PUTNAM PROBLEM SOLVING SEMINAR WEEK 2

The Rules. You are not allowed to try a problem that you already know how to solve. These are way too many problems to consider. Just pick a few problems in one of the sections and play around with them.

The Hints. Try small cases. Do examples. Look for patterns. Draw pictures. Use lots of paper. Talk it over. Choose effective notation. Look for symmetry. Divide into cases. Work backward. Argue by contradiction. Consider extreme cases. Eat pizza. Modify the problem. Generalize. Don't give up after five minutes. Don't be afraid of a little algebra. Sleep on it if need be. And ask!! If the problem has a 2001 in it, what happens if you replace 2001 by 1, or 2, or 3? What's important about 2001 — is it that it is odd, or divisible by 3, etc.?

Useful facts, in a nutshell. Mod. Unique factorization. s and t are relatively prime if and only if you can find a and b such that $as + bt = 1$. Fermat's Little Theorem $a^p \equiv a \pmod{p}$. A7(b) and (c) below. Wilson's Theorem $(p-1)! \equiv 1 \pmod{p}$. The Chinese Remainder Theorem: solving a bunch of equations modulo n is the same as solving it modulo its prime power factors, e.g. $x \equiv 17 \pmod{100}$ is the same as $x \equiv 17 \pmod{4}$ and $x \equiv 17 \pmod{25}$. *More serious stuff:* If $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$, where $\phi(n)$ is Euler's ϕ-function — it is the number of integers between 1 and n that are relatively prime to n. $\phi(n) = n(1 - 1/p_1)(1 - 1/p_2) \cdots (1 - 1/p_k)$ where $p_1, \ldots, p_k$ are the prime factors of n. Hensel's Lemma: roughly, the reason you know you can solve $x^2 \equiv -2 \pmod{3^n}$ for all n. Primitive roots of n: generators of the group $(\mathbb{Z}/n\mathbb{Z})^*$ (e.g. show that 2 is a primitive root $\pmod{3^n}$ for all n).

The Problems. *The first problems relate to the introductory number theory mini-lecture.*

A1. (a) Find integers x and y such that $754x + 221y = \gcd(754, 221)$. (b) Prove that $(a + b)/(c + d)$ is irreducible if $ad - bc = 1$. (c) Prove that the fraction $(21n + 4)/(14n + 3)$ is irreducible for every natural number n.

A2. (a) If $\gcd(a, b) = 1$, prove that $\gcd(a-b, a+b) \leq 2$, (b) $\gcd(a-b, a+b, ab) = 1$, (c) $\gcd(a^2 - ab + b^2, a + b) \leq 3$.

A3. (a) Prove that some positive multiple of 21 has 241 as its final three digits. (b) What are the last two digits of 3^{1234}?

A4. Suppose a, b, c, d, and m are integers, and $m \neq 0$. If $(a - b)/m$ and $(c - d)/m$ are integers, show that $(ac - bd)/m$ is also an integer. (This is the proof

Date: October 16, 2001.

that if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$ — so you aren't allowed to use this fact!)

A5. (a) Show that a perfect square must leave a remainder of 0, 1, or 4 upon division by 8. Show that it can't leave a remainder of 2 upon division by 3. (b) Find all pairs of integers x and y such that $x^2 + y^2 = 1999$. With a minimum of effort, find all pairs of integers x and y such that $x^2 + y^2 = 1000$. (Remarkable fact: A positive integer n can be represented as the sum of two squares only if all primes that are 3 modulo 4 appear to even power in its prime factorization. A positive integer can be represented as the sum of three squares unless it is of the form $4^a(8b-1)$. All positive integers can be represented as the sum of four squares.)

A6.

(a) Show that 1000! ends with 249 zeros.
(b) *(A useful fact!)* Show that the highest power of p dividing $n!$ is $[n/p]+[n/p^2]+[n/p^3]+\cdots$, where $[\cdot]$ is the "greatest integer function". (Just ask if you don't know what that means.)
(c) *(Same useful fact!)* Suppose the sum of the digits of n when written in base p is n_p. Show that the highest power of p dividing $n!$ is $(n - n_p)/(p-1)$.

A7. Find all functions f which satisfy the three conditions (i) $f(x,x) = x$, (ii) $f(x,y) = f(y,x)$, (iii) $f(x,y) = f(x, x+y)$, assuming that the variables and the values of f are positive integers.

A8. The measure of a given angle is $180/n$ degrees, where n is a positive integer not divisible by 3. Prove that the angle can be trisected by Euclidean means (straightedge and compass).

Primitive Pythagorean Triples

A primitive Pythagorean triple is an ordered triple of positive integers (a,b,c), pairwise relatively prime, that are the sides of a right-angled triangle, i.e. $a^2+b^2 = c^2$. Familiar examples are (3,4,5), (5,12,13), (7,24,25), and (8,15,17).

B1. If (a,b,c) is a primitive Pythagorean triple, show that exactly one of $\{a,b\}$ is odd. (Hint: check modulo 4.) Without loss of generality, say a is odd.

B2. Then $a^2 = c^2 - b^2 = (c-b)(c+b)$. Show that $c-b$ and $c+b$ have no common factor.

B3. Show that two relatively prime numbers multiplying to a perfect square must both be perfect squares. In the previous problem, show that $c-b$ and $c+b$ can be taken to be $(m+n)^2$ and $(m-n)^2$ respectively, where m and n are positive integers, $m > n$, and exactly one of m and n is even. (Remember that we're assuming a is odd!)

B4. In the previous problem, show that m and n are relatively prime. (Hint: If they have a common factor d, show that d is a factor of both b and c, which are relatively prime.)

B5. Solve for b and c to get $b = 2mn$, $c = m^2 + n^2$. Then show that $a = m^2 - n^2$.

In conclusion, any primitive Pythagorean triple is of the form

$$(a, b, c) = (m^2 - n^2, 2mn, m^2 + n^2)$$

or $(2mn, m^2 - n^2, m^2 + n^2)$, where m and n are relatively prime positive integers, one of which is even, with $m > n$. (Plug in small values of m and n — what do you get?)

With this result, you can now do lots of interesting things involving Pythagorean triples. For example:

B6. Plug in some large values of m and n to get ridiculously huge Pythagorean triples.

B7. Show that any Pythagorean triple (a, b, c) can be written as a multiple k of a primitive Pythagorean triple.

B8. $312^2 + 459^2 = 555^2$. Which k, m, and n give this triple?

B9. (a) How many Pythagorean triangles are there with hypotenuse 60? (b) Show that the product of the sides of a right angled triangle with integer sides is always divisible by 60.

B10. Suppose (a, b, c) is a primitive Pythagorean triple, and a is odd. Show that $\frac{c-a}{2}$, $\frac{c+a}{2}$, $c + b$, and $c - b$ are all perfect squares.

B11. Try "breaking the rules" and substituting $m = \cos\theta$, $n = \sin\theta$ in the formula for primitive Pythagorean triples. What formula do you get? (Remember the double angle formulas: $\cos 2\theta = \cos^2\theta - \sin^2\theta$ and $\sin 2\theta = 2\sin\theta\cos\theta$.)

B12. Find a right triangle with rational sides and area 5. (Hint: try to scale well-known Pythagorean triples.) One such triangle was discovered by Fibonacci, among others. In fact, 5 is the smallest integer which is the area of a right triangle with rational sides. (Serious math fact: It's a classical unsolved problem to determine all of the integers which are areas of right triangles with rational sides. In 1983, it was shown that a solution to one of the most important conjectures in number theory, the Birch-Swinnerton-Dyer conjecture, would give a solution to this problem as well. If you solve the BSD conjecture, you'll win a million dollars — see http://www.claymath.org/prizeproblems/birchsd.htm, or the link on the Stanford Putnam webpage.)

B13. Fermat's Last Theorem! (In some cases...) Show that there are no solutions to the equation $k^{2000} + l^{2000} = m^{2000}$ where k, l, and m are positive integers, as follows.

(a) Show that if there is a solution, then there is a solution where k, l, and m are pairwise relatively prime.

(b) Show that if there is a solution, then there is a solution of

$$x^4 + y^4 = z^2 \tag{1}$$

where x, y, and z are pairwise relatively prime positive integers.

(c) (This is the big one!) Assume there is a solution $(x, y, z) = (a, b, c)$ to equation (1). Then (a^2, b^2, c) is a primitive Pythagorean triple, so you can use what you know about such triples. Play around with the algebra. (Another primitive Pythagorean triple may come up.) You will hopefully end up with another solution to equation (1) that is in some sense smaller than the solution $(x, y, z) = (a, b, c)$. (Make that precise.) Then the argument by contradiction will go as follows: suppose (x, y, z) is the "smallest" solution of equation (1). Then this method produces a smaller solution — contradiction.

(d) Hence prove a quarter of the cases of Fermat's Last Theorem (when n is divisible by 4).

The rest of the problems all appeared on the Putnam. Don't be intimidated — many are quite gettable!

C1. A *composite* (positive integer) is a product ab with a and b not necessarily distinct integers in $\{2, 3, 4, \dots\}$. Show that every composite is expressible as $xy + xz + yz + 1$, with x, y, and z positive integers.

C2. How many primes among the positive integers, written as usual in base 10, are such that their digits are alternating 1's and 0's, beginning and ending with 1?

C3. Let k be the smallest positive integer with the following property:

There are distinct integers m_1, m_2, m_3, m_4, m_5 such that the polynomial

$$p(x) = (x - m_1)(x - m_2)(x - m_3)(x - m_4)(x - m_5)$$

has exactly k nonzero coefficients.

Find, with proof, a set of integers m_1, m_2, m_3, m_4, m_5 for which this minimum k is achieved.

C4. For any integer a, set

$$n_a = 101a - 100 \cdot 2^a.$$

Show that for $0 \le a, b, c, d \le 99$, $n_a + n_b \equiv n_c + n_d \pmod{10100}$ implies $\{a, b\} = \{c, d\}$.

C5. Let Γ consist of all polynomials in x with integer coefficients. For f and g in Γ and m a positive integer, let $f \equiv g \pmod{m}$ mean that every coefficient of $f - g$ is an integral multiple of m. Let n and p be positive integers with p prime. Given that f, g, h, r, and s are in Γ with $rf + sg \equiv 1 \pmod{p}$ and $fg \equiv h \pmod{p}$, prove that there exist F and G in Γ with $F \equiv f \pmod{p}$, $G \equiv g \pmod{p}$, and $FG \equiv h \pmod{p^n}$.

C6. Let $A_1 = 0$ and $A_2 = 1$. For $n > 2$, the number A_n is defined by concatenating the decimal expansions of A_{n-1} and A_{n-2} from left to right. For example $A_3 = A_2A_1 = 10$, $A_4 = A_3A_2 = 101$, $A_5 = A_4A_3 = 10110$, and so forth. Determine all n such that 11 divides A_n.

C7. Let p be an odd prime and let $\mathbb{F}_p$ denote (the field of) integers modulo p.

How many elements are in the set

$$\{x^2 : x \in \mathbb{F}_p\} \cap \{y^2 + 1 : y \in \mathbb{F}_p\}?$$

Some comments left over from last week. Last week, I asked: The latest calculator has a button, which when pressed, replaces a number x by $x + 1/x$. You type in some positive number, and then start pressing the button repeatedly. What happens? Prove it! The problem, as several people pointed out, should have had $1 + 1/x$ instead. Many people showed that if a limit exists, then it is the golden mean $\tau = \frac{1+\sqrt{5}}{2}$, which is approximately 1.618. But few people could actually prove it. Here are two approaches. (If you are reading this, ask me — it is easier to explain in person than on the printed page.)

First of all, you could show that $x + 1/x$ is closer to τ than x was. This isn't enough; for example, the sequence 1, $1 + \frac{1}{2}$, $1 + \frac{1}{2} + \frac{1}{4}$, $1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8}$, ... gets closer and closer to 3, but its limit is 2. So instead, you could show that $x + 1/x$ is r times closer to τ than x was, where $r < .9$. Do you see why that helps? And in fact you could replace .9 by any number less than 1. (Caution: the number you pick can't depend on x — do you see why, using the "3" example? Also, r can't be 1 — do you see why, using the same example?)

Second, you could use the following important fact: If x_1, x_2, ... is an *increasing* sequence of reals, bounded above by some number M, then the sequence approaches a limit. Once you know that the sequence has a limit, you're home free, by the comments above. (This sounds like a hard theorem, but I prefer to see it as one of the *definitions* of the real numbers. In fact, I'm betting that most of you *think* you know what the real numbers are, but aren't really sure — this is the result of brainwashing in the school system. It's *useful* brainwashing to be sure: most people don't need to know what real numbers are; they just need to *think* they know. As an example of this confusion, try to sort out if .999... = 1. A better way to think of real numbers is axiomatically. For example, first describe the rules of addition and multiplication, which you can do in six axioms. Then add axioms describing the idea of magnitude; this requires three more. Finally, the tenth and sometimes most mysterious axiom is just the fact above: if x_1, x_2, ... is an increasing sequence of reals, bounded above by some number M, then the sequence approaches a limit. From this you can show that the real numbers behave the way you think they do. If you want to here more about this story, just ask me.)

To see how happy you are with these ideas, you can try the following Putnam problem:

C8. For any pair (x, y) of real numbers, a sequence $(a_n(x, y))_{n\geq 0}$ is defined as follows:

$$\begin{aligned} a_0(x, y) &= x, \\ a_{n+1}(x, y) &= \frac{(a_n(x, y))^2 + y^2}{2}, \qquad \text{for } n \geq 0. \end{aligned}$$

Find the area of the region $\{(x, y)|(a_n(x, y))_{n\geq 0} \quad \text{converges}\}$.

This handout, and other useful things, can (soon) be found at

http://math.stanford.edu/~vakil/stanfordputnam.html