Midterm of *Numbers, equations, and proofs*

Instructor: Alireza Salehi Golsefidy

Oct 20, 2008

Hi! This is a 24-hour exam. This means as soon as you open this file your exam starts, and it finishes after twenty four hours. You are not allowed to look at your notes, any book, internet, etc. You are not allowed to talk about the exam to anyone, till you hand in your exam. You will hand in your exam in the beginning of Thursday class.

1- (10 points) Without using unique factorization of integer numbers, show that if a and b are coprime and a divides bc then a divides c.

2- (10 points) State and prove Euler's theorem.

3- (10 points) Show that $\phi(mn) = \phi(m)\phi(n)$ if m and n are coprime.

4- (10 points) If p is a prime number and $\mathrm{Ord}_p a = n$, then any element of order n is of the form a^i, where $\gcd(i, n) = 1$.

5- (10 points) Let a, b, c and d be integer numbers such that $ad - bc = 1$, show that

$$\gcd(am + bn, cm + dn) = \gcd(m, n).$$

6-a) (10 points) Show that if $m \neq n$, then $(2^{2^n} + 1, 2^{2^m} + 1) = 1$.

b) (15 points) Show that for any $n > 3$ odd number larger, there is p a prime number such that

$$\begin{cases} p \nmid n \\ p | 2^{\phi(n)} - 1. \end{cases}$$

7- Let p be a prime number.

a) (5 points) Let $P_1(x)$ and $P_2(x)$ be two polynomials with integer coefficients. Is it true that if $P_1(n) \equiv P_2(n) \pmod{p}$ for any n, then $P_1(x) \equiv P_2(x) \pmod{p}$ as two polynomials? Explain your answer.

b) (10 points) Show that $x^p - x \equiv x(x-1) \cdot \cdots \cdot (x - (p-1)) \pmod{p}$.

c) (5 points) Use part (b) to give an alternative proof of Wilson's theorem.

8-a) (5 points) Show that there are infinitely many primes of the form $4k-1$.

b) (10 points) Show that there are infinitely many primes of the form $4k+1$.

9- (10 points) Show that for any positive integer n, there is k a positive integer such that none of

$$k+1,\dots,k+n,$$

is an integral power of a prime number.

10-a) (5 points) Show that for any n integer number larger than 1, n does not divide 2^n-1.

b) (10 points) Let $n_1, n_2, \dots, n_k$ be positive integer numbers. If

$$n_2|2^{n_1}-1, n_3|2^{n_2}-1, \dots, n_k|2^{n_{k-1}}-1, n_1|2^{n_k}-1,$$

then $n_1 = n_2 = \cdots = n_k = 1$.