# PUTNAM PROBLEM SOLVING SEMINAR WEEK 3: NUMBER THEORY

**The Rules.** These are way too many problems to consider. Just pick a few problems you like and play around with them. You are not allowed to try a problem that you already know how to solve. Otherwise, work on the problems you want to work on.

**The Hints.** Work in groups. Try small cases. Plug in smaller numbers. Do examples. Look for patterns. Draw pictures. Use lots of paper. Talk it over. Choose effective notation. Look for symmetry. Divide into cases. Work backwards. 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. Ask.

**Useful number theory 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 $a^p \equiv a \pmod{p}$. Problems 6(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 $\phi$-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 $p_1, \dots, p_k$ 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.**

**1.** (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 $n$.

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

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

**4.** 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 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!)

**5.** (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

*Date*: Monday, November 3, 2003.

$x$ 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.)

**6.**

(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 $(n - n_p)/(p - 1)$.

**7.** Prove that $\binom{pa}{pb} \equiv \binom{a}{b} \pmod{p}$ for all integers $p$, $a$, and $b$ with $p$ a prime.

**8.** 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.

**9.** 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).

**10.** Let $f(n)$ be the sum of the first $n$ terms of the sequence $0, 1, 1, 2, 2, 3, 3, 4, \ldots$, where the $n$th term is given by $a_n = n/2$ if $n$ is even and $a_n = (n - 1)/2$ if $n$ is odd. Show that if $x$ and $y$ are positive integers and $x > y$ then $xy = f(x + y) - f(x - y)$.

**11.** Let $n$ be a positive integer such that $n + 1$ is divisible by 24. Prove that the sum of the divisors of $n$ is divisible by 24.

**12.** Supposing that an integer $n$ is the sum of two triangular numbers $n = \frac{a^2+a}{2} + \frac{b^2+b}{2}$, write $4n + 1$ as the sum of two squares, $4n + 1 = x^2 + y^2$, and show how $x$ and $y$ can be expressed in terms of $a$ and $b$. Show that, conversely, if $4n + 1 = x^2 + y^2$, then $n$ is the sum of two triangular numbers. (Of course, $a$, $b$, $x$, $y$ are understood to be integers.)

**13.** Show that there are no four consecutive binomial coefficients $\binom{n}{r}$, $\binom{n}{r+1}$, $\binom{n}{r+2}$, $\binom{n}{r+3}$ ($n$ and $r$ are positive integers, and $r + 3 \leq n$) which are in arithmetic progression.

**14.** In how many ways can the integers from 1 to $n$ be ordered subject to the condition that except for the first integer on the left, every integer differs by 1 from some integer to the left of it?

**15.** Find the length of the longest sequence of equal nonzero digits in which an integral square can terminate (in base 10) and find the smallest square which terminates in such a sequence.

**16.** Let $p$ be an odd prime, and let $F(n) = 1 + 2n + 3n^2 + \cdots + (p-1)n^{p-2}$. Prove that if $a$ and $b$ are distinct integers in $\{0, \ldots, p-1\}$ then $F(a)$ and $F(b)$ are not congruent modulo $p$, that is, $F(a) - F(b)$ is not divisible by $p$.

**17.** Assume that a 60 degree angle cannot be trisected with ruler and compass alone. Prove that if $n$ is a positive multiple of 3, then no angle of $360/n$ degrees can be trisected with ruler and compass alone.

**18.** Let $a$, $b$, $c$, and $d$ be positive integers and $r = 1 - a/b - c/d$. Given that $a + c \leq 1982$ and $r > 0$, prove that $r > 1/1983^3$.

**19.** Show that if $n$ is an integer greater than 1, then $n$ does not divide $2^n - 1$.

*This handout can (soon) be found at*

**http://math.stanford.edu/~vakil/putnam03/**

*E-mail address*: `vakil@math.stanford.edu`