Problem Solving in Math (Math 43900) Fall 2013

Week four (September 17) problems — number theory

Instructor: David Galvin

Some useful principles/definitions from number theory

1. **Divisibility**: For integers a, b, $a|b$ (a divides b) if there is an integer k with $ak = b$.

   The greatest common divisor of a, b, $\gcd(a, b)$ (sometimes just written (a, b)) is that number d such that $d|a$ and and $d|b$, and for any other number e with $e|a$ and $e|b$, we have $e < d$ (but in fact it turns out that we have $e|d$ if $d = \gcd(a, b)$ and $e|a$, $e|b$; this follows easily from looking at the prime factorizations of a and b, see below).

   The least common multiple of a, b, $\text{lcm}(a, b)$ is that number f such that $a|f$ and and $b|f$, and for any other number g with $a|g$ and $b|g$, we have $f < g$ (but in fact, as with gcd, it turns out that we have $f|g$ if $f = \text{lcm}(a, b)$ and $a|g$, $b|g$).

   If $\gcd(a, b) = 1$ (so no factors in common other that 1) then a and b are said to be *coprime* or *relatively prime*.

2. **Primes**: If $p > 1$ only has 1 and p as divisors, it is said to be *prime*; otherwise it is *composite*.

   The fundamental fact about prime numbers (other that there are infinitely many of them!) is that every number $n > 1$ has a *prime factorization*:

   $$n = p_1^{a_1} \dots p_k^{a_k}$$

   with each p_i a prime, and each $a_i > 0$. Moreover, the factorization is *unique* if we assume that $p_1 < \ldots < p_k$.

3. **Euclidean algorithm**: Euclid described a simple way to compute $\gcd(a, b)$. Assume $a > b$. Write

   $$a = kb + j$$

   where $0 \leq j < b$. If $j = 0$, then $\gcd(a, b) = b$. If $j > 0$, then it is fairly easy to check that $\gcd(a, b) = \gcd(b, j)$. Repeat the process with the smaller pair b, j, and keep repeating as long as necessary. For example, suppose I want $\gcd(63, 36)$:

   $$\begin{aligned} 63 &= 1.36 + 27 \\ 36 &= 1.27 + 9 \\ 27 &= 3.9. \end{aligned}$$

   We conclude $9 = \gcd(27, 9) = \gcd(36, 27) = \gcd(63, 36)$.

4. **Bézout's Theorem**: Given a, b, there are integers x, y such that $ax + by = \gcd(a, b)$. Moreover, the set of numbers that can be expressed in the form $ax' + by' = c$ for integers x', y' is exactly the set of multiples of $\gcd(a, b)$.

   The proof comes from working the Euclidean algorithm backwards. I'll just do an example, with the pair $63, 36$. We have

$$\begin{aligned} 9 &= 36 - 1.27 \\ &= 36 - 1(63 - 1.36) \\ &= -1.63 + 2.36 \end{aligned}$$

   so we can take $x = -1$ and $y = 2$.

   Once we have found an x and y, the rest is easy. Suppose $c = k\gcd(a, b)$ is a multiple of $\gcd(a, b)$; then $(kx)a + (ky)b = c\gcd(a, b)$. On the other hand, if $ax' + by' = c$ then since $\gcd(a, b)|a$ and $\gcd(a, b)|$ we have $\gcd(a, b)|c$, so c is a multiple of $\gcd(a, b)$.

   The most common form of Bézout's Theorem is that if $(a, b) = 1$ then every integer k can be written as a linear combination of a and b; in particular there is x, y with $ax + by = 1$.

5. **Modular arithmetic**: When dealing with remainders of numbers on division, the language of modular arithmetic is extremely useful. Write

$$a \equiv b \pmod{k}$$

   if a and b leave the same remainder on division by k, or equivalently if $k|(a-b)$, or equivalently equivalently if $a = mk + b$ for some integer m (so, e.g., $13 \equiv 4 \pmod 3$ because they both leave remainder 1, but $13 \not\equiv 4 \pmod 5$, since 13 leaves a remainder of 3 and 4 a remainder of 4.) Here are two easy and incredible useful facts:

   Fact 1: if $a \equiv b \pmod k$ and $c \equiv d \pmod k$ then $a + c \equiv b + d \pmod k$

   and

   Fact 2: if $a \equiv b \pmod k$ and $c \equiv d \pmod k$ then $ac \equiv bd \pmod k$.

   If $a \equiv b \pmod k$ then we also say that a and b are in the same *congruence class* modulo m (an example of a congruence class modulo 3 is the set $\{3k+2 : k \in \mathbb{Z}\} = \{\ldots, -4, -1, , 2, 5, \ldots\}$). The set of congruence classes modulo m is denoted by $\mathbb{Z}/m\mathbb{Z}$.

6. **Useful facts/theorems**:

   (a) **Inverses**: If p is a prime, and $a \not\equiv 0 \pmod p$, then there is a whole number b such that $ab \equiv 1 \pmod p$.

   (b) **Fermat's theorem**: If p is a prime, and $a \not\equiv 0 \pmod p$, then $a^{p-1} \equiv 1 \pmod p$.
   More generally, for arbitrary m (prime or composite) define $\varphi(m)$ to be the number of numbers in the range 1 through m that are coprime with m. If $(a, m) = 1$ then $a^{\varphi(m)} \equiv 1 \pmod m$. (When $m = p$ this reduces to Fermat's Theorem.)
   We refer to φ as *Euler's totient function.* A quick way to calculate its value: if m has prime factorization $m = p_1^{a_1} \ldots p_k^{a_k}$, then

$$\varphi(m) = m \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

(c) **Chinese Remainder Theorem**: Suppose $n_1, n_2, \ldots, n_k$ are pairwise relatively prime. If $a_1, a_2, \ldots, a_k$ are any integers, there is a number x that simultaneously satisfies $x \equiv a_k \pmod{n_k}$. Moreover, modulo $n_1 n_2 \ldots n_k$, this solution is unique.

The problems

1. Let a and b be two integer for which $a - b$ is divisible by 3. Prove that $a^3 - b^3$ is divisible by 9.

2. Find all integers n such that $2^n + n | 8^n n + n$.

3. Let x, y and z be integers with the property that

$$\frac{1}{x} - \frac{1}{y} = \frac{1}{z}.$$

   Prove that both $\gcd(x, y, z)xyz$ and $\gcd(x, y, z)(y - x)$ are both perfect squares.

4. Let $n > 1$ be an integer and p a prime such that $n|(p - 1)$ and $p|(n^3 - 1)$. Prove that $4p - 3$ is a perfect square.

5. Show that the sum of consecutive primes is never twice a prime.

6. Prove that $2^{70} + 3^{70}$ is divisible by 13.

7. Define $f(n)$ by $f(1) = 7$ and $f(n) = 7^{f(n-1)}$ for $n > 1$. Find the last two digits of $f(7)$. (Note that $f(7)$ is an exponential tower of 7's, 7 high.)

8. Several positive integers are written on a chalk board. One can choose two of them, erase them, and replace them with their greatest common divisor and least common multiple. Prove that eventually the numbers on the board do not change.

9. How many primes numbers have the following (decimal) form: digits alternating between 1s and 0s, beginning and ending with 1?

10. Take a walk on the number line, starting at 0, by on the first step taking a step of length one, either right or left, on the second step taking a step of length two, either right or left, and in general on the kth step taking a step of length k, either right or left.

    (a) Prove that for each integer m, there is a walk that visits (has a step ending at) m.

    (b) Lt $f(m)$ denote the shortest number of steps needed to reach m. Show that

$$\lim_{m \to \infty} \frac{f(m)}{\sqrt{m}}$$

    exists, and find the value of the limit.