MAT 311 Introduction to Number Theory

Problem Set 2

Some Solutions

Problem 2. Let $x > 0$ be such that $x + 1/x$ is an integer (x itself doesn't have to be an integer). Prove that $x^n + 1/x^n$ is an integer for every natural n.

Solution. The base of induction, $n = 1$, is trivial.
Now observe that

$$(x^n + 1/x^n)(x + 1/x) = (x^{n+1} + 1/x^{n+1}) + (x^{n-1} + 1/x^{n-1})$$

and argue by complete induction: suppose that $x^k + 1/x^k$ is integer for all $k = 1, 2, \dots n$. Then $x^{n+1} + 1/x^{n+1} = \text{integer}\cdot\text{integer} - \text{integer}$ is also an integer.

Problem 3. Prove that there are infinitely many primes of the form $p = 4m + 3$. **Hint:** Show that every number of the form $4m + 3$ must have a prime divisor of the same form, and mimic Euclid's proof of infinitude of primes.

Solution. Suppose that there is only a finite number of such primes, $p_1, p_2, \dots, p_k$. Consider $n = 4p_1p_2 \dots p_k - 1$, and observe that none of the numbers $p_1, \dots p_k$ divide n. By the prime decomposition theorem, n can be represented as a product of (one or more) prime factors. None of these can be among p_i's; 2 cannot enter because n is clearly odd. It follows that n is a product of prime factors each of which is congruent to 1 mod 4. But then their product, n, must also be congruent to 1 mod 4; however $n = 4p_1p_2 \dots p_k - 1 \equiv -1 \equiv 3$, a contradiction.

Problem 4. The following identities will be needed to solve Questions 5 and 6 (**hint hint**). Prove them by any method.
(a) $x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots + xy^{n-2} + y^{n-1})$ for all natural n.
(b) $x^n + y^n = (x + y)(x^{n-1} - x^{n-2}y + x^{n-3}y^2 - \cdots - xy^{n-2} + y^{n-1})$ for all n odd.

Solution. These are easiest to see if you multiply out carefully and notice that most terms cancel.

Problem 5. Suppose that $2^n - 1$ is a prime number. Show that n must be also prime.

Solution. Suppose n is composite, then $n = lk$, with $k, l > 1$. Then

$$2^n - 1 = 2^{lk} - 1 = (2^l)^k - 1^k = (2^l - 1)[(2^l)^{k-1} + (2^l)^{k-2} + \dots 1]$$

by Question 4. Since $l > 1$, $2^l - 1 > 1$ is a non-trivial divisor, so $2^n - 1$ cannot be prime.

Problem 6. Suppose that $2^n + 1$ is a prime number. Show that $n = 2^k$ for some k.

Solution. Suppose n is not a power of 2, then it has an odd prime divisor, say k, and can be written as $n = lk$. Then

$$2^n + 1 = 2^{lk} + 1 = (2^l)^k + 1^k = (2^l + 1)[(2^l)^{k-1} - (2^l)^{k-2} + \cdots + 1]$$

by Question 4, since k is odd. This shows that $2^n + 1$ is composite, since the factor $2^l + 1$ is greater than one but less than $2^n + 1$.