first six problems (except for 5(d)), and any two of the last three problems.

Problem 1: Let p and q be primes. Show that $pq + 1$ is a perfect square if and only if p and q are twin primes.

Problem 2: Let a and n be positive integers ≥ 2 .

(a) Show that if $a^n - 1$ is prime, then $a = 2$ and n is prime. Give a counterexample to the converse. (A good calculator might help for this last part.)

(b) Show that if $2^n + 1$ is prime, then n is a power of 2. (We remarked in class that $n = 2^5$ is in fact a counterexample to the converse; indeed, Euler was the first to notice, in 1732, that $2^{2^5} + 1 = 4294967297 = 6700417 \cdot 641$.)

Problem 3: Let $f(n)$ be a polynomial with integer coefficients. Show that $f(n)$ cannot be prime for all positive integers n . Here's an example: $n^2 - n + 41$ is prime for lots of small values of n ; but not all of them! Why not? Can you use this idea to prove the general result? (Careful; sometimes you might need to change variables.)

Problem 4: Let a and b be integers, $b \neq 0$.

(a) Show that there exist integers q, r_0, ϵ such that

$$a = bq + \epsilon r_0, \quad 0 \leq r_0 \leq b/2, \quad \epsilon = \pm 1.$$

Show that r_0 is uniquely determined by a and b , that q is uniquely determined by a and b unless $r_0 = b/2$, and that ϵ is uniquely determined by a and b unless $r_0 = 0$ or $b/2$.

(b) Further, show that

$$\epsilon = (-1)^{\lfloor \frac{2a}{b} \rfloor}.$$

(You may assume that $r_0 \neq 0$ or $b/2$, because otherwise you can take ϵ to be whatever you want!)

Remark: We will refer to this as the *modified division algorithm*, and we will use it later in a somewhat unexpected context.

Problem 5: This problem deals with the Diophantine equation $x^2 + y^2 = 2z^2$. As before, we call a solution *trivial* when $xyz = 0$, and *primitive* when x, y, z are all positive integers with no common factor. From now on, we'll let (x, y, z) be a primitive solution.

(a) To warm up, show that x, y, z are all odd.

(b) I'll write down a few primitive solutions other than $(1, 1, 1)$:

$$(1, 7, 5), (7, 17, 13), (7, 23, 17), (17, 31, 25), (1, 41, 29), (23, 47, 37), (31, 49, 41).$$

Compare with a list of primitive Pythagorean triples, ordered by size of the hypotenuse. What patterns do you see? Make some conjectures.

(c) Prove your conjectures. In particular, you should be able to exhibit a very nice, very explicit bijection between the set of primitive Pythagorean triples and the set of primitive solutions to $x^2 + y^2 = 2z^2$. (Yes, yes, there is a bijection between these two sets because they're both infinite and countable! But you can do a little better than that.)

(d) Try to do part (b) and (c) for $x^2 + y^2 = 5z^2$. See what you can say about $x^2 + y^2 = az^2$, in general. (Obviously this problem is quite open-ended!)

Problem 6: Now let's attack the equation $x^2 + 2y^2 = z^2$. Again, apply the same definitions of trivial and primitive. Let x, y, z be a primitive solution.

(a) To warm up, show that x and z are odd and y is even.

(b) Show that either

$$(x, y, z) = (u^2 - 2v^2, 2uv, u^2 + 2v^2) \text{ or } (x, y, z) = (2u^2 - v^2, 2uv, 2u^2 + v^2)$$

where u and v are relatively prime positive integers. (There are two ways to do this problem, just like there were two ways to characterize PPT's.)

Problem 7: (a) Let n be a positive integer. Give criteria, based on the prime factorization of n , that are necessary and sufficient for n to be a sum of two integer squares. (Hint: See Exercise 4.3.15 in Prof. Shifrin's book *Abstract Algebra*.)

(b) Give a formula for $r_2(n)$ = the number of representations of n as a sum of two squares. I've been a bit vague about what a "representation" is, so give a definition that eliminates redundancy as much as possible; e.g. $r_2(5)$ should be 1.

Problem 8: (a) Find all the integer solutions to the equation $y^2 = x^3 - 1$. (Hint: bring the 1 over to the other side, and work in $\mathbb{Z}[i]$. What is the gcd of $y + i$ and $y - i$?)

(b) (Fermat) Find all the integer solutions to the equation $y^2 = x^3 - 4$. (Hint: work in $\mathbb{Z}[i]$, and you should be careful to remember that 2 is not irreducible; it is a unit times $(1 + i)^2$.)

Problem 9: (a) Recall the five facts about the integers we discussed in class (division algorithm, PID, gcd properties, Euclid's lemma, unique factorization). Show that (with the obvious modifications) they all hold in $\mathbb{Z}[\sqrt{-2}]$. (Hint: try to copy the "standard" proof of the division algorithm in $\mathbb{Z}[i]$.)

(b) (Fermat) Find all the integer solutions to the equation $y^2 = x^3 - 2$. (Hint: bring the 2 over to the other side, and use part (a).)