Problem Set VI

Elementary Number Theory

Due Mar. 11th

Think about all the problems and try to come up with ideas to solve them and write those. Write a complete solution for at least two of the problems. The solutions have to be clear and convincing for a skeptical classmate. You need to know the following facts for this set of

problems. In what follows, all the numbers are integers, by which we mean any element of the set $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$.

- We say that m *divides* n, or that n *is divisible by* m, if $n = mk$ for some integer k. In this case, we write $m|n$. m is also called a *divisor* of n. For example, $3|12$, $15|135$, $1|n$ and $n|n$ for all integers n.

- A positive intger $p \geq 2$ is called a *prime* if p and 1 are the only divisors of p. For example: 2, 11, 43 are primes, while 35 is not, since both 5 and 7 divide 35. Note that 2 is the only even integer, which is also a prime.

- **Division Algorithm.** If a and b are arbitrary integers, $b > 0$, there are unique integers q, quotient, and r, remainder, such that

$$a = qb + r, \qquad 0 \leq r < b.$$

  q and r are uniquely determined by a and b. It is easy to see that a is divisible by b if and only if the remainder is zero. For example: for $a = -7$ and $b = 3$ we have $q = -3$ and $r = 2$, since $-7 = (-3)(3) + 2$.

- **Congruences.** Given integers n, m and k, we say that n is *congruent to m modulo k*, if n and m have the same ramainder when we divide them by k. In this case, we write $n \equiv m(\text{mod } k)$. For example: $27 \equiv 0(\text{mod } 3)$, $17 \equiv 5(\text{mod } 4)$ and $12 \equiv 1002(\text{mod } 11)$. Equivalently, $n \equiv m(\text{mod } k)$ if and only if k divides $n - m$. The relation $\equiv$ has the following property:

  If $n \equiv m(\text{mod } k)$ and $n' \equiv m'(\text{mod } k)$, then

$$n + n' \equiv m + m'(\text{mod } k)$$

  and also

$$nn' \equiv mm'(\text{mod } k).$$

1. In class, we saw different criteria for dtermining the remainder of an integer when divided by 3 or 7. We proved that for 3.

(a) Try to prove it for 7. To remind you, this was the algorithm:

Consider n and divide it by 50. Take the quotint and remainder and add them together. The obtained number will have the same remainder as n when divided by 7.

(b) Now prove that the following criteria works for 11:

Consider n in its decimal presentation. From right, take its first digit, subtract the second digit, add the third digit and so on until when you are done with all of its digits. The result will have the same remainder as n, when we divide them by 11. For example, consider 238153 and compute $3-5+1-8+3-2=-8$. Remainder of -8 when divided by 11 is 3, since $-8=(-1)(11)+3$, so is the reminder of 238153: $238153 = 2165 \times 11 + 3$.

2. What is the rightmost digit of 4^{2004}? What about 7^{2004}?

3. If N is the product of k consecutive positive integers prove that N is divisible by $k!$.

4. Prove that for any set of n integers, there is a subset of them whose sum is divisible by n.

5. (a) Show that $2^{2x+1}+1$ is divisible by 3.

   (b) Prove or disprove: $2^x \equiv 2^y (\text{mod } n)$ if $x \equiv y (\text{mod } n)$.

6. (a) Prove that there are infinitely many primes!

   (b) Prove that there are infinitely many primes of the form $4n+3$ and infinitely many primes of the form $6n+5$, where n is an integer.

7. For any $n \geq 1$, prove that there exists an n-digit number with odd digits which is divisible by 5^n.