CS2335 Special Topics in Discrete Structure

Homework 5

Due: 1:10 pm, December 14, 2009 (before class)

1. Suppose $F(x)$ is a polynomial such that all the coefficients are integers. Furthermore, it is known that $F(0) = F(1) = 1$. Show that F does not have any integral root. (In other words, there is no integer z such that $F(z) = 0$.)

2. Show that if n is an odd number, then

$$1 \times 3 \times 5 \times \cdots \times (2n-1) \ + \ 2 \times 4 \times 6 \times \cdots \times (2n)$$

is a multiple of $2n+1$.

3. Let p be a prime. Show that if there exists n such that

$$n^2 \equiv -1 \pmod{p},$$

then $p \not\equiv 3 \pmod 4$. *Hint: Fermat's little theorem.*

4. Let p be a prime. Let a and b be two integers coprime to p. Show that

$$ax \equiv b \pmod{p} \quad \text{if and only if} \quad x \equiv a^{p-2}b \pmod{p}.$$

5. Prove that if $n^j \equiv 1 \pmod{m}$ and $n^k \equiv 1 \pmod{m}$, then

$$n^{\gcd(j,k)} \equiv 1 \pmod{m}.$$

Hint: Properties of GCD.

6. Prove that $\varphi(n^m) = n^{m-1}\varphi(n)$.

7. Compute $\varphi(999)$.

8. (Challenging: No marks) A number n is a perfect number if the sum of all the proper divisors of n (i.e., all divisors excluding n itself) is exactly n. For instance, 6 and 28 are both perfect numbers, because

$$\begin{array}{lclcl} \text{sum of proper divisors of 6} & = & 1+2+3 & = & 6, \quad \text{and} \\ \text{sum of proper divisors of 28} & = & 1+2+4+7+14 & = & 28. \end{array}$$

In the following, we shall show an interesting result by Euler:

Theorem 1. *An even number n is a perfect number if and only if $n = 2^m(2^{m+1}-1)$ and $2^{m+1}-1$ is prime.*

(a) Prove that if $n = 2^m(2^{m+1}-1)$ and $2^{m+1}-1$ is a prime, then n is a perfect number.

(b) Suppose n is an even number, so that we can express n as 2^mQ for some odd integer Q. Also, suppose $\sigma(Q)$ denotes the sum of all divisors of Q (i.e., including itself). Show that if n is a perfect number, then

$$2^{m+1}Q = 2n = (2^{m+1}-1)\sigma(Q).$$

(c) Using the result from part (b), show that Q is a multiple of $2^{m+1} - 1$.

(d) Suppose that $Q = (2^{m+1} - 1)q$. Show that the following is true:

$$2^{m+1}q = \sigma(Q) \geq q + Q = 2^{m+1}q.$$

(e) Using the result from part (d), show that Q must be a prime and $Q = 2^{m+1} - 1$. In other words, $n = 2^m Q = 2^m(2^{m+1} - 1)$ for some prime $Q = 2^{m+1} - 1$.

9. (Challenging: No marks) Show that for all $n > 1$, $2^n \not\equiv 1 \pmod{n}$.