Homework 3

due on Wednesday, January 31

Read sections 1.3, 1.4, 1.5 in the book. Solve the following problems.

Problem 1. Read the proof of Proposition 1.22 (page 32) in the book. Using simialr method prove that there are infinitely many prime numbers of the form $3n+2$.

Problem 2. Let $a>1$ and $n>1$ be positive integers.

a) Prove that if a^n-1 is a prime then $a=2$ and n is a prime.

b) Prove that if a^n+1 is a prime then a is even and $n=2^k$ for some k (Hint: if n is not a power of 2 then n has an odd divisor).

Hint. The identity $a^n-b^n=(a-b)(a^{n-1}+a^{n-2}b+a^{n-3}b^2+\ldots+ab^{n-2}+b^{n-1})$ should be helpful. Prove this identity.

Problem 3. Recall that when p is a prime number and $n\neq 0$ an integer then $e_p(n)$ is the largest integer a such that $p^a|n$.

a) Prove that if $n>1$ and $p>n$ is a prime then $e_p(n!)=0$

b) Recall thal $\lfloor x\rfloor$ denotes the largest integer not exceeding x. Prove that if n,k are positive integers then

$$\left\lfloor\frac{n+1}{k}\right\rfloor=\begin{cases}\lfloor\frac{n}{k}\rfloor & \text{if } k\nmid(n+1)\\ 1+\lfloor\frac{n}{k}\rfloor & \text{if } k|(n+1)\end{cases}.$$

c) Prove that if $n>1$ and $p\leq n$ is a prime then

$$e_p(n!)=\left\lfloor\frac{n}{p}\right\rfloor+\left\lfloor\frac{n}{p^2}\right\rfloor+\left\lfloor\frac{n}{p^3}\right\rfloor+\ldots$$

(note that the sum is actually finite since $\lfloor n/p^k\rfloor=0$ when $p^k>n$.

Hint. There are several ways to prove this, but I suggest a proof by induction on n. Note that $e_p((n+1)!)=e_p(n!)+e_p(n+1)$ and use part b) (this is why b) is part of this problem).

d) Use c) to write the prime factorization of 20!.

e) Find the number of zeros with which the decimal representation of 99! terminates.

Problem 4. a) Prove that if a, b, c are integers and $\gcd(a, c) = 1 = \gcd(b, c)$ then $\gcd(ab, c) = 1$.

b) Prove that if $\gcd(a, b) = 1$ then $\gcd(a^n, b^m) = 1$ for all positive integers m, n.

c) Prove that if $\gcd(a^n, b^m) = 1$ for some positive integers m, n then $\gcd(a, b) = 1$.

d) Prove that if n is a positive integer and $a^n | b^n$ then $a | b$.