

MATH 4400/6400
HOMEWORK 1
COMMENTS AND SOLUTIONS

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.

Solution: If p and q are twin primes, say $q = p + 2$, then it is easy to see that $pq + 1 = (p + 1)^2$. On the other hand, suppose $pq + 1 = r^2$. Then $pq = (r - 1)(r + 1)$. Considering prime factorizations, it is clear that p divides one of the factors on the right, and q the other factor. But then p and q have to equal those respective factors. So p and q differ by 2. \square

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.)

Solution: (a) Clearly $(a - 1)|(a^n - 1)$, so this gives a nontrivial factor of $a^n - 1$ unless $a = 2$. So if $a^n - 1$ is prime, then $a = 2$. But if $b|n$, $b \neq 1$, $b \neq n$, then $(2^b - 1)|(2^n - 1)$; and so $2^n - 1$ will not be prime in that case either. So if $2^n - 1$ is prime, n is prime.

However, $2^{11} - 1$ is composite, equal to $23 \cdot 89$. Remark: if $p \equiv 3 \pmod{4}$, and $2p + 1$ is prime, then $(2p + 1)|2^p - 1$. We will be able to prove this soon.

(b) Write $n = 2^a b$ where b is odd. I claim that $2^{2^a} + 1$ divides $2^n + 1$. To see this, note that $(x + 1)|x^b + 1$ for any x (a fact you can establish by realizing that $x \equiv -1 \pmod{x + 1}$), so just let $x = 2^{2^a}$.

So this gives a nontrivial factor of $2^n + 1$, unless $b = 1$. \square

Problem 3: Let $f(n)$ be a polynomial with integer coefficients. Show that $f(n)$ cannot be prime for all n . Here's an example: $n^2 - n + 41$ is prime for lots of small values of n ; but not all of them! Can you generalize this? Be careful about your generalization. (You might need to change variables.)

Solution: If the constant term c_0 of $f(n)$ is not ± 1 or 0, then we can use the fact that $c_0|f(kc_0)$ for all integers k ; as k grows, we know that $|f(kc_0)| \rightarrow \infty$. In particular, eventually it gets bigger than $|c_0|$ itself. So for sufficiently large k , c_0 is a nontrivial divisor of $f(kc_0)$.

What do we do if $c_0 = \pm 1$ or 0? We consider $f(n + a)$, where a is any integer. If the constant term of this polynomial, considered as a polynomial in n , is not ± 1 or 0, then we can apply the above paragraph to $f(n + a)$ to conclude what we want about $f(n)$. But again, $|f(x)| \rightarrow \infty$ as x grows, so take a sufficiently large so that the absolute value of $f(a)$ (which is the constant term of $f(n + a)$) is at least 2. This change of variables allows us to reduce to the above paragraph. \square

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.

Solution: (a) Write $a = bq' + r$, with $0 \leq r < b$. If $r \leq b/2$, then we can take $\epsilon = 1$, $q = q'$, $r_0 = r$. If $r > b/2$, then we can take $\epsilon = -1$, $r_0 = b - r$, $q = q' + 1$. As for uniqueness, suppose there are two different choices $(\epsilon_1, r_{01}, q_1)$ and $(\epsilon_2, r_{02}, q_2)$. Then we get

$$b(q_1 - q_2) = \epsilon_2 r_{02} - \epsilon_1 r_{01},$$

and clearly the absolute value of the right side is at most b . It equals b only when r_{02} and r_{01} are both equal to $b/2$ (and the ϵ_i and q_i are different). Otherwise the difference is 0, so $q_1 = q_2$, and the only way any choices can be different is if r_{02} and r_{01} are both 0 but the ϵ_i are different (and the q_i are the same).

(b) Assume $r_0 \neq 0$ or $b/2$. In general, we have

$$\frac{2a}{b} = 2q + \epsilon(2r_0).$$

If $\epsilon = 1$, then $\lfloor \frac{2a}{b} \rfloor = 2q$; and if $\epsilon = -1$, then clearly $\lfloor \frac{2a}{b} \rfloor = 2q - 1$. So there you go. \square

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!)

Solution: (a) If x and y are both even, then z is as well, which contradicts primitivity. And if exactly one of x and y is odd, then $2z^2$ is odd, which is absurd. So x and y are odd. Now look mod 4, to see that $2z^2 \equiv 2 \pmod{4}$, so that z is odd.

(b) In the definitions here, I should probably have called $(1, 1, 1)$ a trivial solution. Let's pretend I did that. Anyway, I'll prove what I can in part (c).

(c) The main result is that there is a bijection between PPTs (x, y, z) and primitive solutions (a, b, c) to our equation. Assume $x < y$ and $a < b$ (note if $a = b$, then $c = a$, so we're back to the trivial solution $(1, 1, 1)$). Now the bijection proceeds as follows: $a = y - x$, $b = y + x$, $c = z$; and the other direction is $x = (b - a)/2$, $y = (b + a)/2$, $z = c$. Once you've written it down, it's clear that this gives a bijection between solutions to the Pythagorean equation and solutions to our equation (the maps are inverses of each other). Maybe the only thing to check is that it preserves primitivity. Clearly $\gcd(y - x, y + x, z)$ is either 1 or 2 (why?), and it can't be 2 because $y - x$ and $y + x$ are both odd. On the other hand, anything dividing $(b - a)/2$, $(b + a)/2$, and c must divide a, b, c , but these have no common factor, so there you go.

(d) This is a more difficult problem, even for $a = 5$. In general, one Pythagorean triple gives rise to exactly two primitive solutions to $x^2 + y^2 = 5z^2$. The key fact seems to be that 5 can be written as the norm of two non-associate elements of $\mathbb{Z}[i]$, whereas 2 can only be written as the norm of one such element. I'll let you work out the details. \square

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.)

Solution: (a) If x is even and z is even, then $2y^2$ is divisible by 4, so y is even, which contradicts primitivity. Now if exactly one of x and z is odd, we get $2y^2$ is odd, which is absurd. So x and z are both odd. But looking at the equation mod 4 gives that $2y^2$ is divisible by 4, so y is even.

(b) Let's do it the geometric way. Let $X = x/z$, $Y = y/z$, and consider the point $(-1, 0)$ on $X^2 + 2Y^2 = 1$. Let m be a positive real number less than $1/\sqrt{2}$, so that the line with slope m through $(-1, 0)$, which is $Y = m(X + 1)$, hits the ellipse in the first quadrant. Then we get

$$X^2 + 2m^2(X + 1)^2 = 1,$$

which leads to

$$((2m^2 + 1)X + (2m^2 - 1))(X + 1) = 0$$

so the solution we want is $X = \frac{1 - 2m^2}{1 + 2m^2}$, $Y = \frac{2m}{1 + 2m^2}$. Let $m = a/b$ in lowest terms; note that $b^2 - 2a^2 > 0$. Then we get

$$\frac{x}{z} = \frac{b^2 - 2a^2}{b^2 + 2a^2}, \quad \frac{y}{z} = \frac{2ab}{b^2 + 2a^2}.$$

This corresponds to a solution $(b^2 - 2a^2, 2ab, b^2 + 2a^2)$. It remains only to consider primitivity. Any odd prime dividing all three of these elements must divide both a and b (check this!), which is absurd. So the gcd of these three elements is 1 or a power of 2. It's 1 if b is odd,

which leads to the first parameterization given in the problem. If b is even, write $b = 2k$, and then divide by 2 to get $(2k^2 - a^2, 2ka, 2k^2 + a^2)$; note that a is odd, so this is primitive. This gives the second parameterization. \square

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.

Solution: (a) The criterion is that if p is a prime congruent to 3 mod 4 dividing n , then p must appear to an even power. Clearly this is sufficient, because if this is true then n can be written as $(p_1 \cdots p_k)a^2$, where p_i are all 1 mod 4; then all the p_i can be written as sums of two squares and $a^2 = a^2 + 0^2$, so the result follows from the multiplicativity formula for sums of two squares (that is, if x and y are sums of two squares, then so is xy). Now to prove necessity.

Suppose n is the sum of two squares; then it is the norm of some element $\alpha = (\pi_1 \cdots \pi_c)(p_1 \cdots p_d)$. Here the π_i are irreducible elements of $\mathbb{Z}[i]$ with prime norm equal to 2 or congruent to 1 mod 4; the p_i are integer primes congruent to 3 mod 4. Note that $\bar{\alpha} = (\bar{\pi}_1 \cdots \bar{\pi}_c)(p_1 \cdots p_d)$. Multiplying, we get

$$n = \alpha\bar{\alpha} = (N(\pi_1) \cdots N(\pi_c))(p_1^2 \cdots p_d^2).$$

This is the prime factorization of n . There you have it—all the primes congruent to 3 mod 4 appear with an even power.

(b) Look up Jacobi's Two Square Theorem on the internet! \square

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 $(1 + i)^2$.)

Solution: (a) We get $(y + i)(y - i) = x^3$ in $\mathbb{Z}[i]$. Now note that if y is odd, then $y^2 + 1 \equiv 2 \pmod{4}$, so it cannot be a cube. Thus y is even (and x is odd). Now if α is a common divisor of $y + i$ and $y - i$, it divides $2i$. Then either α is a unit or its norm is even. But its norm cannot be even because $N(y + i)$ is odd. Hence $y + i$ and $y - i$ are relatively prime. Thus $y + i$ is a cube. Write $(a + bi)^3 = y + i$. Compare imaginary parts. Get $3a^2b - b^3 = 1$. So $b(3a^2 - b^2) = 1$. Hence $b = \pm 1$ and $3a^2 - 1 = \pm 1$. The only solution is $a = 0$, $b = -1$, which leads to $y = 0$. Hence $(1, 0)$ is the unique solution to the equation.

(b) We get $(y + 2i)(y - 2i) = x^3$ in $\mathbb{Z}[i]$. A common divisor of $y + 2i$ and $y - 2i$ must divide $4i$. If y is odd, then the same norm argument as above shows that this common divisor must be 1, and we get that $y + 2i$ is a cube. Suppose that y is even. Write $y = 2k$. Get $4(k + i)(k - i) = x^3$. If k is even, then $k + i$ and $k - i$ are relatively prime and neither of them are divisible by $1 + i$, which is impossible. (Look at the powers of $1 + i$ appearing on both sides.) So k is odd, and $k + i$ and $k - i$ are both divisible by exactly one power of $1 + i$. (The norm of $k + i$ is 2 mod 4.) The upshot is that $(k + i)/(1 + i)$ and $(k - i)/(1 - i)$ are relatively prime, and since their product is $(x/2)^3$, they are both cubes. Hence again $y + 2i$ is a cube.

Now write $(a+bi)^3 = y+2i$. Compare imaginary parts: $b(3a^2 - b^2) = 2$. If $b = 2$, $3a^2 = 5$, so no solution. If $b = -1$, then $3a^2 = -1$, so no solution. If $b = 1$, then $a^2 = 1$, so we get $y+2i = (\pm 1+i)^3 = \mp 2+2i$. If $b = -2$, then $a^2 = 1$, so we get $y+2i = (\pm 1-2i)^3 = \mp 11+2i$. So now we've got a total of four solutions: $(2, \pm 2)$ and $(5, \pm 11)$. \square

Problem 9: (a) Recall the five facts about the integers 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).)

Solution: (a) What we must do is give a division algorithm in $\mathbb{Z}[\sqrt{-2}]$. Here we have $N(a + b\sqrt{-2}) = |a + b\sqrt{-2}|^2 = a^2 + 2b^2$. The norm is still multiplicative. Now consider $\alpha, \beta \in \mathbb{Z}[\sqrt{-2}]$. Then let $q \in \mathbb{Z}[\sqrt{-2}]$ be the closest element to α/β . We get that

$$\left| \frac{\alpha}{\beta} - q \right|^2 \leq \left(\frac{1}{2} \right)^2 + 2 \left(\frac{1}{2} \right)^2 = \frac{3}{4}.$$

Then let $r = \alpha - \beta q$. The above inequality implies that $N(r) \leq \frac{3}{4}N(\beta)$. This is good enough! (Notice that this proof method stops working in $\mathbb{Z}[\sqrt{-d}]$ as soon as d gets bigger than 2.) The rest of the usual statements follow from this division algorithm. In part (b) we will use unique factorization.

(b) If y is even, then $x^3 \equiv 2 \pmod{4}$, which is impossible. So y is odd. Now we get $(y + \sqrt{-2})(y - \sqrt{-2}) = x^3$. The gcd of $y + \sqrt{-2}$ and $y - \sqrt{-2}$ divides $2\sqrt{-2}$, so it either has even norm or is a unit. But it can't have even norm because $y + \sqrt{-2}$ has odd norm. So $y + \sqrt{-2}$ and $y - \sqrt{-2}$ are relatively prime. Thus they're both cubes. Write $(a + b\sqrt{-2})^3 = y + \sqrt{-2}$ and compare imaginary parts. Get $3a^2b - 2b^3 = 1$, or $b(3a^2 - 2b^2) = 1$. Clearly $b = 1$ and $a = \pm 1$. Then $(\pm 1 + \sqrt{-2})^3 = \mp 5 + \sqrt{-2}$, and we get the two solutions $(3, \pm 5)$. \square