Math 300.2 Homework 6

Paul Hacking

March 12, 2012

Reading: Gilbert and Vanstone, Chapter 3.

(1) (a) Let S be a finite set. Let A and B be subsets of S. Show that

$$|S \setminus (A \cup B)| = |S| - |A| - |B| + |A \cap B|.$$

(b) Now let m be a positive integer and suppose $m = p^\alpha q^\beta$ where p and q are primes and α and β positive integers. Let $S = \{1, \ldots, m\}$, A the subset of multiples of p, and B the subset of multiples of q. What is $|A|$? What is $|B|$? Describe the set $A \cap B$ and compute $|A \cap B|$. Finally use (a) to compute $|S \setminus (A \cup B)|$.

(c) With the same notation as part (b), explain why $|S \setminus (A \cup B)|$ equals $\phi(m)$, where ϕ is Euler's ϕ function. Now check that your result agrees with the formula for $\phi(m)$ proved in class.

(2) Find all the solutions of the following congruences.

(a) $x^2 \equiv 2 \bmod 7$.

(b) $x^2 + x + 3 \equiv 0 \bmod 5$.

(c) $x^3 + 1 \equiv 0 \bmod 7$.

(3) Let p be a prime number. Show that every integer x satisfies $x^p - x \equiv 0 \bmod p$. [Hint: Use Fermat's little theorem]

(4) Let p be a prime.

(a) Prove that

$$x^2 \equiv y^2 \bmod p \iff x \equiv \pm y \bmod p.$$

[Hint: Use the "difference of two squares" identity $x^2 - y^2 = (x+y)(x-y)$ and HW5Q10(a).]

(b) Now assume that $p \neq 2$ (so the prime p is odd). Show that exactly $(p-1)/2$ of the numbers $1, 2, \ldots, p-1$ are squares modulo p. (We say n is a square modulo p if $n \equiv m^2 \bmod p$ for some integer m.) These numbers are called the *quadratic residues modulo p*.

(c) Find the quadratic residues modulo 11.

(5) Let $f(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0$ be a polynomial of degree n with real coefficients $a_{n-1}, a_{n-2}, \ldots, a_1, a_0$.

(a) Let $\alpha \in \mathbb{R}$. Show that $f(x) = (x-\alpha)g(x) + r$ where $g(x) = x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_1 x + b_0$ is a polynomial of degree $n-1$ with coefficients given by

$$\begin{aligned}
b_{n-2} &= a_{n-1} + \alpha \\
b_{n-3} &= a_{n-2} + \alpha b_{n-2} \\
b_{n-4} &= a_{n-3} + \alpha b_{n-3} \\
&\vdots \\
b_0 &= a_1 + \alpha b_1
\end{aligned}$$

and $r \in \mathbb{R}$ is a constant. [Hint: Expand the product $(x-\alpha)g(x)$ and compare with $f(x)$.]

(b) Show that $f(\alpha) = r$. In particular, if $f(\alpha) = 0$, then $f(x) = (x-\alpha)g(x)$.

(c) Using part (b), prove by induction that the equation $f(x) = 0$ has at most n real solutions.

(6) In this problem we will show that there are infinitely many primes p such that $p \equiv 3 \bmod 4$.

(a) Show that if $a \equiv 1 \bmod 4$ and $b \equiv 1 \bmod 4$ then $ab \equiv 1 \bmod 4$.

(b) Let $p_1, \ldots, p_r$ be prime numbers and define

$$N = 4p_1p_2\cdots p_r - 1.$$

Show that N has a prime factor p such that $p \equiv 3 \bmod 4$, and $p \neq p_1, \ldots, p_r$. [Hint: Every prime number p except $p = 2$ is odd, so $p \equiv 1 \bmod 4$ or $3 \bmod 4$. Now use the fundamental theorem of arithmetic (every number $n > 1$ has a (unique) prime factorization) and give a proof by contradiction using part (a).]

(c) Use part (b) to prove by contradiction that there are infinitely many primes p such that $p \equiv 3 \bmod 4$. [Hint: Modify the proof that there are infinitely many primes given on p. 45 of the textbook.]