Math 189, Winter 2008.

Problem Set 10: Number Theory

You will need a few basic notions of number theory for this set, such as: prime factorization, congruences, and Euclidean algorithm for the greatest common divisor (gcd). A theorem that often turns up is *Fermat's Little Theorem*: If p is a prime and $\gcd(a,p)=1$, then $a^{p-1}=1 \mod p$. A generalization is *Euler's theorem*: if $\gcd(a,n)=1$, then $a^{\phi(n)}=1 \mod n$. Here $\phi(n)$ is the number of integers from $\{1,\dots,n\}$ which are relatively prime to n, and if $n=p_1^{e_1}\cdots p_k^{e_k}$ is the prime factorization,

$$\phi(n)=n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right).$$

Other theorems which are sometimes useful in competition problems are Wilson's theorem and the Chinese Remainder Theorem. These can be learned quickly from any elementary number theory book.

Diophanine equations, which look for solutions in integers, are common in competitions. This is an enormous and deep area of modern number theory, which such problems of course do not require (although it never hurts to know). Instead, here are a few tricks:

- Look at the equation modulo some small number. For example, verify that, for an integer x, x^2 is 0 or 1 modulo 4, x^3 is 0, 1 or -1 modulo 9, and x^4 is 0 or 1 modulo 16. For example, such an argument immediately shows that $x^2=y^2+20000010$ has no solution.
- Factorize. For example, to solve the equation $x^2=y^2+2008$, rewrite it in the form of $(x-y)(x+y)=251\cdot 2^3$. Note that $x+y$ and $x-y$ cannot be of different parity (the sum equals $2x$) and that we can assume $x>y\geq 0$. So $x+y=251\cdot 2^k$, $x-y=2^{3-k}$, $k=1,2$. This gives two positive solutions $(x,y)=(253,249),(503,501)$.
- Pythagorean triples. The equation $x^2+y^2=z^2$ have infinitely many solutions; those solutions without a common factor are given by $x=a^2-b^2$, $y=2ab$, $z=a^2+b^2$, where a and b are positive relatively prime integers of opposite parity and $a>b$.
- Infinite descent. Remember how one proves that $\sqrt{2}$ is irrational, i.e., that $x^2=2y^2$ has no solution? Take x to be the smallest possible. Then x and y cannot have a common factor, but x is divisible by 2, so x^2 is divisible by 4, so y is divisible by 2, contradiction. A more sophisticated example was used by Fermat to show that $x^4+y^4=z^2$ has no nontrivial solutions. (Assume $z>0$ is the smallest. Then x and y have no common factor and we may assume that x is odd and y is even. So $x^2=a^2-b^2$, $y^2=2ab$, and $z=a^2+b^2$. Now if a is even and b is odd, $x^2=-1 \mod 4$, not possible. So a is odd and $b=2c$ is even. Then $ac=(y/2)^2$ is a square, and a and c are relatively prime, so they each must be a square, say $a=a_1^2$, $c=c_1^2$. From $x^2+b^2=a^2$ we get $x^2+(2c_1^2)^2=(a_1^2)^2$, so again there exist relatively prime g and h so that $2c_1^2=2gh$ and $a_1^2=g^2+h^2$. This implies that $g=g_1^2$, $h=h_1^2$ and finally $g_1^4+h_1^4=a_1^2$. However, $a_1\leq a_1^2=a\leq a^2<a^2+b^2=z$, a contradiction with minimality of z.)
- Linear equations. For the equation $ax+by=c$, we may assume $\gcd(a,b)=1$. (Otherwise, either there is no solution, or we can divide out $\gcd(a,b)$.) Then all solutions are given

by $x = x_0 + kb$, $y = y_0 - ka$, $k \in \mathbb{Z}$, where (x_0, y_0) is a particular solution obtained by the Euclidean algorithm. If $a, b > 0$, then a solution with $x, y \geq 0$ exists for all $c > ab - a - b$, and does not for $c = ab - a - b$. To see this, note that the solution is *unique* if we require that $0 \leq x \leq b - 1$. If the corresponding y is negative for this x, then it is for any other. Thus $x = b - 1$, $y = -1$ gives the largest non-represented number $a(b-1) - b = ab - a - b$. (These questions are much more difficult in the case of general linear equation $\sum_{i=1}^{n} a_i x_i = c$. For example, the largest number that cannot be represented by a nonnegative linear combination of 6, 9, and 20 is 43, but there are no simple formulas.)

- Pell equation. This equation (misattributed to Pell) is $x^2 - dy^2 = 1$. It has infinitely many positive solutions (x_n, y_n) given by $x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$, where (x_1, y_1) is the *least* solution, the one with smallest $x + y\sqrt{d}$. It can often be obtained by inspection, e.g., $(3, 2)$ for $d = 2$, $(2, 1)$ for $d = 3$, and $(9, 4)$ for $d = 5$. More generally one needs continued fractions, e.g., $(x_1, y_1) = (649, 180)$ for $d = 13$. (See for example "Diophantine Analysis," by J. Steudling, Chapman & Hall, 2005, for this and much more.)

1. You are standing by a well. In your possession are two containers, a 15 gallon one and a 28 gallon one. However, by pouring water in and out of the two containers, you want to measure exactly 9 gallons of water. Is this possible? What if the capacities of the two containers are 16 and 28 gallons? Finally, answer the question for general integer container capacities a and b, and the desired gallon amount c.

2. (*) In a large company, with n employees, the following game is played at Christmas time. Each employee is assigned a distinct integer from 1 to n. These numbers are then arranged counterclockwise on a circle. In the first step, tag number 2. In each subsequent step, the first number counterclockwise from the tagged number is skipped, the second number is the new tagged number, and the old tagged number is eliminated from the circle. This is repeated until a single number remains, and that number wins the big Christmas prize. For example, if $n = 5$, here are the eliminated numbers: 2, 4, 1, 5, and the winning number is 3.

The CEO invites you to his office, lets you know what n is this year (say, 2007), and gives you 5 minutes (but no computer) to pick a number assigned to you. Which number should you pick? Find the answer for general n.

3. (*) Fix a positive integer n. What is the smallest integer m for which $3^m - 1$ is divisible by 2^n?

4. Show that $a_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$, $n \geq 2$, is never an integer.

5. Compute the two digits on either side of decimal point of $(\sqrt{2} + \sqrt{3})^{2000}$.

6. Determine all pairs of integers (x, y) so that

$$1 + 2^x + 2^{2x+1} = y^2.$$

7. A playground contains 23 kids. Each weighs an integer number of pounds. They want to play soccer by choosing a referee and then dividing themselves into two teams of 11 players, with the proviso that both teams must have the same combined weight. It turns out that they can do this no matter which kid is the referee. Show that all 23 weights are the same.

8.(*) Determine all integer solutions of $x^2 + y^2 + z^2 = x^2y^2$.

9. Let $a_1 = 0$, $a_2 = 1$ $a_3 = 10$, $a_4 = 101$, $a_5 = 10110\ldots$ For $n > 2$, the number a_n is defined by concatenating the decimal expansion of a_{n-1} and a_{n-2} from left to right. Determine all n such that a_n is divisible by 11.

10. (*) Show that, for every integer $n \geq 1$, n does not divide $2^n - 1$.

11. The sequence a_n is defined by $a_1 = 1$, $a_2 = 2$, $a_3 = 24$, and for $n \geq 4$,

$$a_n = \frac{6a_{n-1}^2 a_{n-3} - 8a_{n-1}a_{n-2}^2}{a_{n-2}a_{n-3}}.$$

Show that a_n is always an integer multiple of n.

12. Let $p(x)$ be a polynomial of degree n, and assume that $p(k) = 1/(k+1)$ for $k = 0, \ldots, n$. Compute $p(n+1)$.

13. Show that $x^4 + 3y^4 = 5 + 7z^4$ has no solution in integers x, y, z.

14. The $n \times n$ matrix A has entries $a_{ij} = 2^{|i-j|}$. Is it invertible?

15. Find all positive integer solutions to $3^x + 4^y = 5^z$.

16. (*) The sequence of triangular numbers $t_n = n(n+1)/2$, $n = 1, 2\ldots$ is $1, 3, 6, 10, 15, \ldots$ and the sequnce s_n of perfect squares is of course $1, 4, 9, 16, 25\ldots$ Take the sequence σ_n which contains, in order, numbers common to both s_n and t_n. Show that σ_n obeys a second order linear recursion and write down its first five elements.